DISS. ETH No. 20245

A HYBRID MODELING/SIMULATION APPROACH FOR IDENTIFICATION OF HIDDEN VULNERABILITIES DUE TO INTERDEPENDENCIES WITHIN AND AMONG CRITICAL INFRASTRUCTURES

A dissertation submitted to
ETH ZURICH

for the degree of
Doctor of Sciences

presented by

Cen Nan

Master of Engineering
born 03 December 1979
citizen of Canada

accepted on the recommendation of
Prof. Dr. Lino. Guzzella, examiner
Prof. Dr. Wolfgang Kröger, co-examiner
Dr. Irene Eusgeld, co-examiner

2012, Zurich

ABSTRACT

Modern Critical Infrastructures (CIs), such as systems for electricity generation/transmission/distribution, transportation, and telecommunication are all large, highly integrated, complex, and particularly interconnected. Interdependencies within and among CIs often exert serious influences making them more vulnerable, which is exacerbated by growing demands for more resources and timely information. Failures/ disturbances in one CI could thus easily spread and have influences on functionalities of other CI(s), potentially causing widespread consequences for society. It is vital to get a clear understanding of these often hidden interdependency issues and potential failure cascades, and to tackle them with advanced modeling and simulation techniques.

The challenges regarding identifying, characterizing, and investigating interdependencies within and among CIs are immense and the research work in this area is still at an early stage. The development of an approach for in-depth analysis of these interdependencies generally faces two major technique challenges. The first challenge is to a model a single CI due to its inherent characteristics and dynamic behaviors. The second challenge appears when more than one CI or subsystem within one CI must be considered and interdependencies among them need to be tackled. Currently, a number of approaches have been developed and applied, trying to meet these challenges, e.g., Complex Network (CN) theory, PetriNet(PN)-based modeling, Agent-based Modeling (ABM), etc; each of them having limitations. In practice, there is still no "silver bullet" approach. To fully utilize benefits/advantages of each approach, it is necessary to integrate different types of modeling approaches into one simulation tool. However, one of the key challenges in developing such type of simulation tool is the required ability to create multiple-domain models, and effectively exchange data among these models.

To find a more promising solution for solving these challenges and handling the technical difficulties, a novel hybrid modeling/simulation approach is proposed and developed in this thesis, which combines various simulation/modeling techniques by adopting the technology of distributed simulation and the concept of modular design for the purposes of exploring and assessing CI vulnerabilities due to interdependencies qualitatively and quantitatively. This approach can be considered as a successor of the traditional modeling/simulation approach in case multiple systems need to be simulated simultaneously. It changes the way to design and develop simulation tools for CI interdependency study by allowing the integration of different types of modeling/simulation approaches into one simulation tool to optimize the efficiency of the overall simulation. The implementation of the hybrid approach is not limited to the interdependencies among CIs. The interdependencies among subsystems within a CI can also be represented and analyzed using this approach; therefore, it can be regarded as generic.

Based on the hybrid modeling/simulation approach, a SCADA (Supervisory Control and Data Acquisition) system model is developed by combining the ABM with other modeling/simulation techniques such as Monte Carlo simulation, Fuzzy Logic, and finite state machines using a failure-oriented modeling approach, and an experimental simulation test-bed is created by adopting the HLA (High Level Architecture) simulation standard. Furthermore, the developed SCADA model includes a specific model for the dynamic assessment of the human operator performance implemented using the approach of CREAM (Cognitive Reliability Error Analysis Method). The test-bed is the first successfully developed simulation platform in the research area of the CI interdependency study that is capable of coupling independently developed CI models and reusing models developed for other purposes. Several experiments have been developed and conducted including feasibility and failure propagation experiments, demonstrating the validity of this approach as well as the developed test-bed, for investigating and representing interdependencies within and among CIs.

To further demonstrate the capabilities of the hybrid modeling/simulation approach, an in-depth analysis of interdependencies between a System Under Control (SUC) and its

SCADA system is carried out by developing three sets of simulation experiments, using the Swiss electric power transmission network as an exemplary application. These experiments start from the scope of a substation in which different single technical failures of SCADA substation level components are simulated to determine and rank the severity of each technical failure. Then the second experiment expands the scope of the simulation to a small network of the SCADA system. Finally, the whole network of the SCADA system is included in the third experiment. Based on the results obtained from these experiments conducted on the experimental simulation test-bed, it can be concluded that the proposed hybrid modeling/simulation approach can be utilized to solve the CI interdependency issues, identify means to better protect CIs in the long run, and make them more resilient, e.g., by adopting self-diagnosis techniques to improve the reliability of field level devices, installing a real-time prediction system, etc.

The hybrid modeling/simulation approach proposed in this thesis clears the technical difficulties, for future CI interdependency study to handle complexities related to CI interdependencies. More simulation platforms based on similar approaches will certainly be expected in the near future.

ZUSAMMENFASSUNG

Kritische Infrastrukturen (KIs) (*engl. Critical Infrastructures (CIs)*) wie das Energieversorgungs-, Transport- oder Telekommunikationssystem sind alle weiträumig, hoch und komplex integriert aufgebaut und insbesondere miteinander vernetzt. Diese Vernetzung hat zur Folge, dass sie sich gegenseitig stark beeinflussen können und das System störungsanfälliger wird; durch den wachsenden Bedarf an Ressourcen bzw. zeitgerechter Information wird dieser Effekt zusätzlich verschärft. Störungen und Betriebsausfälle innerhalb einer KI können sich leicht ausbreiten und die Funktionalität anderer KI beeinflussen, was wiederum weitreichende Konsequenzen für die Gesellschaft haben könnte. Es ist von entscheidender Bedeutung, die meist verdeckten Wechselbeziehungen zwischen den einzelnen KIs und die möglichen Ausfallskaskaden gründlich zu verstehen, um ihnen dann mittels fortgeschrittener Modellierungsmethoden bzw. Simulationstechnik begegnen zu können.

Die Wechselbeziehungen zwischen den einzelnen KIs zu identifizieren, zu charakterisieren und zu untersuchen ist eine grosse Herausforderung. Wissenschaftliche Untersuchungen in diesem Bereich befinden sich in einer relativ frühen Phase. Die Entwicklung eines Ansatzes zur vertieften Analyse dieser Wechselbeziehungen ist vor allem mit zwei wesentlichen Herausforderungen konfrontiert: Erstens eine einzelne KI mit ihren inhärenten Eigenschaften und dynamischen Verhalten zu modellieren, und zweitens mehrere KIs und deren gegenseitige Abhängigkeiten zu berücksichtigen. In jüngster Zeit wurden zahlreiche Verfahren wie Complex Network (CN) Theorie, Petri Netz (PN) und Agenten basierte Modellierung (ABM) entwickelt und eingesetzt, um die erwähnten Herausforderungen zu meistern. Jedes dieser Verfahren hat seine eigenen Stärken und Schwächen. In der Praxis gibt es noch keinen „Königsweg“, um die Vorteile jeder Methode zu nutzen und die verschiedenen Modellierungsmethoden in einem Simulationswerkzeug zu integrieren. Eine wesentliche Herausforderung für die Entwicklung eines solchen

„Tools“ ist es, ein „Multi-Domänen Modell“ zu erzeugen und die Daten zwischen den Domänen bzw. Submodellen auszutauschen.

Um einen vielversprechenden Lösungsweg für die Herausforderungen und die technischen Schwierigkeiten zu finden, wurde in dieser Doktorarbeit ein innovatives Hybrid-Modellierungs- bzw. Simulationsverfahren entwickelt und implementiert. Das Verfahren kombiniert verschiedene Modellierungs- und Simulationstechniken-, indem die „Methode verteilter Simulation“ sowie das „Konzept modularen Designs“ adoptiert wurde. Das Ziel des Verfahrens ist, die Anfälligkeit infolge gegenseitiger Abhängigkeiten qualitativ und quantitativ zu untersuchen bzw. evaluieren. Dieses Verfahren kann als Nachfolger traditioneller Modellierungs- und Simulationsverfahren betrachtet werden, die mehrere KIs simultan simulieren. Es verändert die Art und Weise, wie Simulationstools zur Untersuchung der Wechselbeziehungen zwischen den Cis ansetzen, indem es verschiedene Modellierungsverfahren in ein Simulationstool integriert, um die Effizienz der Gesamtsimulation zu optimieren. Die Anwendung des Hybrid-Verfahrens beschränkt sich nicht nur darauf, die gegenseitige Abhängigkeit zwischen den KIs zu untersuchen. Auch die Abhängigkeiten zwischen den einzelnen Subsystemen innerhalb eines KIs können damit analysiert werden, deswegen kann es als generisch gelten.

Mit diesem Hybrid-Verfahren als Basis wurde ein SCADA (Supervisory Control and Data Acquisition) Systemmodel entwickelt. Der ABM-Ansatz wurde mit anderen Techniken wie Monte Carlo Simulation, Fuzzy Logic und Finite State Machines kombiniert, unter Verwendung eines störungsorientierten Modellierungsverfahrens. Ein experimenteller Simulation-Prüfstand wurde mit der Anwendung des HLA (High Level Architecture) Simulationsstandards aufgebaut. Ausserdem beinhaltet das entwickelte SCADA-Modell ein spezifisches Modul für die dynamische Evaluation von Human Operator Performance mittels der auf diesen Fall zugeschnittenen CREAM (Cognitive Reliability Error Analysis Method) Methode. Der Prüfstand ist die erste erfolgreich entwickelte Plattform zur Untersuchung der Wechselbeziehungen zwischen KIs, welchen neu entwickelte

Teilmodelle von CIs und auch für andere Zwecke entwickelte Modelle verknüpfen kann. Einige Experimente einschliesslich solcher zum Nachweis der Anwendbar und der Versagensfortplanzung wurden durchgeführt, um das Verfahren sowie den entwickelten Prüfstand für die Untersuchung/Repräsentation der Wechselbeziehungen zwischen den Subsystemen innerhalb eines CIs bzw. die zwischen verschiedenen CIs zu validieren.

Um darüberhinausgehend die Funktionsfähigkeit und Eignung des Hybrid-Simulationsverfahren zu demonstrieren, wurde eine vertiefte Analyse der Abhängigkeiten zwischen einem „System Under Control (SUC)“ und seinem SCADA System mittels dreier Serien von Simulationsexperimenten durchgeführt. Das elektrische Energieübertragungsnetz der Schweiz diente als technische Referenz. Diese Experimente gehen von der Ebene der Unterwerke (Substation) aus, in denen technisches Versagen von Komponenten des SCADA-Systems angenommen und simuliert wurden, um den Schweregrad des jeweils hervorgehenden Schadens zu bestimmen und einzustufen. Im zweiten Experiment wurde der Geltungsbereich der Simulation auf ein kleines Netzwerk des SCADA-Systems ausgedehnt. In einem dritten Experiment wurde das vollständige SCADA-System untersucht. Aus den Resultaten der genannten Experimente kann geschlossen werden, dass das vorgeschlagene Hybrid-Verfahren geeignet ist, um das Problem der gegenseitigen Abhängigkeiten zwischen den KIs anzugehen sowie Möglichkeiten zum langfristig besseren Schutz der CIs zu identifizieren und sie resilienter zum machen. So kann z.B. durch die Nutzung von Eigendiagnostik-Techniken die Zuverlässigkeit von Geräten der Feldebene erhöht und ein Echtzeit-Vorhersagesystem installiert werden.

Das in dieser Arbeit entwickelte Hybrid-Simulation/Modellierungsverfahren löst einige technische Schwierigkeiten und dient als Basis für weitere Untersuchungen im Bereich von Wechselbeziehungen zwischen kritischen Infrastrukturen.

ACKNOWLEDGMENTS

This thesis is the result of the research work I have carried out at the Laboratory for Safety Analysis (LSA), Swiss Federal Institute of Technology (ETH) Zurich, between 2009 and 2011.

First of all, I wish to express my sincere gratitude to my supervisor, Prof. Dr. Wolfgang Kröger, for giving me the opportunity to conduct this multidisciplinary Ph.D. project as a member of his research team and having confidence in me. I am particularly grateful for his great guidance through the whole process of trying to obtain my PhD degree, his encouragements for exploring different approaches, and his supports for participating many international conferences around the world. The same applies my co-supervisor, Dr. Irene Eusgeld, who have been continuously providing me her great guidance and encouragements during last two years, especially during the period after she moved back to Germany. I owe special thanks to Prof. Dr. Lino. Guzzella for willing to take responsibilities as the reviewer of my thesis and provide me all the helps during this last step of my PhD study.

With pleasure I acknowledge the generous funding support by Swiss Federal Office for Civil Protection (BABS), which is a part of a project on vulnerabilities of critical infrastructures.

Special thanks also goes to my project manager, Patrick Probst, who took care of his new team/office mate, helped me with his knowledge and experiences, and guided me during last two and half years. I also thank Miltiadis Kyriakidis for his supports when I started to search a method for the purpose of HRA modeling, Dr. Andrija Volkanovski for his helps regarding the understanding / analysis of CCF, and Monika Mortimer for the professional cross-reading of papers. I further owe thanks to my colleagues at the lab, Konstantinos Trantopoulos, Zhou Ling, Markus Schläpfer and Evangelos I. Bilis.

I owe a lot to my friends for joining me through times where time sometimes was a very limited commodity. I would like to thank two of my good friends, Jiang Ying and Liu Yi who helped me to translate the abstract from English to German. I also would like to thank Zhang Jialin (Mumu) and Yin Hui, who always have time for me to be my listeners.

I would like to thank my (ex) girl friend, Marina Zhang, who encouraged me to go to Switzerland for chasing my dreams.

I would like to thank to my "role/life model", Prof. Dr. Jim Wright and his wife Elsie Wright, who have guided me though my professional career since the year of 2002 when I moved from Toronto to St.Johns in Canada. I am grateful for his "never-stop" guides and supports during last decade. Dr. Wright passed away in 2010. During his life-long journey, he has influenced lots of people, including myself and many other friends of mine. He will be remembered by all of us each single day during rest of our life.

Finally, I dedicate this thesis to my parents who are always there for me. It is your love, trust and unwavering supports which made this work possible.

TABLE OF CONTENTS

LIST OF TABLES

Number **Page**

LIST OF FIGURES

Number **Page**

1 INTRODUCTION

This chapter addresses the key terms used and motivation behind the research work described in this thesis as well as objectives and main research contributions.

1.1 Critical Infrastructures (CIs)

Critical infrastructures (CIs) can be referred to as a term, according to [1], which describes man-made systems and assets that are essential for the functioning of a society and its economy. These systems vary by nature, e.g., physical-engineered, cybernetic or organizational systems, by environment (geographical, natural) and operational context (political/legal/institutional, economic, etc.) [2]. These systems are also described as "*critical*" or "*essential*" infrastructure systems since they are responsible to provide our society with services crucial for its physical and economic survival. The European Council defines CIs as "*those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments*" [3]. The U.S. Department of Homeland Security defines CIs as "*systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters*" in section 1016(e) of the USA PATRIOT Act of 2001 (42 U.S.C.5195c(e)) [4]. From a Swiss perspective, the Swiss Federal Office for Civil Protection (FOCP) defines CIs as "*facilities and organizations, which deliver goods and services to society, whose disruption, failure or disruption, failure or destruction would have a serious impact on the functioning of society, the economy or the state*" [5]. Ten sectors such as energy, transport or financial services are considered as critical at national level, which can be further categorized into 28 sub-sectors (Table 1.1), such as power supply and oil supply sub-sector within the energy sector. In this thesis, this table will be used for the categorization.

1.1 Critical Infrastructures (CIs)

Table 1.1 Sectors and sub-sectors of Critical Infrastructures defined by Swiss FOCP [5]

Sectors	Sub-sectors	Sectors	Sub-sectors
Energy	Natural gas supply	**Information & Communication Technologies (ICT)**	Information technologies (Internet)
	Oil supply		Media
	Power supply		Telecommunications
Financial services	Banks	**Industry**	Chemical and Pharmaceutical industry
	Insurance companies		Mechanical and electrical engineering industries
Public health	Medical care and hospitals	**Water and Food**	Food supply
	Laboratories		Drinking water supply
Transport	Air transport	**Public administration**	Foreign representations and headquarters of international organizations
	Water transport		National cultural property
	Postal services		Parliament, government, justice, administration
	Rail transport		Research institute
	Road transport	**Public safety**	Armed forces
Waste disposal	Waste		Civil defense
	Wastewater		Emergency organizations
	Very high criticality	-> All sub-sectors are critical -> Criticality refers to the importance of the sub-sectors in terms of interdependency, the population, and the economy -> Even sub-sectors whose criticality is regular may contain highly critical individual elements -> Weighting is based on an ordinary threat level.	
	High criticality		
	Regular criticality		

Table 1.2 CIs that can be considered as technical systems

Sectors	Sub-sectors	Sectors	Sub-sectors
Energy	Natural gas supply	**ICT**	Information technology (Internet)
	Oil supply		Telecommunication
	Power supply		Media
Transport	Road transport	**Water and Food**	Drinking water supply
	Rail transport		Food supply

As described in the above definitions, a CI can be a "technical system" such as a power supply system (Table 1.2), but a CI can also be an "organizational system" such as public administration or public health. With respect to this research work, the proposed approaches are exclusively applicable to the technical systems of CIs, and therefore, only these CIs are considered.

CIs can also be considered as complex systems, as well as complicated systems [6, 7]. Complex systems can be defined as follows: “*Traditionally, a system is said to be complex if its attributes are commonly out of the norm, as compared with other systems. Complex systems are characterized by having a large number of dimensions, nonlinear or nonexistent models, strong interactions, unknown or inherently random plant parameters, time delays in the dynamical structure, etc*" [8]. Additional characteristics of complex systems are adaptive emergent behaviors and feedback loops. The central question here is whether the established methods of risk and reliability assessment developed for complicated systems can be applied to complex systems as well. Complicated systems are not easy to understand either, but they are (even though sometimes with remarkable effort) knowable. Complicated systems are also highly integrated systems but with low dynamics; they can be described with numerous variables. The decomposition of a complicated system for analytical goals is reasonable and common. On the other hand, a complex system can never be fully knowable due not only to rapid changes in its system states (high dynamic) and non-linear behaviors, but also interconnections within the system.

During recent decades, the increasing complexities and interconnectivities of CIs have made them grow into a "system-of-systems" (SoS). There is no universally accepted definition of the term "system-of-systems" yet. Numerous definitions vary depending on the application areas and their focus. Following the definition of a system of systems will be focused on:"*A system-of-systems (SoS) consist of multiple, heterogeneous, distributed, occasionally independently operating systems embedded in networks at multiple levels that evolve over time*" [9]. Alternatively, SoS can be defined using the term complex systems: "*System of systems are large scale concurrent and distributed systems that are comprised of complex systems*" [10].

CIs deserve increased attention as our societies simply rely on most of their goods and services they are expected to continuously supply [7]. In order to protect CIs, different Critical Infrastructure Protection (CIP) programs have been developed by governments around the world. In 2003, U.S. Homeland Security Presidential Directive 7 established a national policy for Federal departments and agencies to identify and prioritize CIs and protect them from attacks. In 2004, the European Council asked the Commission and the

High Representative to prepare an overall strategy to strengthen the protection of CIs including the proposal for additional measures to strengthen existing CI instruments. In 2005, the Swiss Federal Council mandated the FOCP to coordinate efforts in the area of CIP and to establish a CIP working group. Since then, this group has initiated a number of projects in order to achieve a more profound understanding of CIs.

CIs have been continuously exposed to multiple threats and hazards such as natural hazards, technical failures (hazards), and social hazards. A failure caused by these hazards within any CI or even loss of its continuous service may be damaging enough to our society and economy while cascading failures crossing subsystems (within a single CI) and/or even CI-boundaries have the potential for multi-infrastructural collapse and unprecedented consequences, which have been demonstrated and highlighted by several recently documented incidents [11-17]. The Baltimore Howard Street Tunnel Fire (an example of technical failures) on July 18th, 2001 and Hurricane Katrina (an example of natural hazards) on August 28th, 2005 may serve as examples for illustration:

Howard Street Tunnel Fire Case

"*The eastbound CSX freight train L-412-16 with 31 loaded and 29 empty cars from West Baltimore, Maryland, to Philadelphia, Pennsylvania, passed through the Howard Street Tunnel in Baltimore. At 3:08 p.m., 11 of its 60 cars derailed while the lead locomotive was about 1,850 feet from the east portal. For some time, the train crewmembers were not aware of the derailment. When they notified the derailment and tried to contact the CSX dispatcher, the radio contact could not be established since the radio relay system had been rendered by derailing equipment. Four of the eleven derailed cars were tank cars and one contained tripropylene, a flammable liquid. The derailment caused the puncturing (2-inch-diameter hole located near the bottom of the tank) of car carrying tripropylene and the subsequent ignition of this chemical product. The fire spread the contents of several adjacent cars which created the heat, smoke, and fume that blocked the access of the tunnel for five days and virtually shut down the down-town area." [14].*

Figure 1.1 provides more detailed information about which and how CIs were affected during this incident. As shown in this figure, a technical failure (freight train derailment) occurring in the rail transport sub-sector continued to propagate into other CI sectors/sub-sectors. For instance, the break of the water mains (a failure within drinking water sub-sector) due to tunnel fire explosion flooded the tunnel with millions of gallons of water, and

caused damages of power cables and fiber-optic cables. As a result, 1,200 Baltimore buildings lost electricity services and both internet and telephone services were interrupted [12]. Consequences initially triggered by the freight train derailment were worsened due to interdependencies among CIs.

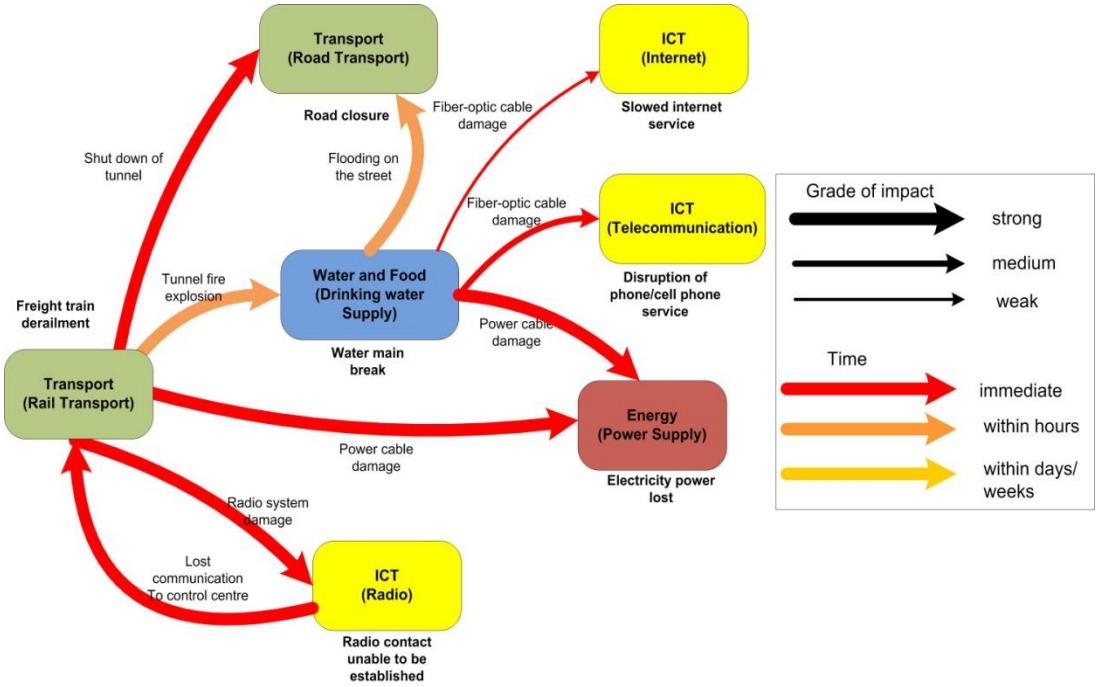


Figure 1.1 Interdependency graph of the 2001 Baltimore Street Tunnel Fire [14]

Hurricane Katrina Case

"On the morning of August 28, Katrina reached to category 5 hurricane status, with maximum sustained winds of 280 km/h and a minimum central pressure of 902 mbar. At 6:10 am. CDT (Central Daylight Time) on August 29, Katrina made its landfall at near Buras-Triumph, Louisiana as a Category 3 hurricane, with maximum winds of 205 km/h and about 30 miles wide storm eye. Katrina brought heavy rain to Louisiana, with 8-10 inches falling on the eastern part of the state. On August 31, Katrina was downgraded to a tropical depression near Clarksville, Tennessee, and later was absorbed by a frontal boundary in the eastern Great Lakes region. Katrina caused severe damage along the Gulf coast from central Florida to Texas. The most severe losses of life and property destructions occurred in New Orleans, Louisiana." [14].

As shown by Figure 1.2, about 6 CI sectors (9 CI sub-sectors) were affected by this natural hazard directly or indirectly. For example, the roads became impassable (failure of

the road transport sub-sector) and electricity power lines were knocked out (failure of power supply sub-sector) due to the flooding caused by the Katrina in the affected areas. Failures of these two CI sub-sectors continued to propagate into another CI sub-sector, public health sub-sector, since most hospitals and medical care locations in affected areas lost electricity and adequate supplies of potable water and food for days after Katrina made landfall due to power outage and impassable roads.

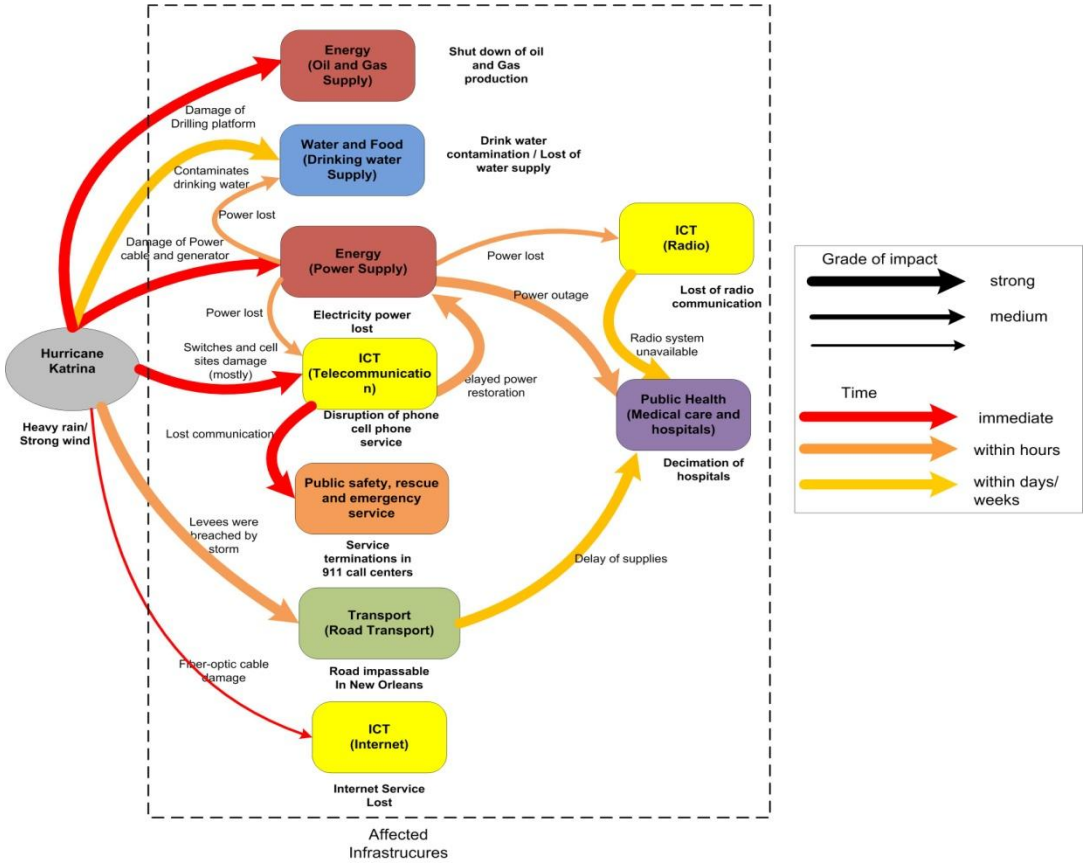


Figure 1.2 Interdependency graph of 2005 Hurricane Katrina [14]

A list of this type of recently documented incidents are summarized in Table 1.3, based on the work done by Kröger et al. [14]. As shown in this table, cascading event sequences are triggered by one single failure or hazard develop into fast cascades crossing subsystems within one CI sub-sector and/or boundaries of various CI sub-sectors due to their interlinks with worsened (negative) consequences. Negative cascading impacts, as exposed in these incidents have started to challenge society to study and cope with the

recently recognized weakness of CIs, i.e., vulnerability caused by interdependencies. It should be noted that due to the size of the table, only parts of its contents are shown here; see Appendix I-2 for more details.

Table 1.3 List of recently documented incidents whose consequences were worsened due to interdependencies within and among CIs [14]

Incident	Date	Affected area(s)	Primary Cause (Natural of Cause)	Affected CIs (Sectors/Sub-sectors)	Consequences
1998 Ice Storm Canada	January, 1998	Eastern Ontario, Southern Quebec of Canada and parts of New York and New England of USA	A massive ice storm created a major disaster in areas in Canada and USA. (Natural hazards)	Number of affected CI sectors: 4 Number of affected CI sub-sectors: 4	* 3.6 million people were affected * Economic damage caused by this storm was estimated to be 3 billion U.S dollars.
2001 Baltimore Howard Street Tunnel Fire	July 18, 2001	Baltimore, USA	A freight train detailed while passing through Howard Street Tunnel in Baltimore and caused the fire explosion due to subsequent ignition of the flammable liquid. (Technical failure)	Number of affected CI sectors: 4 Number of affected CI sub-sectors: 6	12 million U.S. dollars associated with incident.
2001 World Trade Center Attack	September 11	New York, USA	Terrorist attack with two hijacked planes caused the collapse of WTC, New York . (Social Hazards)	Number of affected CI sectors: 7 Number of affected CI sub-sectors: 10	In total 2,993 people were killed, more than 6000 injured.
2003 North America Major Power Blackout	August 24, 2003	Northeastern and Midwestern USA and Ontario, Canada.	Eastlake 5 electricity generation unit shut down automatically (USA). (Technical failure)	Number of affected CI sectors: 6 Number of affected CI sub-sectors: 8	* 10 million people in Canada and 45 million people in USA. * Direct costs are estimated to be $4 billion to $10 billion US dollars.
2003 Italian Power Blackout	September 28, 2003	Italy and pars of Switzerland	Flashover and shut down of the Lukmanier transmission line causing overload of the San Bernardino line which suffered also from a flashover. (Technical failure)	Number of affected CI sectors: 5 Number of affected CI sub-sectors: 10	* A total of 56 million people were affected. * About 120 million Euro finance losses.
2005 Hurricane Katrina	August 23-31 , 2005	Gulf coast from Central Florida to Texas, especially in New Orleans, Louisiana	Hurricane Katrina (a category 4 hurricane) (Natural hazards)	Number of affected CI sectors: 6 Number of affected CI sub-sectors: 8	* Damages cost more than 100 billion U.S dollars. * 1,836 fatalities

1.2 Dimensions of (Inter)dependency

The term *dependency* is defined as an unidirectional relationship between two systems, while *interdependency* is defined as a bidirectional relationship between two systems according to [18]. It should be noted that two systems, as mentioned above, could correspond to one infrastructure (*internal interdependency*) or two infrastructures (*external interdependency*). For example, the interdependency between an Electricity Power Supply System (EPSS) and its Industrial Control System (ICS), responsible for daily system monitoring and control, can be referred as an example of the internal interdependency due to the fact that two (sub)systems are included within the power supply sub-sector. It should be noted that an EPSS can also be referred to as a System Under Control (SUC) if

discussed as a subsystem in the power supply sub-sector. The interdependency between an EPSS and its telecommunication system, which is part of another CI sub-sector (ICT), can be referred as an example of external interdependency. The dependency and interdependency can also be explained from a technical perspective: the term dependency can be regarded as a linkage between two systems (infrastructures) through which the state of one system influences the state of the other, whereas interdependency is a bidirectional relationship through which the state of each system is correlated to the state of the other [18].

Interdependencies are more of great practical relevance than a new theoretical concept, as clearly demonstrated by recently documented incidents (Table 1.3). Interdependencies may cause a series of second order or even third order failures following a primary failure and by this may worsen the consequences and cause unpredictable system behaviors. Rinaldi et al. categorized four general types of CI interdependencies and introduced six dimensions for describing CI interdependencies [18]:

- **Physical interdependency:** the state of each is dependent on the material output(s)/flows(s) of the other, e.g., a pipeline network provides gas to fuel a gas-fired power station while the electricity generated is used to power compressors and controls the gas supply network.
- **Cyber interdependency**: the connection between CIs is via electronic signals, information links, e.g., an ICS system monitors and controls elements of an EPSS.
- **Geographic interdependency**: elements of multiple CIs are in close spatial proximity and a local environmental event can create state changes in all of them, e.g., power cables and fiber-optic cables, installed in a compact area, were both damaged by the flooding during the 2001 Baltimore tunnel fire incident.
- **Logic interdependencies:** interdependency that does not fall into one of the above categories, e.g., the incident of the 2001 world trade centre attack caused drops of shares of several insurance companies.

During the 2003 North America major power blackout, cascading failures were mainly caused by physical interdependencies. For example, 87% of network customers served by the Michigan Internet Communication Association (MICA) experienced service outages simply because almost all network servers had lost their power supplies [19]. This example reveals negative effects caused by physical interdependencies, which can also be seen as external interdependencies between two CIs. Cascading failures can arise not only from external interdependencies (among CIs) but also from internal interdependencies (among subsystems within a CI). In January 2005, approximately 15,000 households lost electrical power due to a failure in the SCADA[1] system in Weert, Netherlands [20]. This incident was triggered by internal interdependencies between the SCADA system and the SUC within the power supply sub-sector.

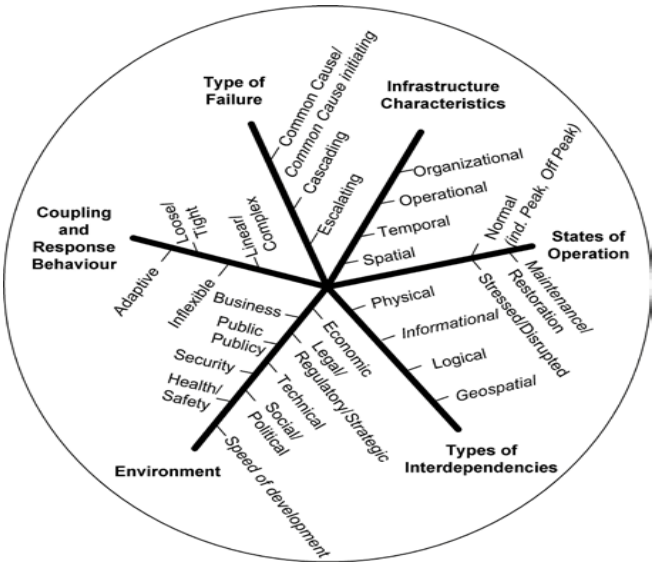


Figure 1.3 Six dimensions for describing CI interdependencies [14]

Figure 1.3 shows six dimensions for describing CI interdependencies, which was originally developed by Rinaldi et al. [2] and modified by Kröger et al. [14] (modifications in italic). As

[1] SCADA represents Supervisory Control and Data Acquisition, which is a typical ICS. More details about SCADA systems will be presented in Chapter 2.

seen in this figure, the degree of coupling can be tight or loose. Tight coupling refers to CIs or subsystems of a CI that are highly dependent on each other, e.g., the coupling between the power supply and telecommunication sub-sector, the coupling between a SUC and a SCADA within one CI sector, etc. In general, failures tend to propagate rapidly crossing tightly coupled subsystems and CIs. Loose coupling refers to CIs or subsystems of a CI that are relatively independent from each other, e.g., the coupling between the drinking water supply sub-sector and information technology (internet) sub-sector. Normally, the failure of a drinking water supply sub-sector rarely affects an information technology sub-sector. However, during the 2001 Baltimore Howard tunnel fire incident, the flooding due to the break of the water mains damaged fiber-optic cables causing local service interruptions of Internet services.

Another important coupling characteristic is the coupling order, which indicates whether subsystems of a CI or CIs are directly connected to one another or indirectly coupled through one or more intervening systems/subsystems [18]. Based on the Figure 1.1, the interdependency graph of the 2001 Baltimore tunnel fire, the interdependency between the rail transport sub-sector and information technology (internet) sub-sector can be regarded as a 2nd order coupling since two sub-sectors were linked with each other though the drinking water supply sub-sector. In general, higher order couplings increase the difficulties of identifying and understanding CI interdependencies and make the protection of CIs more challenging.

Failures that arise due to interdependencies within and among CIs can be classified as follows [14]:

1) **Common cause initiating event**: One event causing failure or loss of service of more than one subsystem within a CI or several CIs, such as failures caused by natural disasters (earthquakes, floods, extreme weather conditions, etc.) due to the spatial proximity.
2) **Cascade initiating event**: Failure of one subsystem within a CI or a CI causing failure or loss of service of at least one other subsystem or CI, e.g., break of mains of the water supply system.

3) **Cascade resulting event**: Failure or loss of service resulting from an event in another subsystem or CI, e.g., electricity service lost due to damage of power cables caused by break of mains of the water supply system.

4) **Escalating event:** Failure or loss of service of one subsystem or CI escalating (domino effect) because of failure of another subsystem (in same CI) or CI affected, e.g., failure of a SCADA system leading to failure of its controlled/monitored SUC and by this affecting restoration of the SCADA system.

It should be noted that all these four types of events have been considered in the research work described in this thesis.

1.3 Concept of Vulnerability

The concept of vulnerability is still evolving and terms are not consensually defined [21-25]. Some definitions consider the system vulnerability as an adverse consequence of the manifestation of the inherent states of the system. For example, Haimes [24] defines the vulnerability as "*the manifestation of the inherent states of the system (e.g., physical, technical, organizational, cultural) that can be exploited to adversely affect (cause harm or damage to) that system*". Johansson et al [26] define this term as "*the degree of loss or damage to the system when exposed to a perturbation of a given type and magnitude",* considering the vulnerability as the arising consequences when a system is exposed to a strain.

In a recently published book, "vulnerable systems" [25], Kröger and Zio further improve the understanding of this term by defining the vulnerability as "*a flaw or weakness (inherent characteristic, including resilience capacity) in the design, implementation, operation, and/or management of an infrastructure systems, or its elements, that renders it susceptible to destruction or incapacitation when exposed to a hazard or threat, or reduces its capacity to resume new stable conditions*". In this book, Kröger and Zio also introduce an approach to quantify the vulnerability using the parameter frequency while a measurand for destruction or incapacitation (loss or damage, respectively) needs specific

elaborations depending on the value placed on the asset by its owner/operator. According to this approach, the vulnerability of an EPSS might be represented in terms of changes of network characteristics following attacks on nodes, e.g., number of nodes/lines lost, or the duration of the associated loss. With respect to this research work, above definition and representation about the system vulnerability will be used. Based on this definition, the term vulnerability includes three elements: (1) the degree of the exposure to hazards ("shocks"), (2) the susceptibility of an element at risk to suffer loss or damage and (3) the resilience [25]. Figure 1.4, which is based on the work done by Bouchon [27], illustrates these three elements and potential response behaviors of a system with low vulnerability and a system with high vulnerability.

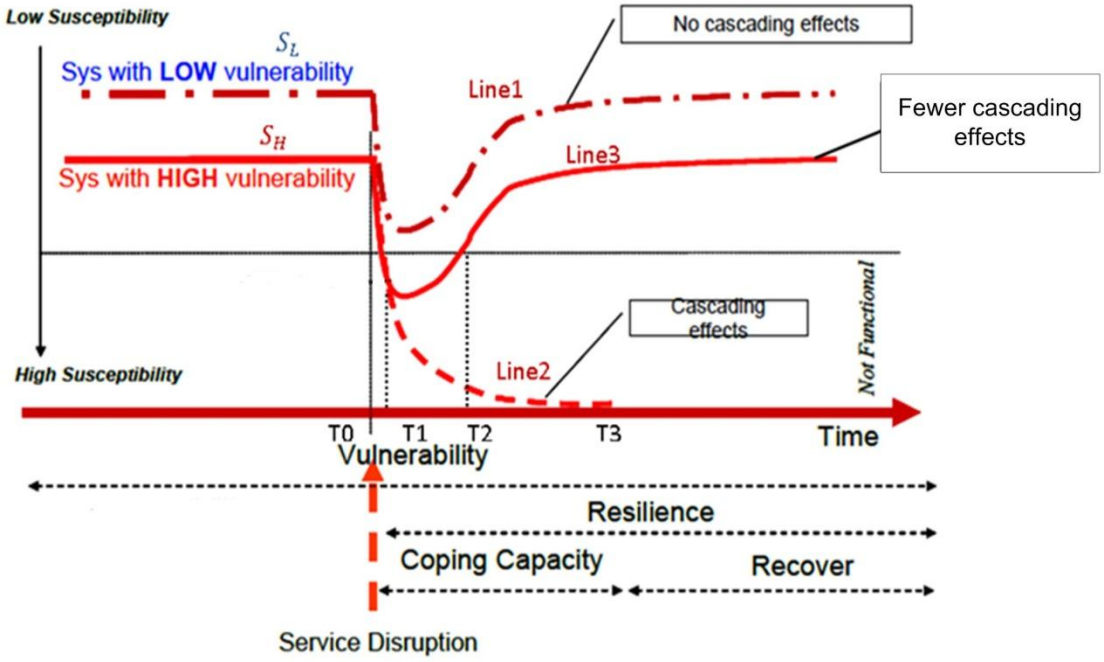


Figure 1.4 Vulnerability elements and associated response scenarios [27]

In Figure 1.4, where the y-axis represents the system susceptibility, observed behaviors of different systems after an incident (or initial failure) are shown (it is assumed that the incident occurs at time T0). The system S_L is assumed to be a system with low vulnerability and no cascading effects are observed after the incident, although the susceptibility of the system increases (shown in Line 1). The system S_H is assumed to be

a system with high vulnerability and cascading effects are observed after the incident. Furthermore, failures continue to propagate until the system S_H completely fails to function at time T3 (shown in Line 2). What could be the outcome if the system S_H had been successfully improved assuming that its high vulnerabilities in this system were identified in advance? Line 3 demonstrates a possible outcome based on this assumption. At time T0, the incident is assumed to occur and corresponding failures start to propagate. At time T1, failures stop propagating and the system starts to recover. At time T2, the system has recovered its functional status (back to normal). Although cascading effects can still be observed from behaviors of the improved system S_H, it (S_H) becomes more resilient to cascading failures and its coping capacity has been improved. This figure can also be considered as an example illustrating the significance of identifying hidden vulnerabilities in advance, which may improve susceptibility and resilience of a system.

1.4 Motivations and Objectives

Several critical questions can be raised by us by analyzing incidents as listed in Table 1.3:

- *Why do final consequences of these incidents become so serious*?
- *Are CIs our daily life depends on sufficiently well designed?*
- *What should or can we do to minimize these negative effects?*

One short answer to the first question is that CIs have become more tightly integrated as well as more interdependent, as already introduced in previous sections. In general, to maintain normal functionalities of one CI, other CIs might be required. As a result, CIs are highly interconnected and mutually dependent in complex ways, both physically and through a host of information and communication technologies [18]. Besides benefits (positive effects), such as real-time system monitoring and remote controlling, interdependencies within and among CIs lead to numerous vulnerabilities (negative effects), which potentially could disable or interrupt their daily operations and make CIs more vulnerable. The CIs are usually designed to cope with incidents that occur somewhat frequently. For instance, the "N-1 criterion", which is a common binding security principle for both planning and operation of electric power transmission systems, has been widely

implemented to compete overload failure if one linkage is lost. However, the large-scale disruptions turned to be more frequent and demonstrated difficulties for current CIs to cope with these types of incidents effectively. Identifying, understanding and analyzing these incidents are still major challenges, magnified by the breadth and complexity of most CIs.

The motivation behind this research is to search for an approach that is capable to address the type of questions stated above from an engineering perspective by getting in-depth insights into cascading system behaviours as a result of the interdependencies within/among CIs and identifying hidden vulnerabilities that might help our society to cope with "low frequency, high consequence" incidents more effectively. The purpose of this "effective cope" is not just to identify the cause of failures and prevent them but also to halt on-going cascading or escalating events before they affect other CI sectors/sub-sectors. The close spatial proximity of several CI sub-sectors within a compact area was one of several causes for the 2001 Baltimore tunnel fire incident. The consequences caused by negative cascading effects could have been minimized if this cause were fully recognized. For example, if power cables, damaged by the flooding during the incident, had been rerouted during their design and implementation stage to keep away from the water mains, then the lost of electricity supply services could have been avoided.

The major objectives of the research are:

1. The propagation of rare and unanticipated but interdependent failures in a cascade is not, or only insufficiently, evaluated by conventional methods [28]. Therefore, the core objective of this research is to develop a novel and comprehensive approach for exploring and assessing the vulnerabilities caused by interdependencies within and among CIs qualitatively and quantitatively using advanced system modelling and simulation techniques. It should be noted the application of this approach should not be limited to the interdependencies among CIs, but also within single CIs, e.g., interdependencies among subsystems (within a CI). In this research work, this approach will be applied to explore and study interdependencies between a SCADA subsystem and its associated SUC within the power supply sub-sector. Furthermore, a modelling

approach needs to be developed, which is capable of integrating Human Reliability Analysis (HRA) into the developed CI model.

2. To create a real-time experimental simulation test-bed for the purposes of implementing the proposed hybrid modelling/simulation approach and demonstrating its applicability and feasibility using the test-bed.

3. To explore interdependencies between a SCADA subsystem and a SUC and identify vulnerabilities related to interdependencies using the developed experimental simulation test-bed.

4. To suggest some improvements of identified weaknesses in the systems analysed.

1.5 Research Contributions

- **A hybrid modeling/simulation approach:** One of the key challenges for a simulation tool representing CI interdependencies is the required ability to integrate multiple-domain models, or to effectively exchange data among these models [29]. This thesis proposes a novel hybrid modeling/simulation approach that is capable of meeting this challenge by adopting the technology of distributed simulation and modular design. Although the distributed simulation technology has been widely used in many other research and industrial areas, e.g., design of control systems, computer simulations, etc., this is the first trial to apply this technology in the CI interdependency research area. This approach allows to divide the overall simulation tool into different simulation modules at first, which could be domain-specific or sector-specific simulation components, and then to distribute them across one simulation platform. The approach, which can be implemented by adopting a simulation standard such as the High Level Architecture (HLA), not just potentially improves the efficiency and flexibility of the developed simulation tool, but also intends to integrate different modeling/simulation approaches and fully utilizes benefits/advantages of each of them.

- **A SCADA system model including the assessment of the human operator performance:** Modeling and simulating a SCADA system is a challenge not just from a scientific point of view but of great practical importance. This thesis

proposes a new modeling approach, as the part of the hybrid modeling/simulation approach, which combines the Agent-based Modeling (ABM), together with other modelling techniques such as Monte Carlo simulation, Fuzzy Logic, and Finite State Machines (FSMs). Using this approach, not just functionalities of a general SCADA system are modeled, but the status (intact/defect) of its hardware components are also considered. With the help of this approach, the flexibility of the developed model is improved and system behaviors can be modified easily by changing parameters of corresponding agents. Moreover, technical failures of simulated devices of a SCADA system can easily be determined and corresponding failure propagation can be visualized/studied. The developed SCADA model includes a specific model for the assessment of human operator performance, for which the CREAM (Cognitive Reliability Error Analysis Method) has been selected and utilized by combining it with new elements such as the ABM and Fuzzy Logic.

- **An experimental simulation test-bed**: An experimental simulation test-bed is built based on the hybrid modeling/simulation approach, introduced above, for the purpose of vulnerability analysis of interdependent CIs. The final goal of this test-bed is to provide sufficient insights into interrelationships within and among CIs, investigate potential negative effects, and identify the presence of unknown and unexpected vulnerabilities of CIs related to the interdependencies. The test-bed is the first successfully developed simulation platform in the research area of the CI interdependency study that is capable of coupling independently developed CI models and reusing models developed for other purposes. Benefiting from the efficiency and flexibility of the adopted distributed simulation standard (HLA), capabilities of this experimental test-bed can be expanded since new simulation components are able to be easily integrated into the test-bed and interacted with existing peer components for many other experiments without major efforts of modifying current architecture of the test-bed.

1.6 Organization of the Thesis

Chapter 2 provides detailed information about SCADA systems, which will be used as one of exemplary systems (another exemplary system is SUC=EPSS) to apply the hybrid modeling/simulation approach presented in this thesis.

Chapter 3 introduces a 5-step methodical framework, based on the framework proposed by Eusgeld and Kröger [30], for analyzing vulnerabilities due to interdependencies within and among CIs. This chapter focuses on the first two steps of the methodical framework: preparatory phase and screening analysis.

Chapter 4 presents a novel hybrid modeling/simulation approach for in-depth analysis of interdependencies within and among CIs. The implementation of this approach includes modeling a SCADA system, development of an experimental test-bed for studying interdependencies between the SCADA system and the SUC.

Chapter 5 presents three sets of experiments conducted using the developed experimental simulation test-bed. The core objects of these experiments are to explore interdependencies between two exemplary systems (SCADA and SUC) and identify hidden vulnerabilities due to their interdependencies.

Chapter 6 presents results assessment and potential technical improvements, by analyzing results collected from experiments presented in Chapter 5. Vulnerabilities identified based on the analysis of the simulation results will be presented and discussed. Furthermore, suggestions for potential technical improvements will be provided in this chapter.

Chapter 7 presents overall discussion and conclusion regarding the research work presented in this thesis. Moreover, this chapter also presents some thoughts regarding future research works.

This thesis is based on 9 publications, which have been peer reviewed/discussed for one book chapter/newsletter/international journals/international academic conferences, and 3 scientific reports for Swiss FOCP. All of these publications and reports are listed in Appendix I-1.

2 SCADA

The purpose of the Supervisory Control and Data Acquisition (SCADA) system[2] is to allow a user (operator) to collect data from one or more remote facilities and send control instructions back to those facilities. For instance, voltage, frequency and phase angle are all important parameters in the power industry, which are continuously monitored for maintaining a normal working environment.

2.1 General Structure of a SCADA System

In general, a SCADA system has two main functions:

- **Monitor function**: transport data from sensors, switches, and other devices installed at remote facilities.
- **Control function**: adjust process parameters by changing the states of switches and actuators, e.g., opening or closing valves.

Compared to other control systems such as PLC (Programmable Logic Controller) and DCS (Distributed Control System), SCADA system is normally used to monitor and control very large industrial process facilities such as electricity transmission facilities and oil and gas production facilities [31]. An important characteristic of SCADA system is its inherent structure complexity. It generally comprises remotely located field level devices, which are connected to a centrally located control room through a variety of communication devices. Furthermore, most SCADA system functionalities require services provided by other systems. For instance, communication systems must be used to transmit commands from

[2] In this thesis, SCADA will be referenced as a system if it is individually introduced and discussed. Nevertheless, if the discussions are related to interdependency study within one CI sector/sub-sector, SCADA will be referenced as a subsystem.

SCADA system to field level devices in order to adjust process parameters. CIs such as the sub-sectors of power supply, telecommunication, and rail transport have been benefiting from using SCADA systems [32-34]. They can be regarded as backbones of these CIs [35]. These infrastructure systems are all large-scale, complex, highly integrated and particularly interconnected. A SCADA system allows for a human operator of such systems, based in a central location, to continuously gather measured process variables, monitor alarms, and to open or close switches, etc. Figure 2.1shows the general structure of a SCADA system.

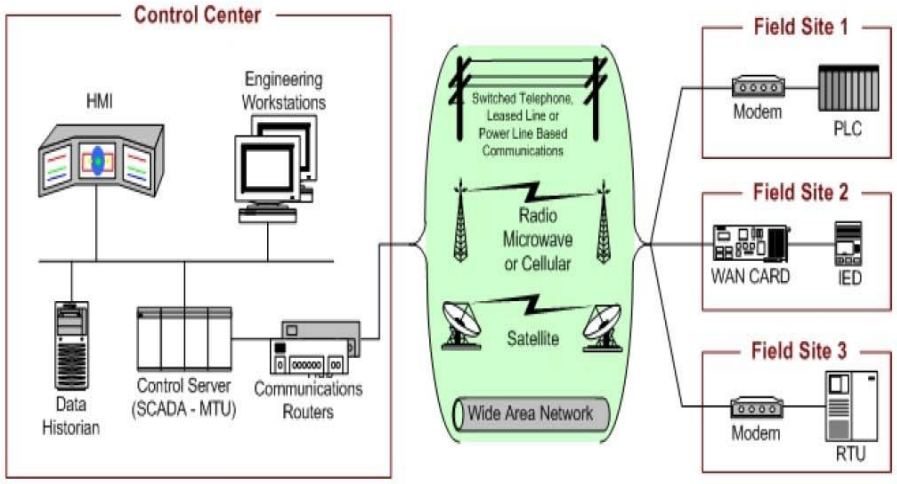


Figure 2.1 General Structure of a SCADA system [36]

2.2 Importance of Securing a SCADA System

Originally, a SCADA system was designed as a point-to-point system connecting a monitoring or command device to a remotely located sensor or actuator. By now, it has evolved into a complex network that supports communication between a central control unit and multiple remote units using advanced information and communication technologies (ICTs) [37-39]. Having said this, extensive uses of ICTs introduce new types of security threats to SCADA systems [40, 41]. Nowadays, a SCADA system could also be connected to a company's cooperate network for the purpose of increasing efficiency and optimizing manufacture [37]. The increased connectivity of a SCADA system has a potential to expose its monitored/controlled safety-critical CI (SUC) to a wide range of

security issues and severe threats such as unauthorized accesses and malicious intrusions, therefore causing cascading failures and incidents with widespread disasters. For example, Stuxnet, a self-replicating computer worm, has recently been hailed for its complexity and capability to challenge the securities of CIs through SCADA systems by modifying the control logic of field level control systems [42, 43]. It should be noted that the only target of Stuxnet was Simatic WinCC, a Wndows-based SCADA system developed by SIEMENS.

Recent surveys show that a number of attacks against SCADA systems have been reported over the years. Two examples are given for illustration:

- In March 2000, about 800,000 liters of raw sewage were released and spilled out into local parks and rivers due to unauthorized accesses to the SCADA system of a sewage treatment plant in Maroochy Shire, Australia, by a former contractor, causing death of marine life, stench and discoloration of water [44, 45].
- In October 2000, the control system in a hydro power plant at Ertan, China, was shut down due to abnormal signals it received. About 890 MW of electricity was lost in 7 seconds and the whole power grid in Sichuan province almost collapsed [46].

There also are numerous unreported incidents by asset owners and operators related to the security issues in SCADA systems [20]. All of these experiences and lessons learned from the past have motivated us to explore and study negative impacts due to interdependencies[3] between SCADA and SUC. Ensuring and securing functionalities of a SCADA system and its controlled/monitored SUC generally face three challenges. While first two extreme challenges are related to the security aspect and the last one is related to the reliability aspect:

[3] It should be noted that interdependencies between SCADA and SUC can also be regarded as (internal)interdependencies, as defined in Chapter 1.

- **Access control restriction**: The negative effects caused by unauthorized accesses to a SCADA system have been demonstrated by the Maroochy Shire accident described above. Therefore, it is essential to prevent or deny unauthorized accesses by a well defined and comprehensive company policy which includes installing efficient gateway systems restricting unnecessary/unauthorized accesses to SCADA systems [47]. More information regarding this challenge can be found in [48] and [45].
- **Improvement of protocol security**: Currently, well-established SCADA communication protocols (e.g., Modbus, Profibus, etc.) are not secured due to the fact that they were designed at a time when industrial control systems were completely isolated from public networks and ICT-based intrusions were considered to be very unlikely [40]. These protocols could be hacked or interrupted and possible consequences are over-written control commands sent from a control centre to field level devices. For instance, the fault safe mode is a widely used mechanism to isolate suspected unsafe processes, which can be activated by control commands (issued by an operator in a control room and transmitted via a SCADA system). These commands, compiled by SCADA communication protocols, could be over-written to disable the fault safe mode by modifying their contents after analyzing the protocols. The protocol security can be improved by introducing cryptography techniques and installing computer firewalls in order to ensure secured data transmission.
- **Investigation of failures of field level devices**: The field level devices used by SCADA systems, such as sensors and actuators, are essential not just for daily operations and the protection of SCADA systems but also for the SUC they are connected to. A minor operation disruption of these field level devices could possibly lead to a significant service loss and even unavailability of all systems (SUC and SCADA). Therefore, it is very important to investigate all possible (technical) failures of these SCADA-related field level devices, which could lead to the identification of hidden vulnerabilities of SCADA systems [49].

2.3 Role of Substations within Power Supply Sub-sector

Within the power supply (CI) sub-sector, a substation can be considered as a node, which connects transmission lines and cables for generation, transmission, and distribution of electric power [50]. For instance, a transmission substation is a node connecting two or more transmission lines, while a distribution station is a node connecting electricity consumers to the transmission system. Generally, most substations are geographically dispersed, often scatted over thousands of square kilometers. This situation raises concerns regarding the monitoring and control of the performance of the power system, which can be handled using a SCADA system. The role of a SCADA system in terms of controlling a SUC within a power supply sub-sector, including electricity generation, transmission, and distribution, is basic: grid operators use a SCADA system to adjust outputs of generation substations by sending commands (instructions) to control systems remotely installed in substations. The transmission and distribution of the electricity can be continuously monitored by transmitting real time data from each substation back to the control centre for further analysis to alert operators for potential abnormal operating problems. Circuit breakers, line disconnectors, tap changers, and other devices can also be manipulated and switched ON/OFF remotely to ensure the system safety and improve the overall performance.

2.4 Standard SCADA System Hierarchy

There are four levels in a standard SCADA system hierarchy, illustrated in Figure 2.2.

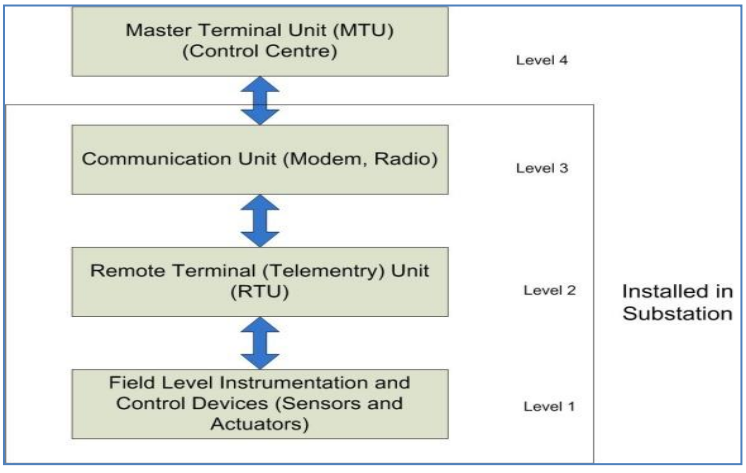


Figure 2.2 Four levels of standard SCADA system hierarchy

2.4.1 Level 1-Field level instrumentation and control devices

Level 1, field level instrumentation and control devices, is the lowest level in the standard SCADA system hierarchy. It is an interface connecting a SCADA system to physical processes (e.g., electric power) and equipment (e.g., general control system). Integrating level 1 devices from a SCADA system with equipment for controlling and monitoring physical processes in substations has recently become more complicated due to the necessity of cost reduction and productivity improvement [51]. For example, a measurement device (e.g., a sensor) could be used by both SCADA system and a general control system of a CI. Sensors and actuators are two examples of devices of level 1 of the SCADA system hierarchy, field level instrumentation and control devices. A sensor is a device that detects a physical variable and converts it into a signal that can be interpreted by an observer or another instrument. The input module of a RTU (Remote Terminal Unit) connects to sensors, for the purpose of measuring information collecting from physical processes of CI. This measured information includes not only analog values such as voltage, current, and temperature, but also digital values such as tap changer position. All analog values (signals) are transformed into a binary format via an A/D (Analog/Digital) converter in order to be stored and transmitted by a SCADA system. The output module of a RTU is attached to actuators that interpret commands from the MTU (Master Terminal Unit) to control or adjust field level controllable equipment.

2.4.2 Level 2-Remote Terminal Unit (RTU)

RTU, level 2 in the standard SCADA system hierarchy, is a rugged industrial common system providing intelligence in the field. It is a standard stand-alone data acquisition and control unit with the capabilities of acquiring data from the monitored process, transferring data back to the control centre, and controlling process equipment located at remote sites. Small sized RTUs usually have less than 10 to 20 analog/digital inputs. Medium sized RTUs have 100 digital and 30 to 40 analog inputs. Figure 2.3 illustrates the signals (data) that interchange between a RTU and its connected field devices of level 1.

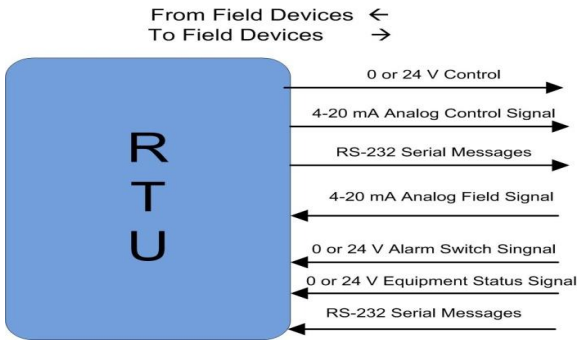


Figure 2.3 The signals that come into and leave the RTU [31]

A typical RTU configuration is shown in Figure 2.4. Generally, there are seven hardware modules included in a RTU:

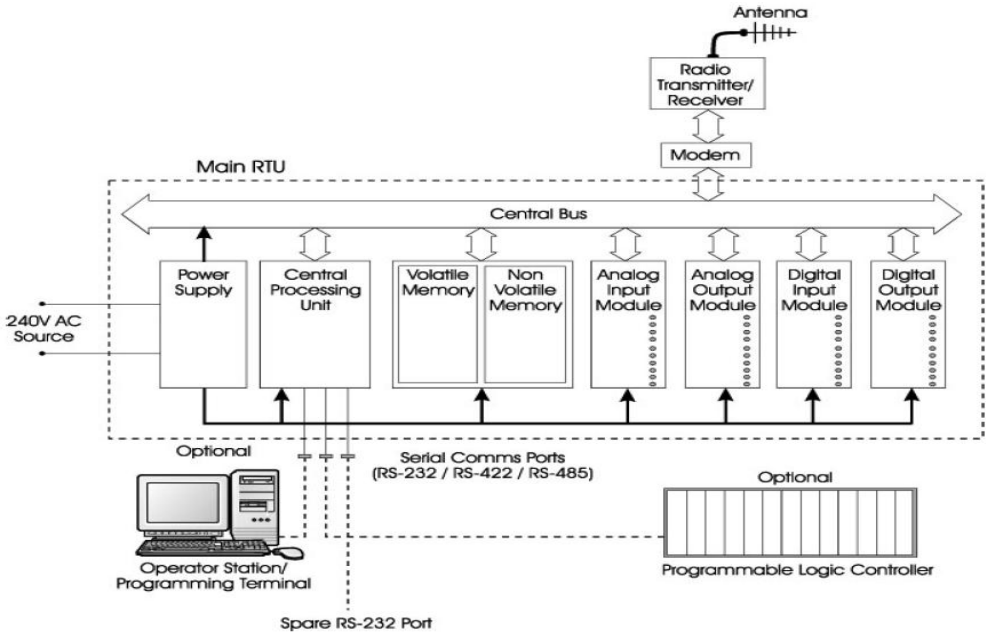


Figure 2.4 Typical RTU hardware configuration [51]

- **Power Supply**: A RTU equipment should be able to operate from 110/240V AC±10% or 12/24/48V DC±10% typically [52]. Batteries and associated chargers are also included in this module in order to provide additional power supply in case of a power outage. Since the power supply module is vital to the proper function of a RTU, it is necessary to continuously monitor battery readings at the control centre.

- **CPU**: The Centre Processing Unit (CPU) included in a RTU is also considered as a control processor for its functionalities of interpreting control commands sent by a MTU and converting them into controller-recognizable serial instructions. Furthermore, this module is useful for calculating complex process control formulas and parameters.
- **Memory**: Generally, a RTU collects data as fast as possible from field instrumentation devices, and mirrors current process states into a real time database, which is stored in a local memory. Presenting current process parameters to a MTU is performed from the same database, which is generally independent of the data acquisition.
- **Analog / Digital Input**: Inputs to a RTU generally fall into two basic types: analog and digital. Energy values are usually obtained from pulse counters, which represent the contents of continuous counter digitally for the specific time period. The status of switching devices and alarm signals represented by status indications are also considered as a source of digital inputs to a RTU. Measured voltage, current, and temperature values are all represented by analog signals, which need to be transformed via an A/D converter into a binary format before storing them in a real time database.
- **Analog / Digital Output**: The analog/digital output hardware module is used to transmit the control commands/instructions to corresponding field devices such as actuators.
- **Operator Station**: Operator station is a computer, which is connected to a RTU via a substation level communication network. Collected information from field instrumentation devices is also available in this computer. With the help of the operator station, a local operator in a substation is able to monitor the current operating environment, change the configuration of field level devices, and handle alarms generated by the RTU locally. It should be noted that only medium or large sized substations are equipped with this equipment.
- **Programmable Logic Controller (PLC):** PLC is a computer based solid-state device that controls industrial equipment and processes. In some substations, PLC is connected to a RTU to implement more sophisticated

process control methods, for example, performing fuzzy logic based process control. Since this thesis only focuses on the general configuration of a RTU, PLC will not be discussed.

All the hardware modules discussed above are connected to one common control bus, from which the data related to each hardware module is available to all other modules. It is also called substation communication network. A RTU, including all hardware modules, is either installed in a control compartment within the housing for indoor equipment or housed in control cabinets for outdoor installations, which could help to protect it from extremes of temperature, weather, etc. A typical configuration of a control compartment, also referenced as a RTU Block in this thesis, is shown in Figure 2.5.

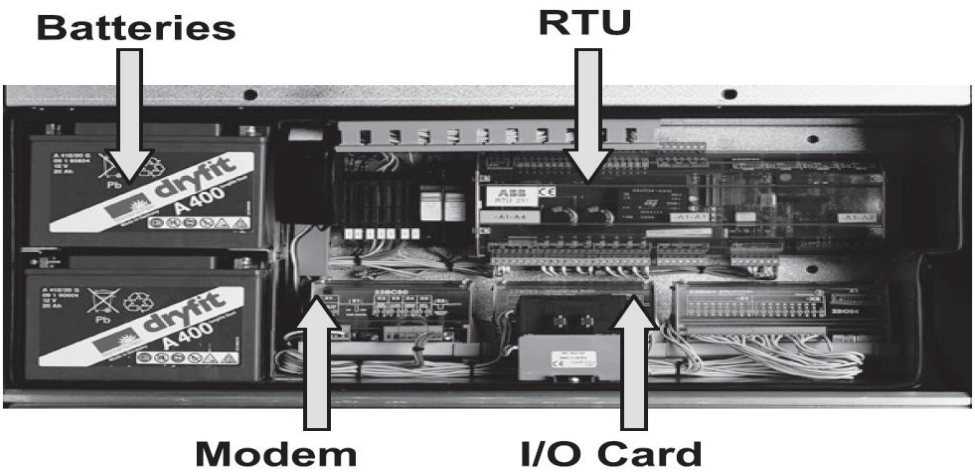


Figure 2.5 Typical control compartment for a RTU [51]

2.4.3 Level 3-Communication Unit (CU)

Communication unit, level 3 in the standard SCADA system hierarchy, provides a pathway for communications between a MTU (in control centre) and RTUs (in substations). Compared to the substation level communication, it is used to transmit collected data (information) to the MTU, the level 4 in the standard SCADA system hierarchy. Different protocols and mediums are adopted by the communication unit. The communication mediums include radios, leased landlines, or possibly even satellites. The communication protocols include Modbus and Profibus. Devices that could be used in this level include:

modems, routers, switches, etc. Most devices in the scope of the first three levels of the SCADA system hierarchy (leve1 to level 3) are installed (hardwired) in a substation.

2.4.4 Level 4-Master Terminal Unit (MTU)

A MTU is a "host computer" that issues all commands, collects all the data from RTUs, stores information, and interacts with SCADA operators[4] who can communicate with substation level components. Compared to RTU, MTU is one "master machine" that is able to initiate the communication, which is either triggered automatically by programs within a MTU or manually by an operator. Generally, three devices should be available in a MTU:

- ***Human Machine Interface (HMI)***: An HMI contains software and hardware that allow operators to monitor current status of a SUC, to modify control settings, and to manually override automatic control operations in the event of an emergency. An HMI also allows a control engineer or an operator to configure set points or control algorithms and parameters in controllers. Moreover, an HMI displays process status information, historical information, reports, and other information to operators, administrators, managers, business partners, and other authorized users.
- ***Control Server***: A control server hosts a DCS or PLC supervisory control software that is designed to communicate with lower-level control devices.
- ***Engineering Working station***: An engineering working station is a computer, which is connected to other MTU devices, e.g., HMI, control server, via LAN. The information transmitted from the field level instrumentation devices is also available to this computer. Specific engineering software can be installed at this workstation. For example, a state estimation software can be used by engineers to predict potential problems occurring in remote field sites .

[4] Operator is personnel who has access to MTU and make decisions according to the monitored field information.

The hardware configuration varies depending on the type and size of a SCADA system. However, general functionalities are similar. Figure 2.6 illustrates general configuration of a SCADA system, which includes all four hierarchy levels of SCADA.

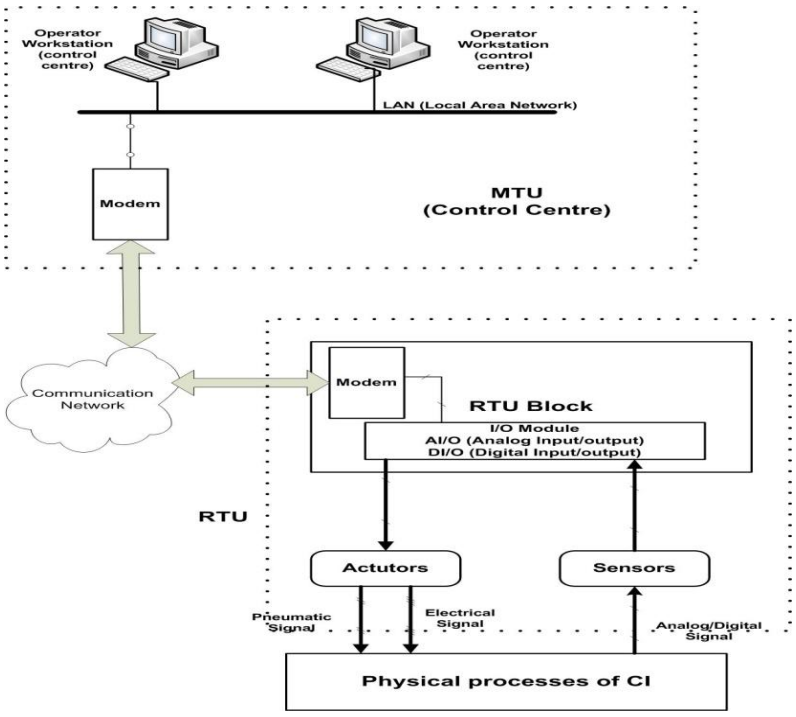


Figure 2.6 General configuration of a SCADA system

2.5 Summary

The interdependency-related vulnerabilities between a SCADA system and associated SUC have been addressed by a number of researchers for many years. Most related publications focus on the investigation regarding pervasive uses of ICT. For example, the communication protocol modbus, which is mainly used by a SCADA system, has become one of the widely discussed topics for securing the data transmission between the control centre and remote substation sites. However, the importance of components installed at substations should not be ignored due to the fact that their failures can also pose serious threats to a SCADA system and even other systems (e.g., SUC) it connects to. Therefore, a hybrid modeling/simulation approach, proposed in this research work and presented in the following chapters, will be applied to explore and investigate interdependencies

between a SCADA system and associated SUC. The investigation mainly focuses on the third challenge described in section 2.2 and the substation level of a SCADA system in terms of devices and equipment.

3 METHODICAL FRAMEWORK FOR ANALYZING INTERDEPENDENCY-RELATED VULNERABILITIES

3.1 Introduction of a 5-step Methodical Framework

The research work described in this thesis follows a methodical framework for analyzing vulnerabilities due to interdependencies within and among CIs, which is a problem-driven approach and based on the framework proposed by Eusgeld and Kröger in [30]. In general, this framework can be divided into 5 steps.

- **Step 1-Preparatory Phase:** the main purpose of this step is to reach a clear understanding regarding the objectives of the task. The CI sub-sectors and/or subsystems within a CI sub-sector for the assessment and investigation need to be determined. The understanding of these systems will facilitate distinguishing between obvious and hidden vulnerabilities [6]. The obvious vulnerabilities can be recognized by the screening analysis, while hidden vulnerabilities need the in-depth analysis using more comprehensive and advanced techniques such as the system modeling and simulation. The boundaries of the studied systems need to be determined as well, which could range from the delimitation of an elementary model, focusing only fundamental components, to the delimitation of a whole infrastructure system, composed by subsystems. Furthermore, it is necessary to identify characteristics of interdependencies among studied systems according to the general understanding, e.g., types of interdependencies. After framing the task, which includes both the system understanding and the boundary determination, the knowledge base should then be checked with respect to available methods/approaches suitable for the framed task.
- **Step 2-Screening Analysis:** The purpose of this step is to reach a further understanding of the previously framed task by acquiring sufficient information/knowledge of main functionalities, interfaces, and components of each studied system, as well as interdependencies among previously determined systems, in order to decide which to evaluate in more detail. Components and

interfaces of each system need to be analyzed systematically, especially for components essential for the normal functionalities of the system. To develop adequate system understanding, it is also necessary to define boundaries and failure modes of these components. In this step, obvious vulnerabilities should be identified using the methods such as empirical investigations and topological analysis. Indicators of the obvious vulnerabilities could be reliability bottlenecks, errors in operation, emergency procedures, etc [30]. One of the most frequently used techniques for topological analysis is the Complex Network (CN) theory. Both empirical investigations and topological analysis will be introduced in detail in section 3.3.

- **Step 3-In-depth analysis:** The In-depth analysis of CI interdependencies is required due to their inherent complexities. Key traditional mathematical models such as Fault Tree Analysis (FTA) often lack capabilities to provide sufficient insights and abilities to adapt to failures of subsystems within a CI or among CIs. Therefore, as one of major objectives of the research work introduced in Chapter 1, a hybrid modeling/simulation approach capable of representing functionalities and complexities of a subsystem and even a CI, as well as interdependencies within and among CIs is created in this step. Based on this approach, corresponding experiments can be designed and developed. More details regarding this approach and corresponding experiments will be introduced and discussed in Chapters 4 and 5.
- **Step 4-Results assessment:** The purpose of this step is to interpret and analyze results obtained in step 3. In this step, the hidden vulnerabilities due to interdependencies within and among CIs should be identified.
- **Step 5-Potential technical improvement**: Mainly based on assessments from step 4, improvements of systems may be proposed to minimize the negative effects caused by vulnerabilities and to better protect CIs in the long run.

3.2 Application of Methodical Framework: Preparatory Phase

3.2.1 Framing the Task

As introduced in Chapter 1, the interdependencies among and within CIs can be described by six dimensions, e.g., type of failure, type of interdependencies, coupling/response behavior, etc. It is very important to decide which CI sub-sectors (analysis among CIs) or subsystems (analysis within a CI) should be analyzed. Then, the general term "to find system(s) vulnerabilities due to interdependencies" can be stated precisely. For instance, two subsystems, SCADA and SUC, within the power supply CI sub-sector are selected for the analysis in this research work:

- SCADA system[5] in this case can be regarded as a general SCADA system, as introduced in Chapter 2, including four levels in a standard system hierarchy.
- SUC within the power supply sub-sector could be a distribution system, a generation system, or a transmission system. In this research work, the Swiss 220kV/380kV electricity transmission network is used as an exemplary SUC, illustrated in Figure 3.1. It is assumed that this transmission network is a stand-alone system and the energy exchange with the neighboring countries are regarded as independent positive or negative power injections at the respective boundary substations.

According to section 2.2, the importance of securing a SCADA system, the task can be framed finally as: *to explore and investigate (internal)interdependencies between a SCADA system and its associated SUC, mainly focusing on substation level of the SUC/SCADA systems in terms of reliability of devices and equipment*. The summary of this step is illustrated in Figure 3.2.

[5] Although SCADA can be regarded as a subsystem within a CI sub-sector, the general term SCADA system will be used in this thesis.

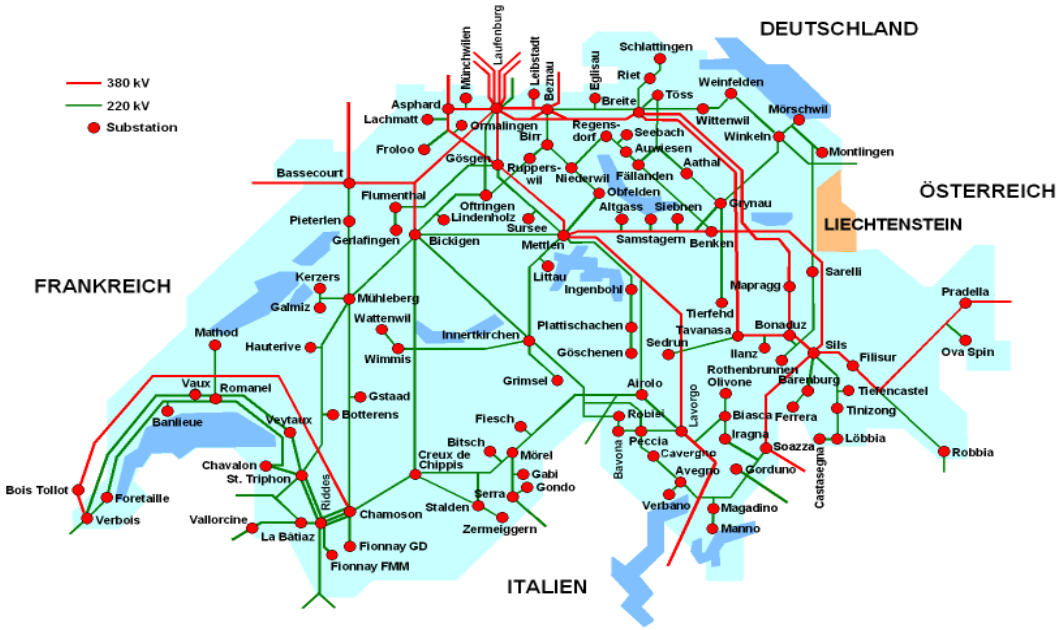


Figure 3.1 the 220kv/380kv Swiss transmission network [53]

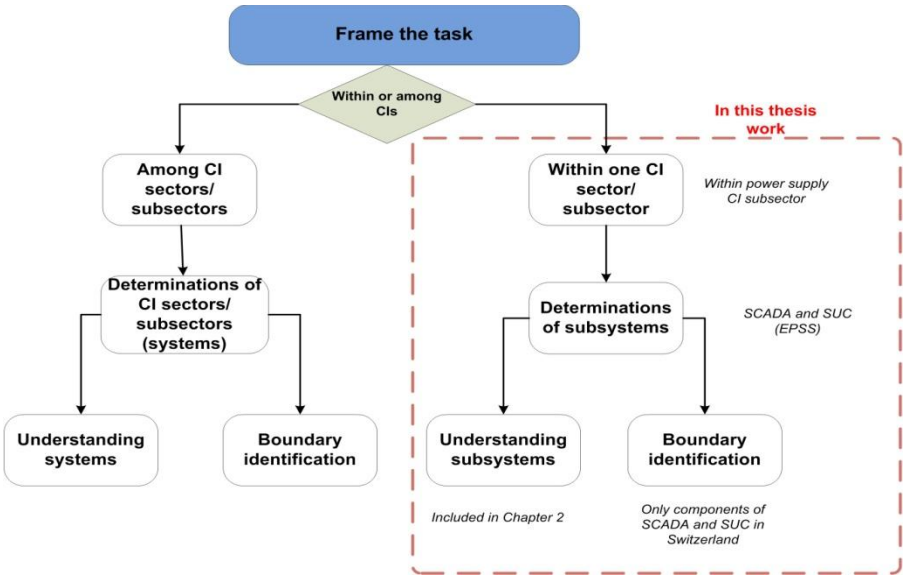


Figure 3.2 Summary of the step 1: Framing the task

3.2.2 General Understanding of Studied Interdependencies

According to the general understanding of a SCADA system and its associated SUC within power supply sub-sector, their **(internal) interdependencies** can be summarized as follows:

- **Physical interdependency (SUC<->SCADA):** The physical interdependency exists since a SCADA system requires the electric power supply, which is the output of the SUC, and some substation level devices of a SCADA system, e.g., Remote Terminal Unit (RTU), field level control devices, etc, have control (manipulation) over its connected SUC.
- **Cyber dependency (SUC->SCADA):** The cyber dependency exists since a SCADA system monitors and controls components of a SUC.
- **Geographic interdependency (SUC<->SCADA):** The geographic interdependency exists between a SCADA system and a SUC since some of their components need to be installed at the same places, e.g., substations.
- **Logic interdependency:** The logic interdependency between SCADA system and SUC does not exist in this case.

Based on the definition of the **degree of coupling**, introduced in Chapter 1, the SCADA system and its associated SUC are **tightly coupled**.

After framing the task and gaining general understanding of studied interdependencies, methods and approaches available for performing the task need to be checked, as part of the first step.

3.2.3 Available Methods/Approaches (State of the Art)

The challenges regarding understanding, characterizing, and investigating interdependencies within and among CIs are immense and research in this area is still at

an early stage [20, 54-56]. In general, the interdependency-related study can be divided into knowledge-based approaches and model-based approaches [6].

3.2.3.1 Knowledge-based approaches

Knowledge-based approaches, e.g., empirical investigations and brainstorming, intend to use data collected by interviewing experts and/or analyzing past events to acquire information and improve the understanding of dimensions and types of interdependencies. One of the early empirical investigation studies built a database according to the collected opportunistically websites of construction, maintenance or operation accidents, reports of the US National Transportation Safety Board and news media searches, in order to address the question whether certain combination of infrastructure failures are more common than others [57]. The database primarily includes accidents that occurred from 1990 through 2004 in connection with failures during construction, maintenance or operation, or due to facility condition related to age of structures. Table 3.1 depicts the ratio of causing failure of another type of infrastructure vs. being affected by failure of another type of infrastructure according to the database. As shown in this table, water mains cause failures of other infrastructures more frequently, while gas lines and telecommunication lines are more likely to be damaged by other infrastructures.

Table 3.1 Effect ratios [57]

1 Type of Infrastructure	2 # of Times Infreastructure (Column 1) Caused Failure of Other Infrastructure	3 # of Times Infrastructure (Column 1) was Affected by Other Infrastructure Failures	4 Ratio of Causing vs. Affected by Failure (Col. 2 divided by Col. 3))
Water mains	34	10	3.4
Roads	25	18	1.4
Gas lines	19	36	0.5
Electric lines	12	14	0.9
Cyber/Fibre optic/Telephone	8	15	0.5
Sewers/Sewage treatment	8	6	1.3

[6] A similar research work that sufficiently categorizes and investigates these approaches is also conducted by Kröger and Zio in [25].

A policy brief of the IRGC (International Risk Governance Council) [58] also introduces an assessment of dependencies between CIs based on brainstorming sessions among experts around the world and categorizes how dependent each infrastructure is on the others, how dependent the others are on it, and also how strong the intra-infrastructure dependencies are, as shown in Figure 3.3. According to this report, among five reference infrastructures, electricity, railways and ICT are most important ones. Most infrastructures have a major dependency on the electricity infrastructure, while the rail infrastructure has a major dependency on other infrastructures. The ICT has a major dependency on others, as well as major dependence for other infrastructures.

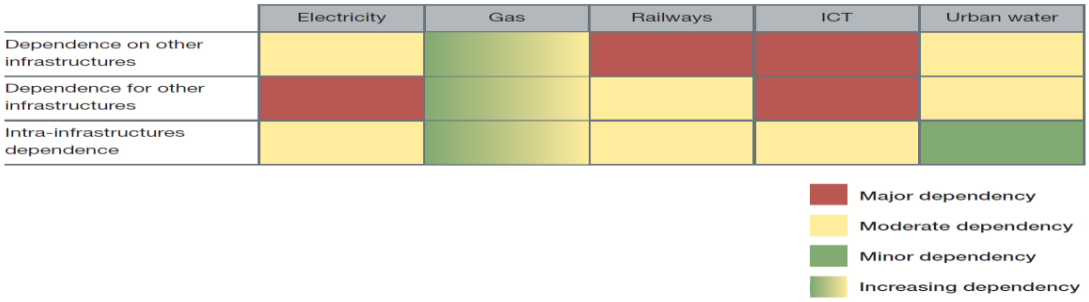


Figure 3.3 Dependencies between CIs according to [58]

Other two examples of knowledge-based approaches are:

- Research work done by Rahman et al. in 2009 who used published infrastructure failure reports to develop an understanding of infrastructure interdependencies by studying a large number of cases and tracing common trends among similar classes of failures [59].
- A technical report from ETH Zurich in 2010 [14], which collected and investigated negative cascading impacts due to interdependencies among infrastructures based on official government reports of seven selected incidents.

The knowledge-based approach is also applied to study interdependencies between the SCADA system and its associated SUC. One example is a survey conducted by Johnson R.E [43]: This survey lists two potentially serious attack vectors on PLC of a SCADA system, based on the analysis of findings from published SCADA-related incidents, by

pass logic attacks and brute "force output" attacks, and proposes methods to improve the security of SCADA systems.

The knowledge-based approach is straightforward and easy to understand. It is capable to provide qualitative assessment on the severity / the degree of studied interdependencies and can be considered as an efficient scanning method. For example, the interdependencies related to electric power systems have been quantified and assessed using the ratio of the duration of an electric power outage to the duration of a subsequent infrastructure failure dependent upon electric power, which is calculated according to published accident reports [60]. However, this is a pure data-driven approach, meaning that the accuracy of results depends on the quality and the interpretation of the collected information.

3.2.3.2 Model-based approaches

Model-based approaches intend to represent interdependencies within and among CIs using advanced model techniques. It is a comprehensive approach, with capabilities providing both quantitative and qualitative assessment. Compared to the knowledge-based approaches, the model-based approaches not just allow to improve the understanding about how failures/disturbances cascade through linked subsystems within a CI or among interconnected CIs, but also to identify hidden vulnerabilities due to the existence of interdependencies. Currently, a number of research projects related to the CI interdependency study are being implemented by developing a variety of models:

- **Complex Network (CN) Theory**: Fundamental elements of the CN theory are originally formed by the graph theory [61]: A graph G(*V*,*E*) is composed by a set of nodes (vertices) V and the set of connections E between them. Each node (or vertex) represents an element of the system, while a link (or edge) represents the relation between corresponding elements. Therefore, a graph can be drawn by plotting nodes as points and edges as lines between them. In general, a graph can be represented/interpreted by well developed parameters such as :
    - the order/size of a graph

- the weight/strength of a link
- the degree/degree distribution/betweenness of nodes
- the distance between nodes
- the clustering coefficient of a graph
- the modularity between graphs

Furthermore, algorithms, e.g., Girvan-Newman algorithm, have been developed to evaluate and analyze the characteristics of the graph. The CN theory is one of most widely implemented technique for topology analysis, which can be used to analyze one or more CIs. Figure 3.4 illustrates a 220kV/380kV Swiss power transmission network that is represented by a graph G(161,219) [6]. In this graph, each node represents a substation (161 substations in total), while each link represents a transmission line (216 transmission lines in total) between two substations. Topological properties such as clustering coefficient and degree of distribution of the nodes in the graph can then be obtained.

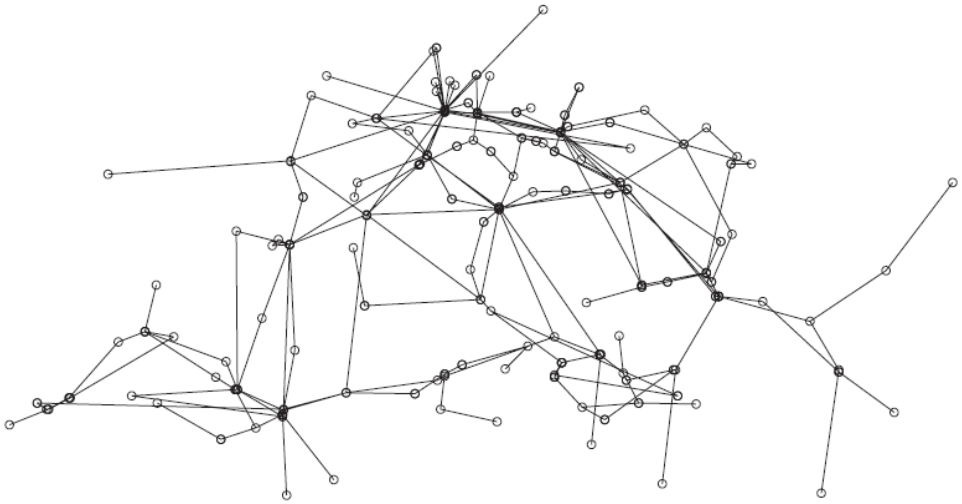


Figure 3.4 The 220kV/380kV Swiss electricity power transmission network (represented by a graph) [6]

The CN theory is also capable to graphically represent the coupling phenomenon among CIs as a set of nodes connected by a set of links and by this to characterize their topology. Figure 3.5 shows a graph representing two

CI sub-sectors, power supply sub-sector (in blue color) and natural gas supply sub-sector (in red color) [62]. In this graph, blue nodes represent generators (with circle) and load nodes, while red nodes represent pumps (with circle) and end-user stations. Blue lines and red lines represent electric wires and branching connecting two gas pipeline segments. Based on this graph, Ouyang et al. conducted several experiments regarding the topological analysis between these two interdependent infrastructure sectors.

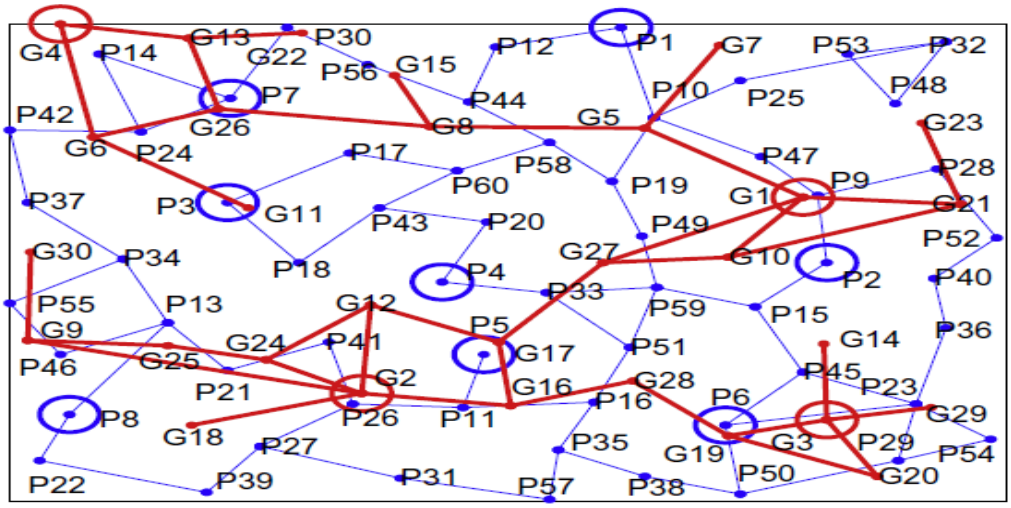


Figure 3.5 A graph representing interdependencies between two infrastructure sub-sectors [62]

Many other efforts have also been made to adopt the CN theory for interdependency-related assessments, demonstrating its capability of modeling relation established through connections among elements of studied CIs [63-65]. The CN theory approach is based on the network model mapping physical configuration of the components (elements) of studied CIs and their (physical or logical) interconnections. The analysis of the topological properties of the network representing given CIs is able to reveal useful information about the structure property, topological vulnerability, and the level of functionality demanded for its components [29, 66]. However, the approach alone lacks the ability to capture uncertain characteristics of CIs due to their inherent complexities and systems' properties when dynamical processes, acting on the

network, occur. Furthermore, interdependency-related vulnerabilities can be studied in more detail if their dynamics, realistic time delays, and failure/repair rates can be considered. It should be noted that it is also not possible to model event-driven links such as an instant command sent from a SCADA system to a SUC using the CN theory approach.

- **Input-output Inoperability Modeling (IIM)**: Originally, this is a framework for studying the equilibrium behavior of an economy describing the degree of interconnectedness among various economic sectors [67]. This approach assumes that each infrastructure system can be modeled as an atomic entity whose level of operability depends on other infrastructures and propagation between infrastructures can be described mathematically based on the basic Leontief high order mathematical model by associating an inoperability level with each infrastructure [68].

$$X_k = \sum \alpha_{kj} X_j + C_k \quad \text{(Equation 3.1)}$$

The Equation 3.1 is the Leontief-based equation representing inoperability among infrastructure systems. In this equation, X_i(i=1,2...,n) denotes the overall risk of inoperability of the complex intraconnected and interconnected jth infrastructure system that can be triggered by one or multiple failures caused by accidents. α_{kj} denotes the probability of inoperability that the jth infrastructure system contributes to the kth infrastructure system due to their interconnectedness. If $\alpha_{\mathrm{kj}} = 1$, then this means that the complete failure of the jth infrastructure will lead the complete failure of kth infrastructure system. C_k denotes the additional risk of inoperability due its inherent complexity of kth infrastructure system. Adopting IIM approach for the CI interdependency study was first proposed by Haimes et al. in [69, 70]. They applied the Equation 3.1 with corresponding models to study impacts of high-altitude electromagnetic pulse on electric power infrastructure. Steola et al.[68] developed an IIM-based methodology to analyze the importance and fragility of Italian infrastructures. Similar research can also be found in [71]. In general, the IIM is a mathematical model, which is best known for its application in the area of macro-economy. By

introducing this model into the area of CI interdependency study, failure spreading behaviors and recovery strategies can be studied [29]. However, parameters selected to compute this model are based on knowledge and experiences of experts, which are hard to validate and not sufficient enough to capture the complexity of interdependency-related issues.

- **PetriNet (PN)-based Modeling:** The PN, developed in 1962 by Carl A. Petri, is a mathematical modeling language for the description of distributed systems. This method has also been used to represent/assess interdependencies among CIs. In this approach, components (subsystems) of infrastructure systems and their states are modeled using basic PN elements such as places, transitions, etc. For example, Sultana and Chen adopted this approach to assess the safety of floodplain infrastructure systems [72]. Compared to other model-based approaches, the PN approach alone has difficulties in modeling interdependencies quantitatively and often needs to be combined with other methods. For example, in the Europe-wide project IRRIS (Integrated Risk Reduction of Information-based Infrastructure Systems), the PN is combined with the Agent-based Modeling (ABM) to analyze and manage interdependencies among CIs [73].
- **Dynamic Control System Theory (DCST):** This theory can be applied as a quantitative analytical method to assess the interdependencies within and among CIs using transfer functions and corresponding frequency responses [74]. In order to apply this method, a studied infrastructure needs to be assumed as a Linear Time Invariant (LTI) dynamic system. The input/output relationship between infrastructures can be represented and quantified by deriving corresponding transfer functions. Mason's formula, which is used to determine the control function of a given control loop after identifying its corresponding signal flow graph, can be applied to develop all required transfer functions such as a transfer function for a component of one infrastructure or an overall global transfer function. Based on the overall transfer function and its corresponding frequency responses, the stability of interdependencies between infrastructures can be evaluated using BODE and NYQUIST diagrams [74]. The approach of DCST is a novel method, which brings the classic control system

theory to the area of the CIP. Instead of using the time domain, two alternative domains (domain of Laplace and frequency) are used for the purpose of the evaluation and assessment. The development of transfer functions is the most essential part of this approach and strongly influences the accuracy of final results, which could be further complicated due to complexities of studied infrastructures. Another drawback of this approach lies in the fact that hidden vulnerabilities caused by interdependencies cannot be estimated since all the links between studied infrastructures have been determined during the transfer function development. The applicability/ feasibility of this approach are still under discussion and need to be proven.

- **Agent-based Modeling (ABM)**: The ABM approach describes a whole system by its individual parts (bottom-up). Each component of the system is normally defined and modeled by an agent, capable to modify its own internal data (parameter and variable), its behaviors (function), its environment, and even adapts itself to environmental changes. An agent can be used to model both a technical component (e.g., a transmission line), and a non-technical component (e.g., a human operator), while different agents interact with each other directly or indirectly. One of the major advantages of this approach is the possibility to integrate various elements such as physical laws, complex systems, system emergence, Monte Carlo methods, etc, into the overall simulation. In [75], the 220kV/380kV Swiss electricity power transmission network, already introduced in previous sections, is modeled/simulated using the ABM approach for the purpose of system reliability analysis, shown in Figure 3.6. Instead of only using nodes and links to represent substations and transmission lines respectively by the CN theory modeling approach, agents are created to model various components of the system such as generators, busbars, transmission lines, loads and operators. The rules of behaviors of each agent are represented by using Finite State Machines (FSMs) and include both deterministic and stochastic time-dependent, discrete events [75]. The model is developed using a two-layer modeling concept, illustrated in Figure 3.7. Within this concept, the lower layer represents the separate modeling of the physical components by means of conventional, deterministic techniques such as power flow

calculations, whereas the upper layer represents the abstraction of the whole system (in this case, electric power system) with all its technical and non-technical components as individual agents. Compared to similar studies using the CN theory, the ABM approach is capable to get a more comprehensive analysis of dynamic system behaviors by "looking-into" (modeling) the component level of the studied system(s) [6]. The ABM approach is not just able to model/simulate single infrastructure systems, multiple infrastructure systems can also be represented assuming that interdependency behaviors will emerge through interactions among all developed agents. Panzieri et al. have developed a multi-agent simulator, CISIA (Critical Infrastructure Simulation by Interdependency Agents), to analyze fault propagation crossing heterogeneous infrastructures, which is able to use rich sources of micro-level data to develop interdependency forecasts [76]. Adopting the ABM approach for the CI interdependency study can also be found in other recent research works such as the development of a simulator for analyzing the information system for Civic Emergency Management [77, 78] and the creation of a simulation environment for investigating the interdependencies among subsystems in an electric power supply system [79].

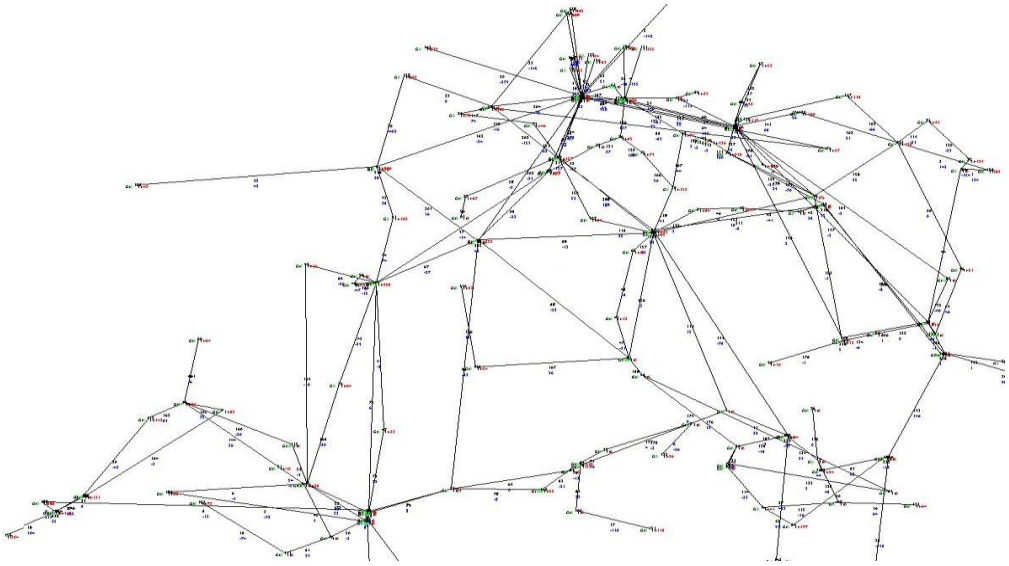


Figure 3.6 The 220 kV/380kV Swiss electricity transmission network (represented by agents) [75]

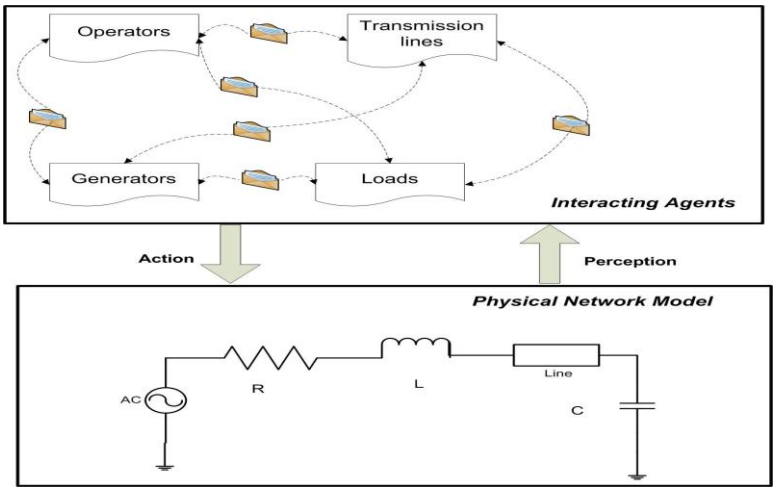


Figure 3.7 Two-layer modeling concept (illustrated using application to the electric power system as an example) [75]

The ABM approach achieves a closer representation of system behaviors by integrating the spectrum of different phenomena, which may occur, e.g., generating a multitude of representative stochastic, time-dependent event chains. However, this approach demands large number of parameters defined for each agent, which require through knowledge of studied system(s).

3.2.3.3 Comparison between two approaches

It is difficult to compare these approaches (knowledge-based and model-based approaches) since all of these approaches have their own advantages and disadvantages. The knowledge-based approaches are straightforward and easy to understand, while the model-based approaches are comprehensive and promise to gain a deeper understanding of behaviors of studied system(s). The level of this so called deeper understanding by each model-based approach also varies. Some approaches are only capable to analyze studied system(s) at the structure/topology level, which can be considered as appropriate approaches for the screening analysis, e.g., CN theory and PN-based modeling approaches, while some approaches are capable to capture and analyze dynamic behaviors of studied systems, e.g., ABM and IIM approach. It should be noted that knowledge-based approaches such as the empirical investigation are also capable for

screening analysis. Among all these approaches, the ABM approach seems more promising than others, not just due to its capability for representing the complexity of any infrastructure systems, but also its modeling flexibility and adaptability. For example, the ABM approach can be integrated with many other modeling/simulation techniques and even be used to implement other models, e.g., CN model, PN, IIM, etc. Some non-technical components such as human behavior can also be modeled/simulated by using the ABM.

3.3 Application of the Methodical Framework: Screening Analysis

In general, as the second step of the methodical framework for analyzing vulnerabilities due to interdependencies within and among CIs, the "screening analysis" includes the development of adequate system understanding and the identification of obvious vulnerabilities.

3.3.1 Development of Adequate System Understanding

Although the studied system(s) has (have) been described and its (their) boundaries have been defined at the stage of the "framing the task" (step 1, section 3.2.1), it is still necessary to further develop an adequate understanding of system, which aims not just to improve accuracy of results obtained from the screening analysis, but also to collect more detailed information for the following in-depth analysis (the third step of the methodical framework). To achieve these goals, components of the systems need to be analyzed at first and then corresponding failure modes for each system component need to be defined. In this section, adequate understanding of the SCADA system within the electric power supply CI sub-sector will be developed. More information regarding adequate understanding of the SUC can be found in [75]. Only components installed at the level 1 and 2 (substation level) of standard SCADA system hierarchy will be analyzed due to the their importance for the interdependency-related vulnerability analysis between SCADA

system and SUC, already introduced in Chapter 2.4. Below several steps needed to be followed in order to develop adequate system understanding are proposed[7]:

- **General component description**: functionality descriptions of the studied component.
- **Component boundary**: specifications about what should be included in the studied component.
- **Event boundary**: description of successful operation of the studied component.
- **Component (functional) failure mode**: description of functions when the studied component fails to perform including the identification of basic cause(s) that could possibly trigger the corresponding failure mode, symptoms and possible consequences of the corresponding failure mode.

3.3.1.1 Field Level Instrumentation Device (FID)

General Component Description

The essential function of a field level instrumentation device is to monitor and gather information of interest to system operators, such as status of a circuit breaker, current/voltage of a transmission line, power generated by a generator, etc. In general, these devices are instruments converting physical variable inputs into signal variable outputs. Voltage sensors, current sensors, temperature sensors, and energy sensors are most important sensors used within power supply CI sub-sector. The voltage sensor, also called the voltmeter, is responsible for measuring the electric voltage. A current sensor, on the other hand, is used to measure the DC current. In most cases, these four types of sensors have been installed widely at the substation level of the SCADA system. A current sensor is shown in Figure 3.8, while Figure 3.9 shows a block type current and voltage combi-sensor, which packages both current and voltage sensors in one molding.

[7] These steps for the development of adequate system understanding is inspired by the steps used to identify the root causes that could potentially contribute to the Common Cause Failures (CCFs) described in [80].

Figure 3.8 A general current sensor [51]

Figure 3.9 Block type current and voltage combi-sensor [51]

Component Boundary

The component boundary of the field level instrumentation device includes: instrumentation gauge lines, sensor or transmitter, indicating instruments (Figure 3.10).

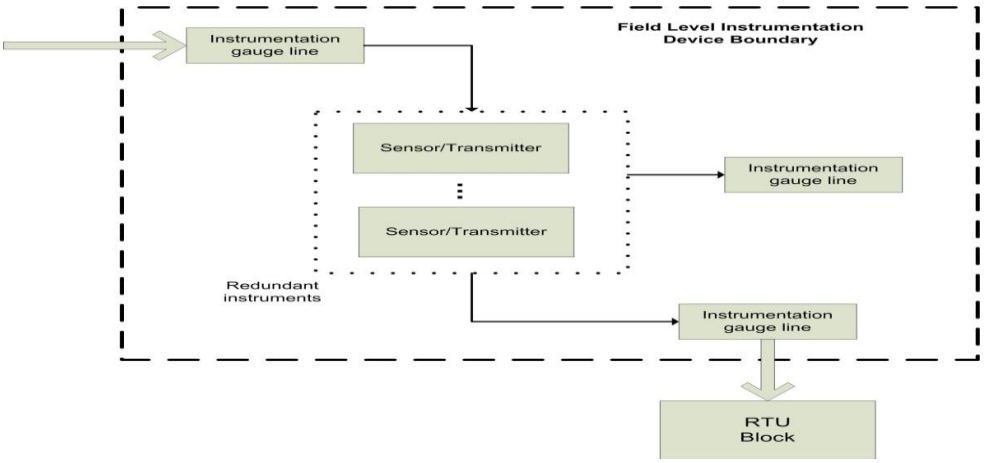


Figure 3.10 Field Level Instrumentation device component boundary

Event Boundary

The successful operation of a field level instrumentation device is defined as monitoring the actual value of physical variables, e.g., voltage and current variables, and transmitting them to the upper level component: RTU.

Failure Mode

1) **Failure to run (too high) (FRH)** : A FID fails to indicate the actual value of its monitored variable and indicates a greater than actual value.

    - **Causes**: **1)** Personnel performance error during maintenance and other activities. This is mainly caused by applying outdated procedures for adjusting FIDs, mistakes during calibrating setpoint values, or erroneously not accounting for technical modifications of the field when calculating setpoint values. **2)** Insufficient attention to the aging of piece parts of FID. For example, calibration drifts to wrong value during warming up.
    - **Symptoms**: FID is out of calibration.
    - **Consequences**: The output of a FID is greater than actual value. A wrong alarm could be generated. Corrective actions will be followed by mistake after the operator recognizes this alarm, for instance, the transmission line will erroneously be disconnected, which could lead to partial (local) power lost.

2) **Failure to run (too low) (FRL)**: A FID fails to indicate the actual value of its monitored variable and indicates a smaller than actual value.

    - **Causes**: Same as for FRH failure mode
    - **Symptoms**: FID device is out of calibration.
    - **Consequences**: The output of FID device is smaller than actual value. The consequence caused by this failure mode could be worse than the one of the FRH failure mode since expected alarms could be missed due to incorrect FID outputs. Corrective actions could be delayed or totally missed and it might be too late for an operator to take further actions. The worst case of the failure mode could lead to partial or even complete blackouts.

3.3.1.2 Field Level Control Device (FCD)

General Component Description

A field level control device of the SCADA system is a device that awaits the signal or data from the RTU to perform necessary control functions, which are initiated manually by operators or automatically by other systems (e.g., safety instrumented systems). Switches, valves, line disconnectors, and motors can all be considered as examples of control devices. An actuator is typically a mechanical device that takes the energy, which is usually created by air, electricity, or liquid, and coverts it into a predefined motion. For example, a circuit breaker (CB) is an example of an actuator, which is a switching device capable of carrying currents under normal system operations and breaking current under specific abnormal conditions such as a short circuit. The main purpose of a CB installed in the substation is to carry load current for long periods of time and to safely interrupt any fault that might occur on the circuit.

Component Boundary

The component boundary of a FCD includes: the control circuit and the control module (Figure 3.11).

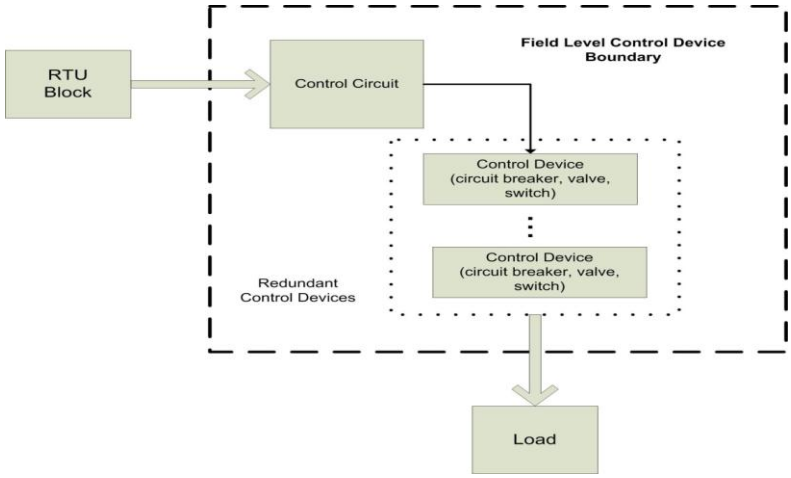


Figure 3.11 Field Level Control Device Component Boundary

Event Boundary

The successful FCD operation is defined as implementing designed control function(s), for example, connecting or breaking current, as demanded.

Failure Mode

1) **Failure to open (FO)**: The closed control device is instructed to open but fails to open.

    - **Causes**: **1)** Insufficient attention to the aging of piece parts. For example, the breaker mechanism is impeded due to an aging part of FCDs. **2)** Personnel performance error during maintenance and other activities. For example, maintenance personnel damage the FCD breaker mechanism.
    - **Symptoms**: Operation of FCD is suspended, the movement of the breaker mechanism is impeded.
    - **Consequences**: The transmission line remains connected, although it should be disconnected due to the safety reason. For instance, if a controlled transmission line fails to be disconnected in case of occurrence of overloading hazard, this could cause a system collapse, possibly leading to partial or even complete blackouts.

2) **Failure to close (FC)**: The opened control device is instructed to close but fails to close.

    - **Causes**: Same as for FO failure mode.
    - **Symptoms**: Same as for FO failure mode.
    - **Consequences**: The transmission line remains disconnected, although it should be connected. This could cause partial power loss of specific area. The severity of consequence for this failure mode could be less than for FO failure mode.

3) **Spurious operation (SO):** The control device opens when it should have stayed closed or closes inadvertently.

- **Causes**: **1)** Design, construction, manufacturing deficiencies. For instance, the setpoint of FCD is set to wrong value during installation. **2)** Personnel performance error during maintenance and other activities. For example, the setpoint is modified to a wrong value by maintenance personnel accidently.
- **Symptoms**: The FCD operation is impeded by incorrect adjustment of the setpoint.
- **Consequences**: The transmission line is connected unexpectedly due to the wrong setpoint, although it should be disconnected or redistributed. As result, the abnormal operation situation appears again and has to be corrected. Suitable corrective action such as transmission line disconnection will be delayed or simply missed. The worst case could be partial or complete blackouts.

3.3.1.3 Remote Terminal Unit (RTU)

General Component Description

Considering the operating condition of most remote substations, a RTU is usually situated inside an environmental enclosure that provides fundamental protection from extremes of temperature and weather. It should be noted that most of components included in the RTU belong to the level 2 of standard SCADA hierarchy except the modem, which is part of the level 3, communication unit. All these components, as well as the enclosure, can be referred to as a RTU block; its fundamental role, especially for the SUC within power supply sub-sector, is as follows:

- Acquiring various types of data through FIDs.
- Accumulating, packaging, and converting data in a predefined form that can be communicated back to the MTU through the communication unit.
- Interpreting commands from the MTU and transmitting them in a predefined form to FIDs.

- Time-stamping local events (in the scope of the substation level) and synchronizing local time with the MTU.
- Performing local calculation, estimation, and process to allow locally performed safety functions.

Component Boundary

The component boundary of the RTU block in this analysis includes power, battery, memory, input module, output module, CPU, modem, and operator station (Figure 3.12).

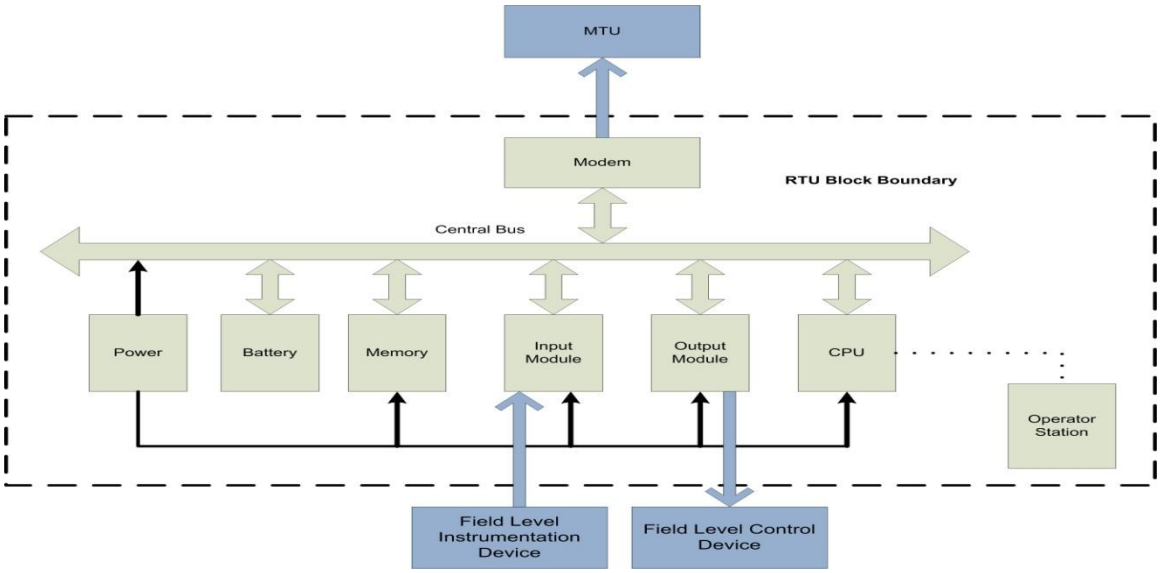


Figure 3.12 RTU Component Boundary

Event Boundary

Successful operation of a RTU block is defined as:

- Acquiring the monitored data from field level devices through its input module and saving them in the memory.
- Transmitting data required by the MTU through communication channels set up by the modem.

- Identifying and converting received commands from the MTU to the RTU-recognizable signal and sending them to respective FCDs through the output module.

Failure Mode

1) **Failure to run with field device (FRF)**: A RTU device is unable to acquire data from and send interpreted commands to its field level device(s) assuming this (these) device(s) can function normally, although it is still able to receive commands from the MTU.

    - **Causes**: **1)** Insufficient attention to the aging of piece parts. For example, communication between a RTU and its field level device(s) is impeded due to the aging connection cable between them. **2)** Personnel performance error during maintenance and other activities. For example, maintenance personnel breaks the connection cable between a RTU and its field level device(s). **3)** Technical defects of a RTU output module.
    - **Symptoms**: Communication between a RTU and its field level device(s) is suspended.
    - **Consequences**: Field level devices will become unavailable to its connected RTU device. Field variables will not be monitored and alarms will not be generated. Interpreted commands from a MTU will not be sent to corresponding devices. This could cause delay or omission of alarms generated and correction action sent by a MTU.

2) **Failure to run due to hardware failure (FRW)**: A RTU device is unable to function normally, i.e. to generate alarms and process commands (send commands to related field level devices) from a MTU correctly.

    - **Causes**: **1)** Insufficient attention to the aging of piece parts. For example, the central bus of a RTU device fails to function due to

maintenance outage. **2)** Defective circuits, wiring faults, excessive stress from environment.

- **Symptoms:** RTU device fails to function.
- **Consequences**: Wrong interpretation of commands sent by a MTU and ignorance of alarms sent by its connected field level devices.

3) **Failure to run due to communication error (FRC)**: A RTU device receives a command from a MTU, but fails to interpret due to data lost.

- **Causes**: Power line noise interference, which could severely affect the data transmission between a RTU and a MTU.
- **Symptoms:** The RTU operation is impeded due to its failure to interpret received command(s).
- **Consequences**: The command from a MTU will not be executed by a RTU, as well as following corrective actions, which could lead to the complete failure of a RTU, as well as the whole substation.

3.3.1.4 Consideration of Common Cause Failures (CCFs)

Generally, failures of these substation level components can be classified either as random failures, systematic failures, and Common Cause Failures (CCFs) [81]. Random failures are physical failures brought on by excessive stresses on the devices. Such failures can happen randomly at any time during the device lifecycle and do not follow any pattern. Systematic failures are a direct consequence of devices and complex situations. Each device has many known opportunities for systematic failures due to design specification mistakes, operation/maintenance mistakes, manufacturing defects, and implementation errors, etc. Both random and systematic failures can be regarded as independent failures. All the failures introduced in the failure modes in the previous section can be considered as independent failures.

Independent failures can induce CCFs in the form of single points of failures or the failure of redundant devices [81]. CCF is a term used to describe multiple failures, which are a direct result of a common or shared root cause and occur (at least almost) at the same time. For example, two redundant FIDs (sensors) are used to check whether or not the

measured process variable (mv) exceeds the safety limit. Due to mistakes caused by installation personnel (human error), both sensors have been miscalibrated. As a result, two sensors will fail to monitor current states of the mv. In this case, the miscalibration of redundant sensors is the root cause of CCFs and failures of two sensors can no longer be treated as independent from each other. The concepts of independent failure and CCF are interrelated; the lack of independency means that there is potential for CCFs. Due to the obvious importance of substations and redundant components installed within them, the negative effects due to CCFs should not be ignored. Therefore, the corresponding research work aiming to examine and assess the effects of CCFs of substation level components of the SCADA system on the overall reliability of the substation (within power supply sub-sector) has been conducted and included in a recent scientific report "Focal Report: Study of CCFs of SCADA System at Substation Level" [82][8]. According to the conclusion of this report, the negative effects of the CCFs of the substation level components on the overall system reliability could be significant. Results obtained from a quantitative CCF analysis presented in this report show that the reliability of a typical substation of the SUC within the power supply sub-sector may significantly decrease due to the existence of CCFs of substation level components. Therefore, it is necessary to give adequate awareness to negative effects of potential CCFs. Due to limited time of this research work, only independent failures are considered at this moment. In future work, CCFs will be included (see Chapter 7 for more details).

3.3.2 Identification of Obvious Vulnerabilities

3.3.2.1 Empirical Investigation

One of the established methods to identify obvious vulnerabilities is to look into statistics. RISI (Repository of Industrial Security Incidents) is a database including a number of technical incidents in which process control, industrial automation or SCADA systems were affected. The purpose of this database is to collect, investigate, analyze, and share

[8] Parts of this report are included in the Appendix II for reference.

important industrial security incidents among a number of companies for the purpose of experience exchanges. These incidents include not just public known incidents, but also incidents from private reports. Figure 3.13 shows the distribution of SCADA-related incidents due to different types of vulnerability as defined in Table 3.2, from a technical report [12], which is based on 141 records collected from the RISI database. According to this figure, almost all incidents can be attributed to vulnerability type 1 - lack of overall security awareness. The second serious vulnerability is type 4 - inadequate examined and maintained system administration mechanisms and software. Inadequately designed ICS networks and insufficient security for remote accesses are also the causes of many ICS incidents.

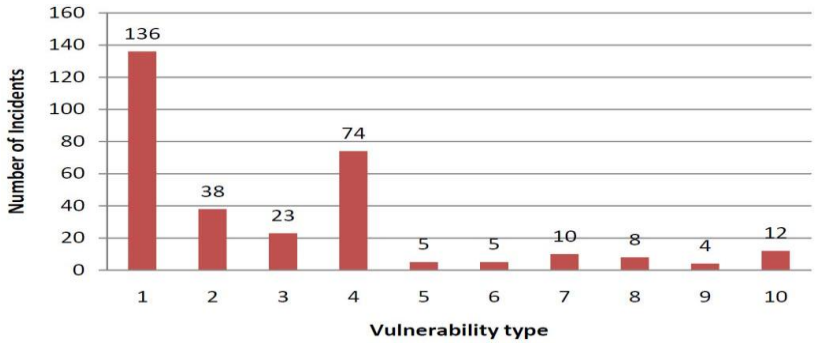


Figure 3.13 Distribution of the number of incidents due to different types of vulnerability [48]

Table 3.2 Top 10 ICS incidents (based on 141 records from RISI) [48]

ID	Type of Vulerabilities	Examples	
1	Inadequate policies, procedures, and culture that govern ICS security	• Cultural clash • Lack of overall awareness	• Absence of security policy • Lack of adequate risk assessment
2	Inadequately designed ICS networks that lack sufficient defense-in-depth mechanisms	• No network security of ICS devices when originally designed	• ICSs are uncapable of secure operations
3	Remote access to the ICS without appropriate access control	• Inappropriate use of dial-up modems • Use of commonly known passwords or no use of passwords • Implementation of non-secure control	• system connectivity to the corporate LAN • Practice of un-auditable and non-secured access by vendors
4	System administration mechanisms and software used in ICSs are not adequately scrutinized or maintained	• Inadequate patch management • Lack of appropriately applied real-time virus protection	• Inadequate account management • Inadequate change control • Inadequate software inventory
5	Use of inadequately secured wireless communication for control	• Use of COTS consumer-grade wireless devices for ICS network data	• Use of outdated or deprecated security/encryption methods
6	Use of a non-dedicated communications channel for control and/or inappropriate use of ICS network bandwidth for non-control purposes	• Internet-based SCADA • Inappropriate use of control channels for non-control data	• Internet/Intranet connectivity initiated from ICS networks
7	Insufficient application of tools to detect and report on anomalous or inappropriate activity	• Underutilized intrusion detection systems • Under-managed network system	• Implementation of immature Intrusion Prevention Systems
8	Unauthorized or inappropriate applications or devices on ICS networks	• Unauthorized software installation to devices • Peripherals with non-control system interfaces	• Non-secure web interfaces for ICS devices • Laptops • USB • Other portable devices
9	Control systems command and control data not authenticated	• Authentication for LAN-based control commands not implemented	• Immature technology for authentication of field devices
10	Inadequately managed, designed, or implemented critical support infrastructure	• Inadequate power supply systems • Inadequate HVAC systems • Insufficiently protected telecommunications infrastructure	• Inadequate or malfunctioning fire suppression systems • Lack of recovery plan • Insufficient testing or maintenance of redundant infrastructure

3.3.2.2 Topological Analysis

Another method to identify obvious vulnerabilities is to apply topological analysis. SCADA in general can be represented as a network. The SCADA system for the SUC of 220kV/380kV Swiss electric power transmission network consists of 149 substations, which connect 219 transmission lines in total[9]. Some substations only connect one transmission line and some connect about 11 transmission lines. Generally, the failures of substations connecting more transmission lines could have more negative effects on the reliability of whole system, compared to substations connecting less transmission lines. Therefore, it is important to identify these substations. Figure 3.14 shows the overview of the SCADA system for the 220 kV/380 kV Swiss electric power transmission network. Each red node represents a substation and each green link represents a transmission line. There are 149 nodes and 219 links in this graph, considering the SCADA system as an undirected and unweighted graph.

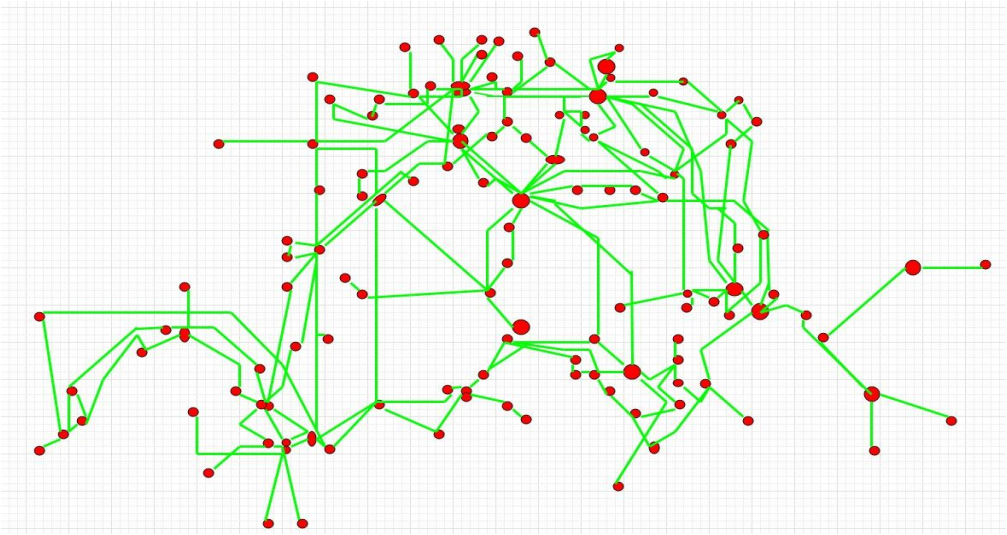


Figure 3.14 Overview of the SCADA system for 220kV/380kV Swiss power transmission network

[9] Due to the lack sufficient information, several substations are not considered by this thesis work.

As shown in Figure 3.15, the degree distribution[10] of the SCADA system peaks at k=2 and also has large values when k=1 and 3, which means that most substations connect less than 3 transmission lines. It should be noted that substations with k=1 are boundary substations. The number of substations with k≥6 is very small. The graph representing the SCADA system for Swiss power transmission network can be regarded as a scale-free network, as defined in [61] and [83]. The characteristic of such type of networks is that most nodes have small degrees but there is a finite possibility of identifying nodes with intermediate and large degrees. The nodes with a higher value of degree play a specific role in the structure of the network [61]. It has been demonstrated in [84] that the removal of these nodes usually causes a quite rapid destruction of the structure of the network. Due to the importance of these nodes (substations), it is assumed that the substations with k≥6 are considered as key substations, listed in Table 3.3.

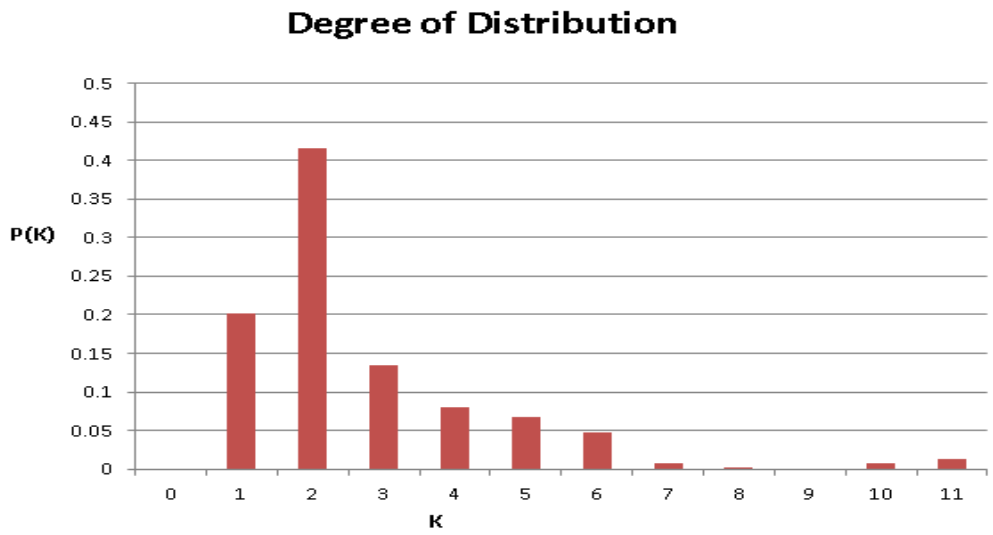


Figure 3.15 Degree distribution of SCADA system for 220kV/380kV Swiss electric power transmission network

[10] The degree distribution P(k) represents the probability that a generic node in the network is connected to k other nodes.

Table 3.3 List of substations (key substations) with degree k≥6

No	Substation location	Degree	No	Substation location	Degree
1	BREITE	11	**7**	ROMANEL	6
2	METTLEN	11	**8**	BONADUZ	6
3	MUEHLEBERG	10	**9**	CHIPPS	6
4	LAUFENBURG	8	**10**	GOESGEN	6
5	BICKIGEN	8	**11**	GRYNAU	6
6	SILS	7	**12**	BEZNAU	6

In a recent technical report [85], five buses with largest flow in the winter model of the 220kv/380kv Swiss power transmission network are identified and listed in Table 3.4.

Table 3.4 Five buses with largest flow in the winter model of the 220 kV/380 kV Swiss electric power transmission network [85]

No	Bus No	Bus ID	Bus Location	Flow SBUS (MVA)
1	108	SSILS_1A	SILS	3364.3
2	57	SLAUFE1A	LAUFENBURG	2856.6
3	43	SGOESG1A	GOESGEN	2819.9
4	25	SBREIT1A	BREITE	2800.8
5	73	SMETTL1A	METTLEN	2492.6

Compared Table 3.4 with Table 3.3, all the five substations containing buses with largest flow are also listed in the table of the key substations.

3.3.2.3 Identified Obvious Vulnerabilities

Based on the empirical investigation and topological analysis, obvious vulnerabilities due to interdependencies between the SCADA system and SUC are summarized below:

- Top 3 vulnerabilities of the SCADA system, based on the analysis of the RISI database, are **1)** the lack of overall security awareness, **2)** inadequate examined and maintained system administration mechanisms/software, and **3)** inadequately designed ICS networks and insufficient security for remote accesses. It should be noted that these vulnerabilities have been included in a

technical report [48] and submitted to FOCP for further proof and future consideration. All these vulnerabilities are related to the inadequacy of the system design, maintenance, and procedure, which could be handled by defining more comprehensive company policies or improving the security of the system. However, none of these vulnerabilities are caused due to interdependencies within or among CIs. Therefore, it is still necessary to identify interdependency-related vulnerabilities.

- According to the degree distribution obtained by analyzing the SCADA system for SUC of 220 kV/380 kV Swiss power transmission network, nodes (substations) with intermediate and large degrees (referring to this reference system as a graph) exist, which are also referred to as key substations in the research work described in this thesis. Based on the CN theory, the removal of these nodes causes a quite rapid destruction of the structure of the network meaning that the failures of these key substations could have negative effects on the reliability of the system significantly. Therefore, these key substations require more attention.
- Some SCADA components such the FID and the FCD are installed at the location where interlinked systems (in this case, SUC and SCADA) overlap. Therefore, these components can also be regarded as interface components. Due to their specific installation location, these interface components are more likely to be affected by the interdependencies and require more attention.
- Redundancy can reduce but not eliminate the possibility of component failures leading to a failure of the whole system. However, redundant components could fail simultaneously due to common causes such as design failures, human errors, lack of maintenance, design inadequacy, etc. The negative effects of CCFs of the system components on the overall system reliability could be significant. Therefore, there must be adequate awareness of potential CCFs.

3.4 Summary

The consequences triggered by interdependencies within and among CIs are difficult to analyze and evaluate due to their inherent complexities. The breakdown of a system

always starts from the slow field level device degradation and then escalates into a fast avalanche of failures of the whole system and even its interconnected system(s). Adverse effects of this type of incident are usually complicated and hard to be fully understood only using techniques such as the empirical investigation and topological analysis. A screening analysis is capable to capture obvious vulnerabilities, but is not sufficient enough to fully understand these vulnerabilities or even identify hidden vulnerabilities. Therefore, interdependencies within and among CIs should be further explored and studied using advanced techniques for in-depth analysis.

4 IN-DEPTH ANALYSIS OF INTERDEPENDENCY-RELATED VULNERABILITIES

After the steps of preparatory phase and screening analysis, a more sophisticated analysis has to be developed: using advanced modeling and simulation techniques to represent interdependencies within and among CIs, which can be considered as the third step of the methodical framework.

A number of model-based approaches for analyzing interdependencies within and among CIs have been introduced and discussed in Chapter 3. Some of these approaches can only be used to represent interdependencies at a structural/topological level, e.g., CN theory, PN-based modelling, etc, while some of them can even be used to gain a more comprehensive understanding of dynamic behaviours caused by CI interdependencies, e.g., ABM, etc. All these approaches have their advantages and disadvantages. To fully understand interdependencies within and among CIs and be sufficiently capable to represent their complexities, a novel approach needs to be developed for an in-depth analysis.

4.1 Challenges to Methods for In-depth Analysis

Investigating vulnerabilities within and among CIs caused by interdependencies through an in-depth analysis generally faces two major technique challenges:

1. **Challenges for Modeling and Simulating Single CI**
   As outlined before, CIs have become increasingly complicated and interdependent. They exhibit a number of characteristics such as dynamic/nonlinear behaviour, and intricate rules of interaction including with the environment due to their openness and high degree of interconnectedness turning them into a "System-of-Systems" (SoS). These characteristics make the modelling and simulation of such a system highly challenging and call for methods capable of representing it, often multiple layered, as a whole and not as a sum of single parts. Therefore, classical approaches and methods based on

decoupling and decomposition such as fault and event trees reach the limit of their capacity [7, 86]. Several approaches have been introduced and discussed in section 3.2.2.3. It should be noted that some of these approaches can be used to model interdependencies within and among CIs, as well as a single CI, e.g., CN theory, PN-based modelling, ABM, etc, while some of them can only be used to model interdependencies, e.g., DCST and IIM. Among these approaches, the CN theory is one of most frequently used techniques for topological analysis, while ABM can be combined with other techniques such as the Monte Carlo simulation and offers the possibilities to include physical laws into the simulation and emulate the behaviour of the infrastructure as it emerges from the behaviour of the individual agents and their interactions. Choosing an appropriate approach to model a single CI is an essential step for simulating CI interdependencies.

2. **Challenges for Simulating Interdependencies within and among CIs**

   The challenges regarding understanding, characterizing, and investigating interdependencies within and among CIs are immense and research in this area is still at an early stage [54, 55]. It has proven necessary to integrate different types of modeling approaches into one simulation tool in order to fully utilize benefits/advantages of each approach and optimize the efficiency of the overall simulation. One of the key challenges for developing such type of simulation tool is the required ability to create multiple-domain models, and effectively exchange data among them [29]. Traditional simulation approaches often intend to integrate multiple simulation components into one simulation platform. This type of simulation approach apparently suffers from two key technical difficulties:

   1) ***Lack of performance*:** The increasing complexity of this type of simulation tool limits its performance, with consequences of continuous consumption of simulation hardware, increasing number of simulated systems, increasing demands for more accurate simulation validation, and increasing requests for more computational resources. This problem could be expected for any simulation tool developed through traditional approaches, and is further complicated when simulating interdependencies among CIs since more than one infrastructure need to be considered and more cross-infrastructure analyses need to be conducted.

2) ***Lack of simulation interoperability*:** According to the U.S. Department of Defense [87], simulation interoperability can be defined as "*the ability of a system to provide data, information, services to and accept the same from other systems, and to use the data, information, and services so exchanged to enable them to operate effectively together*". As the definition indicates, it is important to ensure the effective data exchange capability between systems in order to improve simulation interoperability. However, the traditional simulation approach lacks this capability due to its inherent limitation, especially when it tries to simulate multiple systems in different domains, e.g., one system in time domain and another one in frequency domain.

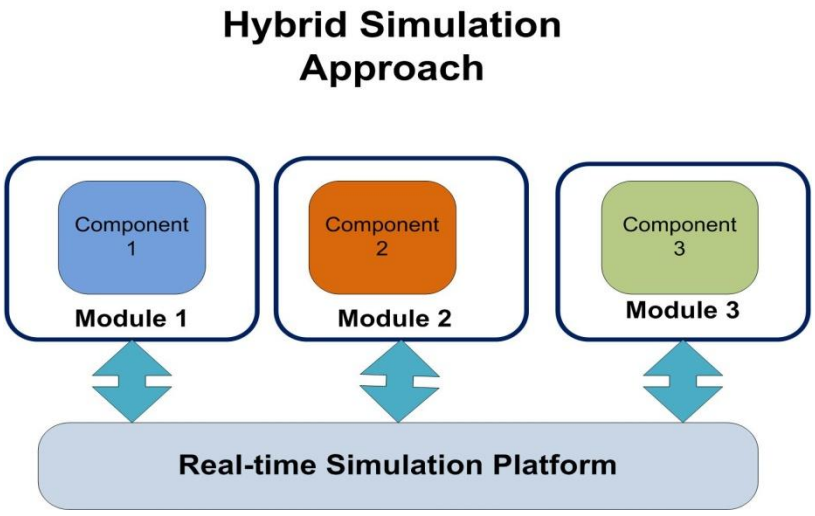


Figure 4.1 Architecture of the hybrid modeling/simulation approach

One solution for solving these challenges and handling these technical difficulties is to distribute different simulation components by adopting the concept of modular design. The overall simulation platform can be divided into different simulation modules at first, which could be domain-specific or sector-specific simulation components, so as to make the best use of computational resources, and then distribute them across one simulation platform. This so-called hybrid simulation approach, illustrated in Figure 4.1, intends to integrate different modeling and simulation techniques together, which can be considered as a successor of the traditional simulation approach in case multiple systems need to be simulated. It changes the way to design and develop simulation tools. Instead of building a

"heavy weight" simulation component, a number of "light weight" components are developed interacting with each other over a real-time simulation platform, which not just potentially improves the efficiency and flexibility of the developed simulation tool but also decreases its overall complexity. Each distributed "light weight" simulation component is only developed to represent its own system characteristics using appropriate modeling approaches. The information and control commands exchanged between simulation components are interpreted and processed over the network connection, which allows quick assembly of independently developed components without full knowledge of their peer simulation components. Benefits achieved from this hybrid modeling/simulation approach can be demonstrated from an exemplary application for an aircraft simulation tool development. Suppose a newly designed navigation component is required to be tested with other components in this tool, before installing it on real aircraft. It is not a good idea to develop a new aircraft simulation tool from scratch only for this purpose. Reusing existing component models with minor modification seems to be more promising and economic, which can hardly be accomplished using the traditional simulation approach. However, if this aircraft simulation tool is developed using the distributed simulation approach and all component models have been developed independently, tests can be easily performed since only navigation component model needs to be created or just modified.

Within the scope of this thesis, an experimental simulation test-bed has been developed based on the hybrid modelling/simulation approach for the purpose of investigating interdependency-related vulnerabilities between the SCADA system and the SUC (System Under Control) within power supply CI sub-sector. The ABM approach combined with other techniques such as Monte Carlo simulation, Fuzzy Logic, and Finite State Machines (FSMs) has turned out to be most promising to model the SCADA system. This model is then coupled with an existing SUC model, which was previously developed for other research purposes [75], over a Local Area Network (LAN). More details about the development of the SCADA system model and the experimental simulation test-bed will be presented in following sections of this chapter:

- Section 4.2: Modeling SCADA system
- Section 4.3: Modeling human operator

- Section 4.4: Implementation of hybrid modeling/simulation approach
- Section 4.5: Development an experimental simulation test-bed

4.2 Modeling SCADA

4.2.1 State of the Art

Modeling and simulating a SCADA system is a challenge from a theoretical point of view but of great practical importance. Nowadays, there are still only few well-developed SCADA models available. Siemens PTI has developed a high performance network modeling package, PSS™SINCAL®, for the planning of electricity, gas, water, and district heating networks. It is an open architecture environment with interfaces for various domain models including SCADA, GIS (Geographic Information System) and other systems. The PSS™SINCAL® is a commercial product which integrates all the models into one compact system. However, this tool can hardly be used for research purposes due to its commercial value. A computer-based simulation of a SCADA system is realized and configured by the Italian National Agency for New Technology (ENEA) through a set of computer machines connected to a LAN [39]. Each machine is developed to simulate a specific functionality of a specific SCADA system. For example, one machine is responsible to simulate a data collecting function by a RTU and another machine is used to simulate the functionality of a control centre where data coming from remote RTUs are collected and presented to operators. This functionally distributed network approach provides a solution for the interfacing issue regarding connections between different system models. A simulation environment is created by Nai Fovino et al., where identified attacks can be simulated for the purpose of assessing the cyber security of a power plant [88]. In this simulation environment, a group of devices are used to simulate a SCADA subsystem. Similar to the previously discussed ENEA's simulation system, a number of computers, servers, and switches are used to simulate different system functions. Although it is an applicable approach to investigate vulnerabilities and weaknesses of the overall system, both simulation environments mentioned above require a number of recourses to keep system running. Their intrinsic complexity could significantly limit the maintainability and problem diagnosing ability in future development. The modification of such SCADA models could become a very challenging job. It is necessary to have a

model which can integrate all components of a SCADA system into one platform. Furthermore, SCADA is an event-driven and service-oriented system. The model representing such type of system is normally coupled with models representing time-based systems such as an electricity transmission system, which increases the overall modeling difficulty since it is hard to include both types of models in one platform. These technical difficulties have motivated us to model the SCADA system using the approach of ABM. First, it is very difficult to model this type of system (event-driven) using classic modeling methods such as the CN theory. Second, this approach can improve the flexibility of developed models. System behaviors can be modified easily by changing the parameters of corresponding agents. It makes the target system customization much easier for future case studies. Last but not least, the agent-based SCADA model is capable to simulate such a distributed control network by running multiple agents simultaneously without increasing the overall complexity of the model. Furthermore, the ABM approach can help researchers to investigate different aspects of system dynamics and study the propagation of unexpected failures in a SCADA system. The major drawback of the ABM approach lies in the difficulties describing all functionalities of the studied system during the model development. Developers need to have a deeper understanding of system behaviors and be able to determine all the inputs and the outputs of the system. Thorough knowledge of an object-oriented programming language, such as Java and C++, is also a "must-have" for developing each agent of the SCADA model.

4.2.2 Structure of the SCADA Model

The SCADA model is developed by integrating agents, objects, database into one platform and is implemented using a simulation software tool: Anylogic 6.4[11]. Figure 4.2 shows the structure of SCADA model represented by UML (Unified Modeling Language). A simplified model structure is illustrated in Figure 4.3. Following components are included in the SCADA model:

[11] More information regarding the software tool of Anylogic can be found at *www.xjtek.com*

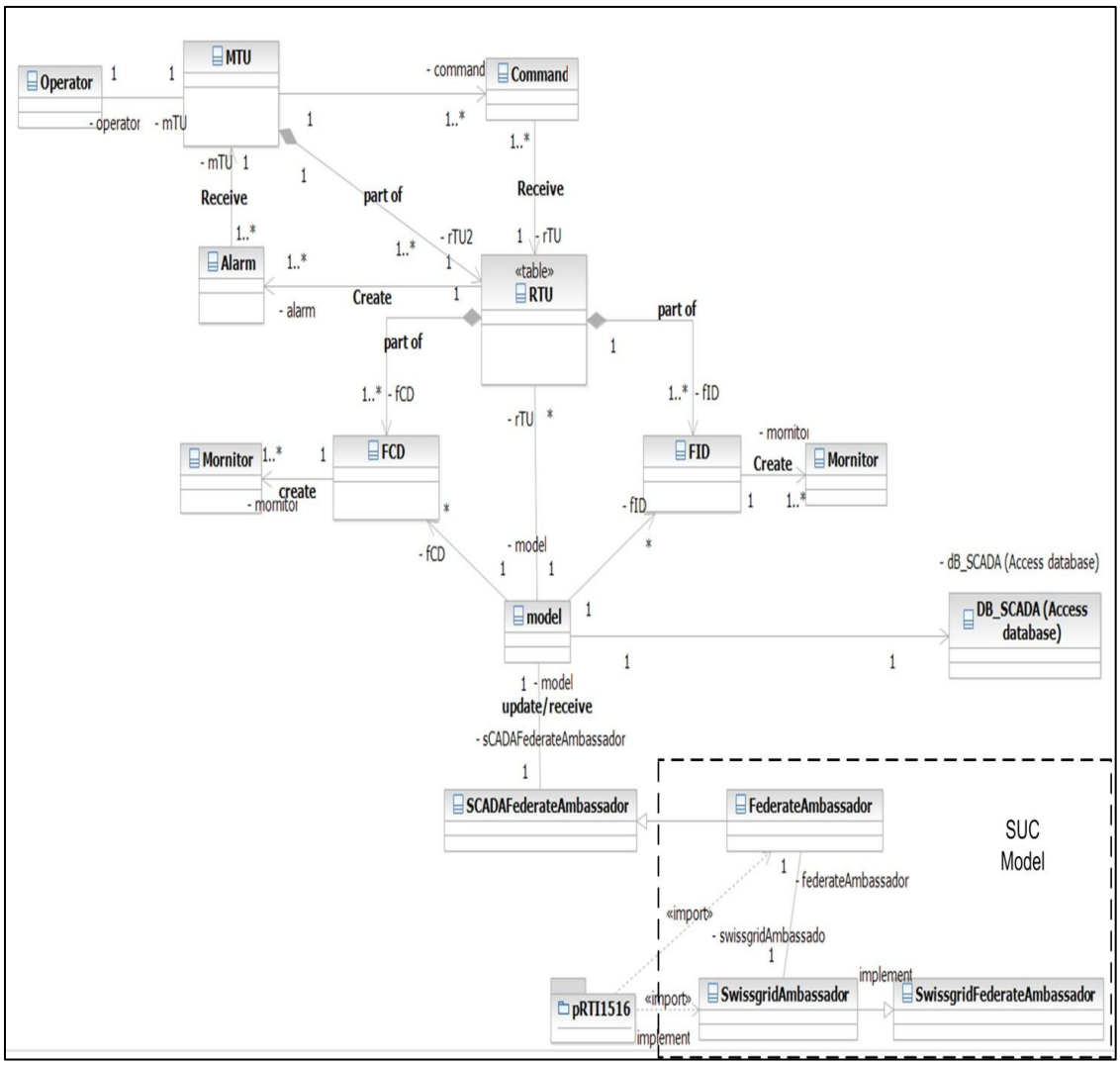


Figure 4.2 Structure of the SCADA model (represented by UML)

- **FCD**: This agent represents a mechanical switching device such as a circuit breaker or a disconnect switch (see section 4.2.4).
- **FID**: This agent represents an instrumentation device such as a sensor or a transducer (see section 4.2.5).

- **RTU**: This agent represents the remote terminal unit device of the SCADA system (see section 4.2.6).
- **MTU**: This agent represents the control centre issuing all control commands, collecting all information from the RTU, and interfacing with the operator(s) (see section 4.2.7).
- **Monitor** : The purpose of this object[12] is to examine received measured variables from FID agents or status variables from FCD agents and inform related agents, for example, RTU agents, in order to generate the alarm in case of identifying abnormal operating situation.
- **Alarm**: The purpose of this object is to inform the MTU agent if the predefined abnormal operating situation is identified, e.g., the measured variable value is greater than its alarm threshold value.
- **Command**: The purpose of this object is to deliver a corresponding command from the MTU agent to a RTU agent after receiving and analyzing the corresponding alarm.
- **Operator** : This agent represents personnel who has access to the MTU and make decisions according to the monitored field data (see section 4.2.2).
- **DB_SCADA:** This is a Microsoft Access based database, which is linked to the SCADA model using Anylogic's connectivity object. The purposes of developing this database are to :
    1) upload all required parameters to corresponding agents during the startup of the model. For instance, each FCD agent is created based on the parameters such as the name of its related FID agent, the name of its

[12] The difference between an agent and an object is that an agent can be regarded as a decision-making entity and an object is more or less a data structure consisting of data fields and methods. An agent can also be called an intelligent object.

linked RTU, etc. All these parameters are saved in a corresponding table of the DB_SCADA database and are uploaded before running the model.

2) record traced sequential events during the simulation. A SOE table (Sequence of Events) is created to record all important events, e.g., the identification of an alarm, opening of a FCD, etc.

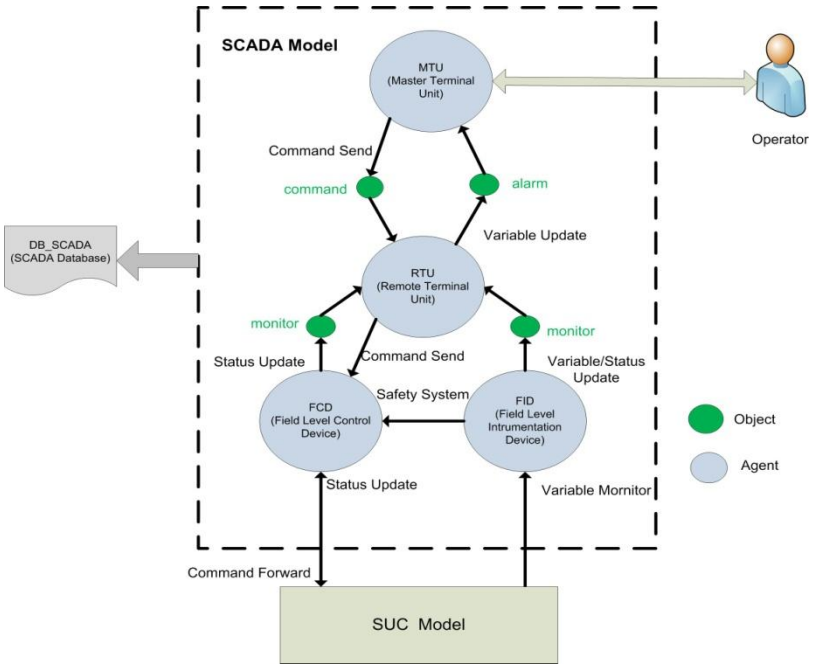


Figure 4.3 Overview of structure of the SCADA model

4.2.3 Failure-oriented Modeling Approach

The components at the substation level of the SCADA system are modeled using a failure-oriented modeling approach (Figure 4.4). In this approach, the "agent state" is defined as a location of control with a particular set of reactions to conditions and/or events of its related agent. For example, open and close are two states defined for a FCD agent. "Device mode" including both operational mode and failure mode is defined as the hardware status of corresponding simulated hardware devices. For example, failure-to-open and failure-to-close are two device modes defined for a field control device simulated by an FCD agent. The transition of various device modes can affect corresponding agent

states. It should be noted that all corresponding failure modes of a SCADA system have been defined in section 3.3.1. With the help of this modeling approach, technical failures of simulated devices of a SCADA system (e.g., FID, FCD and RTU) can easily be determined and corresponding failure propagations can be visualized/studied.

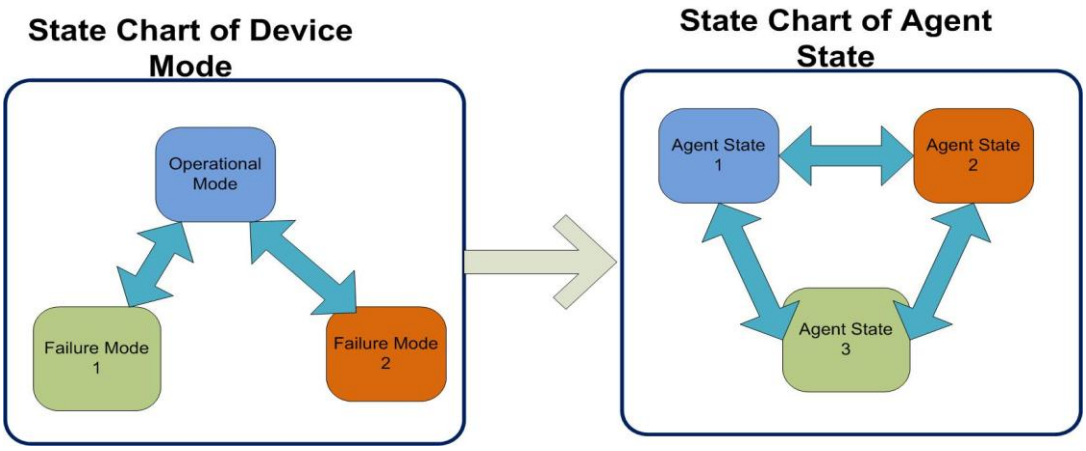


Figure 4.4 Failure-oriented modeling approach

The core of the device mode model is given by the state diagrams illustrated in Figure 4.5, which reflects a continuous-time, discrete-state Markov model describing failure behaviors of a studied device with one operation mode (left) and two failure modes (right). It should be noted that this state diagram is just an example and the number of failure modes is not just limited to two. A device (device i) can take one operation mode and several failure modes. Operation mode refers to the device mode when the device functions normally and failure mode refers to the device mode when the device functions abnormally. The transition time from the operation mode to one of the failure modes, i.e. the time to failure, is assumed to be exponentially distributed with constant failure rates λ, while transition time from one of the failure modes to operation mode is assumed to be exponentially distributed with repair rate μ.

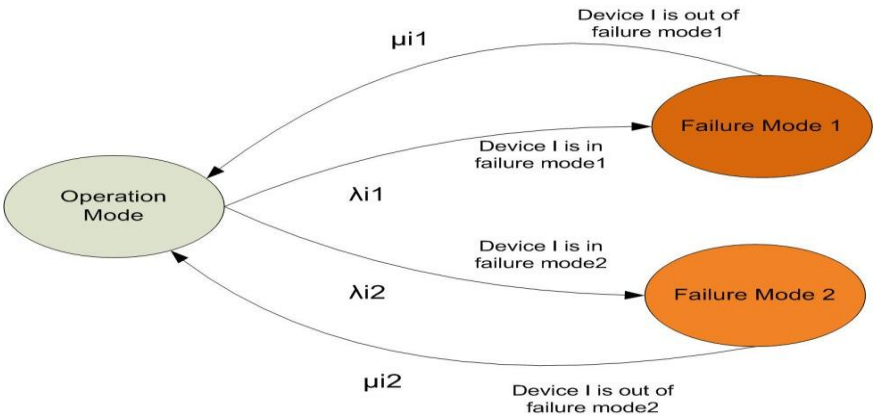


Figure 4.5 State diagram of the device mode model for the device i.

4.2.4 Component Models

4.2.4.1 Development of FCD Component

FCD is an agent that represents the mechanical switching devices such as circuit breakers and line disconnectors. In this model development, it is assumed that the FCD is capable to open or close a transmission line (removing power load) either after receiving a demand from a RTU or being triggered automatically by a local safety system. In the case when the FCD is triggered to disconnect a transmission line by a safety system, the instrumentation function will be performed by its connected FID such as a sensor or transducer. In order to simplify the complexity of the FCD agent, it is assumed that

- The time interval between closure and opening of FCD is zero[13].
- Only complete (100 percent) closure and opening of FCD are taken into account.
- After disconnecting the transmission line, the carried power load equals zero.

[13] This time interval varies depending on different types of FCD devices. For instance, the time for a disconnector used by a electricity transmission system to open under abnormal conditions, e.g., a short circuit, is between 1 to 3 seconds [50].

- Each modeled transmission line is equipped with a safety system, disconnecting the line ONLY if the operator fails to react or respond to the alarm.

Device Modes and Agent States

The device modes of the FCD agent are summarized in Table 4.1. The State diagram of the device mode model for FCD device is illustrated in Figure 4.6.

Table 4.1Summary of device modes of the FCD agent

Device mode	**Description**
OM (Operation Mode)	Modeled FCD device is currently under normal operation with full functionalities of all its components.
FO	Refer to Section 3.3.1.2
FC	Refer to Section 3.3.1.2
SO	Refer to Section 3.3.1.2

The state chart of the states of the FCD agent is shown in Figure 4.7 and summarized in Table 4.2.

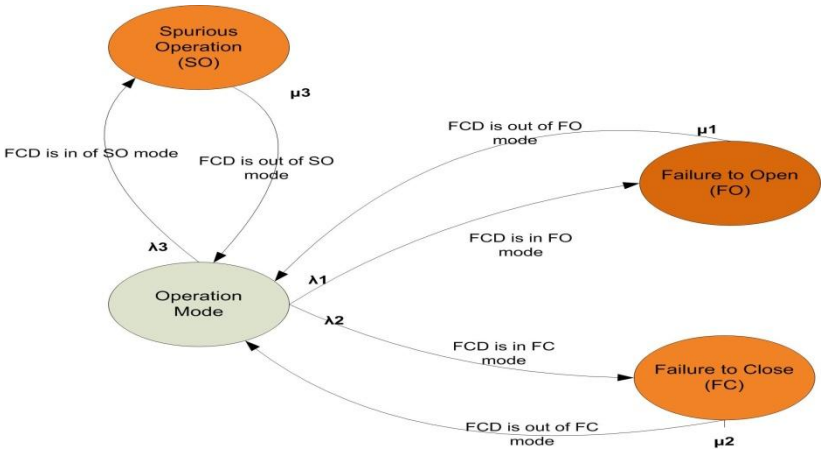


Figure 4.6 State diagram of the device mode model for the FCD agent

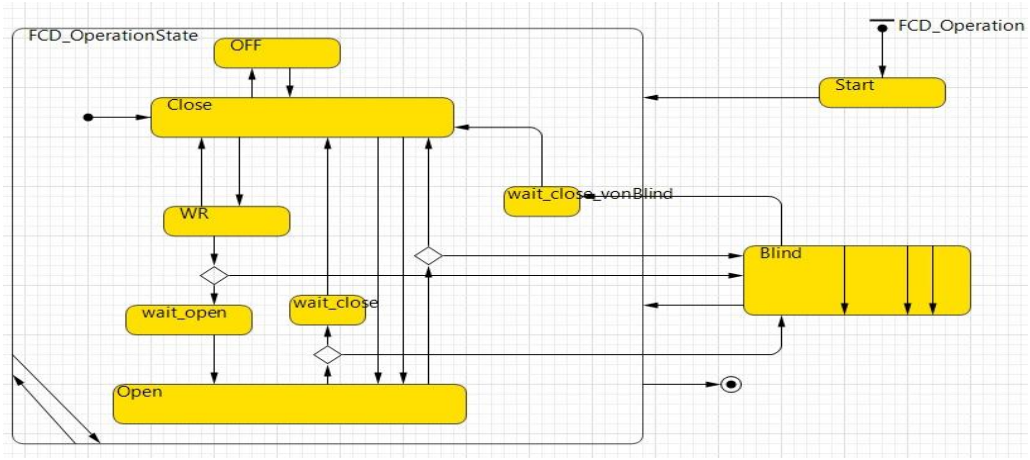


Figure 4.7 FCD agent state chart

Table 4.2 Summary of agent states of the FCD agent

Agent State	**Representation of agent state**
OFF	FCD device is power off
Close	FCD device is power on and remains close
Open	FCD device is power on and remains open
Blind	FCD device is power on, but not capable to operate or response to any received message. It should be noted that blind state is the state where the corresponding agent is not able to respond any changes of parameters or inputs from other agents.
WR (Warning Received)	Warning sent by its associated instrumentation device is received

Parameters

The parameters used to define the FCD model are summarized in Table 4.3.

Table 4.3 Summary of parameters of the FCD agent

Parameter	**Type**	**Default**	**Description**
timeToTrigger	integer	20 minutes *	The time for FCD to be automatically triggered in the case operator fail to response the alarm
timeToConnect*	integer	83 minutes *	The time for FCD to be automatically closed for purpose of connecting the line

***** this default value is based on [89].

4.2.4.2 Development of FID Component

FID is an agent that represents an instrumentation device such as a sensor and a transducer. The responsibilities of this agent include data acquisition, and measured variable monitoring. In this model development, it is assumed that the FID agent is capable to indicate the measured process variable value correctly based on correct set-up calibrations. In order to simplify the complexity the FID agent, it is assumed that the oscillation of indicated measured process variable is insignificant.

Device Modes and Agent States

The device modes of the FID agent are summarized in Table 4.4. The State diagram of the device mode model for FCD is illustrated in Figure 4.8.

Table 4.4 Summary of device modes of the FCD agent

Device mode	**Description**
OM (Operation Mode)	Modeled FID device is currently under normal operation with full functionalities of all its components.
FRH	Refer to Chapter 3.3.1.1
FRL	Refer to Chapter 3.3.1.1

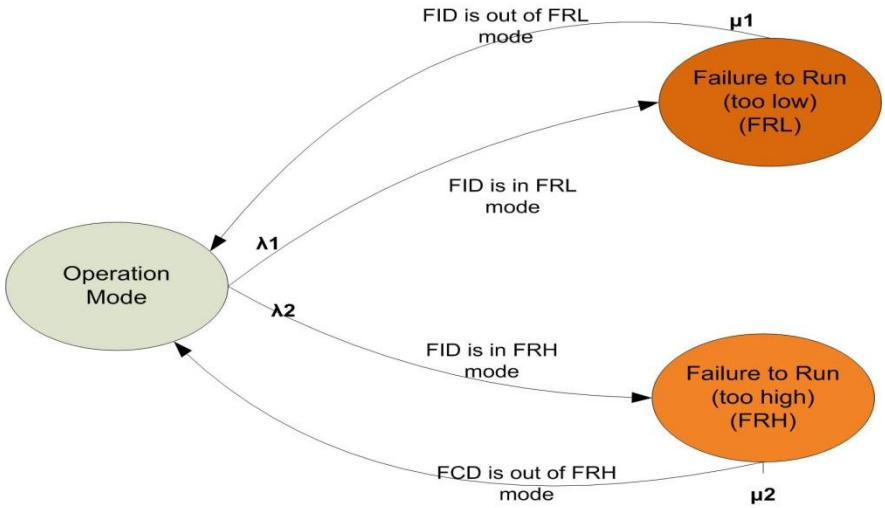


Figure 4.8 State diagram of the device mode model for the FID agent

The state chart of the states of the FID agent is shown in Figure 4.9 and summarized in Table 4.5.

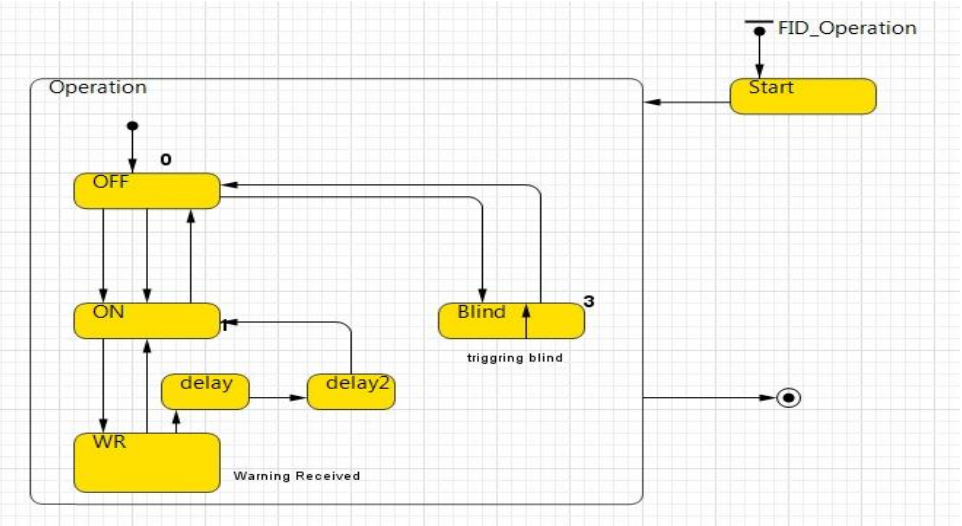


Figure 4.9 FID agent state chart

Table 4.5 Summary of agent states of the FID agent

Agent State	**Representation of agent state**
OFF	FID device is power off
ON	FID device is power on
WR (Warning Received)	Warning is received
Blind	FID device is power on, but not capable to operate (indicate)

Parameters

The parameters used to define the FID model are summarized in Figure 4.6.

Table 4.6 Summary of parameters of the FID agent

Parameter	**Type**	**Default**	**Description**
Alarm_threhold	double	N/A	The threshold value for generating an predefined alarm of its monitored transmission line

Measured variable value monitoring algorithm

The algorithm for monitoring FID measured variable value (*meValue*) is summarized below: Whenever the *meValue* of a FID agent is updated, a monitor object will be created. If this *meValue* is below the alarm_threshold of its monitored transmission line, then the monitor object will be destroyed. If measured variable is over the threshold, then this monitor object will be collected at a queue. An alarm request will be sent to its related RTU agent, only if a certain number of monitor objects have been collected at the queue consecutively. In case the measured value is below threshold before sending an alarm request, the queue will be emptied meaning the number of collected monitor objects returns to zero.

4.2.4.3 Development of RTU Component

RTU is an agent representing the remote terminal unit device located at the substation of the SCADA system. It is assumed that the RTU is capable to:

- acquire various types of data (status and measured variable) from field level devices (i.e. FID and FCD) and send acquired data to MTU whenever required,
- generate alarms based on warnings from field level devices and forward them to MTU when required,
- receive/interpret command(s) sent by MTU and forward it (them) to related field level devices.

The communication between a RTU and a MTU follows the principle of a slave and a master, meaning that only MTU is capable of initialing communication request and RTU is not able to send any data to MTU unless requested by it. However, its generated alarm can be sent to a MTU without receiving request (as soon as possible).

In order to simplify the complexity of a RTU agent, it is assumed that :

- All the components inside one RTU share same the power source and battery.
- During the power outage of a RTU, all alarms and commands saved in its memory will be deleted and not available for future uses.

- The functionalities of memory and CPU will not affect its performance, meaning the situation of lack of memory and poor performance of CPU will not be considered.

Device Modes and Agent States

The device modes of the RTU agent are summarized in Table 4.7. The State diagram of the device mode model for RTU device is illustrated in Figure 4.10.

Table 4.7 Summary of device modes of the RTU agent

Device mode	Description
OM	Modeled RTU device is currently under normal operation with fully functionalities of all its components.
FRF	Refer to Chapter 3.3.1.3
FRW	Refer to Chapter 3.3.1.3
FRC	Refer to Chapter 3.3.1.3

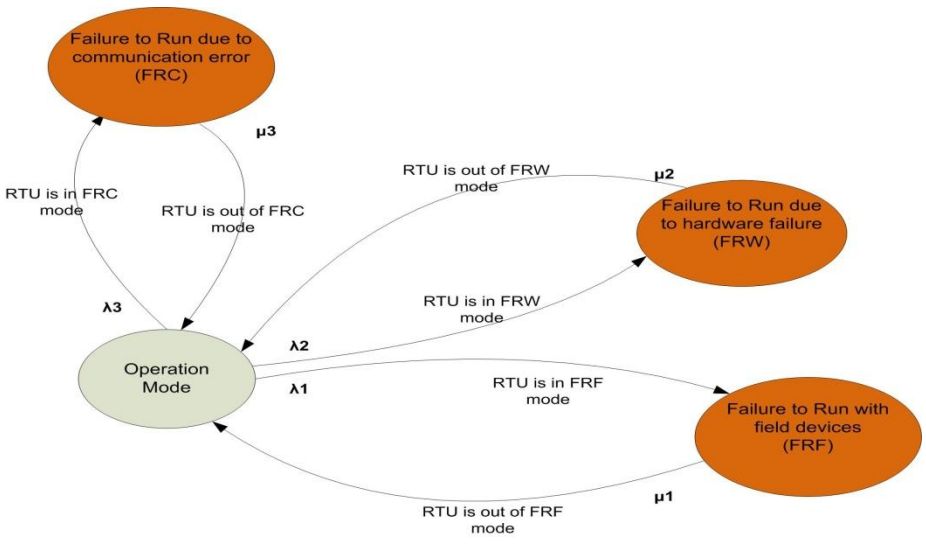


Figure 4.10 State diagram of the device mode model for the RTU agent

The state chart of the agent states of the RTU agent is shown in Figure 4.11 and summarized in Table 4.8.

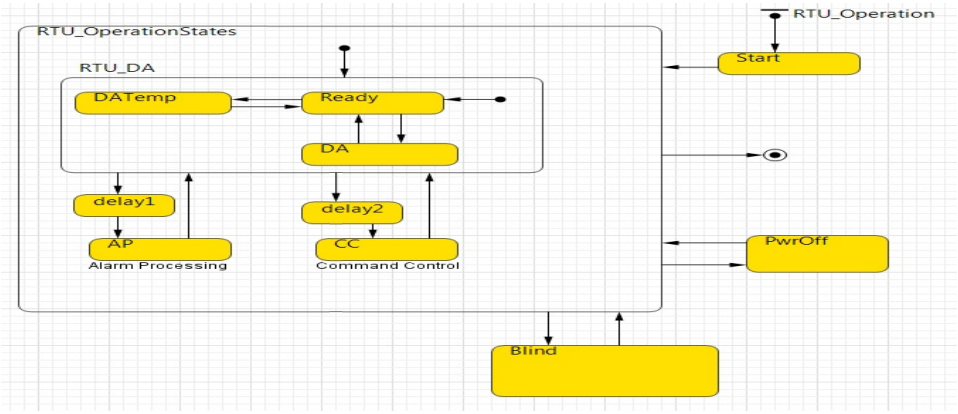


Figure 4.11 RTU agent state chart

Table 4.8 Summary of agent states of the RTU agent

state	**Representation of agent state**
Ready	RTU device is ready to run
DA (Data Acquisition)	RTU device receives most recent information from its connected field devices (FID and FCD)
AP(Alarm Processing)	RTU device receives alarm request from its connected FID or FCD agent. In this state, alarms will be generated and sent to MTU.
CC (Command Control)	RTU device receives the command from the MTU. The command will then be interpreted and forwarded to corresponding FID or FCD agent if no communication error occurs.
Blind	RTU device is power on, but unable to operate.
Power off	RTU device lost power (after the battery of this device has been completely consumed)

Parameters

The parameters used to define the RTU model are summarized in Table 4.9.

Table 4.9 Summary of parameters of the RTU agent

Parameter	Type	Default	Description
Battery capacity	int	20 mins*	Capacities of power batteries installed for corresponding RTU device

*this default value is based on reference [51]

4.2.4.4 Development of MTU Component

MTU is an agent that represents the control centre of the SCADA system. In this model development, it is assumed that a MTU is capable to:

- receive and process alarms sent by its connected RTUs,
- analyze received alarms by interfacing with the operator(s),
- issue control commands and send these commands to related RTUs.

In order to simplify the complexity the MTU agent, it is assumed that:

- All the RTUs only connect to one MTU
- Alarms received by the MTU are processed using the rule of FIFO (Fist In First Out).
- Issued commands will be sent to related RTUs without any time delay

Agent States

The state chart of the agent states of the RTU agent is shown in Figure 4.12 and summarized in Table 4.10.

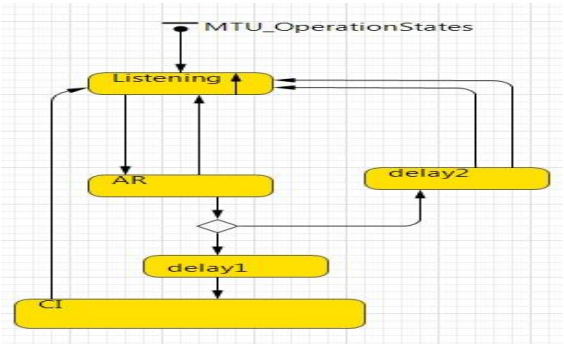


Figure 4.12 MTU agent state chart

Table 4.10 Summary of agent states of the MTU agent

state	Representation of agent state
Listening	MTU device is on and ready to receive information from RTUs
AR(Alarm Receive)	MTU device receives a alarm
CI(Command Issue)	A command is issued by the MTU device after processing corresponding alarm successfully.

4.2.4.5 Application to the Swiss Power Transmission Network

The number of components used to apply the developed model to the SCADA system of the Swiss power transmission network with the number of substation equal to 149, briefly introduced in section 3.2.3.2, is summarized in Table 4.11.

Table 4.11 Number of components used to model SCADA for Swiss power transmission network

No of FCD	No of FID	No of RTU	No of MTU
219	219	149	1

4.3 Modeling Human Operator

During the last decades, the human operator of infrastructure systems has become an essential element for not just maintaining daily operation, but also the security and quality of the system. For example, in a power supply CI sub-sector, a Transmission System Operator (TSO) is the personnel responsible to ensure the safety and efficiency of transmitting electrical power from generation plants to regional or local electricity distribution operators. Generally, the responsibilities of the TSO include monitoring /processing generated alarms, switching off components located at remote substations, sending commands to remote substations, etc. Although the operator's responsibilities are mainly related to system functionalities of monitoring and remote control, examining the reliability of the human operator remains crucial. In this section, the development of

modeling the human operator through the approach of Human Reliability Analysis (HRA), as the part of the MTU agent of the SCADA model, is introduced and discussed.

4.3.1 Introduction of Available HRA Approaches (State of the Art)

Human error is defined as "*Any member of a set of human actions or activities that exceeds some limit of acceptability, i.e. an out of tolerance action (or failure to act) where the limits of performance are defined by the system*" by Swain [90]. In the area of infrastructure systems, the human error has become a cause of great concern to the reliability of interactive technical systems, since most these systems depend on the interaction with operators in order to function appropriately. Therefore, research works related the HRA are important for safety engineers to be able to evaluate human error possibilities and uncertainties of the data concerning human factors [91]. Over the years, many HRA methods have been developed to assess human performance especially human errors. Qualitative methods are focused on the identification of events or errors and there is a common result of task analysis or incident investigation, while quantitative methods are focused on translating identified events/errors into Human Error Probability (HEP) [92].

First generation HRA Methods

The Technique for Human Error Rate Prediction (THERP), the best known first generation HRA method, is probably the most widely used technique to date [91]. It is basically a hybrid approach as it models human errors using both dependence models and Performance Shaping Factors (PSFs). Appropriate HEPs from a list of around 100 factors are selected for a nominal assessment [93]. The use of the THERP causes limitations during human performance analysis since this method intends to characterize each operator action with a binary path (success or failure) and is highly judgmental based on assessor's experiences. Additionally, the representation of PSFs influence on human performance is quite poor [91, 92].

Second generation HRA Methods

ATHEANA (A Technique for Human Event Analysis), one of second generation HRA methods, is designed to support the understanding and quantification of Human Failure Events (HFEs) [94]. This method is based on a multi-disciplinary framework that considers both human-centered factors and plant conditions creating operational causes for human-system interactions [91]. The human-centered factors and influences of plant conditions are dependent of each other, which are combined to create a situation in which the probability of making an error can be estimated. Such a situation is said to have an Error-Forcing Context (EFC). ATHEANA is capable to predict specific errors and most influential factors affecting that specific error and estimate HEPs for all sorts of combinations of various factors and conditions. However, the primary shortcoming of this technique lies in the fact that it is unable to produce final HEP meaning that the outcome of this analysis cannot be quantified [95].

CREAM (Cognitive Reliability Error Analysis Method) is one of the best known second generation HRA methods offering a practical approach to both performance analysis and error prediction [96]. This method presents a consistent error classification system integrating all individual, technological and organizational factors, which can be used both as a stand-alone method for accidental analysis, and as part of larger design methods for interactive systems. In this method, human error is not considered to be stochastic, but shaped by different factors such as the context of the task, physical/psychological situation of the human operator, time of day, etc. One of the main features of this method is that it includes a useful cognitive model and framework which can be used in both retrospective and prospective analysis [97]. CREAM is capable of providing the final estimated HEP which can be used as part of overall system analysis.

In the research work described in this thesis, the CREAM method is selected to model the human operator for several reasons:

1. CREAM represents a second generation HRA method with improved applicability and accuracy compared to most of the first generation methods, which is able to extend the traditional description of error modes beyond the binary categorization

of success-failure and secondly it accounts explicitly for how the (performance) conditions affect the performance.

2. CREAM has not just been developed from the underlying Cognitive Control Model (COCOM)[14], but uses it to organize some of categories describing possible causes and effects on human action.
3. CREAM can be used for performance prediction since quantified results can be provided as the final outcome. This capability makes the integration of the model developed using this approach with other models possible, which is a critical requirement for this project.

More information regarding the further detailed introduction of the approach of CREAM is included in Appendix III.

4.3.2 Applying CREAM to Model Human Operator in MTU

Appling the CREAM for the purpose of developing human operator model as part of the MTU agent of the SCADA model can be divided into five steps:

- Step 1: Constructing Event Sequence
- Step 2: Determining COCOM Functions
- Step 3: Identifying most likely cognitive function failures
- Step 4: Assessing Common Performance Conditions (CPCs)
- Step 5: Determining Failure Probability

It should be noted that the development of these steps are based on the working steps suggested by [96] and [92].

[14] COCOM models human performance as a set of control modes: strategic, tactical, opportunistic and scrambled and proposes a model of how transitions between these control modes occur. See Appendix III for more information.

Model Assumptions:

1) Two teams of operators work in the control centre: one team work during day time (day shift) and another during night time (night shift).
2) The communication between team members is efficient meaning there are no language issues.

4.3.2.1 Step1: Constructing Event Sequence

The task analyzed using the CREAM model is "moderate transmission line overload alarm handling", which can be divided into several subtasks. Figure 4.13 shows the respective Hierarchical Task Analysis (HTA). As seen from this figure, the overall operation of the task (task 0) involves four sequential subtasks. First, operators need to check whether or not the alarm monitor system is ready to work properly (subtask 0.1). The monitor system could include devices such as monitors, alarms, etc. Then operators start to keep checking the monitor system regularly to ensure the new generated alarm will not be missed (subtask 0.1.1). If a new overload alarm is generated and sent by field level devices to the alarm monitor system, operators will be notified meaning that this identified alarm will be handled (subtask 0.1.1.1). Finally, a control command will be sent by operators from the control centre to corresponding field devices (subtask 0.1.1.1). The descriptions of each subtask and the related cognitive activity are shown in Table 4.12.

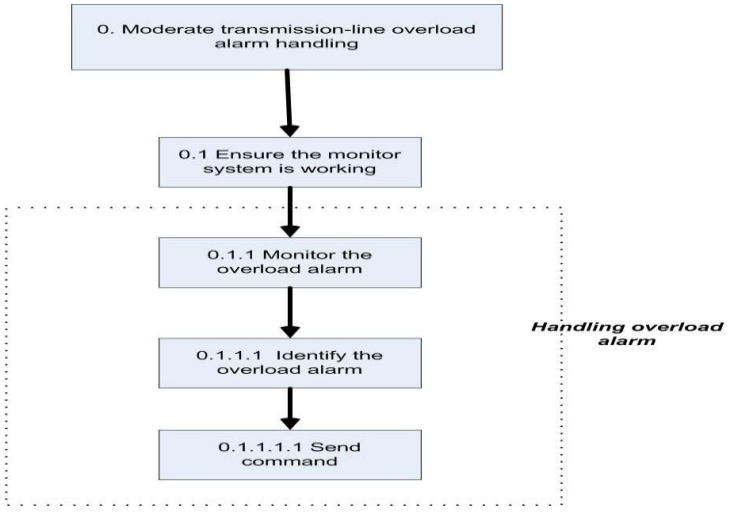


Figure 4.13. Relations between the CPC scores and the control modes.

Table 4.12 . Description of all subtasks

Subtask	Goal	Task step or activity	Cognitive activity
0.1	Ensure the alarm monitoring system is working	Check whether or not the alarm monitoring system works properly.	Verify
0.1.1	Monitor the overload alarm	Keep monitoring the new generated alarm(s).	Monitor
0.1.1.1	Identify a new overload alarm	A new generated alarm is recognized.	Identify
0.1.1.1.1	Send command	Send the command to corresponding field device.	Execute

4.3.2.2 Step 2: Determining COCOM Functions

In this step, all possible COCOM functions need to be determined for each identified subtask. The model assumes that there are four basic cognitive functions: observation, interpretation, planning, and execution. Each defined typical cognitive activity can be described in terms of which combination of these four cognitive functions it requires. For example, the "monitor" activity involves "observation" as well as "interpretation". A generic cognitive-activity-by-cognitive-demand is shown in Table 4.13.

Table 4.13 A generic cognitive-activity-by-cognitive-demand matrix [96]

Activity type	COCOM function			
	Observation	Interpretation	Planning	Execution
Co-ordinate			*	*
Communicate				*
Compare		*		
Diagnose		*	*	
Evaluate		*	*	
Execute				*
Identify		*		
Maintain			*	*
Monitor	*	*		
Observe	*			
Plan			*	
Record		*		*
Regulate	*			*

Scan	*			
Verify	*	*		

Based on the table above, all subtasks (cognitive activities) identified in step 1 are assigned with corresponding COCOM functions. Furthermore, It is important to determine a dominant function if the defined cognitive activity involves more than one COCOM functions. For example, subtask 0.1 (ensuring the alarm monitoring system is working), has been assigned with COCOM activity "verify" that involves two COCOM cognitive functions: "observation" and "interpretation". Based on the description of the analyzed task, this subtask involves more "observation" function and less "interpretation" function. In this case, the "observation" is the dominant COCOM function. Table 4.14 lists all possible cognitive functions defined for each subtask and one dominant cognitive function of each subtask is highlighted in red color.

Table 4.14 Determination of cognitive functions

Subtask	**Goal**	**Cognitive activity**	**Obs**	**Int**	**Plan**	**Exe**
0.1	Ensure the alarm monitoring system is working	Verify	•	•		
0.1.1	Monitor overload alarm	Monitor	•	•		
0.1.1.1	Identify a new overload alarm	Identify		•		
0.1.1.1.1	Send command	Execute				•

Obs: observation, Plan: planning, Int: interpretation, Exe: execution

4.3.2.3 Step 3: Identifying Most Likely Cognitive Function Failures

For each cognitive function, generic cognitive function failures have been defined in [96], shown in Table 4.15.

Table 4.15 Generic cognitive function failures [96]

Cognitive function	**Potential cognitive function failure**	
Observation errors	O1	Observation of wrong object. A response is given to the wrong stimulus or event
	O2	Wrong identification made, due to e.g. a mistaken cue or partial identification.

	O3	Observation not made (i.e., omission), overlooking a signal or a measurement
Interpretation errors	I1	Faulty diagnosis, either a wrong diagnosis or an incomplete diagnosis
	I2	Decision error, either not making a decision or making a wrong or incomplete decision.
	I3	Delayed interpretation, i.e., not made in time.
Planning errors	P1	Priority error, as in selecting the wrong goal (intention)
	P2	Inadequate plan formulated, when the plan is either incomplete or directly wrong
Execution errors	E1	Execution of wrong type performed, with regard to force, distance, speed or direction.
	E2	Action performed at wrong time, either too early or too late
	E3	Action on wrong object (neighbor, similar or unrelated)
	E4	Action performed out of sequence, such as repetitions, jumps, and reversals.
	E5	Action missed, not performed (i.e., omission), including the omission of the last actions in a series ("undershoot").

It is possible to use all pre-defined cognitive function failures for each cognitive activity. However, in order to make the CREAM more practical in use, one most likely cognitive function failure should be identified and used [96]. This can be done based on the understanding and knowledge of the analyzed task. For example, three cognitive function failures can be defined for the subtask 0.1: O1, O2, and O3. O1 represents the observation of a wrong object, while O2 represents the wrong identification made and O3 represents the observation not made. According to the description of this task, it is more reasonable to assume that the possibility of missing an overload alarm is higher. Therefore, the cognitive function failure O3 can be identified as the most likely function failure for subtask 0.1.

4.3.2.4 Step 4: Assessing Common Performance Conditions (CPCs)

The purpose of this step is to examine and assess the CPCs under which the analyzed task is performed. In order to simplify this assessment, it is necessary to make a number of assumptions, e.g.,

- working conditions (in control centre) are *compatible*
- adequacy of organization is *efficient*
- the availability of procedures/plans is *acceptable*
- the adequacy of training and preparation is *adequate with high experience*

- the crew collaboration quality is *efficient*

Based on the assumptions above, the five of nine CPCs are assigned with a fixed CPC level, while the level of each remaining CPC (Adequacy of Man-made Machine Interface (MMI) and operational support, time of day, number of simultaneous goals, and available time) is updatable depending on actual performance conditions. For example, the level of "time of day" can be "day time" or "night time", which depends on the time when the analyzed task is performed. It should be noted that the level assigned for each remaining CPC will be consistently updated during the simulation. Dependencies between CPCs are summarized in Table 4.16. It is necessary to adjust CPCs by considering those dependencies.

Table 4.16 Summary of dependencies between CPCs

CPC	**Depends on following CPCs**				
Working conditions	Adequacy of organization	Adequacy of MMI	Available Time	Time of Day	Adequacy of training and preparation
Number of simultaneous goals	Working conditions	Adequacy of MMI	Adequacy of Procedures/plans		
Available Time	Working conditions	Adequacy of MMI	Adequacy of Procedures/plans	Number of simultaneous goals	Time of Day
Crew collaboration quality	Adequacy of organization	Adequacy of training and preparation			

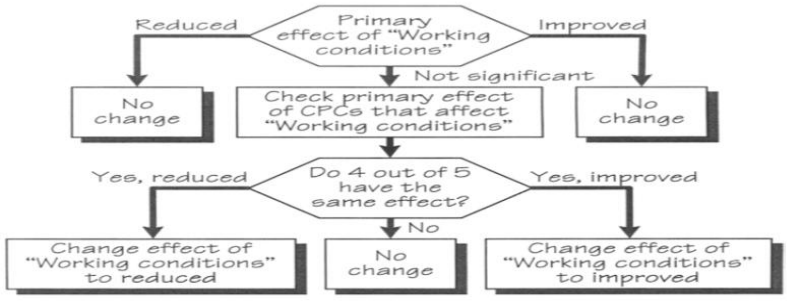


Figure 4.14 Rule for assessing dependency of "working conditions" [96]

A simple working rule for solving this dependency concern was developed in [96] and is illustrated in Figure 4.14, which uses "working condition" as an example. As seen from this figure, if the case of "working conditions" is considered, five other CPCs should be considered (dependencies between CPCs are summarized in Table A-III 3). First, the primary effect of "working conditions" on performance reliability is examined. If the effect is "improved" or "reduced", then there is no need to examine the dependencies. According to the assumptions above, the primary effect of "working conditions" is *not significant.* If the effect is "improved" or "reduced", then there is no need to examine the dependencies. According to the assumptions above, the primary effect of "working conditions" is *not significant* (relation between each CPC and performance reliability is shown in Table A-III 2). Therefore, it is necessary to check the primary effect of CPCs that affect "working conditions" according to the rule. The criterion of considering the assessment of dependencies in this case is that only if 4 out of 5 CPCs have the same effect (improved or reduced) on performance reliability then the effect of "working conditions" needs to be changed. Based on previous assumptions, the primary effect of "adequacy of organization" is *not significant*, while the primary effect of "adequacy of training and preparation" is *improved*. The primary effect of "adequacy of MMI" is uncertain and could be *improved* or *not significant*, same as the primary effects of "available time" and "time of day". Therefore, it is necessary to adjust the CPC "working conditions" considering the dependencies between CPCs. A similar rule can also be applied to assess dependencies between other CPCs. In the case of "crew collaboration quality", the criterion is that both of two dependent CPCs have the same primary effect. In the case "number of goals", the criterion is that two out of three dependent CPCs have the same primary effect. In the case of "available time", the criterion is that four out of five dependent CPCs have the same primary effect. Table 4.17 is a modified table of Table 4.16 based on previous assumptions.

As seen from Table 4.17, three of these four CPCs should be considered for the adjustment due to the assessment of dependencies. Two of these three CPCs are considered to be adjusted due to CPC "working conditions". For example, four out of five dependent CPCs of "available time" have "not fixed" effects on the performance reliability, which could possibly meet the pre-defined criterion (four out of five CPCs have same

primary effects). The effects of the CPCs on performance reliability can be quantified using the weighting factor. For instance, in the case where the expected effect is "not significant", the weighting factor is set to be 1. In the case where the expected effect is "improved", the weighting factor can be set to be less than 1 meaning that the final calculated HEP will likely be decreased (because the performance reliability will likely be improved). Conversely, in the case where the expected effect is "reduced", the weighting factor can be set to be more than 1 meaning that the final calculated HEP will likely be increased (because the performance reliability will likely be reduced). Proposed corresponding weighting factors for all CPCs in [96], shown in Table 4.18, will be used as the reference in the current model development.

Table 4.17 Summary of dependencies between CPCs based on previous assumptions

CPC	**Depends on following CPCs**				
Working conditions *(Need to be adjusted)*	**Adequacy of organization** Level: Efficient Effect: not significant	**Adequacy of MMI** Level: Not fixed Effect: Not fixed	**Available Time** Level: Not fixed Effect: Not fixed	**Time of Day** Level: Not fixed Effect: Not fixed	**Adequacy of training and preparation** Level: Adequate (high experience) Effect: Improved
Number of simultaneous goals *(Need to be adjusted)*	**Working conditions** Level: Not fixed Effect: Not fixed	**Adequacy of MMI** Level: Not fixed Effect: Not fixed	**Adequacy of Procedures/plans** Level: Acceptable Effect: not significant		
Available Time *(Need to be adjusted)*	**Working conditions** Level: Not fixed Effect: Not fixed	**Adequacy of MMI** Level: Not fixed Effect: Not fixed	**Adequacy of Procedures/plans** Level: Acceptable Effect: not significant	**Number of simultaneous goals** Level: Not fixed Effect: not fixed	**Time of Day** Level: Not fixed Effect: Not fixed
Crew collaboration quality *(No need to be adjusted)*	**Adequacy of organization** Level: Efficient Effect: not significant	**Adequacy of training and preparation** Level: Adequate (high experience) Effect: Improved			

Table 4.18 Proposed weighting factors for CPCs [96]

CPC name	Level	COCOM function			
		OBS	INT	PLAN	EXE
Adequacy of organisation	Very efficient	1.0	1.0	0.8	0.8
	Efficient	1.0	1.0	1.0	1.0
	Inefficient	1.0	1.0	1.2	1.2
	Deficient	1.0	1.0	2.0	2.0
Working conditions	Advantageous	0.8	0.8	1.0	0.8
	Compatible	1.0	1.0	1.0	1.0
	Incompatible	2.0	2.0	1.0	2.0
Adequacy of MMI and operational support	Supportive	0.5	1.0	1.0	0.5
	Adequate	1.0	1.0	1.0	1.0
	Tolerable	1.0	1.0	1.0	1.0
	Inappropriate	5.0	1.0	1.0	5.0
Availability of procedures / plans	Appropriate	0.8	1.0	0.5	0.8
	Acceptable	1.0	1.0	1.0	1.0
	Inappropriate	2.0	1.0	5.0	2.0
Number of simultaneous goals	Fewer than capacity	1.0	1.0	1.0	1.0
	Matching current capacity	1.0	1.0	1.0	1.0
	More than capacity	2.0	2.0	5.0	2.0
Available time	Adequate	0.5	0.5	0.5	0.5
	Temporarily inadequate	1.0	1.0	1.0	1.0
	Continuously inadequate	5.0	5.0	5.0	5.0
Time of day	Day-time (adjusted)	1.0	1.0	1.0	1.0
	Night-time (unadjusted)	1.2	1.2	1.2	1.2
Adequacy of training and preparation	Adequate, high experience	0.8	0.5	0.5	0.8
	Adequate, low experience.	1.0	1.0	1.0	1.0
	Inadequate.	2.0	5.0	5.0	2.0
Crew collaboration quality	Very efficient	0.5	0.5	0.5	0.5
	Efficient	1.0	1.0	1.0	1.0
	Inefficient	1.0	1.0	1.0	1.0
	Deficient	2.0	2.0	2.0	5.0

Based on the Table above, effects of CPCs of all identified subtasks are assessed, which are shown in Table 4.19. As seen from this table, five out of nine CPCs are set to be fixed for each subtask, while four CPCs have not. However, the minimum (highlighted in blue) and maximum (highlighted in red) value of uncertain weighting factors can be determined. Then the minimum and maximum total weighting factor can be obtained where minimum value represents the best case scenario and maximum value represents the worst case scenario.

Table 4.19 Assigned weighting factors for each subtask

CPC name	Level	Subtask			
		0.1	0.1.1	0.1.1.1	0.1.1.1.1
		O3	O3	I3	E2
Working conditions	Compatible	1.0	1.0	1.0	1.0
Adequacy of organization	Efficient	1.0	1.0	1.0	1.0
Procedure and plan	Acceptable	1.0	1.0	1.0	1.0
Training and preparation	Adequate, high experience	0.8	0.8	0.5	0.8
Crew collaboration	Efficient	1.0	1.0	1.0	1.0
Adequacy of MMI and operational support (updatable)	Supportive	**0.5**	**0.5**	**1.0**	**0.5**
	Tolerable	**1.0**	**1.0**	**1.0**	**1.0**
Time of day (updatable)	Day time	**1.0**	**1.0**	**1.0**	**1.0**
	Night time	**1.2**	**1.2**	**1.2**	**1.2**
Number of goals (updatable)	Fewer than current capacity	**1.0**	**1.0**	**1.0**	**1.0**
	Match current capacity	**1.0**	**1.0**	**1.0**	**1.0**
	More than current capacity	**2.0**	**2.0**	**2.0**	**2.0**
Available time (updatable)	Adequate	**0.5**	**0.5**	**0.5**	**0.5**
	Temporarily inadequate	1.0	1.0	1.0	1.0
	Continuously inadequate	**5.0**	**5.0**	**5.0**	**5.0**
Total weighting factor (Minimum)		**0.2**	**0.2**	**0.25**	**0.2**
Total weighting factor (Maximum)		**9.6**	**9.6**	**6**	**9.6**

4.3.2.5 Step 5: Determining Failure Probability

To determine the Cognitive Failure Probability (CFP), each identified most likely cognitive function failure is firstly assigned with a nominal CFP, which can be conducted using the information from Table A-III 5. Then, these nominal CFPs are adjusted considering the effects of the CPCs using weighting factors obtained from step 4. Table 4.20 and Table 4.21 list the adjusted CFP for each subtask, while Table 4.20 uses minimum weighting factors representing best case scenario and Table 4.21 uses maximum weighting factors representing worst case scenario.

Table 4.20 Adjusted CFPs for cognitive function failures (best case scenario)

Step	Task step or activity	Error mode	Nominal CFP	Weighting factor	Adjusted CFP
0.1	Ensure the alarm monitoring system is working	O3	0.07	0.2	0.014
0.1.1	Monitor overload alarm	O3	0.07	0.2	0.014
0.1.1.1	Identify a new overload alarm	I3	0.01	0.25	0.0025
0.1.1.1.1	Send the command	E2	0.003	0.2	0.0006

Table 4.21 Adjusted CFPs for cognitive function failures (worst case scenario)

Step	Task step or activity	Error mode	Nominal CFP	Weighting factor	Adjusted CFP
0.1	Ensure the alarm monitoring system is working	O3	0.07	9.6	0.672
0.1.1	Monitor overload alarm	O3	0.07	9.6	0.672
0.1.1.1	Identify a new overload alarm	I3	0.01	6	0.06
0.1.1.1.1	Send the command	E2	0.003	9.6	0.0288

The final CFP can be obtained by choosing the maximum one from all calculated adjusted CFPs using the Equation 4.1:

$$CFP_{final} = max(CFP_i), i = 1, n \quad \text{(Equation 4.1)}$$

where CFP_i is an adjusted CFP value and n is the number of values calculated.

In the case of best case scenario, three out of nine CPCs have "improved" effects on the performance reliability and none of the CPCs have a "reduced" effect ($\sum improved = 3, \sum reduced = 0$). According to

Figure A-III 2 (relations between CPC scores and control modes), the corresponding control mode is "Tactical" and the probability interval is from 0.001 to 0.1. The calculated final CFP, shown in Table 4.20, is 0.014, which falls into the interval. In the case of worst case scenario, one out of nine CPCs have an "improved" effect on the performance reliability and three of the CPCs have "reduced" effects ($\sum improved = 1, \sum reduced = 3$). According to

Figure A-III 2, the corresponding control mode is "Scrambled" and the probability interval is from 0.1 to 1. The calculated final CFP, shown in Table 4.21, is 0.672, which falls into the interval.

4.3.3 *Assessing CPCs in Real-time During the Simulation*

4.3.3.1 Assessing CPC-Adequacy of MMI and Operational Support

In this experiment, it is assumed that a team of experts providing operational supports to operators work with operators. Normal working hours for this team is from 8 am to 18 pm (excluding lunch hour between 12 and 13 pm). During normal working hours, operational supports are assumed to be sufficient. During other times, the operational supports are assumed to be tolerable. Based on these assumptions, the "Adequacy of MMI and Operational Support" can be assessed during the simulation by examining the current time of the model:

- If current time is between 8 am and 12 pm or between 13 pm and 18 pm, then the level of “Adequacy of MMI and Operational Support " is set to *Supportive.*
- For other times, the level of "Adequacy of MMI and Operational Support " is set to *Tolerable.*

4.3.3.2 Assessing CPC-Time of Day and Number of Simultaneous Goals

The 'Time of Day" can be assessed during the simulation by examining the current time of the model based on following assumptions:

- If current time is between 8 am and 20 pm, then the level of "Time of Day" is set to *Day Time*. If not, then the level "Time of Day" is set to *Night Time*.

According to Table A-III 1, the CPC “Number of simultaneous goals” can be described as "*the number of tasks a person is required to pursue or attend to at the same time*". In this analyzed task, it can be regarded as the number of alarms received in the control centre that are still not handled by operators. Therefore, this CPC can be assessed during the simulation by examining the number of alarms that are still not processed based on following assumptions:

- If more than 3, then the level of "Number of simultaneous goals" is set to *More than current capacity*
- If equal to 3, then the level "Number of simultaneous goals" is set to *Match current capacity*
- If less than 3, then the level "Number of simultaneous goals" is set to *Fewer than current capacity*

4.3.3.3 Assessing CPC-Available Time

According to Table A-III 1, the CPC "Available time" can be described as "*the time available to carry out a task and corresponds to how well the task execution is synchronized to the process dynamics*". Compared with other updatable CPCs (i.e. "Adequacy of MMI and operational support", "Time of day", and "Number of simultaneous goals"), it is more difficult to evaluate (assess) this CPC quantitatively due to following reasons:

1) It is difficult to set a numerical threshold by which the corresponding level can be decided.
2) The assessment depends on the knowledge and experiences related to the specific task.
3) Many other issues could also have direct effects on the assessment of "Available time". For example, the number of current simultaneous tasks and time left for operators to handle one task could both have significant influences.

A knowledge-based approach to assess CPC-"available time"

In order to assess "Available time", a knowledge-based approach using the fuzzy logic theory is proposed. Fuzzy logic theory, first developed by Zadeh [98], almost five decades ago, has emerged over the last several years as a useful tool for modeling processes which are too complex or fuzzy for conventional quantitative techniques or when the available information from the process is qualitative, inexact or uncertain [91]. The way that fuzzy logic addresses the qualitative information is similar to the way human beings make inferences and take decisions. Fuzzy logic models fill a gap between purely mathematical approaches and purely logic-based approaches. Instead of requiring accurate equations to model real-world behaviors, fuzzy logic is capable to accommodate the ambiguities of real-world human language and logic with its inference techniques. Fuzzy inference systems (FIS), which is developed based on fuzzy logic theory, have been successfully applied in fields such as automatic control, data classification, expert system, and decision analysis [99]. Adopting the approach of FIS for the study of the HRA is also not a new concept. In 2006, a modeling application of CREAM methodology based on fuzzy logic technique has been developed by Konstandinidou and his colleagues, which can be regarded as a pilot application demonstrating the successful 'translation' of the CREAM into the language of fuzzy logic [91]. Below a brief explanation of fuzzy logic and fuzzy sets is given, and for details refer to [98].

A fuzzy logic system is a nonlinear system whose behavior is described by a set of linguistic rules. For example, rules such as:

IF (service is good) THEN (give more tips)
IF (service is alright) THEN (give average tips)
IF (service is bad) THEN (give less tips)

Unlike other regular mathematical systems, the FIS is related to the classes with unsharp boundaries where the output is only a matter of degrees. It is primarily about linguistic vagueness through its ability to allow an element to be a partial member of set, so that its membership value can lie between 0 and 1 [100]. Central to the FIS are fuzzy sets and membership functions. A fuzzy set A is defined as a set of ordered pairs:

A= {(x,μ_A(x))| x ∈ X} where A is called the fuzzy sets and μ_A(x) is called the membership function (MF).

In order to build a knowledge-based approach to assess the "Available time" in real-time, it is assumed that this CPC is mainly affected by two parameters:

- ***Time left*** : In the task analyzed using this model, each overload alarm must be handled in a predefined time period. If operators fail to process on time, then the overloaded line will be disconnected automatically in order to prevent the thermal damage to the transmission line. In this task, it is assumed that the moderate overloads can be tolerated for up to 20 minutes [75] [101].
- ***Number of simultaneous goals***: If there would be a number of simultaneous alarms, then the time to handle some of these alarms will be delayed.

Development of Fuzzy Logic Inference system

Assessing "Available time" through a knowledge-based approach using a FIS can be performed as follows:

Inputs :

1) TimeLeft : The remaining time of each overloaded alarm to be handled
2) NumOfGoals: The number of simultaneous alarms that is required for operators to handle

Output :

The cognitive level: "Available time": *adequate*, *temporarily inadequate*, *continuously inadequate*

Membership Functions

The MF essentially embodies all fuzziness for a particular fuzzy set [102]. The shape of membership functions used for both input and output are triangular.

1) Three membership functions are selected for both inputs, with linguistic values: "insufficient", "sufficient", and "more sufficient" for input "TimeLeft" and "fewer than capacity", "match current capacity", and "more than capacity" for input

"NumOfGoals". The range for each MF is shown in Table 4.22 and the graph is shown in Figure 4.15. It should be noted that the membership functions defined below are based on the understanding and knowledge of the analyzed task.

Table 4.22. Ranges of MFs for both inputs

Input	insufficient	sufficient	more sufficient
TimeLeft (min)	<10	>6 and <16	>10
Input	fewer than capacity	match current capacity	more than capacity
NumOfGoals	<3	>1 and <5	>3

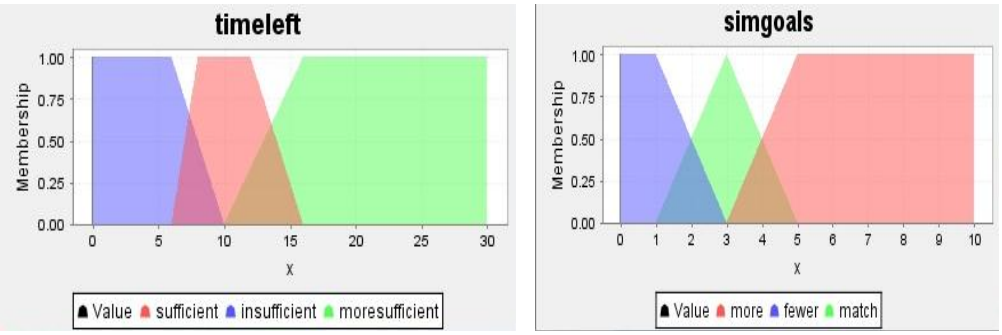


Figure 4.15. Membership function graphs of both inputs

2) Three output (consequence) functions are selected. The purpose of these functions is to determine the likelihood of the conclusion which is true, given a premise. The range for each MF is shown in Table 4.27 and MF graph is shown in Figure 4.18.

Table 4.23 The range of MF of output

Level of "Available time"	Continuously inadequate	Temporarily inadequate	Adequate
Consequence	<4	>2 and <6	>4

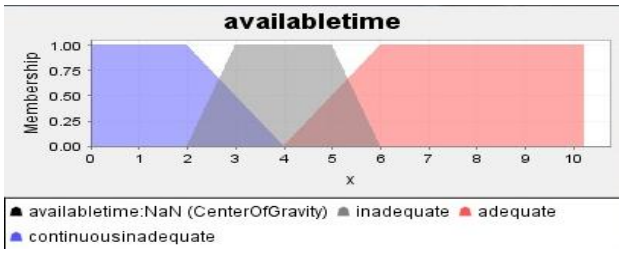


Figure 4.16The graph of consequence membership functions

Rules:

Table 4.24 displays all fuzzy decision-making rules derived from knowledge base, developed based on the understanding and knowledge of the analyzed task. For example, the rule in the circle can be read as:

If *Time Left is sufficient* ***AND*** *the number of simultaneous goals is matching current capacity,* ***then*** *the level of "Available time" is set to adequate.*

Table 4.24 Rule table

Level of "Available time"		**Number of simultaneous goals**		
		Fewer than capacity	Match current capacity	More than capacity
Time left	Insufficient	Inadequate	Inadequate	Continuous inadequate
	Sufficient	Adequate	Adequate	Inadequate
	More sufficient	Adequate	Adequate	Inadequate

Defuzzification method: Centre of Gravity (COG) method is implemented as the defuzzification method for combining all the consequences to make decisions, which is illustrated in the equation below. Basically this method calculates the weighted average of the centre values of the consequence membership functions (Equation 4.2).

$$u^{crisp} = \frac{\sum_i b_i \int \mu_{(i)}}{\sum_i \int \mu_{(i)}} \qquad \text{Equation 4.2}$$

where b_i *denotes the centre of consequence membership and* μ_i *denotes the membership function*

Test runs: In order to demonstrate the applicability of this knowledge-based approach, several test runs are performed.

Test run#1: In this test run, it is assumed that

- Time left for operator to handle an overload alarm is 12 minutes
- The number of simultaneous tasks is 2

Therefore, the inputs to the developed FIS are 12 for "time left" and 2 for "NumOfGoals". The output of the FIS after the defuzzification is 7.24. All corresponding membership function graphs are shown in Figure 4.17. As observed from this table, the level of "Available time" can be set to adequate.

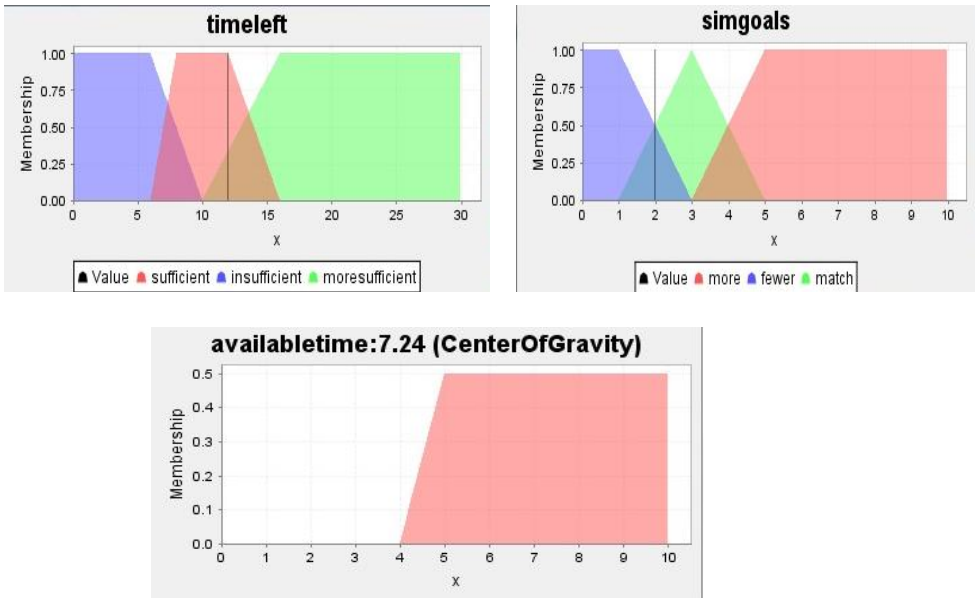


Figure 4.17 Membership function graphs of both inputs and the output for test run#1

Test run#2: In this test run, it is assumed that

- Time left for operator to handle an overload alarm is 5 minutes
- The number of simultaneous tasks is 4

Therefore, the inputs to the developed FIS are 5 for Time left and 4 for NumOfGoals. The output of the FIS after the defuzzification is 2.87. All corresponding membership function graphs are shown in Figure 4.18. As observed from this figure, the level of "Available time" can be set to continuous inadequate.

One of advantages of integrating the approach of FIS into HRA lies in the fact that it provides a fundamentally simple way to handle complex problems without making itself exceedingly complex. It is straightforward, flexible, and easy to develop and understand. However, the approach of the FIS is a data-driven approach, meaning that the accuracy of the output is dependent on the quality of expert knowledge and experiences. Therefore, the membership functions, as well as developed rules, need to be carefully calibrated.

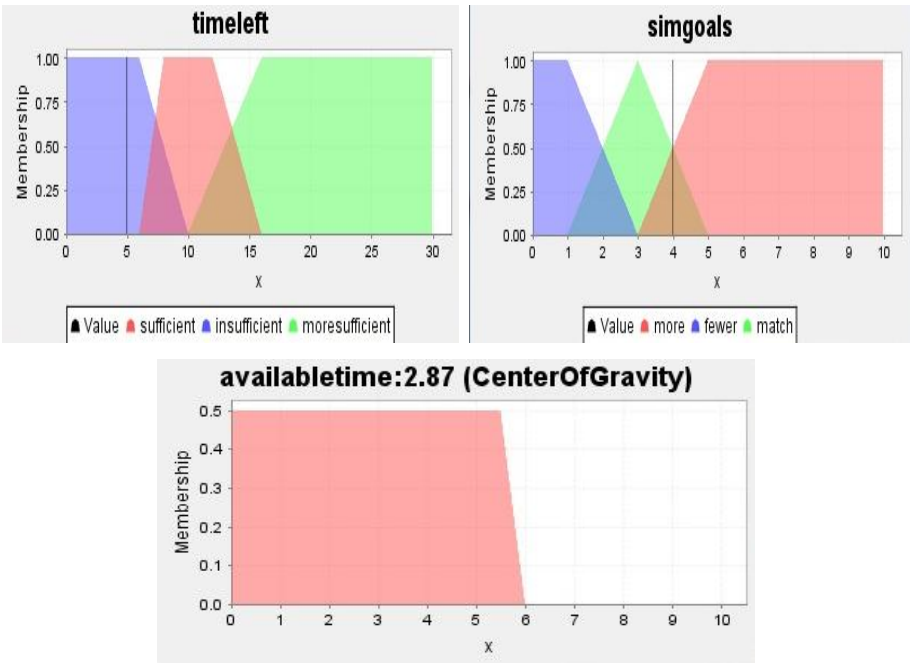


Figure 4.18. Membership function graphs of both inputs and the output for test run# 2

4.3.4 Summary

In this section, a novel approach to model human operator performance is proposed and implemented as part of the MTU agent in the developed SCADA model. This is the first effort to develop a human operator performance model assessing CPCs dynamically using the ABM approach. During the simulation, if there is a request for the operator to handle an alarm, CPCs will be assessed according to current simulation environment, e.g., time of day, simultaneous goals, etc, and corresponding CFP (HEP) will be calculated as an input to the MTU agent. In this research work, only four CPCs are assessed and five CPCs are assumed to be fixed without further assessment due to limited data sources, which will affect the accuracy of output (HEP) of this model.

4.4 Implementation of Hybrid Modeling/Simulation Approach

To meet the second challenge of in-depth analysis, i.e., simulating interdependencies within and among CIs, a hybrid modeling/simulation approach has been briefly introduced in section 4.1. How to implement such a hybrid approach will be presented in this section.

4.4.1 HLA Simulation Standard (state of the art)

While currently no standards exist specifically for addressing cross sector (infrastructure) modeling, several standards do exist for exchanging information between distributed simulations [55, 103]. Among these standards are the two best known and widely accepted frameworks: *HLA* (High Level Architecture) and *Distributed Interactive Simulation* (DIS). HLA is a standard framework that supports simulations composed of various simulation components [104]. It was developed originally by the US Department of National Defense with the goal of incorporating interoperability, modularity, and reusability into ambitious long-term simulation objectives [105]. DIS, defined in IEEE standard 1278, is another framework for linking real-time distributed simulations. The purpose of DIS is to create real-time, synthetic, and virtual representations of warfare environments by interconnecting separate simulators [103]. The interconnection between different simulations in a DIS platform is achieved by broadcasting Protocol Data Units (PDUs) through User Datagram Protocol (UDP). Both HLA and DIS standard support the integration of real-time simulation models and data exchange between various computing environments. However, there are two major weaknesses in DIS. One weakness lies in the fact that the communication protocol UDP used by DIS is a simple data transmission technique without implicit hand-shaking dialogues for guaranteeing reliability, ordering, or data integrity. Because of this shortcoming the information transmission between simulators/models on a DIS-based simulation platform becomes unreliable. The second weakness of DIS is its incapability of supporting event driven and faster (than real-time) applications [55]. Simulating interconnections between individual domain-specific simulators requires an explicitly precise / flexible time management and reliable data communication environment. For instance, in some cases, simulation time needs to be set much faster (than real time) in order to obtain the results more efficiently. Therefore, the inherent weaknesses of the DIS potentially limit its capability to implement a more secure and efficient distributed simulation environment.

HLA baseline definition was completed in 1996. In 1998, the first complete HLA interface specification was released to the public [106]. In 2000, HLA was approved as an open standard by the organization of the Institute of Electrical and Electronic Engineers: IEEE Standard 1516-2000 [107]. Since then, the HLA standard has been revised and improved.

The most current one is HLA-Evolved. One distinguished advantage compared to other simulation standards offered by HLA for the simulation industry is its support of live participants, meaning that the representation of the live world such as a human being, a real process instrumentation device or a controller, etc., can be integrated into the simulation world. Moreover, it is also capable to project data from the simulation world back into the real world [106]. A functional view of the HLA is given in Figure 4.19.

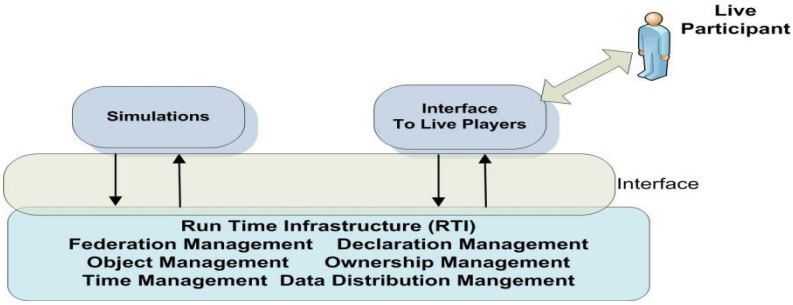


Figure 4.19 Functional view of the HLA standard [108]

State of the Art

As an open IEEE standard, HLA has been widely adopted across various fields of the simulation industry during the last decade. The EPOCHS (Electric Power and Communication Synchronizing Simulator) is an early attempt to distribute several individual simulators by adopting the standard of HLA, which utilizes multiple research and commercial systems from various domains [109, 110]. An HLA-based system for geo-computation in a grid environment was designed and developed at Inha University of Korea for the purpose of CDM (Communication Data and Management) performance evaluation [111]. Computer experiments conducted by Lees and Logan show that "*the overall simulations have been sped up after distributing simulation components based on the standard of HLA*" [112]. Similar results are also observed by Zhao while working on an agent framework for controlling activity flows between the ISS (Interactive Simulation Systems) components [113]. Furthermore, HLA has been applied to other industry fields such as the U.S. border operation study [114], rail traffic safety system simulation [115], and many others [116-118].

The option of adopting HLA for the CI interdependency study has also been discussed during recent years. In 2007, HLA is one of several interface solutions to be considered for

trying to connect several individual simulators to study interdependencies between heterogeneous interconnected CIs [119]. In 2009, a communication middleware serving other distributed CI simulators was proposed by a team in a EU research project "Design of an Interoperable European federated Simulation network for critical Infrastructures (DIESIS)" [103]. This middleware, adapted from the HLA standard, aims to provide a reliable one-to-one real-time communication platform for diverse simulators over the WAN (Wide Area Network).

Generally, HLA consists of three essential elements:

1) **Federate/Federation rules :**

   Defined by the HLA standard, each distributed component is referred to as a federate and the collection of federates that comprise a simulation is referred to as the federation. A set of 10 HLA rules that the federation and all participant federates must follow, are defined by the standard IEEE1516-2000 to be considered as HLA compliant. These rules can be grouped into a set of 5 rules for HLA federates and 5 rules for the federation, both shown in Table 4.25.

2) **Object Model Template (OMT):**

   All objects and interactions implemented by a federate should be visible to all other participant federates across the federation, if necessary, to guarantee the interoperability between federates. Therefore, they must be specified in detail with a common format. OMT provides a standard for declaring corresponding information of two HLA object models: the HLA Federate Object Model (FOM) and the HLA Simulate Object Model (SOM). FOM describes the set of objects, attributes and interactions shared by all federates under one federation. SOM describes all objects, attributes, and interactions that one federate can offer. One federation only requires one FOM and each federate must have one SOM.

3) **Interface specification :**

   The HLA interface specification identifies how federates interact with the federation, as well as with each other and is implemented by RTI (Run Time

Infrastructure) during the federation execution. The HLA interface specification defines runtime services provided to federates by the RTI, and by federates to RTI.

Table 4.25 Federate / Federation rules [107]

Federation Rules		**Federate Rules**	
Rule	**Rule Description**	**Rule**	**Rule Description**
1	Federations shall have an HLA FOM, documented in accordance with the HLA OMT.	6	Federates shall have an HLA SOM, documented in accordance with the HLA OMT.
2	In a federation, all simulation-associated object instance representation shall be in the federates, not in the RTI.	7	Federates shall be able to update and/or reflect any instance attributes and send and/or receive interactions, as specified in their SOMs.
3	During a federation execution, all exchange of FOM data among joined federates shall occur via the RTI.	8	Federates shall be able to transfer and/or accept ownership of instance attributes dynamically during a federation execution, as specified in their SOMs.
4	During a federation execution, joined federates shall interact with the RTI in accordance with the HLA interface specification.	9	Federates shall be able to vary the conditions (e.g., thresholds) under which they provide updates of instance attributes, as specified in their SOMs.
5	During a federation execution, an instance attribute shall be owned by at most one joined federate at any given time.	10	Federates shall be able to manage local time in a way that will allow them to coordinate data exchange with other members of a federation.

4.4.2 Run Time Infrastructure (RTI)

While HLA is architecture, a simulation standard but not software, RTI is the software. It is the core element of the HLA standard providing common services to all federates. Interactions between federates in a federation, as well as between federates and federation, are all accomplished via RTI. Generally, RTI consists of three major components, shown in Figure 4.20 [105].

- RtiExec: a global known process that manages the creation and destruction of federation execution.

- FedExec: a federate-based process that manages federates joining into and resigning from the federation.
- LibRTI: a C++ or Java library that provides all RTI services for developers, defined by the HLA interface specification.

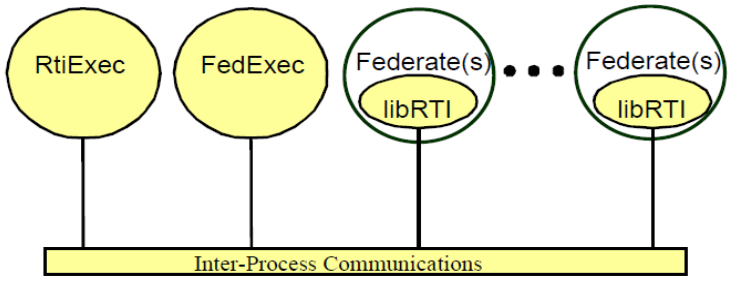


Figure 4.20 Three major RTI components [105]

Major interplays between a federate and its joined federation, defined by the HLA interface specification and implemented by RTI, are shown in Figure 4.21. If a federate attempts to join an existing federation and become a participant federate, a "join" request must be sent to the federation. After receiving the approval response from the federation, it becomes a participant federate and must publish/subscribe corresponding object and interaction classes. Specified by the HLA standard, both object class and interaction class can be used to define a possible empty set of named data, which are called *attribute* and *parameter* respectively. The purpose of these two classes, which are also called HLA-related classes, is to store the data that will be transmitted between federates. The only difference between the two classes is that the interaction class will be destroyed after its contained data has been received[15]. While the purpose of publishing HLA-related classes by a federate is to inform other federate(s) possible updates from these classes, the purpose of subscribing HLA-related classes by a federate is to inform other federate(s)

[15] HLA standard does not describe which class should be implemented during the simulation development, which is a developer's task to decide according to simulation requirements. It is possible that both classes are implemented or only one class is implemented, in one federate.

what classes it (federate) would like to receive updates from. During the simulation, whenever published HLA-related classes of the federate are updated, the updated data will be broadcasted to all available federates across the federation. However, only federates who have previously subscribed these classes will be able to receive the updated data. If the federate attempts to quit the joined federation, all its owned HLA-related classes must be deleted/removed from the federation before sending a "resign" request to the federation. As soon as this request is received by the federation, the federate will then be removed from the federation. Although there are many other important federate-federation interplays such as federate time synchronization, time management, HLA-related classes ownership management, etc., they all belong to advanced topics of the HLA standard and are not subjects of this research work.

Developing RTI software is a complicated and tedious task. For example, it took several software engineers about three years to complete the first public version of a RTI software tool, which is called Portico RTI. Therefore, developing own RTI software is not recommended. A list of ready-to-use RTI software tools is shown and compared in Table 4.26. A list of URLs for further information on these tools can also be found below:

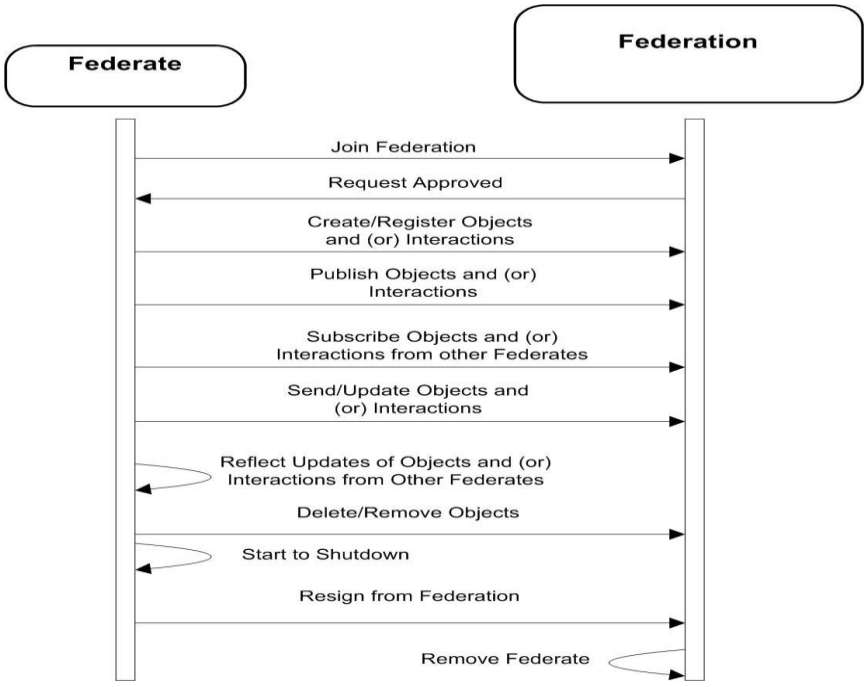


Figure 4.21 Major Federate-Federation interplays (Adapted from [105], modified by the author)

Table 4.26 Comparison of several RTI software tools

	Pitch pRTI™	**MÄK RTI™**	**Portico RTI**	**CERTI**
Type	Commercial	Commercial	Open (Free)	Open (Free)
Supported HLA Standard(s)	HLA 1.3 , IEEE (HLA) 1516, HLA Evolved	HLA 1.3 , IEEE (HLA)1516, HLA Evolved	HLA 1.3	HLA 1.3
libRTI Language	C++, Java	C++	C++, Java	C++
Software Support ?	Yes	Yes	No	No
Console Interface Included ?	Yes	Yes	No	No
Maxim Number of Federates Supported	> 10	>10	Limited	Limited
Continuous Developments ?	Yes	Yes	NO	Yes
Web Communication Supported ?	Yes	Yes	NO	NO

Pitch pRTI™ : www.pitch.se (2010)

MÄK RTI™: www.mak.com (2009)

Portico RTI: http://porticoproject.org (2010)

CERTI: http://savannah.nongnu.org/projects/certi/ (2010)

4.4.3 Recommended Work Steps

The implementation of the hybrid modeling/simulation approach by adopting the HLA simulation standard can be divided into the following steps :

- **Step 1: Feasibility study**
  Not all simulation components are able to be distributed, especially for the components representing subsystems of a system. A "pre-screening" investigation is highly recommended before considering distributed simulation as an option. Whether or not distributing simulation components, which means breaking down their interlinked functions, will affect the final outcomes of the overall simulation is the main concern. The feasibility of distributing simulation components, especially

when modeling multiple subsystems existing under one system, should be carefully studied and verified.

- **Step 2: RTI software tool selection**
  The following questions can be used to steer the decision on which RTI software tool should be selected:
    - Which HLA standard is required or preferred by the developers?
    - What is the major programming language for developing distributed components (e.g., Java or C++)?
    - How many federates are planned to be developed?
    - Is web-supported RTI software tool required for the development?
    - Is it necessary to reuse any existing simulators?
    - Is RTI software support from vendor necessary?

- **Step 3: Object/Interaction class definition**
  For a federate, it is important to determine which variables will be updated and which will be of interest for other peer federates. Then, HLA related classes (object/interaction class) can be precisely defined and implemented, which is an essential step for the FOM definition.

- **Step 4: Local RTI interface development**
  After the RTI software has been selected, the local RTI interface that contains the classes and methods used to connect to the federation must be implemented for each federate. All HLA-related functions that are responsible to exchange data between federates are conducted by the local RTI interface. As part of the federate, the local RTI interface should be developed in the same programming language used to develop the federate. Implementing the local RTI interface for a previously non-HLA-compliant simulation component needs to be conducted carefully, since any mistake during the modification could result in the failure of the whole component.

- **Step 5: Simulation tuning**

Simulation tuning is the last step to implement the HLA-compliant simulation platform, which will help to improve the efficiency and accuracy of the overall simulation. Several capabilities such as simulation interoperability, time synchronization and data exchange rate, provided by the HLA standard can be studied and then improved by modifying the corresponding simulation parameters to optimize the simulation performance.

4.4.4 Drawbacks of the Hybrid Modeling/Simulation Approach

The major drawbacks of the implementation of the hybrid modeling/simulation approach using the HLA simulation standard are:

- **Significant increases of resources and time during implementation**
  Resources and time required to implement an HLA-compliant simulation platform could be significant comparing to non-HLA-compliant simulation platforms. This is mainly caused by the development of a local RTI interface component for each federate.
- **Update latency**
  Update latency, which means the interval between sending an update by one federate and receiving this update by another federate, could be significant enough to affect the outcomes of real-time simulation. It should be noted that negative effects of this drawback can be alleviated by improving/upgrading the hardware environment of the simulation platform such as by using computers equipped with a better CPU.
- **Not a "plug-and-play" standard**
  All HLA-related (object and interaction) classes must be declared in advance before the simulation. As a consequence, adding or even modifying these classes becomes impossible during the simulation.
- **Incompatibility between HLA standards**
  An example of this drawback is that a federate developed based on the standard of HLA 1.3 is not able to join the federation developed based on the standard of HLA1516, unless being upgraded to HLA1516; this means that any future changes to the HLA standard may have significant impact on local implementations.

Although the HLA simulation standard has these drawbacks and has been questioned regarding its feasibility in the research field of CI interdependency study, it is still a most applicable and feasible standard for the implementation of the hybrid modeling/simulation approach.

4.5 HLA-compliant Experimental Simulation Test-bed

4.5.1 Architecture of Test-bed

An HLA-compliant experimental simulation test-bed has been developed, which integrates the SCADA model and SUC model into one simulation platform in order to investigate interdependency-related vulnerability between these two systems. The test-bed consists of four major components: SUC model, SCADA model, RTI server, and a simulation monitor system, shown in Figure 4.22. All these components are connected over one Local Area Network (LAN).

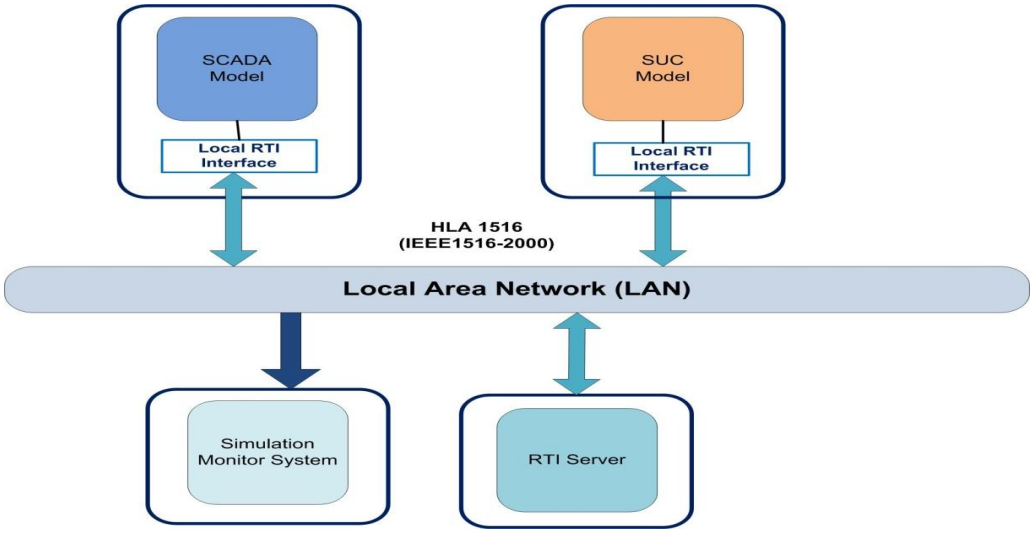


Figure 4.22 Architecture of experimental simulation test-bed

- **The SCADA model:** An event-driven, agent-based model, which is developed on the software platform of Anylogic 6.4 (for more details see section 4.2).
- **The SUC model:** A time-stepped, agent-based model, which is developed on the software platform of Anylogic 5.5. Originally, as discussed in section 3.2.3.2, the

aim of this model was to investigate various system operating situations, which could potentially result in a blackout of the Swiss electricity power transmission network [6]. The SUC model simulates electricity power system scenarios in a continuous time by means of conventional techniques such as power flow calculations. The agents are used to model both technical components such as generators, and non-technical components such as grid operators. Each agent is represented by its attributes, e.g., physical constraints on technical components such as thermal limits of transmission lines, and by rules of behavior, which include both deterministic and stochastic time-dependent processes. Since it was previously designed as a stand-alone model, no inputs from external simulators have been specified. Further technical details regarding this simulator are given in [75].To include this model in the experimental test-bed, a Java-based independent HLA-compliant interface is developed, which is responsible to process all inputs (outputs) to (from) the model.

- **The RTI server:** It acts as the centre of the experimental test-bed. This component is responsible for simulation synchronization and communication routing between all components, through the local RTI interface of each model. The RTI server is a globally known component. Each federate communicates with this server via its own local RTI interface and starts to follow central federation management.
- **Simulation Monitor System**: The simulation of two models can be observed using a real-time monitor system. The outlook of this monitor system is shown in Figure 4.23. Each green line in this figure represents a simulated transmission line from the SUC model and each red circle represents a simulated RTU from the SCADA model [16].

[16] In this research work, it is assumed that each substation contains one RTU only

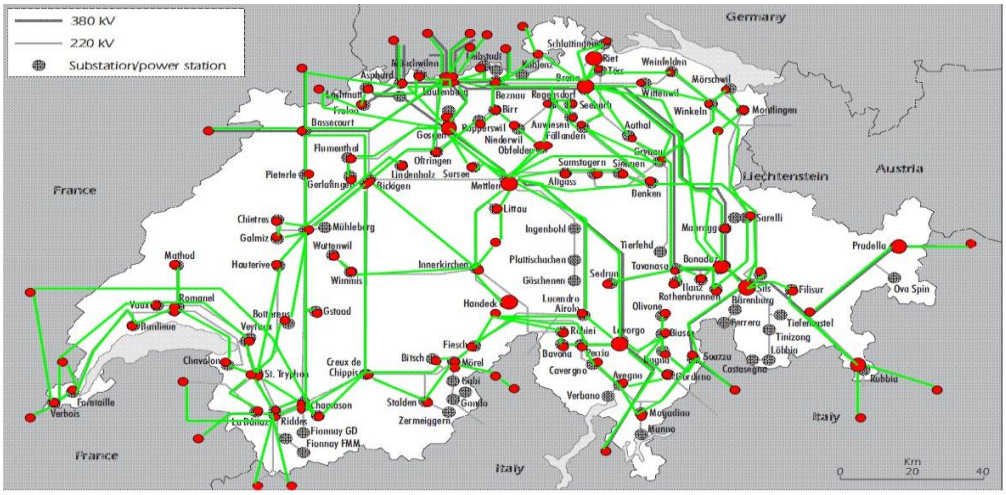


Figure 4.23 The outlook of the simulation monitor system

4.5.2 Test-bed Development

The HLA-compliant experimental simulation test-bed has been developed following the five steps introduced in section 4.4.3.

- **Step 1: Feasibility study**
  The main purpose of the SCADA subsystem for the SUC subsystem within power supply CI sub-sector is to allow an operator or user to collect data from distant substations and send control commands in case of detection of deviations from normal working conditions. Interlinked functions, meaning the functions that involve both systems, are present due to the functional interconnections between them. Distributing these two simulation components, representing the corresponding systems, indicates that all interlinked functions must be disconnected first. They will be re-connected via interfaces after all (see Figure 4.22). It is very important to ensure that the decomposition of the interlinked functions will not affect the accuracy of the overall simulation results. The information exchange between SCADA and SUC is conducted through two major coupling functions: control and monitor. The monitor function should be easily broken down due to the fact that the data/information from SUC is acquired only by SCADA. It is a function with only one direction: from SUC to SCADA. Decomposing this function does not affect the

performance of the overall system simulation. The control function is a bi-directional function and requires careful study. Functionally, the control function is implemented by two types of process control systems: Basic Process Control System (BPCS) and Safety System (SS), illustrated in Figure 4.24.BPCS represents basic control systems installed in most field devices such as level, flow, and pressure control system. It is an active system and operates at all times to maintain a normal working environment. SS can be considered as a passive system and acts like a safety guard of operating processes. Disconnection of the control function needs to assume that BPCS remains in the SUC, and SS belongs to SCADA system. This is because the function of BPCS is mainly automatically carried out by a locally controlled field device. The SS requires the data input from SUC, which can be obtained by the monitor function. Therefore, the control function can also be considered as one direction function: from SCADA to SUC, and decomposing this (discrete event)function does not affect the performance of the overall system simulation.

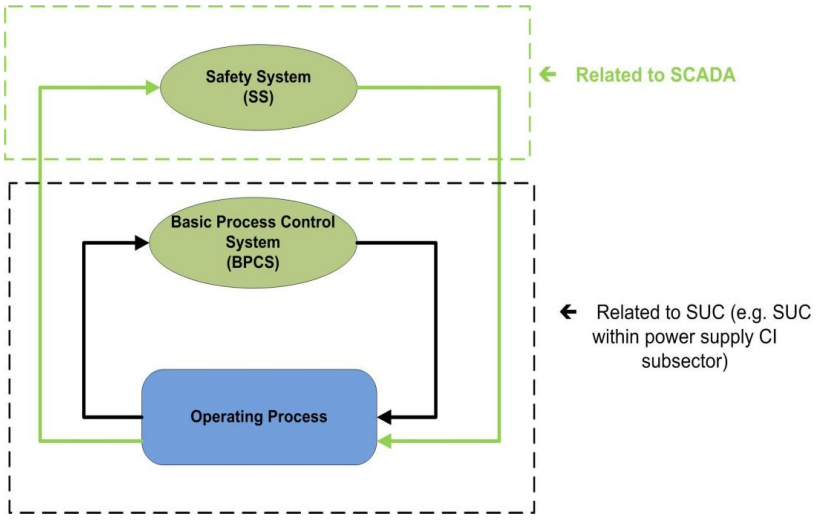


Figure 4.24 Two types of process control system: BPCS and SS

- **Step 2: RTI software tool selection**

  In order to choose an appropriate RTI software tool, the list of questions introduced in the previous section has been studied with answers shown in Table 4.27. The

selected software tool pRTI™[17] from Pitch Technology is the leading HLA run time infrastructure for the international IEEE 1516 standard, certified by DMSO in 2003, and is now used by thousands of customers in major high-tech companies all over the world.

Table 4.27 Answers for RTI software tool selection investigation

Question	**Answer**
Which HLA standard is required or preferred for developers ?	*HLA 1516 is the preferred HLA standard by all developers*
What is the major programming language developing models of distributed components ?	*Anylogic, a java based model development software, is the major development tool in this project*
How many federates are planned to be developed ?	*Two (this number will grow in the future)*
Is the web-supported RTI software required for the development ?	No, but a web-supported RTI software is preferred by all developers
Is it necessary to reuse any existing simulators ?	Yes, one non-HLA-compliant model (SUC) must be used
Is RTI software support from vendor necessary ?	Yes, it is very important to have continuous support for RTI software

- **Step 3: Object/Interaction class definition**
  Distributed simulation components should be capable of representing interconnections between the two studied systems. An example of this type of interconnection is that the SCADA system requires the measured process

[17] More information regarding pRTI™ and Pitch Technology can be found from www.pitch.se.

variable, which is the output of the SUC, and on the other hand, the SUC requires the most recent operating status of the field control device, which is the output of the SCADA system. Descriptions of several object classes already defined in this simulation development are shown in Table 4.28.

Table 4.28 Descriptions of several object definitions

			Federate (Simulator)	
Object	**Attribute**	**Type**	**SCADA**	**SUC**
Transmission Line	*measured Variable*	Double	subscribe	publish
	status Variable	Boolean	publish	subscribe
	control Command	Integer	publish	subscribe

- **Step 4: Local RTI interface development**

  Local RTI interface can be implemented by inheriting and modifying corresponding classes and methods from the RTI software tool pRTI™. Since the SUC model was previously designed as a stand-alone model, no inputs from external simulators were specified. To integrate this model into the test-bed, it has been revised as HLA-compliant by adding an independent local RTI interface without any modification to the model.

- **Step 5: Simulation tuning**

  After completing the development of local interfaces, the performance of overall simulation needs to be verified and optimized before conducting further experiments. For example, it is very important to ensure that the data exchange among distributed simulation components is reliable meaning that there should be no data lost during the simulation. Some (simulation standard) software tools provide user interfaces which can be used to adjust various simulation parameters such as the maximum size of each exchanged message, maximum buffer sizes, etc. More details regarding the simulation tuning will be presented in the next sections.

4.5.3 RTI Performance Experiment

Data exchange rate, as a result of RTI performance, is one of major concerns if multiple simulation components are included in one simulation tool and need to communicate with each other. To achieve more accurate simulation results, it is essential to have a reliable tool that is able to continuously handle large numbers of data exchanges. Therefore, a specific experiment was developed and simulators with different configurations were included in the experiment. The main purpose of this experiment is to investigate how fast the data exchange rate can be and how hardware configuration of the simulator can affect the performance of overall simulation. In this experiment, the numerical test dataset is continuously generated by the SUC model and sent to the SCADA model though its HLA-compliant interface. An extra statistic function in the SCADA model, specifically implemented for this experiment, is responsible for collecting the test dataset sent by the SUC model and calculate its updating rate (how many datasets the interface simulator receives at each second).

In order to examine the effect of hardware configuration on the performance of the overall simulation, this experiment will be performed three times while different computers are used to install the SUC model; Table 4.29 shows the summary of this experimental environment and differing hardware configurations. Configuration 3, equipped with Intel core quad 3 GHz CPU, turned out to be better than other configurations.

Table 4.29 Summary of RTI performance experiment

Summary of Simulation Environment for RTI Performance Experiment	
Number of Models	2 (SUC and SCADA model)
Network Configuration	LAN(100M)
Exchange Dataset Type	String
Simulation Speed	160X
Hardware Configuration for Interface Simulator	Computer equipped with CPU: Intel Core Quad 3 GHz
Hardware Configurations for SUC model at each experiment conduction	**Configuration 1**: Computer equipped with CPU: Intel Pentium™ 4 , 1.80 GHz **Configuration 2**: Computer equipped with CPU: Intel

	T2500 , 2 GHz **Configuration 3**: Computer equipped with CPU: Intel Core Quad 3 GHz

The results collected from this experiment are shown in Figure 4.25 and summarized in Table 4.30, where the average and maximum updating rate of the numerical test dataset received by the SCADA model is recorded and displayed. As shown in this figure, the average updating rate varies at each conduction of the experiment. For example, the numerical test dataset is updated 50 times per second (in average) when the SUC model is installed on the computer with hardware configuration 1 during the first experiment conduction while the numerical test dataset is updated 179 times per second on average when SUC model is installed on the computer with hardware configuration 3 during the third experiment conduction. This can be explained by better performance of hardware configuration 3 (with better CPU). As discussed before, the dataset exchanging through different simulators in this HLA-compliant simulation test-bed is all conducted by the central RTI component. Therefore, it is understandable that the simulator hardware configuration plays an important role in order to achieve more efficient simulation performance through the central RTI component. The maximum test dataset updating rate, observed during the third experiment conduction, is about 226 times per second and can be considered as a reasonable number for future simulation needs.

Table 4.30 Summarized simulation result of RTI performance experiment

Experiment Conduction Number	**Average Updating Rate (updates/second)**	**Maximum Updating Rate (updates/second)**
1	50	63
2	115	138
3	179	226

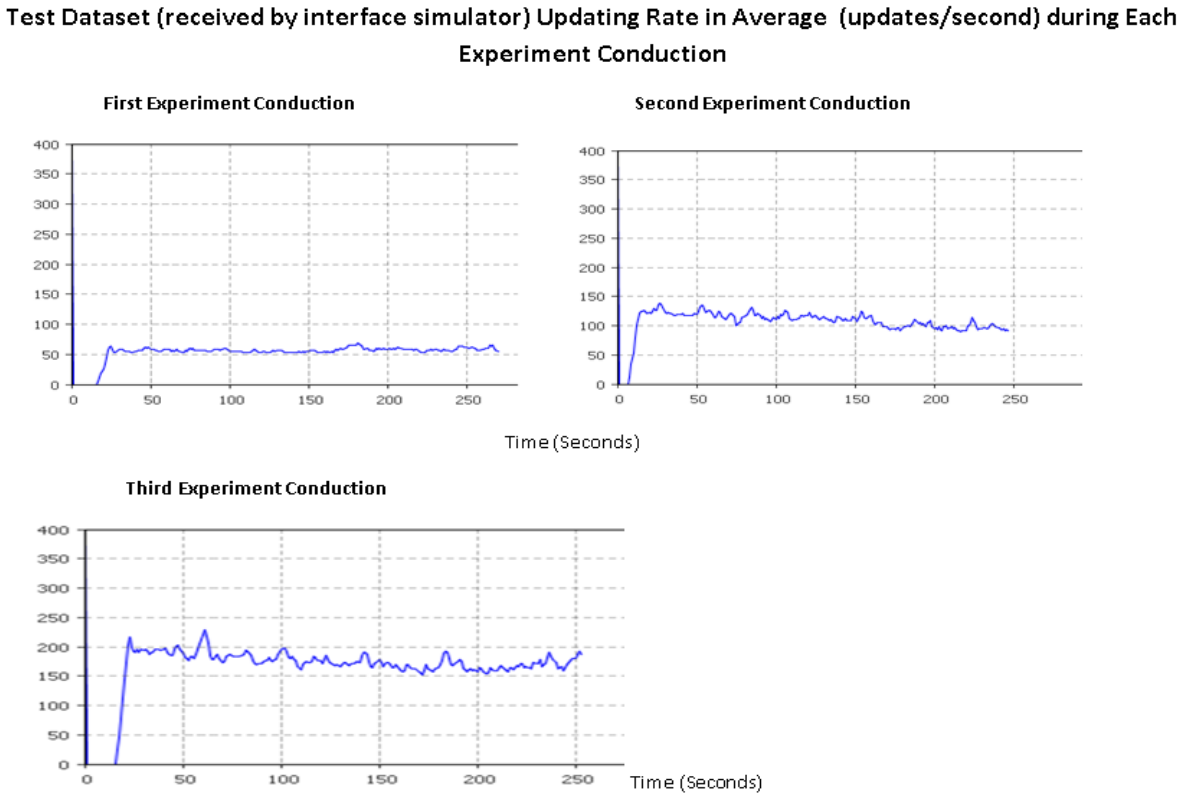


Figure 4.25 Simulation results of RTI performance experiment

4.5.4 Time Regulation/ Synchronization of the Test-bed

Although time always moves forward during the simulation, the perception of "current time" might differ among participating simulators. Therefore, the issue of regulation/synchronization should be addressed, especially for "time-stepped" distributed simulation components. Within one distributed simulation environment (which can also be referred as one federation), each federated component (referred as a federate) may join the simulation at a different time. It is normal that the "starting time" of one federate might be different compared with another federate. When all federates have joined the federation, each federate follow its own "time" to advance the simulation. After a certain simulation period, the variation between "current time" of different federates might be significant and therefore, affects the final simulation results.

In order to minimize the synchronization issue of the simulation based on the HLA standard, RTI 1.3 specification provides functions and mechanisms such as a time management policy for synchronizing activities between federates participating in one federation, which have been included in the selected RTI software tool. However, implementing most of these functions and mechanisms into the current experimental test-bed is extremely time-consuming and requires computer hardware with better performance. Moreover, it slows down the speed of the overall simulation. Therefore, a simplified and more efficient time management approach has been developed to ensure the time synchronization between federates.

First, one *regulating federate* (RF) needs to be selected, which should be the first joined federate, and made responsible for regulating all other *following federates* (FF). It should be noted that there are no specific requirements for the selection of the RF. However, it is very important that the RF is a "time stepped" federate. For example, in the current experimental test-bed, the SUC model is selected as the RF and SCADA model is selected as the FF. The "current time" of the RF is used as the *Federation Virtual Time* (FVT). The RF joins the federation and declares an initial synchronization point in the federation. Then, this federate pauses its simulation until all other FFs join the federation and recognize the initial synchronization point. When all federates recognize the synchronization point, the "current time" of the RF is defined as starting point of the FVT and shared by all participant federates. At this moment, all FFs start to calculate the simulation time variation rate according to the current time of the RF. For example, if a FF runs faster than a RF, then its simulation time variation rate should be larger than 1, otherwise smaller than 1. The "current time" of the RF is continuously updated to all FFs and the value of simulation time variation rate is continuously re-calculated. Based on the value of the simulation time variation rate, the value of the current FVT can be continuously estimated by each FF. Instead of using real local simulation time, all time related functions/parameters implemented by each FF adopt FVT as standard local simulation time. Therefore, all federates participating in one federation begin to advance their own simulation at a synchronized time step and activities between federates can be considered as synchronized.

This simplified time management approach is straightforward and easy to implement. It combines the functions of synchronization point declaration/reorganization provided by the

RTI software tool with the user-defined time sharing functions and improves the efficiency of the overall simulation. However, the accuracy of value of the simulation time variation rate is affected by several factors such as the updating rate of the "current time" of the RF and the performance of the local area network that is used to send the updated RF "current time".

4.6 Validating the Hybrid Modeling/Simulation Approach

To demonstrate the capabilities of the hybrid modeling/simulation approach, as well as the developed test-bed, for investigating and representing interdependencies within and among CIs, several experiments have been designed and developed including feasibility and failure propagation experiments.

4.6.1 Feasibility Experiment

The purpose of this experiment is to study the feasibility of the HLA-compliant distributed simulation environment as an approach to simulate interdependencies. Both SCADA model and SUC model of the test-bed are used in this experiment. In order to be able to visualize the interdependency phenomena between SCADA and SUC, the scenarios that will trigger power line overload alarm are generated manually during the simulation.

Generally, the maximum load each power transmission line can carry has been previously determined by its vendor and is called *overload threshold*. If the real power flowing through a transmission line exceeds its overload threshold, this line is considered to become overloaded. An accidentally overloaded transmission line could cause a system collapse (partial or even complete blackouts). Therefore, suitable corrective actions should be taken in order to alleviate the overloaded transmission lines. Normally, whenever a monitored transmission line is overloaded, an alarm will be generated and sent to the operator in the control centre (MTU) by the RTU of the SCADA system. If, after a certain period, the operator fails to react to the overload alarm, then the protection devices such as disconnectors (example of FCD) will automatically disconnect the overloaded transmission line in order to minimize the negative consequence of the problem. It should be noted that the procedure for handling a power line overload alarm is complicated and

that other factors should also be considered. In order to simplify this problem, it is assumed that the overload alarm failed to be handled correctly only if the operator fails to react to the alarm in time and the protection device fails to trigger. In this experiment, it is assumed that the overload threshold of the selected transmission line (line i) is 139.5MW[18]. Three case study scenarios are developed by modifying parameters of corresponding agents in order to observe three different outcomes after the occurrence of the transmission line overload.

Case Study 1: Neither operator nor protection device react

In this case study, it is assumed that the operator fails to react to the detected overload alarm before timeout and the protection device fails to disconnect the overloaded transmission line. The observed simulation result is illustrated in Figure 4.26. Line (i) is the overloaded transmission line and line (j) is another transmission line, which is directly connected to line (i). As shown in this figure, line (i) becomes overloaded when the power load exceeds the overload threshold. Since both simulated operator and protection device in the SCADA model have been configured to not respond to the power overload alarm, no correcting actions will be performed. Therefore, the overloading amount in line (i) keeps increasing. As a consequence, the transmission line overloading continues to propagate. For example, the amount of power transmitted in line (j) also increases from 240 MW to 258 MW, which could possibly cause this line to become overloaded and trigger more service interruptions.

[18] In this experiment, the overload threshold value of line (i) has been modified to 139.5MW from the value of reference system (SUC of Swiss electric power transmission system) for the purpose of security and experiment simplification.

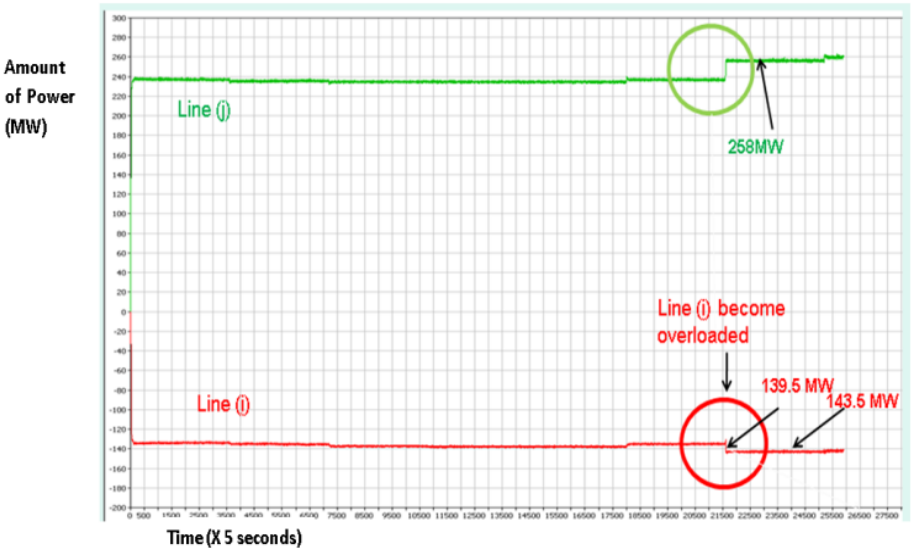


Figure 4.26 The observed simulation result from case study 1

Case Study 2: Operator reacts to the alarm

In this case study, it is assumed that the operator reacts to the detected overload alarm before timeout and takes corrective actions successfully. The observed simulation result is shown in Figure 4.27. Compared to the result from case study 1, the amount of power transmitted in line (i) starts to drop to 108 MW after becoming overloaded. This is because the simulated operator in the SCADA model receives the alarm sent by the SUC model and sends the commands for corrective actions back successfully before timeout (MTOR). It should be noted that the sign of amount of power changes for the power flow in line (i) from negative to positive. This is due to the change of the direction the power flow in line (i). As the consequence, the amount of power transmitted in line(j) is also affected by the power drop of line(i).

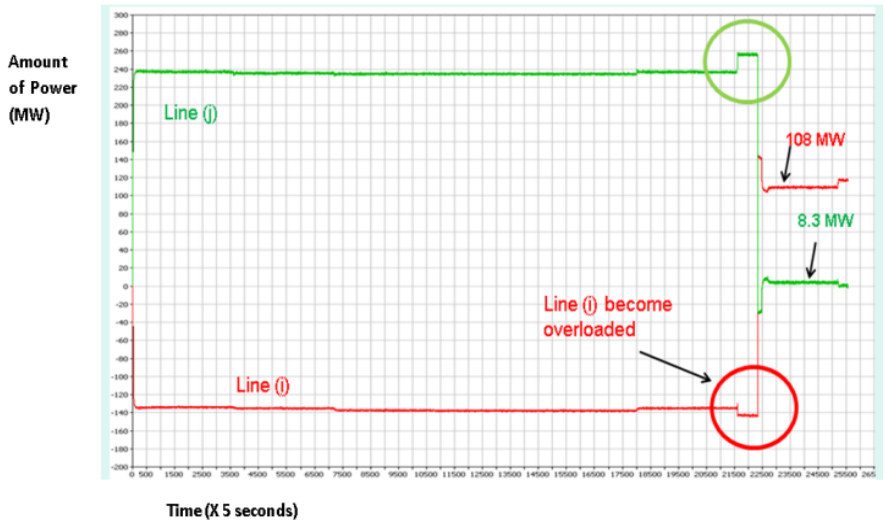


Figure 4.27 The observed simulation result from case study 2

Case Study 3: The protection device is triggered after operator fails to react to alarm

In this case study, it is assumed that the protection device is triggered and disconnects the overloaded transmission line successfully after the operator fails to react to the detected overload alarm before timeout. The observed simulation result is shown in Figure 4.28. Compared to the results from case study 1 and 2, the amount of power transmitted in line (i) drops to 0 MW after becoming overloaded due to the shutdown of line(i) by the protection device.

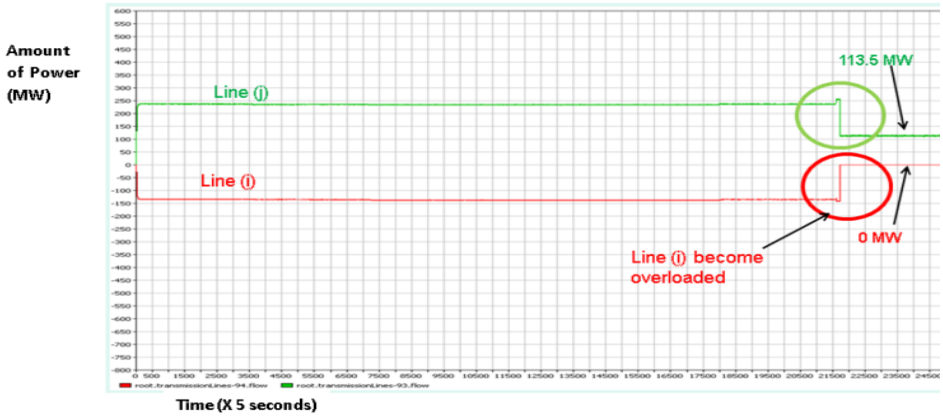


Figure 4.28 The observed simulation result from case study 3

Summary of the Feasibility Experiment

The observed simulation results from three case studies, summarized in Table 4.31, show that the propagation of cascading failures between infrastructure systems due to interdependencies can be simulated and visualized with the help of the experimental test-bed. Although the simulators are distributed, overall simulation performance is not affected and interconnections between simulators can still be efficiently handled.

Table 4.31 Summarized simulation results of the feasibility experiment

Case Study	Failure of the operator to react	Failure of the protection device	Observed results
1	Yes	Yes	Power of interconnected line (j) starts to increase
2	No	N/A*	Power of overloaded line(i) starts to drop
3	Yes	NO	Power of overloaded line(i) drops to zero

4.6.2 Failure Propagation Experiment

Failures occurring in subsystem(s) of one CI could propagate into other subsystem(s) within one CI or even other CIs due to the existence of interdependencies. To study this phenomenon and related issues, an experiment mainly focusing on the investigation into the consequences of failure propagation between the SCADA system and the SUC, has been developed and conducted. In this experiment, the FID agent represents a power flow transducer (PT_i) measuring power flow (in unit of MW) transmitted in a selected transmission line ($Line_i$) that is represented by the SUC model. It is assumed that the PT_i is calibrated incorrectly due to aging of part of the PT_i, which can be considered as an example of technical failure. Table 4.32 shows a list of sequential events after the incorrect modification of the PT_i's calibration value recorded by the SOE table of the DB_SCADA database during the simulation. As shown in the table, at time 52.43 seconds, the PT_i's calibration is modified incorrectly. As a consequence, the output of the PT_i is more than its measured variable value should be. According to this wrong value, the RTU generates a

wrong overloading alarm and sends it to the MTU inducing the operator in the control room to make a wrong decision, i.e., to redistribute the power flow of the transmission $Line_i$. As the result, the amount of power transmitted in $Line_i$ decreases, although it should not. The measured variable from PT_i , as part of the SUC, acts as physical input into the SCADA system. This relationship can be considered as the **physical interdependency**, which causes the failure of PT_i to propagate from the SUC to the SCADA system and go back to the SUC.

Table 4.32 Sequential events after incorrect calibration modification of $\mathrm{PT_i}$

Stamped Time	**Events**
52.43	Line(i)'s FID calibration has been modified, offset is + 9.67 (FID)
140	Line(i) is overloaded and a warning has been generated (FID)
156.09	RTU has generated an alarm and sent it to MTU (RTU)
174.85	Operator recognizes the alarm (MTU)
183.24	Operator reacts correctly and distributing algorithm will be taken (MTU)
212.31	Command has been processed by operator successfully, redistribution command sent out (MTU)
223.05	Power flow of line(i) decreases (SUC model)

According to investigation results, collected and analyzed based on both feasibility and failure propagation experiments, it can be concluded that three types of interdependencies can be simulated using the current experimental simulation test-bed: physical, cyber, and geographical interdependency. Logic interdependency is not considered during these experiments since it is not included in this research work.

4.7 Summary

Generally, the in-depth analysis for the investigation of interdependency-related vulnerabilities faces two major challenges. The first challenge is to model a single infrastructure system due to its complex characteristics. The second challenge appears when more than one infrastructure systems must be considered and interdependencies among them need to be tackled. To find a promising solution for solving these challenges, a novel hybrid modeling/simulation approach is proposed and developed in this chapter, which combines various simulation/modeling techniques by adopting the technology of the distributed simulation and the concept of modular design for the purposes of exploring and assessing the vulnerabilities due to these interdependencies.This approach can be considered as a successor of the traditional modeling/simulation approach in case multiple systems need to be simulated simultaneously. An experimental simulation test-bed has been developed demonstrating the capability and feasibility of this test-bed, as well as of the hybrid modelling/simulation approach, through feasibility and failure propagation experiments. To further investigate interdependencies between the SCADA system and the SUC, several analytical experiments have been designed and conducted, which will be presented in next chapter.

5 DESIGN OF EXPERIMENTS

Three experiments are developed for the investigation of interdependency-related vulnerability between the SCADA system and the SUC, all performed on the HLA-compliant experimental simulation test-bed.

- **Experiment I-Substation level single failure mode experiment**: This experiment is designed and conducted to evaluate different failure modes of each substation level component (FID, FCD, and RTU). The aim of this experiment is to determine the severity of negative effects of each failure mode on the service unavailability of a substation according to the analysis of collected simulation results.
- **Experiment II-Small network level single failure mode experiment:** This experiment expands the scope of the first experiment from a substation to a small network. More substations and transmission lines (40 substations and 50 transmission lines) are included in this experiment. Different failure modes of each substation level components are triggered during the experiment. Compared to the first experiment, interdependencies between the SCADA system and associated SUC are considered instead of the consideration of dependency from the SCADA system to the SUC only. The aim of this experiment is to identify the failure modes/devices that can cause more negative effects due to interdependencies between both studied systems. It should be noted that this experiment is based on the assumption that all substations are homogenous meaning that the structure and devices included in each substation are the same.
- **Experiment III-Whole network worse-case failure modes experiment:** This experiment extends the scope of the experiment to the whole network including all

simulated components of the SCADA system and the SUC (149 substations and 219 transmission lines). The aim of this experiment is to simulate the worse-case scenarios[19] for the whole network in which negative consequences caused by interdependencies between the SCADA system and the SUC can be observed and analyzed. In this experiment, not only single failure modes are simulated, double failure modes occurring simultaneously are also considered.

5.1 Substation Level Single Failure Mode Experiment

5.1.1 Design of Experiment I

One substation, the substation Winkeln, is randomly selected in this experiment which monitors and controls two transmission lines: line 103 and 119. As shown in Figure 5.1, the selected substation is highlighted using a red spot and the transmission lines are highlighted using green lines. In this experiment, this substation is referred to as sub-001 including RTU001 and two selected transmission lines refereed to as line103 and 119 respectively.

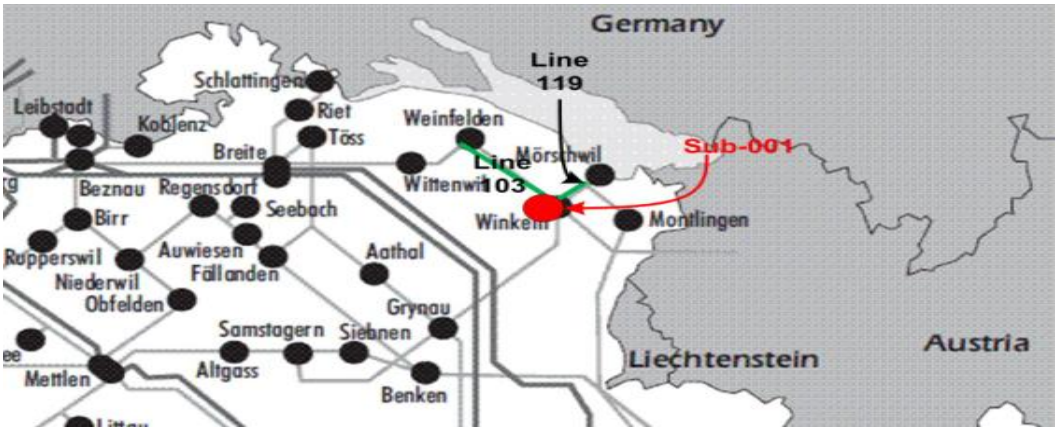


Figure 5.1 Selected components used in the Experiment I

[19] See section 5.2.1 for the definition of worse-case scenarios

Table 5.1 lists the summary of failure modes defined for each studied component (see chapter 4 for more details).

Table 5.1 Summary of definitions of failure modes used in Experiment I

Agent	Failure Mode	Description
FCD	FO	FCD received a demand to open but failed to open.
	FC	FCD received a demand to close but failed to close.
	SO	FCD opened when it should have stayed closed or closed when it should have stayed opened.
FID	FRL	The output of FID drifted below the actual value of monitored variable.
	FRH	The output of FID drifted above the actual value of monitored variable.
RTU	FRF	RTU is unable to acquire data from and send interpreted command to field devices assuming they function normally, although it is still able to receive commands from MTU.
	FRW	RTU is unable to function.
	FRC	RTU receives the command from MTU, but fails to interpret due to lost data.

A number of tests related to each failure mode of different substation level components are performed in this experiment, based on the failure-oriented modeling approach (see more details in section 4.2.3). During each test, the scenarios that will trigger power line overload alarm are generated at the beginning of the simulation, introduced in Chapter 4. Each test starts in the operation mode (a device mode) and one of agent states[20]. Within a given time period, the device mode of a respective component will go to one failure mode. The transition time from the operation mode to this failure mode is assumed to be exponentially distributed with constant failure rates λ. After a given time period, the device mode will go back to operation mode. The transition time from this failure mode to operation mode is assumed to be exponentially distributed with repair rate μ. The transitions between different device modes will have an influence on all corresponding agent states resulting in the change of behaviors of the SCADA system and SUC as the responses to the triggered power load alarm. If there is a request for the human operator in the MTU to make any decision, the model of the human operator will be activated and the human error probability (HEP) will be calculated according to current situations, e.g.,

[20] The first agent state in which each agent starts varies depending on its simulated component, e.g., a FCD agent starts in the *close* state and a RTU agent stats in the *ready* state. See section 4.2.4 for more details.

time of the day, number of simultaneous goals, etc. All the events occurred during each test are recorded in the corresponding SOE table of the DB_SCADA database. It should be noted that only one failure mode is assumed during each test. The simulation period of each test is assumed to be 3 days[21]. All reliability parameters used in this experiment, such as failure rate and repair rate for each failure mode, are adapted from [120], but have been modified in order to observe the consequences more efficiently. For example, the average failure rate (λ) of FCD SO mode is λ = 6.9E-4 (1/day). The modified average failure rate of this failure mode during a single failure mode test is λT =6.9 (1/day), meaning that the failure rate has been increased. In this experiment, this can also be referred to as the *scaling factor*, which can be calculated by the formula λT/λ. In the example above, the scaling factor is 1E4. It should be noted that multiplying rates in a Markov model with a scaling factor to gain a scaled model is a common approach [121, 122]. The modification of failure rates will possibly affect the accuracy of the simulation results. The main goal of this experiment is to exam and compare all failure modes and the accuracy is not necessarily the most important criteria in this experiment. At the end of each test, the parameter *service unavailability* is calculated according to Equation 5.1 to quantify simulation results.

- **Service Unavailability:** The aim of this parameter is to quantify the severity of service interruptions in the substation level caused by the studied failure mode. The parameter is calculated using following formula:

$$Service\ Unavailability = \frac{\sum_{i=1}^{m} T_i}{T_{Total}} \qquad \text{(Equation 5.1)}$$

Where T_i *is the time period when studied service becomes i-th unavailable*
m is total times when studied service becomes unavailable
T_{Total} *is the total studied time period*

[21] The reason to set the simulation time as 3 days is based on several trial tests conducted before starting the experiment. Results obtained from these tests show that after 3 days (simulation time), both SCADA system and SUC become stable and no abnormal events are observed.

It should be noted that this experiment is limited to the substation sub-001 and the service unavailability parameter is only applied to services provided by this substation. The tests related to the agent of each substation level component are summarized below. See Appendix IV for the corresponding SOE table and detailed description of each test conducted in this experiment.

5.1.2 Experiment I-FCD Agent

Three failure modes are defined for each FCD agent: FO, FC, and SO. The State diagram of the device mode for each FCD agent is illustrated in Figure 5.2.

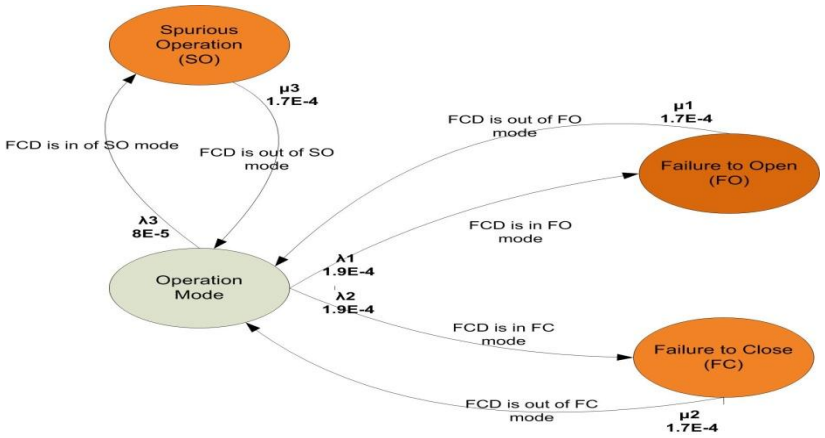


Figure 5.2 State diagram of the device mode model for a FCD agent

The reliability parameters used in all FCD failure mode tests are summarized in Table 5.2.

Table 5.2 Summary of reliability parameters used in FCD failure mode tests

Failure Mode	**Failure rate (λ, 1/sec)**	**Modified failure rate (λ_T, 1/sec)**	**Failure rate modification factor**	**Mean time to repair (μ, 1/sec)**
FO	1.9 E -10	1.9 E -4	1E6	1.7E-4
FC	1.9 E -10	1.9 E -4	1E6	1.7E-4
SO	8 E -9	8 E -5	1E4	1.7E-4

Three types of FCD single failure mode tests are summarized in Table 5.3 and Figure 5.3. As observed from corresponding SOE tables (Appendix IV), FO failure mode of the FCD

device would cause less negative impacts on the system unavailability if the operator recognizes the alarm and takes corrective actions. For example, if one line becomes overloaded and the operator redistributes the overloaded line, then no negative events will be observed. However, if the operator ignores the overload alarm and fails to take corrective actions, then the overloaded line will fail and be disconnected due to the FO failure mode. FC failure mode of the FCD device could have two most negative consequences. The first is that the transmission line controlled by a failed FCD device (in FC mode) remains disconnected and the second is that the transmission line connected to the disconnected line could also possibly become overloaded. The overloaded line remains disconnected and unavailable for an extra period of time. During SO failure mode tests, the overload threshold value is decreased. As a result, unexpected alarms are generated and following corrective actions are then taken, although they should not be. During some tests, these unnecessary corrective actions even cause another line to overload. Therefore, SO failure mode has more negative effects on the average service unavailability compared with other failure modes (FC and FO) of the FCD device.

In summary, all these three failure modes could cause serious consequences such as an increase of the service unavailability. Among these failure modes, negative consequences caused by SO failure mode seem more significant.

Table 5.3 Summary of (substation level) FCD single failure mode tests

Failure mode	**Average Service Unavailability**	**Confidence Interval (α=0.05) %**
FO	0.4%	[0.0; 0.8]
FC	2.5%	[1.4; 3.6]
SO	5.4%	[4.4; 6.4]

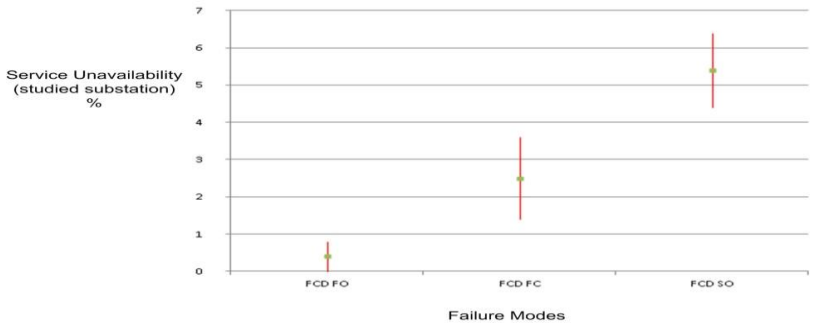


Figure 5.3 Summary of (substation level) FCD single failure mode tests

5.1.3 Experiment I-FID Agent

Two failure modes have been defined for FID agent: Failure to Run (too high) (FRH), and Failure to Run (too low) (FRL). The State diagram of the device mode model for FID agent is illustrated in Figure 5.4.

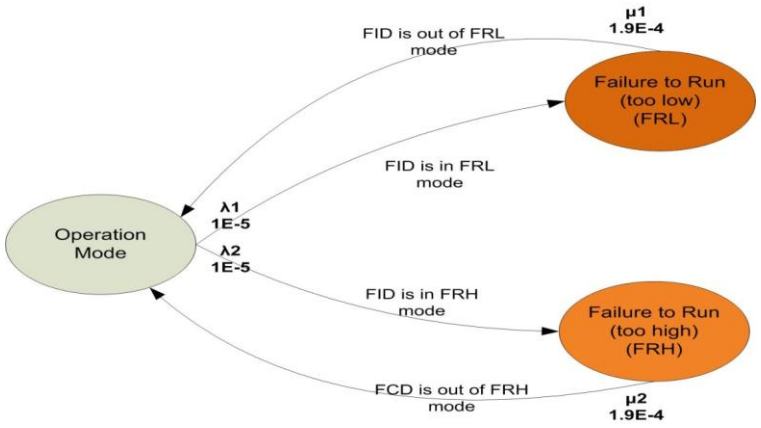


Figure 5.4 State diagram of the device mode model for a FID agent

The reliability parameters used in all FID failure mode tests are summarized in Table 5.4.

Table 5.4 Summary of reliability parameters used in FID failure mode tests

Failure Mode	**Failure rate (λ, 1/sec)**	**Modified failure rate (λ_T, 1/sec)**	**Failure rate modification factor**	**Mean time to repair (μ, 1/sec)**
FRL	1 E -10	1 E -5	1E5	1.9E-4
FRH	1 E -10	1 E -5	1E5	1.9E-4

Summary of FID substation level single failure mode tests

Table 5.5 Summary of substation level FID single failure mode tests

Failure mode	**Average Service Unavailability**	**Confidence Interval (α=0.05) %**
FRL	0	N/A
FRH	2.5%	[1.7; 3.4]

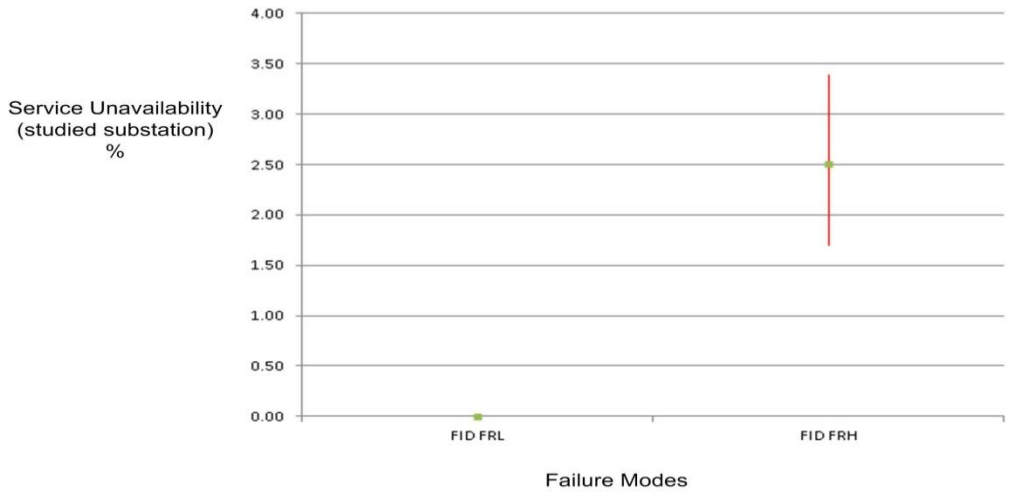


Figure 5.5 Summary of substation level FID single failure mode tests

Two types of FID single failure mode tests are summarized in Figure 5.5 and Table 5.5. The FRL failure mode is triggered by an unexpected decreased calibration value of a simulated FID device, possibly due to a maintenance failure. In this case, it is very possible that some alarms have been missed due to this calibration mistake and further corrective actions are then ignored. However, during this experiment, the unavailability of service is not affected (0%). The reason could be that the scope of this experiment is for one substation, not the whole network, and the total simulated period (3 days) is not long enough to observe any further events such as the overload of its connected line(s). The FRH mode is triggered by an unexpected increased calibration value of the FID device. Results collected from FRH mode tests are similar to previous FCD SO tests, while the threshold value is modified during FCD SO tests and calibration offset is modified during FID FRH tests. The observed consequences caused by triggering FRH failure mode include the abnormal disconnection of the affected transmission line and its connected line. Compared to FRL mode tests, FRH mode could cause more negative consequences such as service interruptions.

5.1.4 Experiment I-RTU Agent

Three failure modes are defined for the RTU agent: Failure to Run with field devices (FRF), Failure to Run due to hardware failure (FRH), and Failure to Run due to

communication error (FRC). The State diagram of the device mode model for RTU agent is illustrated in Figure 5.6.

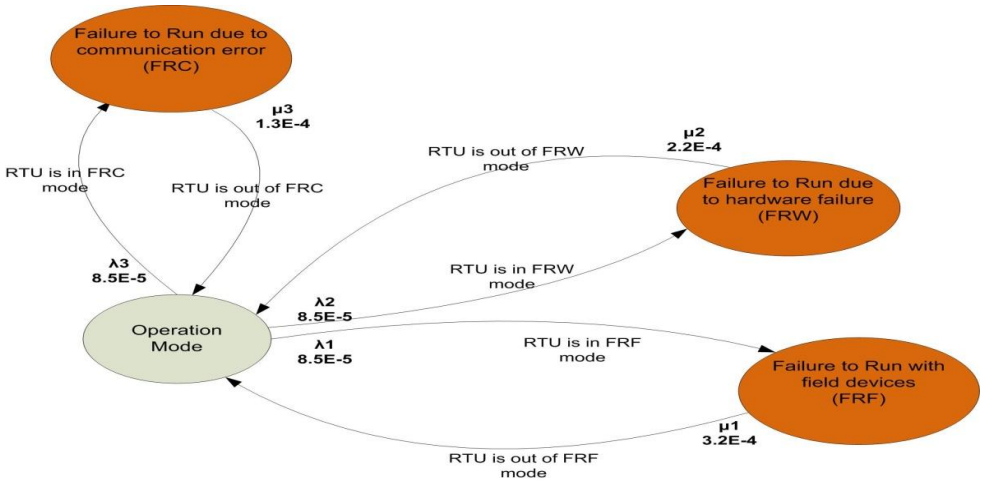


Figure 5.6 State diagram of the device mode model for a RTU agent

The reliability parameters used in all RTU failure mode tests are summarized in Table 5.6.

Table 5.6 Summary of reliability parameters used in RTU failure mode tests

Failure Mode	**Failure rate (λ, 1/sec)**	**Modified failure rate (λ_T, 1/sec)**	**Failure rate modification factor**	**Mean time to repair (μ, 1/sec)**
FRF	1.7 E -11	8.5 E -5	5E6	3.2 E-5
FRW	6 E -9	8.5 E -5	1.4E4	2.2E-4
FRC	9.5 E -9	8.5 E -5	0.9E4	1.3E-4

Summary of RTU substation level single failure mode tests

Table 5.7 Summary of substation level RTU single failure mode tests

Failure mode	**Average Service Unavailability**	**Confidence Interval (α=0.05) %**
FRF	26 %	[21; 34]
FRW	4.3 %	[3.3; 5.1]
FRC	3.8%	[2.8; 4.8]

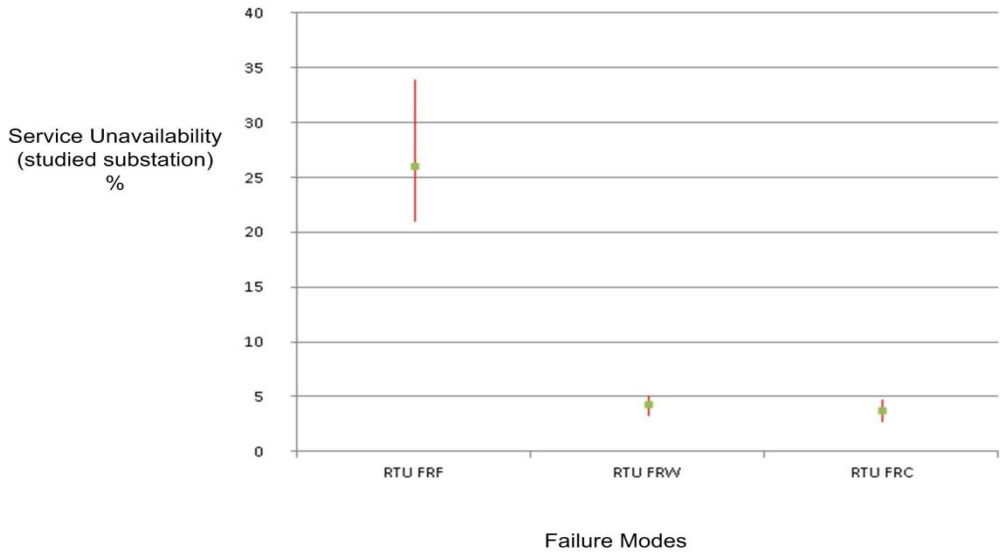


Figure 5.7 Summary of RTU single failure mode tests

Three type of FID single failure mode tests are performed during this experiment: RTU FRF, RTU FRW, and RTU FRC, summarized in Figure 5.7 and Table 5.7. The FRC mode represents the communication failure between the MTU and the RTU. The RTU receives a command from the MTU, but fails to interpret it due to the communication error. Therefore, field level devices simply disconnect the affected transmission line and cause service interruption.

The FRF mode is triggered by breaking up the connection between the RTU and its connected field level devices, meaning that the RTU will not be able to receive any update from those disconnected devices and forward any command to them. Observed consequences caused by triggering the RTU FRF failure mode include the loss of alarms from field devices and commands to field devices, causing the unavailability of the RTU device to its field devices.

The FRW mode is triggered by hardware failure of the RTU device, meaning that the RTU becomes fully blind to both field level devices and the MTU. In this situation, no alarms and commands can be processed by the RTU and no updates can be received from the failed RTU by the MTU. Observed consequences caused by the FRW mode are similar to the FRF mode. However, the FRF mode has much more negative effects on the average service unavailability than the FRW mode. The reason for this could be that the repair rate

of FRF mode is much smaller than FRW mode, indicating that the mean time to repair (MTTR) of this failure mode is much longer, according to the reference [120]. Therefore, in some FRF tests, services provided by this studied substation have been interrupted continuously.

5.1.5 Summary of Experiment I

Results collected from all the tests conducted in single failure mode experiment are summarized in

Table 5.8 and Figure 5.8.

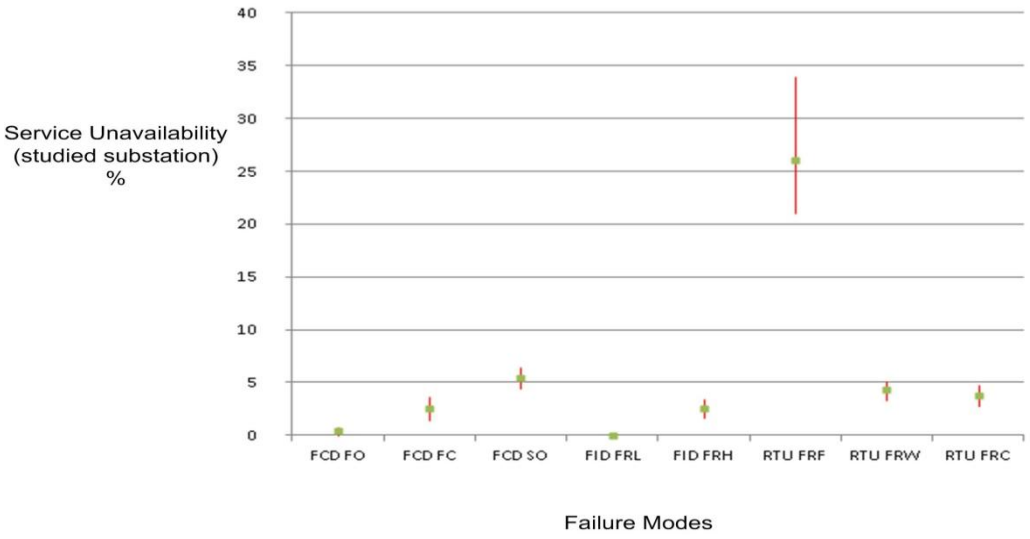


Figure 5.8 Summary of results from all the tests of single failure mode experiment

Table 5.8 Summary of results from all the tests of single failure mode experiment

Agent (Device)	**Failure mode**	**Service Unavailability (in average)**	**Confidence Interval (α=0.05) %**
FCD	FO	0.4%	[0.0; 0.8]
	FC	2.5%	[1.4; 3.6]
	SO	5.4%	[4.4; 6.4]
FID	FRL	0	N/A
	FRH	2.5%	[1.7; 3.4]
RTU	FRF	26%	[21; 34]
	FRW	4.3%	[3.3; 5.1]
	FRC	3.8%	[2.8; 4.8]

As shown in the table and figure above, among all the simulated SCADA-related devices, negative effects caused by failures of the RTU device seem more significant on its associated SUC. The disconnection between the studied RTU device and its connected field devices could result in about 26 percent of average service unavailability and the hardware failure of the RTU device could result in 4.3 percent of average service unavailability (at substation level). Compared to the FID device, failures of the FCD device have more adverse effects on average service unavailability. Furthermore, wrong alarms are generated due to the failure of the SCADA-related devices in some cases such as the FRH mode of the FID device and the negative effects are aggravated due to the failure of the SCADA related devices in some cases such as FRF mode of the RTU device, observed during this experiment.

5.2 Small Network Level Single Failure Mode Experiment

5.2.1 Design of Experiment II

12 key substations have been identified and listed in Table 3.3. In this experiment, the substation of BEZNAU is selected as the substation where the failure modes of substation level components are triggered during the simulation. Figure 5.9 shows a close look of the substation BEZNAU and parts of transmission lines in the small network. Compared to the Experiment I, 40 substations and 50 transmission lines are included in this experiment. Three transmission lines are controlled and monitored by the RTU device installed in this substation: line127, 194, and 66. After observing several simulation runs, line 127 has a higher overload frequency than other transmission lines at the same substation. Therefore, line 127 is selected as the key transmission line of this experiment, meaning that during each simulation test the overload alarm of this line is triggered at first.

For each simulated single failure mode, two types of tests are implemented: normal and worse-case test. The related modeling scenarios are summarized below:

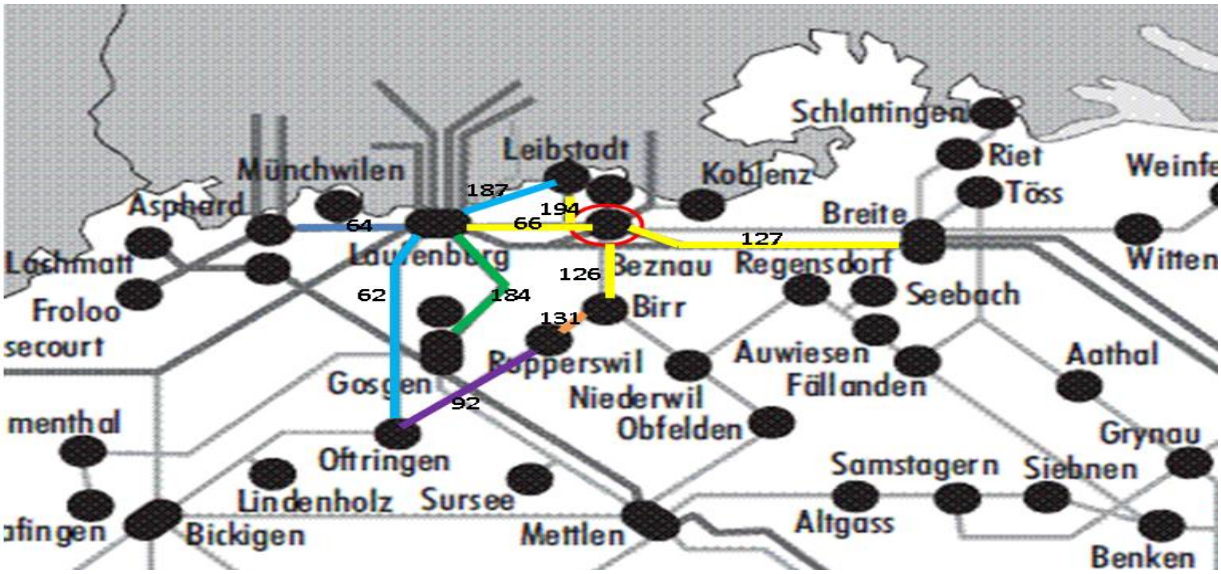


Figure 5.9 A close look at the substation BEZNAU

- **Normal Test**: The modeling scenarios of this test are similar to of the tests in Experiment I. In each test, the scenarios triggering a power line (line 127) overload alarm are generated at the beginning of the simulation. Each test starts in the operation mode (a device mode) and one of agent states. Compared to the Experiment I, the transition from the operation mode to respective failure mode at the beginning of each test is triggered manually instead of within a given time based on the failure rate[22][23]. The purpose of this adjustment is to ensure that the transition time from the operation mode to each failure mode is the same and the aim of this experiment is to evaluate the consequences caused by each failure mode. It should be noted that the transition from each failure mode back to the operation mode still depends on the corresponding repair rate, introduced in Experiment I. The simulation period of the normal test is assumed to be 5 days[24].

[22] This approach of failure/fault injection, as well as the failure rate acceleration used in Experiment I, has been widely accepted in fault tolerance/reliability tests in computer science [123] [124].

[23] Experiment II can then be considered as a semi-quantitative experiment due to this adjustment.

[24] The reason to set the simulation time as 5 days is as same as the simulation time set in Experiment I.

- **Worse-case Test**: In this experiment, this so called "worse-case" represents the situation when the operator is unable to handle any alarm received by the control centre (MTU) due to natural or technical failures (hazards),e.g., the failure of the control panel, flooding/fire in the control centre, etc. The purpose of performing experimental tests under this assumed situation is to observe corresponding consequences if the SCADA system fails to monitor and control the SUC through the MTU. Due to the fact that the value of the HEP is very low (normally equals to 0.014 and see section 4.3 for the explanation), it is difficult to observe this situation during normal tests. Therefore, in this test, the value of the HEP is assumed to be 1 meaning all the alarms cannot be handled correctly. It is assumed that this worse-case situation will go back to normal after one day and the simulation period of this test is assumed to be 1 day.

In this experiment, a new parameter is developed to quantify the results collected from each simulation:

- **ASSAI (Average Substation Service Availability Index):** This parameter represents the ratio of the total number of hours that the service provided by all the substations was available during a given time period to the total hours demanded (Equation 5.2).

$$\text{ASSAI}= \frac{N_S \times (number\ \ of\ hours) - \sum_{i=1}^{N} R_i}{N_S \times (number\ \ of\ hours)} \qquad \text{(Equation 5.2)}$$

where R_i=restoration time for ith substation (if service interruption exists)

N_S = Total number of substations

This parameter is originally adapted from an IEEE parameter called ASAI (Average Service Availability Index), which is the ratio of the total number of customer hours that service was available during a given time period to the total customer hours demanded. The aim of adapting this parameter is to provide a way to quantify the system vulnerability based on the definition in [25], introduced in Chapter 1.

Another parameter, **the number of overload alarms**, is used to count how many overload alarms are generated during each simulation test.

In order to qualify the negative effects caused by each failure mode, Degree of Impact (DI) is defined in this experiment, which can be calculated using three parameters as indicators obtained during each test: ASSAI, the number of affected SCADA components (interdependent failures), and the number of affected SUC components (dependent failures). All these three indicators receive values between 1-5 according to corresponding semi-quantitative definition, shown in Table 5.9 to 5.11. Furthermore, a weighting factor (W_i) is defined for each indicator indicating its importance for calculating the corresponding DI (Table 5.12). As shown in this table, the weighting factor for indicator ASSAI is higher than for other indicators since this indicator (parameter) plays more important role for the quantification of negative effects than others. The degree of impact caused by each failure mode can be obtained according to Equation 5.3:

$$DI = \sum_{i=1}^{N} W_i \, I_i \quad \text{(Equation 5.3)}$$

Where N=the number of indicators

W_i = the weighting factor for ith indicator

The DI caused by the failure mode can be categorized by five levels: V*ery Weak*, *Weak*, *Middle*, *Strong*, *Very Strong*, shown in Table 5.13.

Table 5.9 Parameter ASSAI as Indicator 1

I_1 **(ASSAI)**	**Real Value**
1	=1
2	[0.999, 1)
3	[0.99, 0.999)
4	[0.94, 0.99)
5	<0.94

Table 5.10 Parameter the number of affected SCADA components (interdependent failures) as Indicator 2

I_2	**Real Value**
1	0
2	(0, 1]
3	(1, 2]
4	(2, 3]
5	>3

Table 5.11 Parameter the number of affected SUC components (dependent failures) as Indicator 3

I_3	**Real Value**
1	0
2	(0, 4]
3	(4, 8]
4	(8, 12]
5	>12

Table 5.12 Weighting factor

W_i **(Weighting factor)**	**Real Value**
W_1 (For Indicator ASSAI)	4
W_2 (For Indicator interdependent failures)	4
W_3(For indicator dependent failures)	2

Table 5.13 Categories of DI

Level of DI	**Scope of DI**
Very Weak	=10
Weak	(10, 20)
Middle	[20,30)
Strong	(30, 40)
Very Strong	>=40

It should be noted that the development of this parameter (DI) provides a means to qualify negative impacts caused by interdependencies within and among CIs. All the values set up for indicators and weighting factors are based on author's knowledge and experiences and could vary if more experts' knowledge and experiences are included.

See Appendix IV for the corresponding SOE table and summary of each test of this experiment.

5.2.2 Experiment II-FCD Agent

5.2.2.1 FCD FO Mode

Normal Test: As observed from the SOE table of one of FCD FO normal tests (Table A-IV 19), the studied line 127 became overloaded and its corresponding FCD device was in FO failure mode shortly after that. Therefore, this line failed to be disconnected. As a result, the line remained overloaded and another (overload) alarm was generated. According to this test, none of its connected lines were affected (no alarms from other lines are observed). The service availability was also not affected (ASSAI=1). The summary of this test is included in Appendix IV (Table A-IV 18). As observed from this table, 9 out of 10 tests show the same results. None of the other lines in the small network are affected. However, in one test (test #2), line 194, which is also controlled by the RTU at the substation Beznau, became overloaded. This overload alarm was possibly triggered by an unhandled overload alarm of line 127, showing there exists the potential possibility that the FO failure mode can cause other further negative consequence (cause other lines to be overloaded). The dependencies between two systems observed in FO normal tests are shown in Figure 5.10.

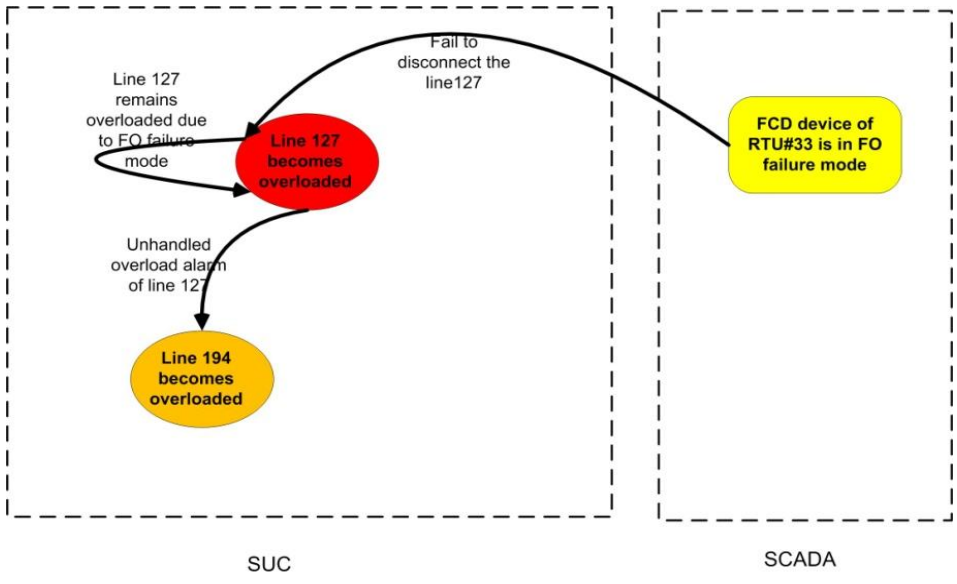


Figure 5.10 Affected components due to dependency according to results from FCD FO normal test

Worse-case test: As observed from the SOE table of one of FCD FO worse-case tests (Table A-IV 20), this worse-case test demonstrates similar results. Observed from all FO worse-case tests, similar results are observed.

5.2.2.2 FCD FC Mode

Normal Test: In this test, failure mode FC is triggered during the period when this FCD was opened to disconnect its controlled transmission line. Therefore, line 127 remained disconnected. The disconnection of line 127 became connected after this failure mode (FC) was fixed. As observed from the SOE table of one of FCD FC normal tests (Table A-IV 21), the sudden disconnection of line 127 caused both line 66 and line 194 to overload as well. It should be noted that all these three transmission lines are controlled by the same RTU at the substation Beznau. Due to the FC mode, line 127 remained disconnected, although it should be connected after the overload alarm of this line was handled. The sudden disconnection of line 127 is the cause that both its connected line 66 and 194 become overloaded, FC mode only extends the line 127 disconnection period and therefore, decreases the overall service availability (ASSAI = 0.9995). The summary of this test is included in Appendix IV (Table A-IV 22). About 8 out of 10 FC normal tests show similar results. Line 194 and 66 became disconnected due to the sudden disconnection of line 127. However, observed in 2 of 10 tests, line 187, which is controlled by the RTU at the substation Laufenberg, became overloaded. After analyzing corresponding SOE tables, this was caused by the sudden disconnection of the line 194. Dependencies between the SCADA system and the SUC observed in this test are shown in Figure 5.11.

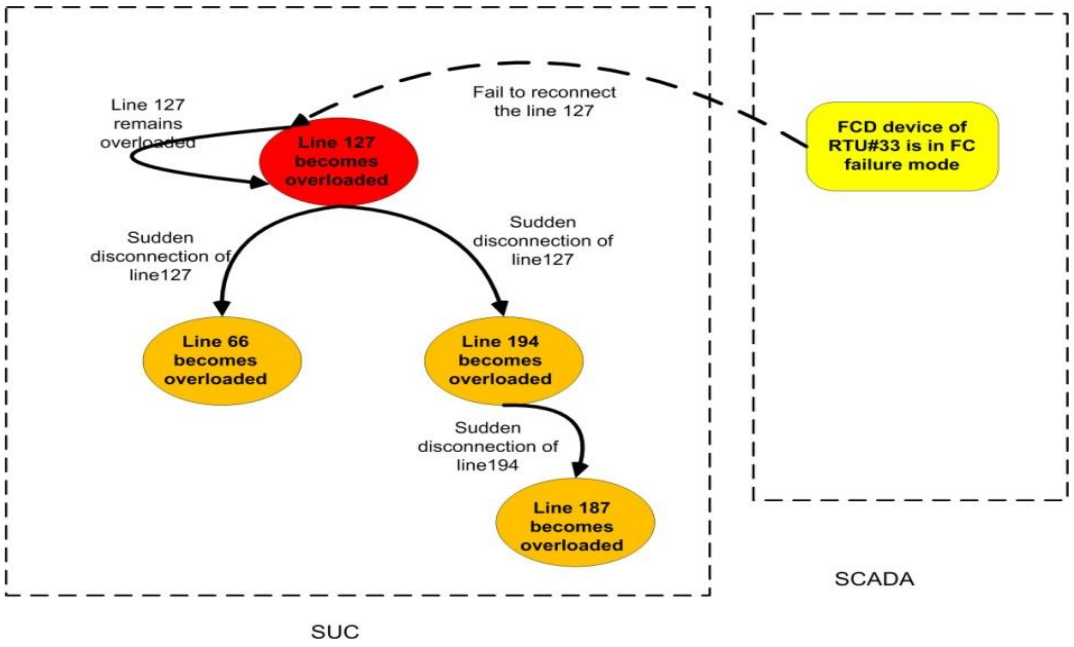


Figure 5.11 Affected components due to dependency according to results from FCD FC normal test

Worse-case Test: According to the SOE table from one of FC worse-case tests (Table A-IV 23), the sudden disconnection of the transmission line had negative effects on other transmission lines it connects to. In this test, line 194 and 66 first became overloaded (recall the fact that line 127, 194 and 66 are controlled by the same RTU), which have been observed in previous FC normal tests. As consequence of the sudden disconnection of line 66, line 62/184/187/64 all became overloaded. As shown in Figure 5.9, these transmission lines are all connected to each other at certain degree. In this test, power loss of two RTUs is also observed. Since line 62 and line 64 are both controlled by the RTU-038 (Laufenburg), the disconnections of these lines are the cause of the power service loss of the RTU-038 (after the consumption of the UPS device). Due to the same reason, RTU-037 also lost its power supply. Again, this worse-case test demonstrates that the sudden disconnection of one transmission line could have negative effects on other transmission line(s). Although the sudden disconnection of the line 127 is not caused by the FC mode, FC mode extended the line 127 disconnection period and therefore, decreased the overall service availability. The summary of this test is included in Appendix IV (Table A-IV 24). Interdependencies observed in this test are shown in Figure 5.12.

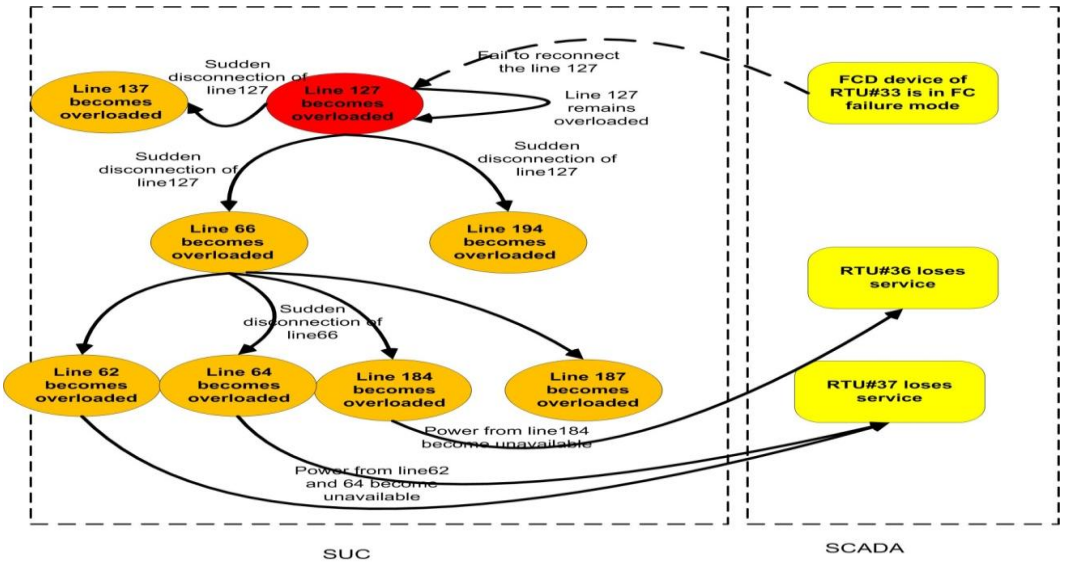


Figure 5.12 Affected components due to interdependency according to results from FCD FC worse-case test

5.2.2.3 FCD SO Mode

Normal Test: In this test, the overload threshold value of the FCD for the studied transmission line (line 127) was modified to a smaller number. Therefore, line 127 became overloaded and an overload alarm was sent to the MTU. As observed from the SOE table of one of SO normal tests (Table A-IV 25), the overload threshold value of the FCD of this line was modified and this line became overloaded. The sudden disconnection of the line 127 caused both its connected line 66 and 194 overloaded. The situation returned to normal after this failure mode is corrected. The summary of this test is included in Appendix IV (Table A-IV 26). Dependencies observed in this test are shown in Figure 5.13.

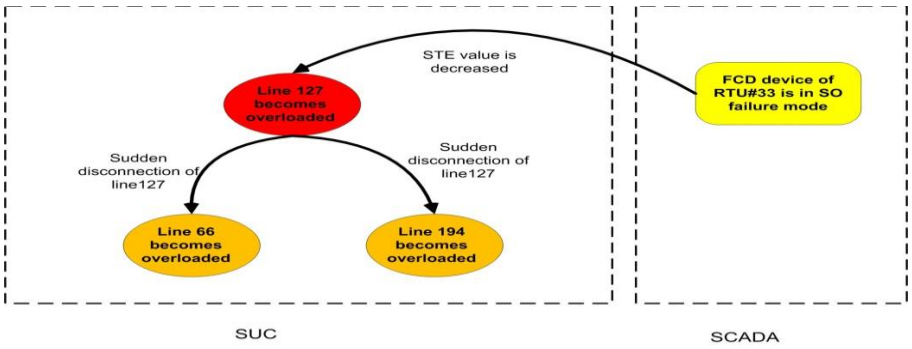


Figure 5.13 Affected components due to dependency according to results from FCD SO normal test

Worse-case test: As observed from the SOE table of one of FCD SO worse-case tests (Table A-IV 27), similar results are observed as previous FCD FC worse-case tests. Compared to that test, the only difference is that the first overload alarm of line 127 was caused by the SO mode of the related FCD. The failure of the FCD of the SCADA system affected several transmission lines of the SUC and the negative effects of this failure even propagated back to the SCADA system causing two RTUs temporarily out of the service. Interdependencies between the SCADA and the SUC observed in the FCD SO worse-case tests are demonstrated in Figure 5.14. The summary of this test is included in Appendix IV (Table A-IV 28).

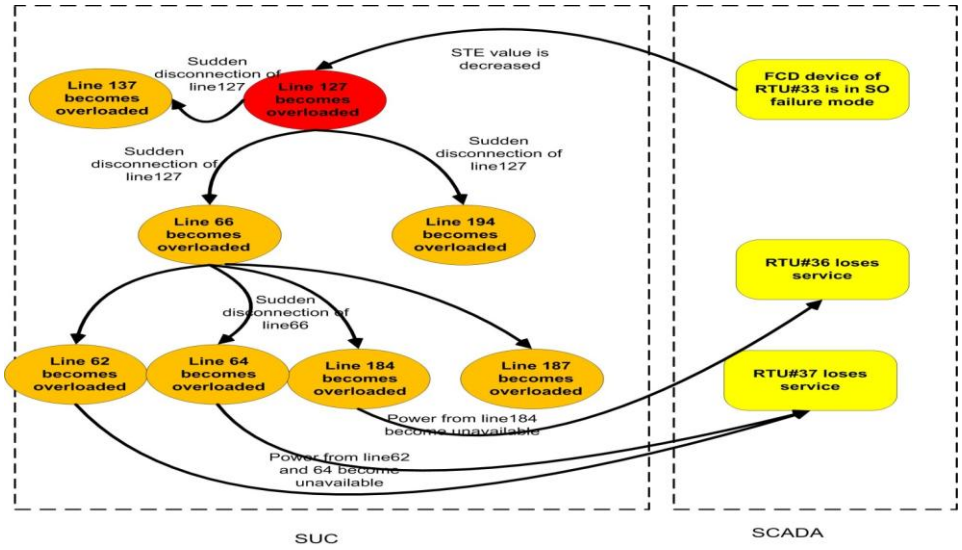


Figure 5.14 Affected components due to interdependency according to results from FCD SO worse-case test

5.2.2.4 Summary

The results of all FCD failure mode tests are summarized in Table 5.14.

Table 5.14 Summary of FCD Failure Mode Tests

Failure Mode	Average number of alarms	ASSAI (average) / Vulnerability	Average number of affected SUC components	Average number of affected SCADA components	Degree of Impact caused by the failure mode
FCD FO normal test	2	1.0	0	0	DI=10 **Very Weak**

FCD FC normal test	3.2	0.9996	2.2	0	DI=16 **Weak**
FCD SO normal test	3.1	0.9998	2	0	DI=16 **Weak**
FCD FC worse-case test	35	0.9604	8.1	2.1	DI=40 **Very Strong**
FCD SO worse-case test	45	0.9357	7.6	2.7	DI=42 **Very Strong**

Normal Test: The consequences caused by the FCD FC mode and the SO mode are similar during this test (in terms of average number of overload alarms and average ASSAI), although the causes of these two failure modes are different. The sudden disconnection of line 127 caused both line 66 and 194 to overload. Due to the appropriate response of the operators, negative effects had been minimized.

Worse-case Test: In both worse-case tests (FC and SO), the sudden disconnection of line 127 is the cause of the following events such as the service loss of RTUs, unexpected overload alarms, etc. The cause of the sudden disconnection of the line 127 is the combination of the lack of responses from operators in control center and the failure of the hardware located in the substation meaning that the hardware failure is not sufficient enough to affect the system service availability significantly (compare results between normal tests and worse-case tests). Comparing results between FC and SO worse-case tests, SO tests demonstrate more negative effects according to the calculated parameters (average number of alarms and average ASSAI) since the FC mode is not able to cause the overload of the line 127 and only worsen the situation. However, the SO failure mode is able to cause the overload of the line 127 and triggers the overload alarm before the time it should be. Furthermore, the worse-case tests also demonstrate that interdependencies between the SCADA system and the SUC can worsen negative effects of cascading failures (recall interdependency graphs).

5.2.3 Experiment II-FID Agent

5.2.3.1 FID FRL Mode

Normal Test: In this test, the calibration value of the FID device of line 127 was modified to a smaller number. Therefore, line 127 did not become overloaded or the overload was delayed. As observed from the SOE table of one of the FRL normal tests (Table A-IV 29), the overload alarm was delayed due to (lower) drifting of the FID calibration value for about one and half days. Line 194 and 66 also became overloaded due to the sudden disconnection of the line 127, which has been observed during previous tests. The summary of this test is included in Appendix IV (Table A-IV 30).

Worse-case Test: According to the results from previous normal case tests, the overload alarm of line 127 was normally delayed for more than one day. The simulation period of the worse-case test is one day. Therefore, the worse-case test is not applicable to be performed in this case.

5.2.3.2 FID FRH Mode

Normal test: In this test, the calibration value of the FID device of the studied transmission line (127) was modified to a higher number. Therefore, the line became overloaded. This test is similar to the FCD SO test. The difference between these two tests is that the calibration value of the FID device is modified in this test and the overload threshold value of the FCD device is modified in the other one. As observed from the SOE table of one of the FRH normal tests (Table A-IV 31), the calibration value of the FID device of line 127 was modified at first. Then this line became overloaded. As the consequences, lines 66 and 194 also became overloaded. In this test, line 66 remained overloaded after the power load was redistributed by the operators. The summary of this test is included in Appendix IV (Table A-IV 32). Dependencies observed in this test are shown in Figure 5.15.

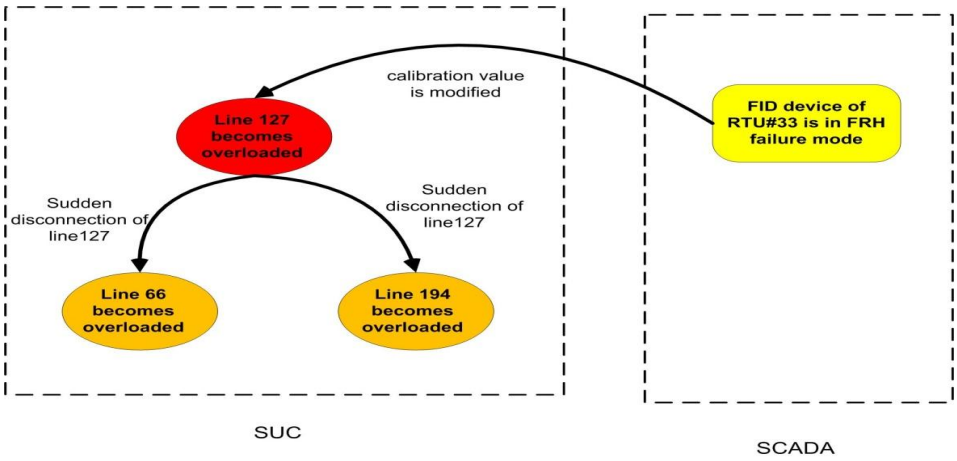


Figure 5.15 Affected components due to dependency according to results from FID FRH normal test

Worse-case Test: The observed results of this test are similar to the ones of previous FCD SO tests. The failure of the FID device caused the overload of line 127 and then other transmission lines were further affected. Moreover, the RTU devices also got affected (power loss of several RTU devices). The summary of this test is included in Appendix IV (Table A-IV 33). Interdependencies observed in this test are shown in Figure 5.16.

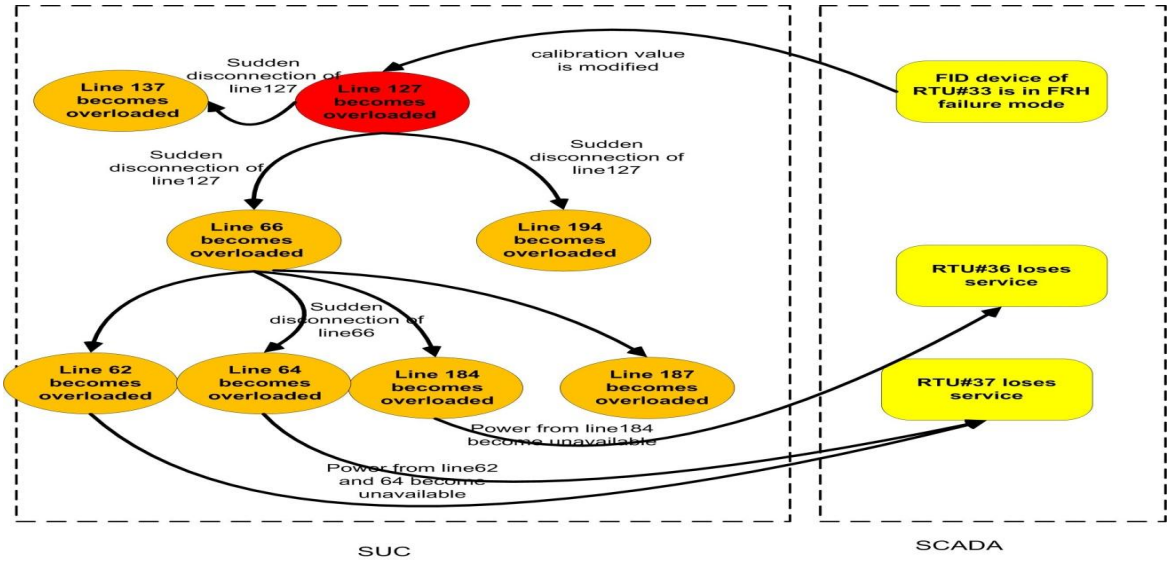


Figure 5.16 Affected components due to interdependency according to results from FID FRH worse-case test

5.2.3.3 Summary

Table 5.15 Summary of Small Network Level FID Failure Mode Tests

Failure Mode	Average number of alarms	ASSAI (average) /Vulnerability	The number of affected SUC components	The number of affected SCADA components	Degree of Impact caused by the failure mode
FID FRL normal test	3.6	0.9997	2.6	0	DI=16 Weak
FID FRH normal test	4.7	0.99977	2.5	0	DI=16 Weak
FID FRH worse-case test	48	0.9358	9.2	3.0	DI=44 **Very Strong**

The results from all FID failure mode tests are shown in Table 5.15 and summarized below:

Normal Test: The results observed from the FRL mode normal tests are similar to results observed from tests of FRH mode, although the FRL mode extends the period before the first overloaded line (more than one day) and FRH shortens this period. Since the simulation period of this test is 5 days, the service availabilities calculated from both tests are very close according to the values of average ASSAI.

Worse-case test: Results collected from worse-case tests of FID FRH mode are similar to the results from previous FCD SO mode tests. The threshold of the overload alarm of line127 is affected (modified) in both cases. This is the reason why parameters calculated during both tests are very close (average number of alarms and ASSAI).

5.2.4 Experiment II-RTU Agent

5.2.4.1 RTU FRF Mode

Normal Test: As observed from the SOE table of one of the RTU FRF tests (Table A-IV 34), line 127 was disconnected after the ignorance of an overload alarm. After that, the RTU#33 controlling and monitoring the line lost connection to its field devices. The FCD of

line 127 then failed to be connected due to its FRF mode. This failure mode was not handled until this failure was fixed. After that, line 127 became connected. During this test, several alarms were lost and the RTU device failed to send any command to its connected field devices. The summary of this test is included in Appendix IV (Table A-IV 35). Dependencies observed in this test are shown in Figure 5.17.

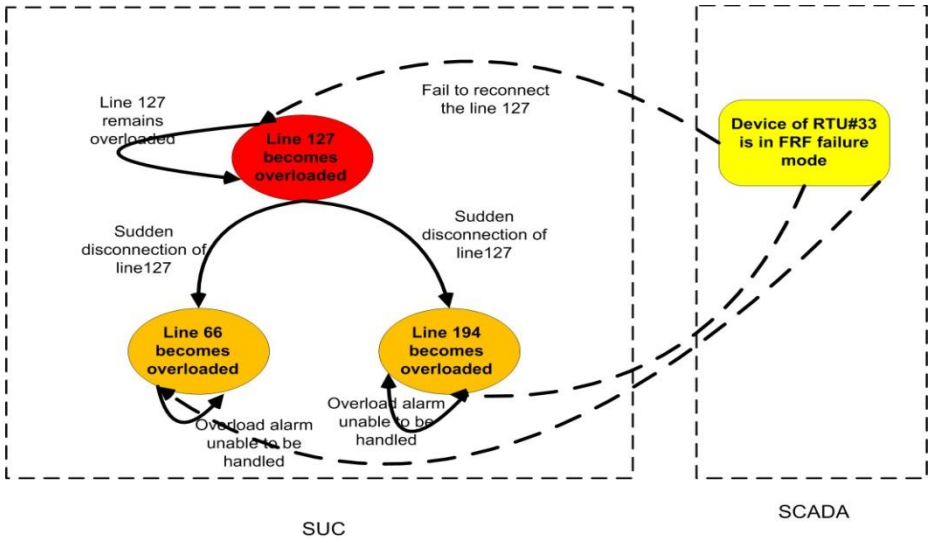


Figure 5.17 Affected components due to dependency according to results from RTU FRF normal test

Worse-case test: As observed from a SOE table from one of the RTU FRF worse-case tests (Table A-IV 36), results are similar to normal tests. The RTU device lost its connection to the field devices and two overload alarms were lost. The summary of this test is included in Appendix IV (Table A-IV 37).

5.2.4.2 RTU FRW Mode

Normal Test: According to a SOE table from one of the normal tests (Table A-IV 38), the results are similar to the FRF mode normal tests. However, the repair time of this failure mode is shorter than of FRF mode (according to [120]). Therefore, the average ASSAI is more than the one calculated in FRF mode tests. The summary of this test is included in Appendix IV (Table A-IV 39). Dependencies observed in this test are shown in Figure 5.18.

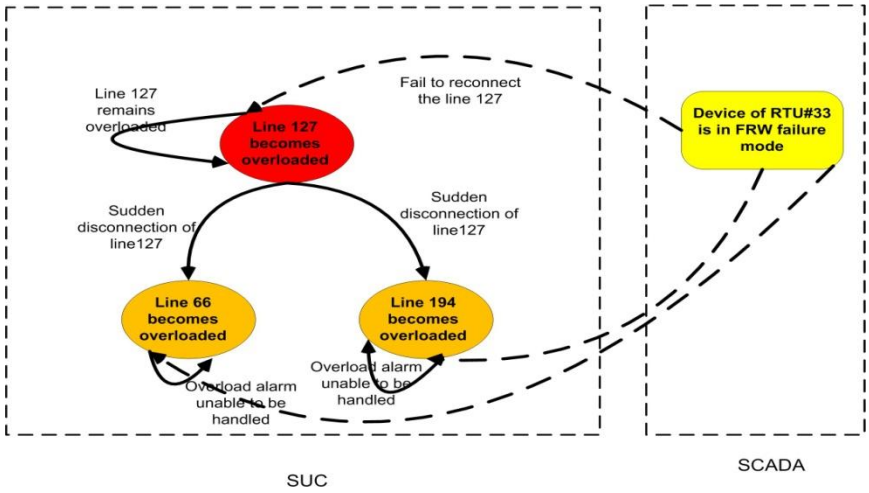


Figure 5.18 Affected components due to dependency according to results from the RTU FRW normal test

Worse-case Test: According to the SOE table from one of the worse-case tests (Table A-IV 40), similar results are observed as shown in the previous FRF mode worse-case tests. The summary of this test is included in Appendix IV (Table A-IV 41).

5.2.4.3 RTU FRC Mode

Normal Test: In this test, it is assumed that there are potential communication issues between the MTU and the RTU, at the time that line127 became overloaded and an alarm was sent to the MTU. According to the SOE table from one of the FRC normal tests (Table A-IV 42), the line 127 became overloaded and then the communication error between the MTU and the RTU device (RTU#033) was assumed. Due to this failure, the RTU device was unable to interpret the command to redistribute the power load of line 127 sent by the MTU device and this line became disconnected by its FCD device for safety reasons. Results from all FRC normal tests are summarized in Appendix IV (Table A-IV 43). Dependencies observed in this test are shown in Figure 5.19.

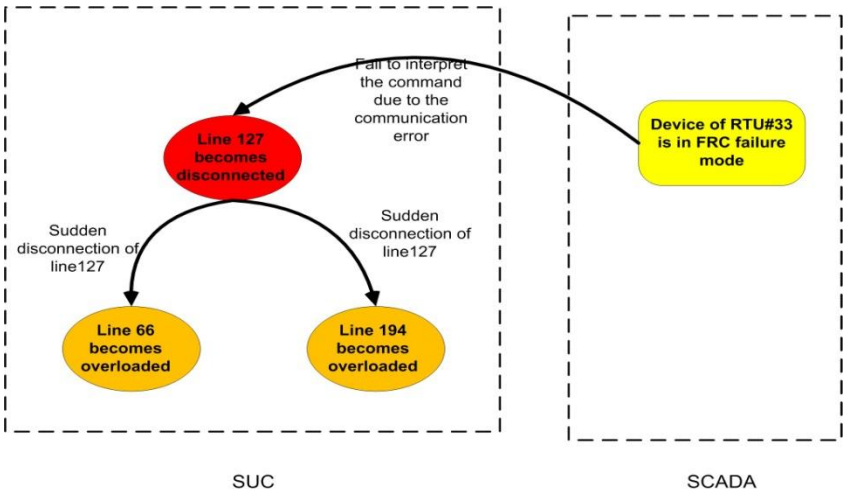


Figure 5.19 Affected components due to dependency according to results from the RTU FRC normal test

Worse-case Test: As described in previous FRC normal tests, the FRC failure mode tests assume that the operators are able to handle the first overload alarm and send the corresponding command back to the corresponding RTU device. This assumption is not applicable to worse-case tests since this type of test assumes that the operators are not able to handle all received alarms during a 1 day period. Therefore, worse-case tests are not conducted for FRC failure mode.

5.2.4.4 Summary of Tests Related to RTU Agent

Table 5.16 Summary of RTU Failure Mode Tests

Failure Mode	Average number of alarms	ASSAI (average) / Vulnerability	The number of affected SUC components	The number of affected SCADA components	Degree of Impact caused by the failure mode
RTU FRF normal test	2.4	0.997	2	0	DI=20 **Middle**
RTU FRW normal test	2.1	0.9996	2.5	0	DI=20 **Middle**
RTU FRC normal test	3.7	0.9998	2.6	0	DI=16 **Weak**

RTU FRF worse-case test	1	0.9940	2	0	DI=20 **Middle**
RTU FRW worse-case test	1	0.9980	2	0	DI=20 **Middle**

Normal tests: The results observed from normal tests of FRF mode are similar to results from FRW mode and the average ASSAI of these two failure modes are very close. The reason is the studied RTU loses the connection to its controlled field level devices during both failure mode tests and becomes blind causing problems such as loss of alarms and extended period of line disconnection. The FRC mode is triggered when communication issues appear between the MTU and the RTU. As a result, the related RTU has difficulties interpreting any command sent by the MTU. The consequence caused by this failure mode is the disconnection of the corresponding transmission line. However, the service availability of the system is not affected significantly, according the calculated average ASSAI.

Worse-case tests: Results from the RTU worse-case tests show that the average number of overload alarms and ASSAI is much less than results from the same tests of other devices (FID and FCD). This does not mean that negative effects caused by failures of RTU devices on the system service availability are much less significant (recall ASSAI). Due to disconnection between the RTU and its connected field level devices, several overload alarms are lost and, therefore, the negative effects caused by sudden disconnection of the transmission line are unable to propagate. This is the reason why the average number of overload alarms is much less than in worse-case tests of field level devices (i.e. FID and FCD). It can be concluded from this test that the correct function of human operators in the control centre becomes less important if RTU devices lose the connection to its field level devices.

5.2.5 Summary of Experiment II

The small network level single failure mode experiment is summarized in Figure 5.20. Two types of tests are developed in this experiment: normal tests and worse-case tests. In normal test, it is assumed that alarms are handled by operators at the control centre

(MTU) of the SCADA system (except for the first overload alarm). Worse-case tests simulate scenario situations when the operator is unable to handle any alarm received by the control centre (MTU) possibly due to natural or technical failures (hazards),e.g., the failure of the control panel, flooding/fire in the control centre, etc. As shown in these tests, on average, negative effects due to interdependencies are aggravated during worse-case tests since a very strong DI caused by three of the failure modes are observed. The DI caused by FID FRH mode is 44 meaning its impact is very strong. The DIs caused by failure modes of the RTU are between middle and weak, which seems not as serious as for the FID and FCD. However, due to the role of this device (the failure of this device means interruption of service provided by the SCADA components installed at the corresponding substation), it is still worthy to develop further tests on this device, as well as on the FID device in the following experiment: whole network experiment.

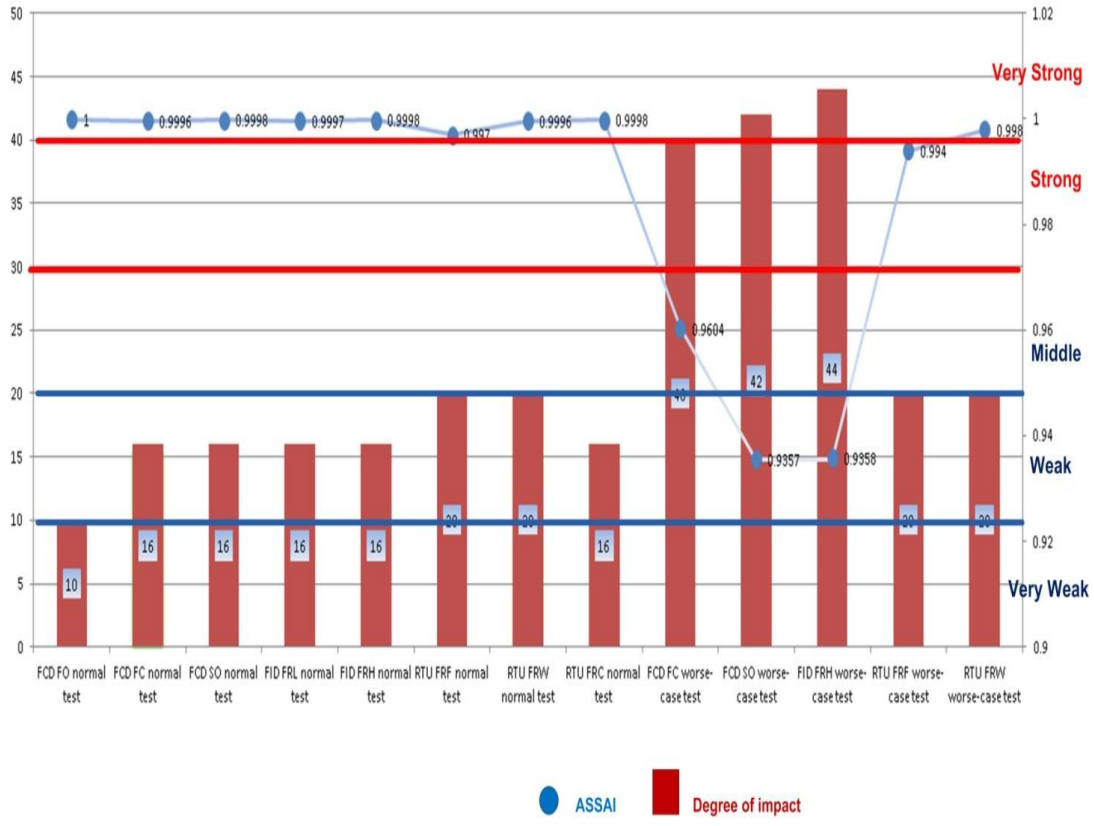


Figure 5.20 Summary of small network level single failure modes experiment

5.3 Whole Network Worse-Case Experiment

5.3.1 Design of Experiment III

The modeling scenarios of this experiment are as the same as scenarios defined in the worse-case tests of the Experiment II (see section 5.2.1 for more details). Therefore, this experiment can also be considered as a semi-quantitative experiment.

Selection of Key Substations

In this experiment, two substations out of 12 (see Table 3.3) are selected as exemplary key substations for the investigation: GOESGEN and METTLEN (see Figure 5.21).

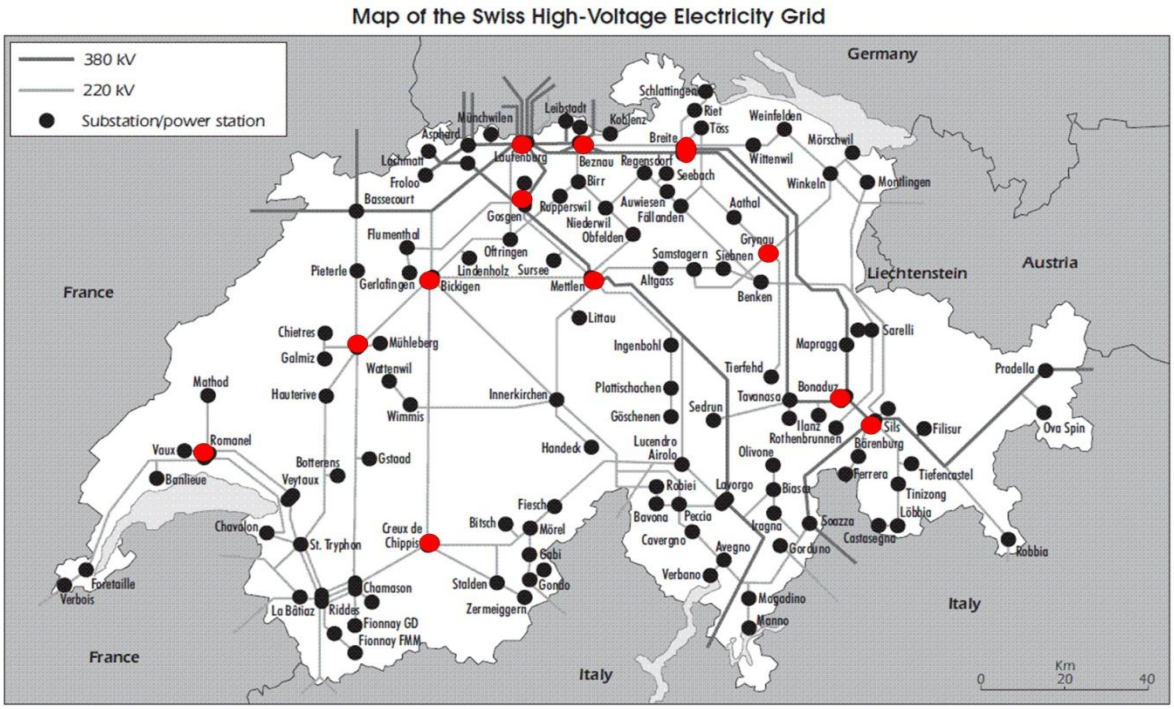


Figure 5.21 Locations of 12 key stations

Selection of Non-key Substations

Two non-key substations and are randomly selected for this experiment without preferences: LITTAU and GISWIL.

Selection of Failed Components

Two technical failures are also simulated in this experiment:

- **Failure 1- FID failure**: According to the results from the last experiment, small network experiment, the (calculated) DI caused by FID FRH mode is 44 meaning the impact is very strong. Due to this high degree of impact, this failure is considered as one example of worse scenarios in this experiment.
- **Failure 2 - RTU failure**: Although the calculated DIs caused by the failure of RTU are between middle and weak, it is still worthy to simulate one of the failure modes of RTU device (FRW mode) since the failure of this device means interruption of service provided by the SCADA components installed at the corresponding substation.

In total, 8 different types of tests are developed in this experiment, listed in Table 5.17.

Table 5.17 List of eight tests in this experiment

Test No	Failure mode	Failure type	Substation type	Substation name/location
1	FID FRH	Single	key substation	GOESGEN S1
2	FID FRH	Single	Non-key substation	GISWIL S1
3	RTU FRW	Single	key substation	GOESGEN S1
4	RTU FRW	Single	Non-key substation	GISWIL S1
5	FID FRH	Double	key substations	GOESGEN S1& METTLEN S2
6	FID FRH	Double	Non-key substations	GISWIL S1 & LITTAU S1
7	RTU FRW	Double	key substations	GOESGEN S1 &METTLEN S2
8	RTU FRW	Double	Non-key substations	GISWIL S1& LITTAU S1

5.3.2 Experiment III- Single Failure Tests

In each FID failure mode test, the studied transmission line (line 205 in key substation tests and line 47 in non-key substation tests), controlled and monitored by the RTU of the corresponding substation (GOESGEN in key substation tests and GISWIL in non-key substation tests) became overloaded at first. It is assumed that the FID device for this line is in malfunction meaning that the measured value is higher than it is supposed to be (FID

FRH Mode). During each test run, the calibration value of FID was modified and this caused the wrong overload alarm to be sent to the control centre. However, no redistribution command was sent to the RTU device of the corresponding substation. After a certain time, the studied transmission line was disconnected by its own FCD for safety reasons.

In the RTU failure mode test, the studied transmission line (line 205 in key substation tests and line 47 in non-key substation tests, controlled and monitored by the RTU device of the corresponding substation (GOESGEN in key substation tests and GISWIL in non-key substation tests) became overloaded at first. It is assumed that the RTU device installed in the corresponding substation was in (hardware) malfunction and became blind to other components connected to it, e.g., FID(s) and FCD(s).The disconnected line then remained disconnected since no disconnect command could be sent by the RTU device.

All tests are conducted about 10 times and the simulation time for corresponding summary table of each test of this experiment.

The following parameters are collected in each single failure test:

- **Number of lost alarms**: Number of lost alarms due to abnormal disconnection of the impacted line.
- **Number of affected SUC components**: this parameter indicates the number of overloaded transmission lines caused by the abnormal disconnection of the impacted line.
- **Number of affected SCADA components**: This parameter indicates the number of RTU devices (at different substations) that lost power caused by the abnormal disconnection of the impacted line.
- **ASSAI**: Average Substation Service Availability Index.

5.3.2.1 TEST No.1: FID failure (one key substation)

The summary of this test is included in Appendix IV (Table A-IV 44). About 18 transmission lines become overloaded and disconnected. Locations of these lines are given in Figure 5.22.

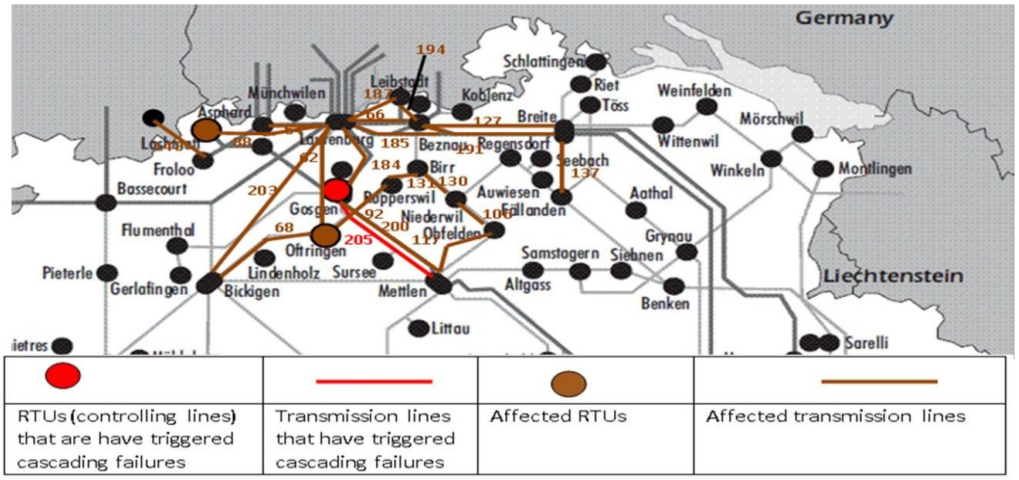


Figure 5.22 Locations of studied substations and lines

Most of the affected transmission lines are connected with each other directly or indirectly. The abnormal disconnection of one line can cause snowball effects and affect other lines. Two RTUs, at substation LACHMATT and OFTRINGEN, are also affected. The transmission lines controlled by these two RTUs are disconnected. After complete consumption of power batteries installed for corresponding RTUs, no (electricity) power is available for both RTUs. In this experiment, it is assumed the power provided by the battery is 20 minutes [51].

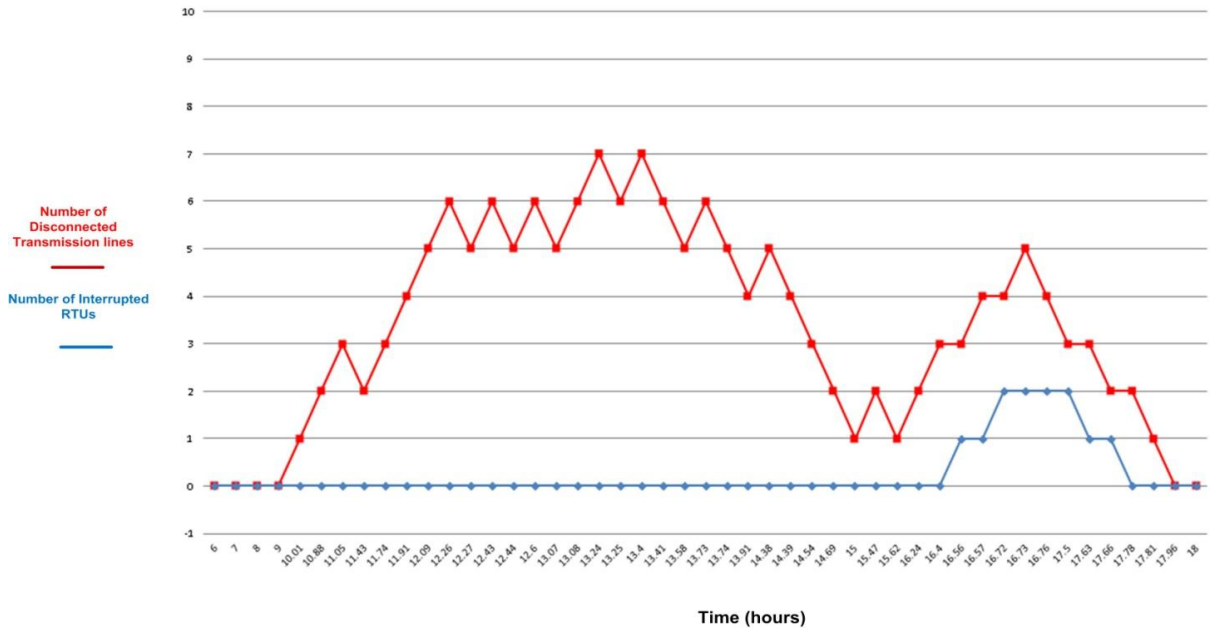


Figure 5.23 Affected SUC and SCADA components in Test No.1

Figure 5.23 shows how the SCADA system and the SUC affect each other recorded from one of 10 tests. At time 10 hours, line 205 was disconnected due to the wrong overload alarm caused by the technical failure of its FID and the absence of a human operator. At time about 13.25 hours, the number of disconnected lines reached the maximum value. Then this number started to drop and only one line was disconnected. After time 15.62 hours, more transmission lines became disconnected. Observed at time 16.56 hours, RTUs were also affected and the number of interrupted RTU devices was 1. The maximum number of interrupted RTUs was 2 at time 16.72 hours. After that, the numbers of disconnected lines and interrupted RTUs started to drop and returned to zero at time around 18 hours. As observed from this test, failures of SUC components seem not to affect its interconnected SCADA system instantly. It took about 6 hours before failures started to propagate from one system to another system, which can be considered as the *delay of dependency failures*.

5.3.2.2 TEST No. 2: FID failure (one non-key substation)

The summary of this test is included in Appendix IV(Table A-IV 45). No transmission line was affected by the failure of line 47. Locations of these lines are given in Figure 5.24.

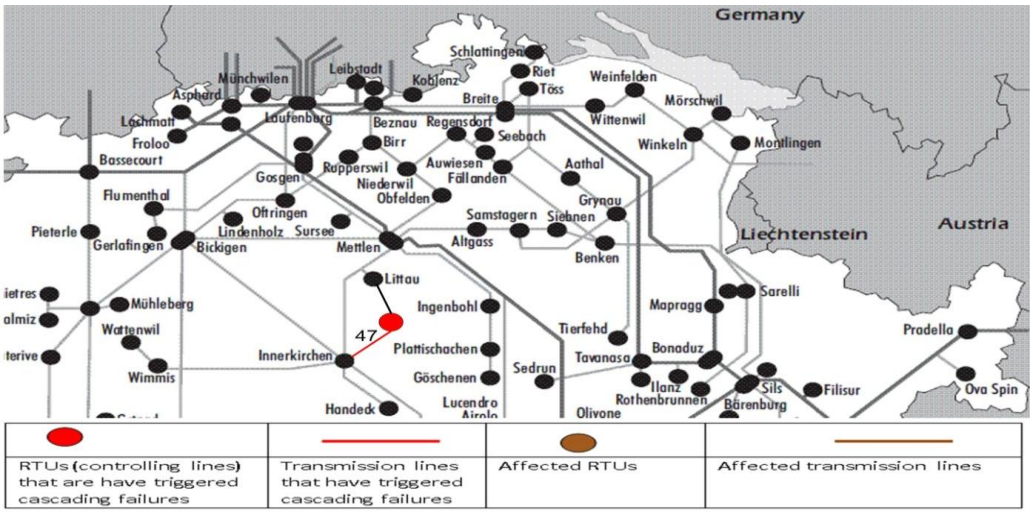


Figure 5.24 Locations of studied substations and lines in Test No.2

As observed from this test, none of the SUC components or SCADA components was affected. Figure 5.25 shows what occurs after triggering the technical failure of the FID for

line 47. Compared to Test No.1, FID failure of a key substation, the consequences observed in this test seem much less significant.

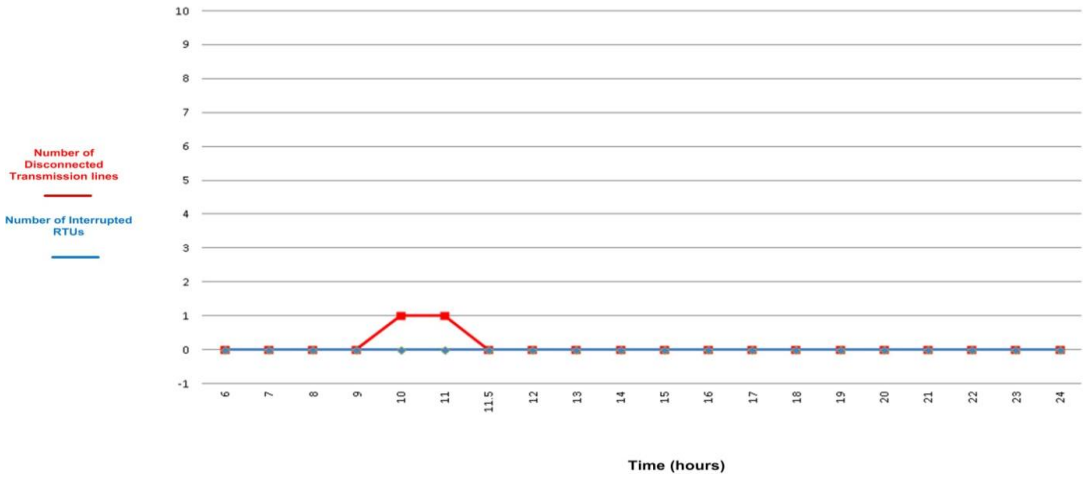


Figure 5.25 Affected SUC and SCADA components in Test No.2

5.3.2.3 TEST No.3: RTU failure (one key substation)

The summary of this test is included in Appendix IV(Table A-IV 46). About 3 transmission lines were affected by the failure of the studied RTU device: line 200, line 194, and line 187. Both lines 194 and 187 became overloaded and disconnected. However, line 200 remained connected since the overload alarm for this line was lost due to the hardware failure of the RTU, which monitors and controls this line. No interruptions of SCADA components were observed in this test. The locations of the affected SUC components are given in Figure 5.26. As illustrated in this figure, the disconnection of line 205 caused the overload of both lines 187 and 194. Although line 205 was not connected to either of these two lines, its sudden disconnection still affected the power load of these two lines.

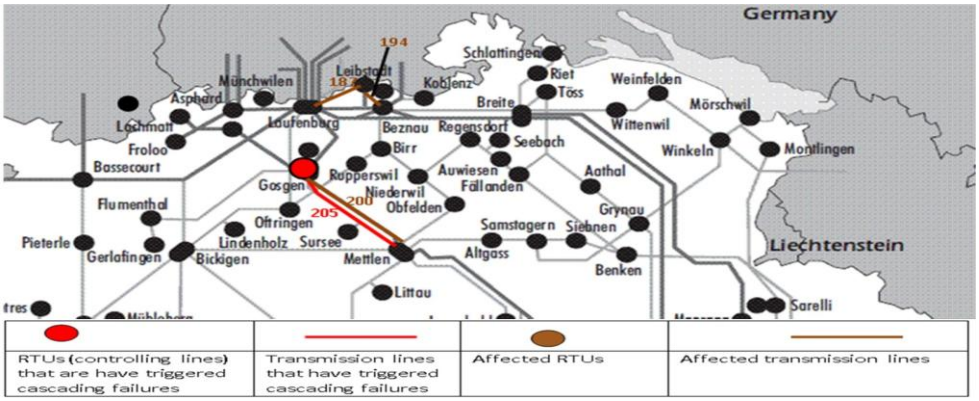


Figure 5.26 Locations of studied substations and lines in Test No. 3

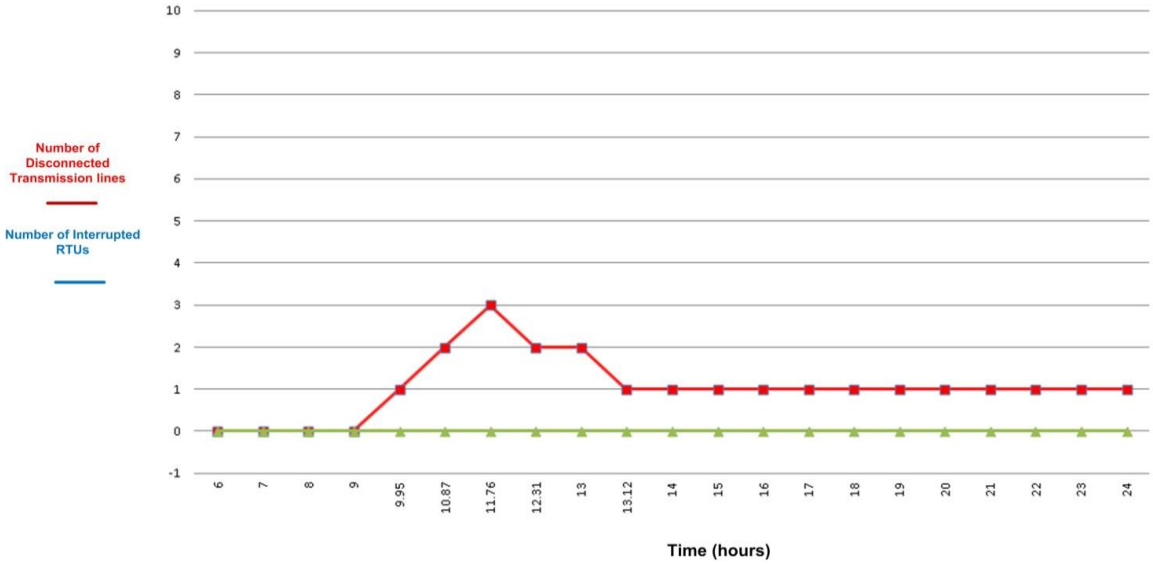


Figure 5.27 Affected SUC and SCADA components in Test No. 3

Figure 5.27 shows what occurs after triggering the technical failure of the RTU of substation GOSGEN. As seen from this figure, line 205 remained disconnected due to the technical failure of the related RTU device.

5.3.2.4 TEST No. 4: RTU failure (one non-key substation)

The summary of this test is included in Appendix IV (

Table A-IV 47). No transmission lines becomes overloaded and disconnected . Locations of these lines are given in Figure 5.28.

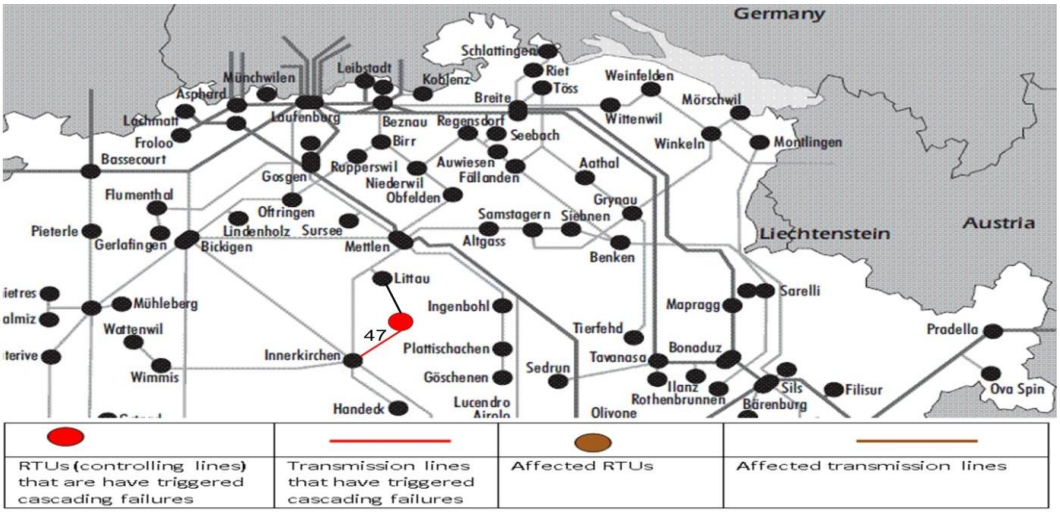


Figure 5.28 Locations of studied substations and lines in Test No. 4

The technical failure of the RTU of the substation GISWIL caused none of the abnormal disconnections of other transmission lines. As observed from this test, none of the SUC components or SCADA components are affected. Figure 5.29 shows what occur after triggering the technical failure of the studied RTU device.

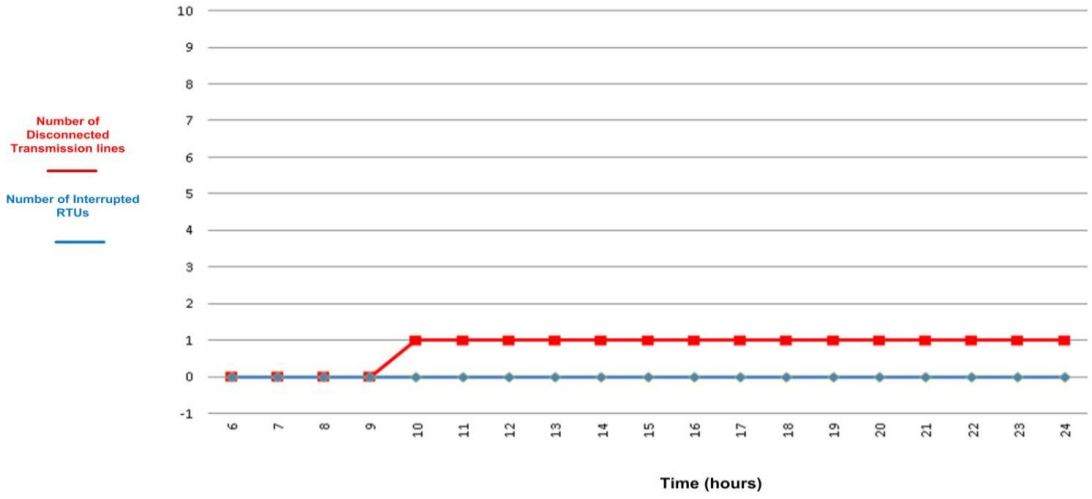


Figure 5.29 Affected SUC components and SCADA components

5.3.2.5 Summary of Single Failure Tests

All four tests conducted during single failure experiment are summarized in Table 5.18 and illustrated in Figure 5.30.

Table 5.18 Summary of Single failure tests

	FID failure (key substation)	FID failure (non-key substation)	RTU failure (key substation)	RTU failure (non-key substation)
Number of affected SUC components	18	0	3	0
Number of affected SCADA components	2	0	0	0
Number of lost alarms	0	0	1	0
ASSAI / Vulnerability	0.9910	0.9996	0.9953	0.9962
Degree of impact	34(Strong)	14 (Weak)	20 (Middle)	18 (Weak)

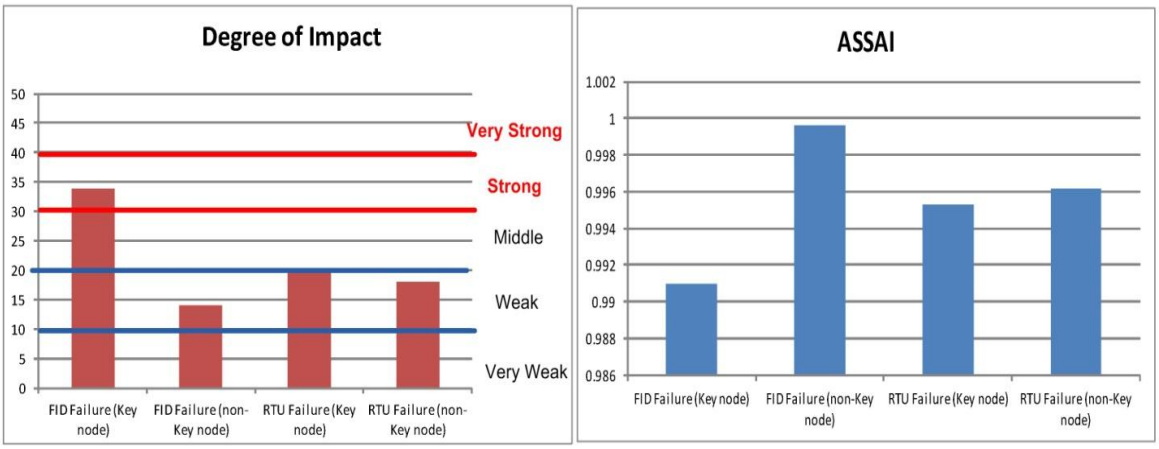


Figure 5.30 Summary of single failure tests

As shown in Figure 5.30, cascading impact caused by the key node FID failure is strong, highest compared to other single failure tests, as both SUC and SCADA components are affected by this technical failure. The number of affected SUC components is 18, meaning that 18 transmission lines become overloaded. The number of affected SUC components observed during RTU key node failure is only 3, much less than the number observed during FID key node test. In FID failure test, the failure starts from the SCADA component

(recall the calibration change of the FID device) and then propagates into the SUC causing disconnection of the line 205, controlled by the failed FID. After a certain period, the failure propagates back to SCADA causing failures of two RTUs (power lost). In the RTU failure tests, the SCADA component does not cause the disconnection of line 205. The failure of the RTU worsens the situation and overload alarms are ignored. However, in this case, the failure does not cause significant cascading effects in the SUC and does not propagate into SCADA. As demonstrated by these two tests, the failures of field level devices, which can also be considered as direct interfaces between two systems (SCADA and SUC), could cause more significant negative effects and trigger more cascading failures propagating within and between systems.

5.3.3 Experiment III: Double Failure Tests

Double failure tests consider two independent simultaneous failures of the same type of devices. Similar to single failure tests, same parameters are recorded. Instead of one transmission line, two transmission lines from two substations (2 key substations or 2 non-key substations) are included in these tests. See Table 5.17 for transmission lines and corresponding substations used in these tests.

5.3.3.1 TEST No.5: FID failure (double key substations)

The summary of this test is included in Appendix IV (Table A-IV 48). About 28 transmission lines became overloaded and disconnected. Locations of these lines are given in Figure 5.31. As shown in this figure, the abnormal disconnection of the line 205 and 116, triggered by the technical failure of the FIDs of these lines, caused the abnormal disconnections of several transmission lines. Most of these transmission lines are connected with each other directly or indirectly. Compared to previous single FID failure tests, more transmission lines and RTUs were affected (18 transmission lines and 2 RTU devices were affected in single FID failure test). The consequences caused by double (in two key substations) technical failures became worse compared to single (one key substation) technical failure tests. The calculated DI is *very strong*, compared to *strong* calculated in single failure tests.

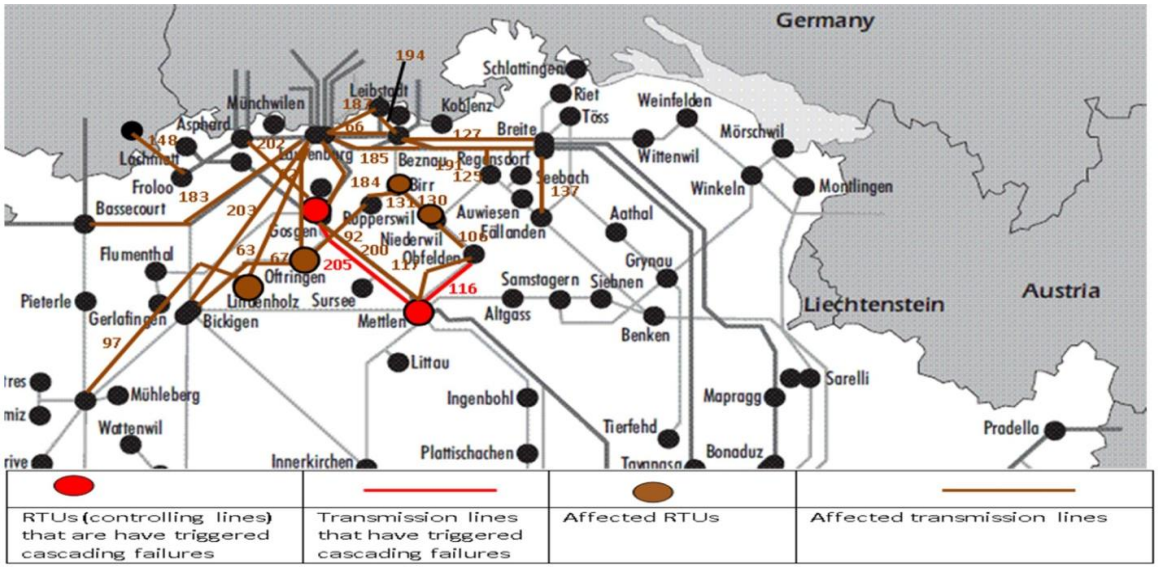


Figure 5.31 Locations of studied substations and lines in Test No. 5

Figure 5.32 shows how the SCADA system and the SUC affect each other. Similar to the results shown in Figure 5.23, it takes a certain period before failures finally propagate from the SUC into the SCADA. The maximum number of simultaneously affected SUC components (transmission lines) is 8, 1 more than the maximum number of total affected SUC components observed during single FID technical failure, although the total number of affected SUC components increases significantly. Furthermore, both SUC and SCADA become less resilient in double failure tests since it takes more time for them to go back to normal state. The time when two systems go back to normal state is 18 hours in the single failure test, while the "back to normal" time increases to 22 hours in this test.

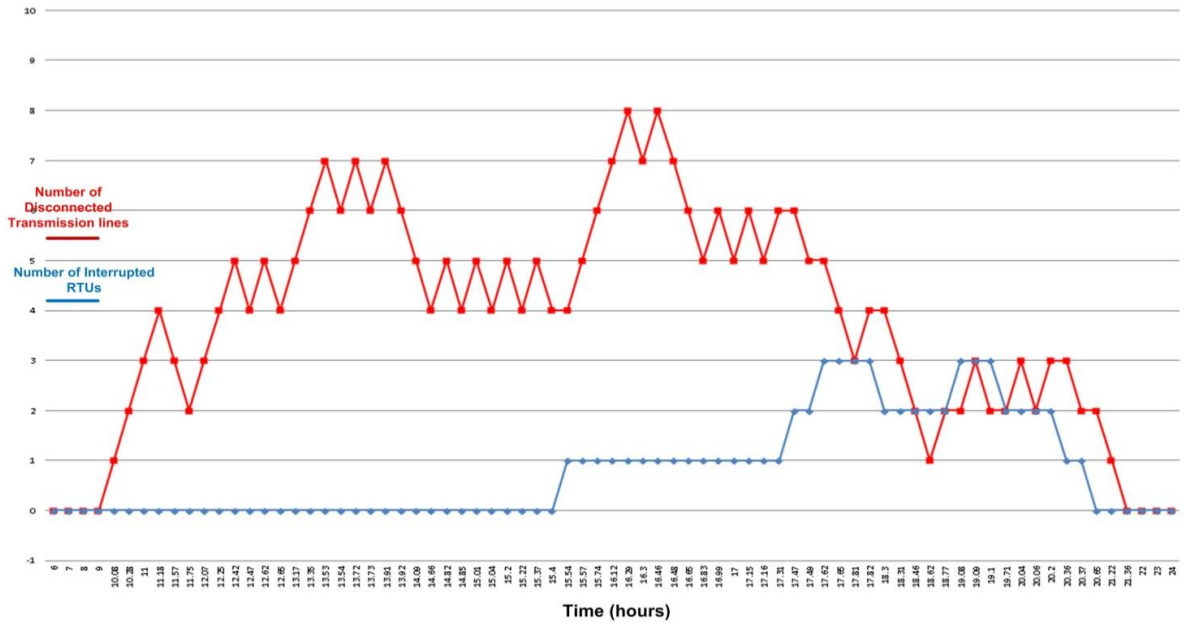


Figure 5.32 Affected SUC and SCADA components in Test No.5

5.3.3.2 TEST No.6: FID failure (double non-key substations)

The summary of this test is included in Appendix IV (Table A-IV 49). No transmission lines become overloaded and disconnected due to failures of studied FIDs. Locations of these lines are given in Figure 5.33. Figure 5.34 shows what occur after triggering technical failures of the FID devices for the line 47 and 157.As shown in this figure, the abnormal disconnections of line 47 and 157, triggered by the technical failures of the FIDs for these two lines, caused none of the abnormal disconnections of other transmission lines. As observed from this test, none of the SUC components or SCADA components was affected. Compared to the single non-key substation FID failure test, the ASSAI decreases from 0.9996 to 0.9991 since two SUC component failures are triggered in this test. However, the calculated DI remains the same (equals to 14 in this test). Increasing the number of non-key node failures to 2 does not increase the overall degree of impact.

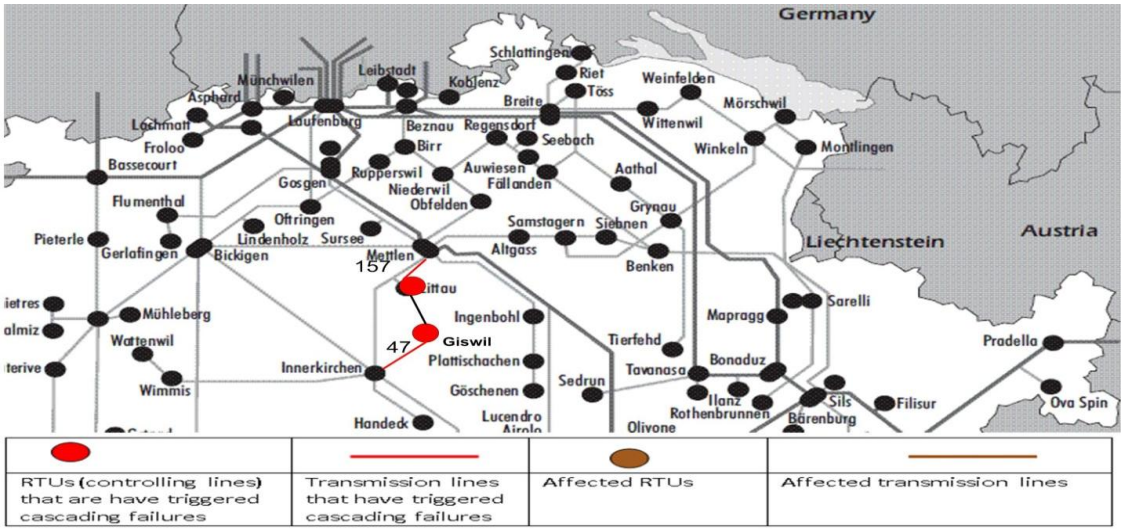


Figure 5.33 Locations of studied substations and lines in Test No.6

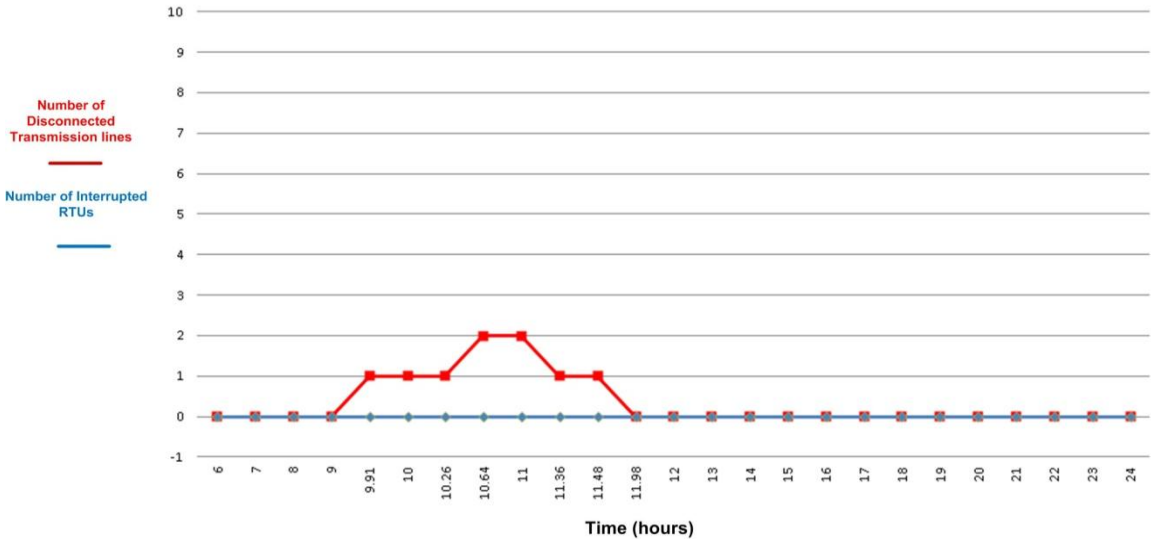


Figure 5.34 Affected SUC components and SCADA components in Test No.6

5.3.3.3 TEST No.7: RTU failure (two key substations)

The summary of this test is included in Appendix IV (Table A-IV 50). About 10 transmission lines were affected by the failures of the RTUs. The locations of the affected SUC components are given in Figure 5.35. Lines 200 and 117 remained connected since alarms for these lines were lost due to the hardware failures of the RTU devices monitoring and controlling these lines. No interruptions of SCADA devices are observed in this test. Compared to results observed from single RTU failure test, more SUC

components are affected and the degree of impact increases from 20 to 28. The consequences caused by double technical failures become worse compared to single technical failures.

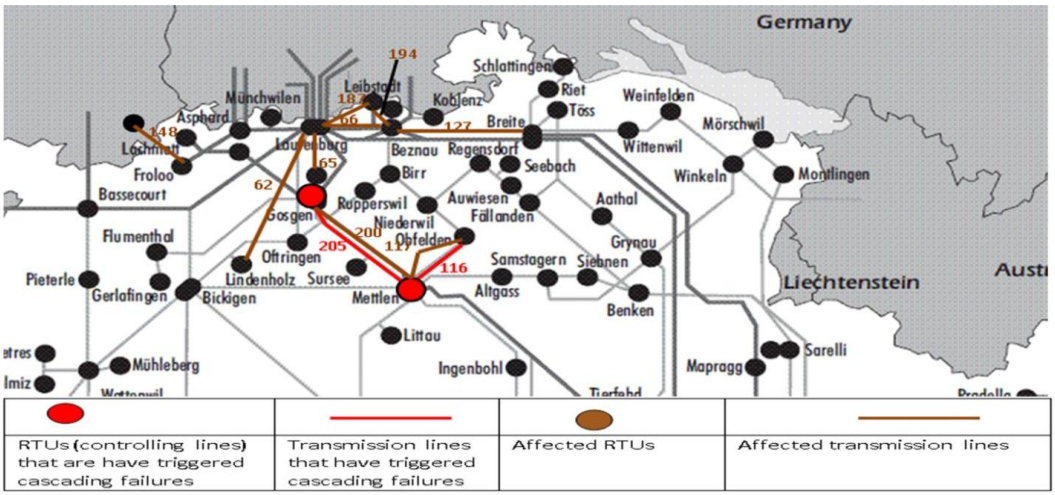


Figure 5.35 Locations of studied substations and line in Test No.7

Figure 5.36 shows what occurs after triggering the technical failure of the RTUs of substation GOSGEN and MELTTLEN. As seen from this figure, line 205 and 116 remain disconnected due to the technical failures of corresponding RTU devices.

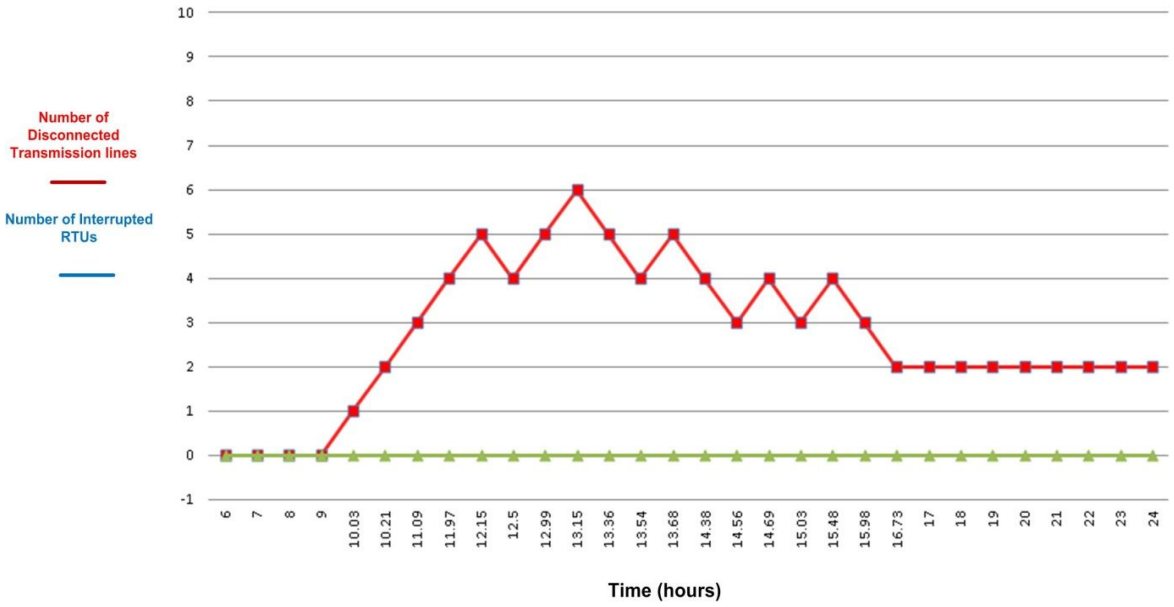


Figure 5.36 Affected SUC and SCADA components in Test No.7

5.3.3.4 TEST No.8: RTU failure (two non-key substations)

The summary of this test is included in Appendix IV (Table A-IV 51). No transmission lines became overloaded and disconnected. Locations of these lines are given in Figure 5.35.

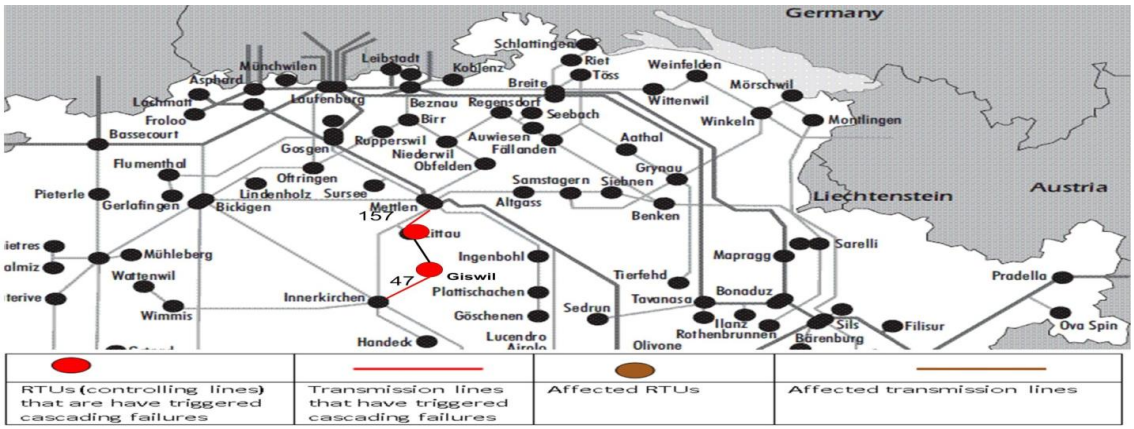


Figure 5.37 Locations of studied substations and lines in Test No.8

Figure 5.38 shows what occurs after triggering the technical failures of the RTU devices for the line 47 and 157. As shown in this figure, the technical failures of two RTUs have no negative effects on other SUC and SCADA components. Compared to the single RTU failure test, the ASSAI decreases from 0.9962 to 0.9923 since two SUC component failures are triggered in this test. However, the calculated DI remains the same (equal to 18 in both tests). Increasing the number of non-key node failures to 2 does not increase the overall DI.

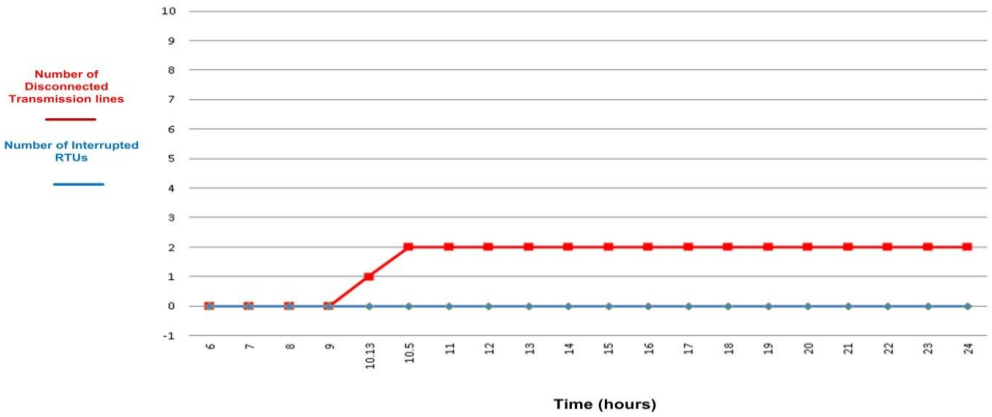


Figure 5.38 Affected SUC and SCADA components in Test No. 8

5.3.3.5 Summary of Double Failures Tests

The results of four tests conducted during double failure experiment are summarized in Table 5.19 and illustrated in Figure 5.39.

Table 5.19 Summary of double failure tests

	FID failure (key substations)	**FID failure (non-key substations)**	**RTU failure (key substations)**	**RTU failure (non-key substations)**
No of affected SUC components	28	0	10	0
No of affected SCADA components	4	0	0	0
No of lost alarms	0	0	2	0
ASSAI	0.9776	0.9991	0.9889	0.9923
Degree of impact	42 (Very Strong)	14 (Weak)	28 (Middle)	18 (Weak)

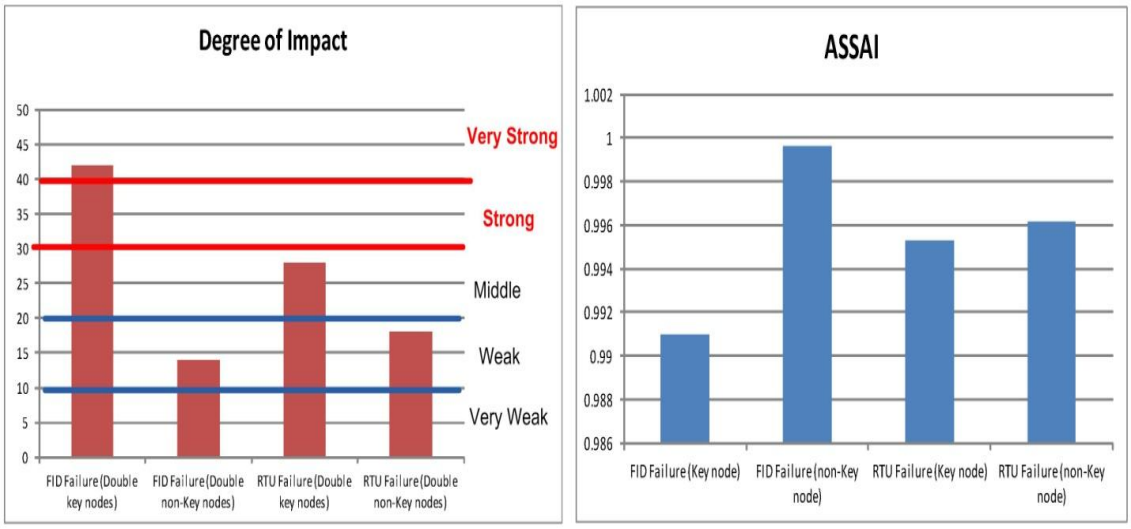


Figure 5.39 Summary of double failures tests

As shown in Figure 5.39 and Table 5.19, the results observed from these tests are similar to previous single failure tests. Cascading impacts caused by double FID failures (in key substations) are strong, the highest ones among all the tests. The number of affected SUC

components is 28, meaning that 28 transmission lines become overloaded. The number of affected SUC components observed during RTU key-substation tests is 10, less than the number observed during FID key-substation tests. More SUC components and SCADA components are affected if FID technical failures are triggered in two key stations. Both double FID and RTU failure tests on the non-key substations show much less negative consequences. The calculated DI observed in these two tests is weak and none of the SUC components and SCADA components are affected.

5.3.4 Summary of Experiment III

Table 5.20 Summary of the experiment III

	No of affected SUC components	**No of affected SCADA components**	**No of lost alarms**	**ASSAI / Vulnerability**	**Degree Of impact**
FID failure (single key substation)	18	2	0	0.9910	34 (Strong)
FID failure (double key substations)	28	0	0	0.9976	42 (Very Strong)
FID failure (single non-key substation)	0	0	0	0.9996	14 (Weak)
FID failure (double non-key substations)	0	0	0	0.9991	14 (Weak)
RTU failure (single key substation)	3	4	1	0.9953	20 (Middle)
RTU failure (double key substations)	10	0	2	0.9889	28 (Middle)
RTU failure (single non-key substation)	0	0	0	0.9962	18 (Weak)
RTU failure (double non-key substations)	0	0	0	0.9923	18 (Weak)

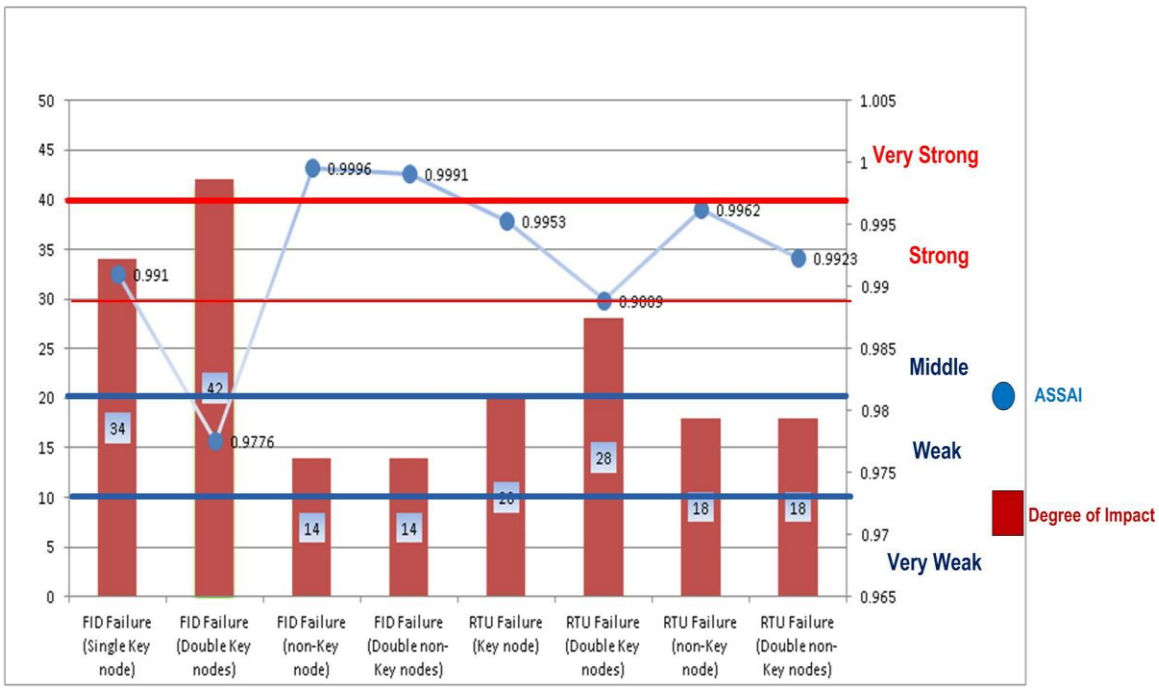


Figure 5.40 Summary of the experiment III

The results from all the tests in the whole network worse-case failure experiment are shown in Table 5.20 and Figure 5.40. This experiment focuses on the worse-case scenarios by assuming the operator is unable to handle any alarm received by the control centre (MTU) due to natural or technical failures (hazards), e.g., the failure of the control panel, flooding/fire in the control centre, etc. Two types of tests are developed in this experiment: single and double failure tests. In single failure tests, only failures occurring at one substation are simulated, while failures occurring at two substations are simulated in double failure tests. Instead of all three substation level devices, only two devices, FID and RTU, are included in this experiment. As demonstrated in these tests, failures of FIDs in both single and double failure tests show very strong DIs and the smallest calculated ASSAI. It is also observed in this experiment that the increase of the number of key substations could also lead to more significant negative consequences.

6 OVERALL RESULTS ASSESSMENT AND POTENTIAL TECHNICAL IMPROVEMENTS

The present chapter, which can be considered as the step 4 and 5 of the methodical framework, interprets and analyzes the simulation results obtained from three experiments, presented in Chapter 5, in order to identify hidden vulnerabilities between the SCADA system and its monitored/controlled SUC. Furthermore, potential technical improvements of systems are proposed to minimize the negative effects caused by those vulnerabilities and to better protect CIs in the long run.

6.1 Results Assessment

The overall simulation results from all three experiments, described in Chapter 5, are summarized in Table 6.1. It should be noted that due to the fact that the scope of Experiment I is limited to one substation, parameters such as ASSAI and Degree of Impact are not applicable to this experiment.

Table 6.1 Summary of all three experiments

Experiment		Test Name	Substation Unavailability	ASSAI	Degree of Impact
Substation Level Failure Single Mode		FCD FO mode	0.4%	N/A	N/A
		FCD FC mode	2.5%	N/A	N/A
		FCD SO mode	5.4%	N/A	N/A
		FID FRL mode	0	N/A	N/A
		FID FRH mode	2.5%	N/A	N/A
		RTU FRF mode	26%	N/A	N/A
		RTU FRW mode	4.3%	N/A	N/A
		RTU FRC mode	3.8%	N/A	N/A
Small network Level Single Failure Mode	Normal-case	FCD FO mode	N/A	1.0	10 (Very Weak)
		FCD FC mode	N/A	0.9996	16 (Weak)
		FCD SO mode	N/A	0.9998	16 (Weak)
		FID FRL mode	N/A	0.9997	16 (Weak)
		FID FRH mode	N/A	0.9998	16 (Weak)
		RTU FRF mode	N/A	0.9970	20 (Middle)
		RTU FRW mode	N/A	0.9996	20 (Middle)
		RTU FRC mode	N/A	0.9998	16 (Weak)
	Worse-case	FCD FC mode	N/A	0.9604	40 (Very Strong)
		FCD SO mode	N/A	0.9357	42 (Very Strong)
		FID FRH mode	N/A	0.9358	44 (Very Strong)
		RTU FRF mode	N/A	0.9940	20 (Middle)
		RTU FRW mode	N/A	0.9980	20 (Middle)

Whole Network Worse-case Failure Modes	Single Failure	FID failure (key substation)	N/A	0.9910	34 (Strong)
		FID failure (non-key substation)	N/A	0.9996	14 (Weak)
		RTU failure (key substation)	N/A	0.9953	20 (Middle)
		RTU failure (non-key substation)	N/A	0.9962	18 (Weak)
	Double Failure	FID failure (key substations)	N/A	0.9976	42 (Very Strong)
		FID failure (non-key substations)	N/A	0.9991	14 (Weak)
		RTU failure (key substations)	N/A	0.9889	28 (Middle)
		RTU failure (non-key substations)	N/A	0.9923	18 (Weak)

* ASSAI : Average Substation Service Availability Index

After analyzing these simulation experiment results, vulnerabilities between the SCADA system and the SUC due to their interdependencies can be summarized as follows:

1. **Importance of field level devices should not be underestimated by researchers**: As defined in section 2.4.1 (Chapter 2), field level devices such as FID and FCD belong to level 1, the lowest level in the standard SCADA system hierarchy. It is an interface connecting a SCADA system to its controlled/monitored physical processes (SUC). Therefore, these devices can be regarded as interface devices as well. In general, most past research works especially modeling efforts related to SCADA systems often focus on RTU devices, which belongs to level 2 in the standard SCADA system hierarchy, and ignore the existence of this type of devices [39, 125, 126]. However, as observed during worse-case tests in the last two experiments, negative consequences caused by failures of the field level devices could also be significant. In the substation level single failure mode experiment, among all the SCADA-related substation level devices, failures of the RTU device cause more negative consequences. As observed in the small network level single failure mode experiment, collected results from normal case tests show that negative consequences caused by failures of the RTU device still seem significant (highest degree of impacts and the lowest ASSAI). However, if assuming that the operator is unable to handle any alarm (worse-case scenarios), consequences caused by failures of field devices become worse compared to failures of RTU devices. The simulation results observed in three worse-case single failure mode tests related to field devices (FID FC, FCD SO, and FID FRH) in this experiment demonstrate very strong degree of impact and smallest ASSAI. This phenomenon is also observed in the whole network worse-case scenario failure modes experiment. In this experiment, the ASSAI obtained from key

substation single FID failure test is 0.991, while it is 0.9996 in key substation single RTU failure test. In same tests, the DI caused by single FID failure is strong, while it is middle in RTU failure test. Furthermore, the propagation of failures between the SCADA system and SUC is also observed during FID worse-case tests, but not during RTU worse-case tests[25].

2. **A predictable delay of dependency failures is important:** As observed in FID key substation failure tests and FID double key substation failure tests of the third experiment, the propagation of failures crossing interlinked systems needs time, it is not instant. It takes a certain period before the failures could propagate from one system to another due to interdependencies between them. This period can be defined as the *delay of dependency failures.* For example, this delay is about 7 hours in FID single key substation tests and about 6 hours in FID double key substation tests. Based on these two tests, it seems that the delay of dependency failures is proportional to the degree of impact and inversely proportional to the ASSAI meaning worse consequences shorter delay period. This period is very important for minimizing negative effects caused by interdependencies. If failures were to stop cascading during this period, then propagation of failures into another system could possibly be avoided.

3. **Negative consequences caused by failures of devices in key substations are significant:** 12 key substations have been identified and listed in Table 3.5. The third experiment also demonstrates the importance of key substations of the SCADA system since increasing the number of failed key substations and non-key substations show very different results. In this experiment, negative consequences caused by failures of devices become more significant if the number of failed key

[25] One explanation for this phenomenon is that the RTU device loses its connection to its field level devices during tests of FRF and FRW. As a result, the RTU device is unable to handle any alarm sent by these devices. This is also the reason why the results observed from normal and worse-case RTU tests are similar. Therefore, although results from worse-case tests show that the negative consequences caused by field devices are more significant than by RTU devices, RTU devices are as important as field level devices.

substations increases. For example, the ASSAI value calculated in FID single key substation failure tests is 0.991, while the value drops to 0.9776 when failures of two key substations are triggered (degree of impact increases after increasing the number of failures of key substations in this case). This phenomenon is observed during RTU failure tests as well. However, increasing the number of failures of non-key substations seems to cause no significant negative effects. The degree of impact remains the same after triggering failures of two non-key substations during both FID and RTU non-key substation tests. For example, the ASSAI value calculated in FID single non-key substation failure tests is 0.9996, while the value merely drops to 0.9991 in FID double non-key substation failure tests (degree of impact remains the same after increasing the number of non-key substations in this case). Therefore, the reliability of key substations of the SCADA system is important.

4. **The role of the human operator in the control centre is important:** The human operator in the control centre plays a very important role in the SCADA system. Although the lack of responses from human operators might not be the cause of failures of substation level devices, negative consequences caused by the failures of these devices could worsen significantly. As demonstrated in all the experiments, if the human operator is able to respond to overload alarms adequately and send commands to corresponding RTUs for further corrective functions, failures could not propagate and negative consequences could be significantly minimized. In the second experiment, for instance, the ASSAI value calculated in FID FC normal case tests is 0.9996, while this value drops to 0.9604 in the same failure mode worse-case test. The degree of impact also changes from weak to very strong. Maintaining normal functionalities of the human operator in the control centre as well as required hardware of the control centre, can minimize negative consequences caused by failures of substation level devices and even stop propagation of those failures. Therefore, the absence of the human operator has to be strictly avoided.

6.2 Potential Technical Improvements

Although the propagation of cascading failures due to interdependencies cannot be completely prevented, according to the results collected from these experiments, following suggestions are proposed, which could be useful to minimize the negative effects caused by this type of cascading failure and improve the coping capacity of the SCADA system:

1. **Increasing the reliability of field level devices:** Several measures can be recommended. **1). Increasing redundancy.** As mentioned in section 6.1, it is very important to maintain normal functionality of field level devices such as instrumentation devices and control devices due to their specific installation locations (where interlinked systems overlap). Installing more redundant devices could be one option to reduce the possibility of device failures. **2). Implementation of diversity**. However, redundant devices could also fail simultaneously (CCFs) due to common causes such as human errors, lack of maintenance, design inadequacy, etc. Design diversity can be used for the protection against CCFs. For instance, field level devices from different vendors could be selected as redundant devices. **3). Implementation of self-diagnosis**. For the field level devices installed at key substations, it is worthy to implement some more sophisticated and advanced techniques in order to reduce probability of CCFs, e.g., adoption of self-diagnosis techniques. For example, a real-time monitoring system can be installed for diagnosing current operation status of instrumentation devices, which is responsible to monitor outputs of redundant instrumentation devices in real-time. If these outputs vary significantly meaning at least one of devices must be in malfunction, then an alarm can be sent informing maintenance personnel.

2. **Prevention of failure propagation:** In order to minimize the negative effects caused by the propagation of cascading failures, a real-time prediction system for a whole SCADA system can be implemented for analyzing most recent information (monitored variables) from all substations of the SCADA system. This system should be developed to be able to identify early symptoms of failures which will trigger cascading failures and eventually propagate from one system to another. The correct identification must be conducted during the period of delay of

dependency failures and further actions can be performed in order to successfully stop the propagation.

3. **Increasing the capacity of batteries for RTUs of the SCADA system**: One of the major causes for service interruptions of RTUs is the loss of power supply due to full consumption of their batteries in case of preferred power loss (caused by interdependencies). This type of interruptions could be minimized by increasing the battery capacity in the case when power supply from another source is temporarily unavailable.

4. **Setting up a remote emergency centre:** Worse-case tests have demonstrated the importance of maintaining the normal functionalities of the control centre including human operators. In the case when natural disasters occur, e.g., earthquake, flooding, etc, not just operators will not be able to perform any safety actions, devices installed in the control centre, e.g., control panels, working stations, monitors, etc., will also be likely to fail to function. The control centre will lose all the information and essential facilities to maintain normal operation of its monitored system. Setting up an emergency centre that is located a certain distance away from the current control centre is necessary and should not be neglected. During the normal situation, this so called remote emergency centre receives/updates/backups current field information directly from the control centre. During the emergency situation, the role of the current control centre can be transferred to the remote emergency centre where operators should be able to continuously monitor/control the system (SUC) and restore the system data according to previously stored/backup information. Although setting up a remote emergency centre will require significant financial supports and the necessity of using this centre is relatively low, the whole society will certainly benefit from this work in the future.

7 CONCLUSIONS AND FUTURE WORKS

In this last chapter, conclusions regarding the research works presented in this thesis are given. In addition, suggestions and an outlook for future research works are also provided in this chapter.

7.1 Conclusions

Interdependencies within and among Critical Infrastructures (CIs) have dramatically increased the overall complexity of related systems, causing the emergence of unpredictable behaviours and negative impacts, in particular, and making them more vulnerable to cascading failures with widespread consequences. It is vital to identify and study vulnerabilities caused by these interdependencies through an advanced modelling/simulation approach, which generally faces two major technique challenges. The first challenge is to model a single CI due to its inherent characteristics. The second challenge appears when more than one CI or subsystem within one CI must be considered and interdependencies among them need to be tackled. Currently, a number of modeling approaches have been developed and applied, trying to meet these challenges, e.g., Complex Network (CN) theory, PetriNet(PN)-based modeling, Agent-based Modeling (ABM), etc; each of them having limitations. To fully utilize benefits/advantages of each approach, it is necessary to integrate different types of modeling approaches into one simulation tools. However, one of the key challenges for developing such type of simulation tool is the required ability to create multiple-domain models, and effectively exchange data among these models. Motivated by these challenges, four research objectives have been listed in Chapter 1 and are given below:

1. To develop a novel and comprehensive approach for exploring and assessing the vulnerabilities caused by interdependencies within and among CIs qualitatively and quantitatively using advanced system modelling and simulation techniques. It should be noted the application of this approach should not be limited to the interdependencies among CIs, but also within single CIs, e.g.,

interdependencies among subsystems (within a CI). In this research work, this approach will be applied to explore and study interdependencies between a SCADA subsystem and its associated SUC within the power supply sub-sector. Furthermore, a modelling approach needs to be developed, which is capable of integrating Human Reliability Analysis (HRA) into the developed CI model.

2. To create a real-time experimental simulation test-bed for the purposes of implementing the proposed hybrid modelling/simulation approach and demonstrating its applicability and feasibility using the test-bed.

3. To explore interdependencies between the SCADA system and the SUC and identify vulnerabilities related to interdependencies using the developed experimental simulation test-bed.

4. To suggest some improvements of identified weaknesses in the systems analysed

The research work described in this thesis has achieved all these objectives, which follows a 5-step methodical framework, proposed by Eusgeld and Kröger [30], for analyzing vulnerabilities due to interdependencies within and among CIs. This thesis intends to focus on the third step, in-depth analysis, for which a novel hybrid modelling/simulation approach has been proposed and developed capable to represent these interdependencies. It proved capable to perform both qualitative and quantitative or semi-quantitative analyses of interdependency-related system functionalities. This approach integrates different types of modelling/simulation techniques into one simulation tool by adopting the concept of modular design. The core of this approach is the idea to divide the overall simulation tool into different simulation modules at first, and combine them in a distributed simulation platform. The simulation standard of High Level Architecture (HLA) is selected to implement this approach and distribute different simulation components. Furthermore, an HLA-compliant experimental simulation test-bed has been developed, which is based on the proposed hybrid modeling/simulation approach. As demonstrated in the feasibility experiment and failure propagation experiment, this test-bed as well as the hybrid modeling/simulation approach, is capable to simulate all types of interdependencies within and among CIs. Although, the original aim of this test-bed is to explore and investigate hidden vulnerabilities between the SCADA system and its monitored/controlled

System Under Control (SUC), the capabilities of the test-bed can be regarded as generic and be expanded, benefiting from the efficiency and flexibility of the HLA simulation standard, to study interdependencies among other CI sectors/sub-sectors, e.g., transport sector, ICT sector, etc. Furthermore, real devices such as a sensor and a PID controller can be integrated into the test-bed.

In order to utilize the experimental simulation test-bed to study interdependency-related vulnerabilities between the SCADA system and the SUC, a SCADA model is developed by combining the ABM with other modelling/simulation techniques such as Monte Carlo simulation, Fuzzy Logic, and Finite State Machines (FSMs). In this model, substation level devices such as FIDs, FCDs, and RTUs are modelled using the failure-oriented modelling approach, proposed in this thesis. A specific model has been developed to include human operator performance, for which CREAM (Cognitive Reliability Error Analysis Method) has been selected and utilized in combination with new elements such as the ABM approach and Fuzzy Logic. The developed SCADA model is then integrated into the test-bed coupling it with the SUC model, an existing agent-based model developed for other purposes, for the overall simulation. Three sets of experiments are further designed and performed, using the Swiss electricity transmission network as an exemplary application. Experiments start from the scope of a substation in which different single technical failures of corresponding SCADA substation level devices are triggered (simulated) to determine and rank the severity of each failure, which can be regarded as a quantitative experiment. Then the second experiment expands the scope of the simulation to a small network of the SCADA system focusing on the analysis of consequences caused by each technical failure semi-quantitatively. Finally, the third experiment includes the whole network of the SCADA system into the simulation.

These experiments demonstrate the importance of mapping complex physical systems from the real world in the simulation world and then project data from the simulation world back into the real world. Technical failures can be triggered and propagation of these failures can be observed during the simulation, especially failures crossing boundaries between the SCADA system and the SUC for the purpose of consequence investigation during the simulation. The simulation results can then be collected and analyzed for further improvements of the system, e.g., the system reliability, coping capacity, etc. Furthermore,

the last experiment also considers the worse-case scenarios and shows how both systems will function if the human operator is unable to handle any alarm. Based on the results from these experiments conducted on the test-bed, hidden vulnerabilities of the studied SCADA system due to its interdependencies with the SUC have been identified, which can hardly be obtained without an appropriate simulation tool due to the complexity of real systems (CIs). Two of some interesting findings based on these identified vulnerabilities are 1) the importance of field level devices such as instrumentation devices and control devices, which has been underestimated by previous SCADA related research works, and 2) the identification of the delay of dependency failures, which is the time period in which the propagation of failures could be halted if correct actions were performed. The propagation of cascading failures due to interdependencies cannot be completely prevented. Nevertheless, based on the results collected from these experiments, suggestions for system improvements are provided that could be useful to minimize the negative effects caused by this type of cascading failures and improve the coping capacity of the SCADA system. For example, self-diagnosis techniques are suggested to be adopted to protect field level devices against CCFs and a remote emergency centre is suggested to be set up in order to handle extreme situations in case natural disasters occur.

7.2 Outlooks of Future Interdependency Study

The society needs to face the fact that interdependencies within and among CIs are more complicated than imagined and research works related to this topic will possibly not become easier in the future. Each approach developed or adapted for this topic has its own advantages and disadvantages. In practice, there is still no "silver bullet" approach. Therefore, related research works should not be limited to the arguments about which approach is better and which one is not. Combining different approaches into one simulation tool by adopting the technique of distributed simulation using appropriate

simulation standards already proves its feasibility and applicability, already presented in this thesis, and will hopefully be accepted by researchers in the field of CI interdependency study[26], or even in the field of reliability study. With the help of this approach, even classic approaches such as the FTA can be integrated with advanced modelling approaches such as the ABM approach and used for more advanced and comprehensive system reliability analysis.

It should be noted that the implementation of this type of simulation approach is not an easy work. Lots of computer programming (coding) works are definitely required. The fundamental structure of the whole simulation tool needs to be re-constructed and the interface of each individually developed component must be compatible with its peer components. Time regulation among various distributed components is another technical challenge that needs to be carefully handled. Except these technical difficulties, more benefits will be expected for future developments after the implementation/development of this approach, e.g., improved flexibility and modularization of simulation development, distribution of simulation work load, and possibilities of bringing real devices into the simulation and reusing models/simulators developed for other purposes.

7.3 Future Works

The following list gives a brief overview of future works that can be done for further improvement:

1. **Including Communication Unit into the SCADA model**: As mentioned in Chapter 2, the research works described in this thesis mainly focuses on the substation level devices of the SCADA system. Communication protocols, e.g., Modbus, Profibus, etc, communication devices, e.g., routers, modems, etc, as parts of the Communication unit are not implemented in the current SCADA model.

[26] This has been endorsed by Kröger and Zio in [25]

During future works related to a refinement of the development of the SCADA model, the communication unit should be implemented.

2. **Cyber attacks:** Cyber attacks such as hacking and interrupting the communication protocols that could possibly overwrite control commands sent by a control centre to field devices of the SCADA system are also worthy to be investigated after completing the development of the communication unit of the SCADA model. Similar to the failures of substation level devices, cyber attacks can be regarded as one of the entry points, which could trigger cascading failures that will eventually propagate from one CI to another one.

3. **Proper measures for vulnerability need to be developed:** The measurement for the term vulnerability used by the research work described in this thesis is the ASSAI, which is simple and straightforward. For the future CI interdependency study, more comprehensive measures need to be developed, which can be used to fully represent the complicities of the vulnerabilities within and among CIs and be able to quantify them as well.

4. **More experiments focusing on the delay of dependency failures are recommended to be developed:** The delay of dependency failures is identified during the third experiment of this research work. The importance about this period is that if the correct actions can be performed during this period, cascading failures could be stopped. Several questions can then be raised, for example

    - The length of this period is determined by which factors/parameters?
    - Is the delay period related to the interface devices among interconnected systems ?

    More experiments can be developed regarding these questions. These experiments can continuously use current modeled systems (SCADA and SUC) and expand experiments to an even wider scope, e.g., interdependencies among CI sectors/sub-sectors.

5. **CCFs are recommended to be included into the simulation:** As presented in Chapter 3, there must be adequate awareness to the fact that negative effects of the CCFs on the reliability of the SCADA system could be significant. It is important to consider CCFs as part of the overall simulation. From a technical point of view, benefiting from the approach of ABM, integrating CCFs into the SCADA model is not difficult. However, from a reality point of view, having reasonable data resources for CCFs is more important and difficult to obtain. Therefore, CCFs could be taken into account if a reasonable data resource became available.

6. **Model of human operators needs to be improved**: Research works described in this thesis introduce a new approach to model human operators by implementing the approach of HRA (CREAM in this thesis) using the ABM approach, which can be regarded as a pioneer work in this research field. Currently, four out of nine CPCs (Common Performance Conditions) are selected to be assessed during the simulation. In order to improve the accuracy of this model, more CPCs should be assessed if more data about other five CPCs became available.

7. **Natural hazard events can be included into the simulation:** As presented by the example of Hurricane Katrina in Chapter 1, negative consequences triggered by natural hazards can be significant enough causing failures crossing CI-boundaries leading to multi-infrastructural collapse. What happened in Fukushima reminds us again that we can never underestimate the power of natural hazards. In the third experiment, we already demonstrate that it is possible to simulate worse-case scenarios using the current test-bed from the technique point of view. Therefore, it is necessary to map these natural hazards from the real world into the simulation world using the current experimental test-bed and evaluate their (negative) consequences.

8. **Upgrade SUC model to Anylogic 6.4:** The model of the SUC used in the research works of this thesis was developed almost four years ago using the software of Anylogic 5.5. This software cannot fully handle large amounts of data exchange, which is required for the distributed simulation. Therefore, upgrading the SUC model to the version of Anylogic 6.4 is totally recommended.

9. **Further development of the test-bed:** Benefiting from the efficiency and flexibility of the adopted HLA simulation standard, capabilities of the current experimental test-bed can be expanded since new simulation components can easily be integrated into the test-bed and interact with existing peer components for many other experiments without major efforts of modifying the current architecture of the test-bed. For example, real field devices such as a sensor and a PID controller can be integrated into the test-bed. These field devices will be directly connected to the RTU agent developed in the SCADA simulator. More practical experiments, such as vulnerability analysis of a typical substation, can be conducted.

List of Abbreviations

ABM	Agent-based Modeling
ALSP	Aggregate Level Simulation Protocol
ASAI	Average Service Availability Index
ASSAI	Average Substation Service Availability Index
ATHEANA	A Technique for Human Event Analysis
CB	Circuit Breaker
CFP	Cognitive Failure Probability
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CN	Complex Network
COCOM	Cognitive Control Model
COG	Centre Of Gravity
CPC	Common Performance Condition
CREAM	Cognitive Reliability Error Analysis Method
CU	Control Unit
DCS	Distributed Control System
DCST	Dynamic Control System Theory
DI	Degree of Impact
DIS	Distributed Interactive Simulation
DMSO	U.S. Defense Modeling and Simulation Office
DoD	U.S. Department of Defense

CDM	Communication Data and Management
EFC	Error-Forcing Context
EPOCHS	Electric Power and Communication Synchronizing Simulator
EPSS	Electric Power Supply System
FC	Failure to Close
FCD	Field level Control Device
FF	Following Federate
FID	Field level Instrumentation Device
FIFO	First In First Out
FIS	Fuzzy Inference System
FLSC	Swedish Air Force Air Combat Simulation Centre
FO	Failure to Open
FOCP	(Swiss) Federal Office of Civil Protection
FRC	Failure to Run due to Communication error
FRF	Failure to Run with Field device
FRH	Failure to Run (too high)
FRL	Failure to Run (too low)
FRW	Failure to Run due to Hardware failure
FSM	Finite State Machine
FTA	Fault Tree Analysis
FOM	Federate Object Model
FVT	Federation Virtual Time
HEP	Human Error Probability

HLA	High Level Architecture
HMI	Human Machine Interface
HRA	Human Reliability Assessment
HTA	Hierarchical Task Analysis
ICT	Information and Communication Technology
ICS	Industrial Control System
IEEE	Institute of Electrical and Electronic Engineers
IIM	Input-output Inoperability Modeling
IRRIS	Integrated Risk Reduction of Information-based Infrastructure Systems
ISS	Interactive Simulation Systems
LAN	Local Area Network
LTI	Linear Time Invariant
MF	Membership Function
MTTR	Mean Time To Repair
MTU	Master Terminal Unit
MV	Measured Variable
OMT	Object Model Template
PLC	Programmable Logic Controller
PN	PetriNet
PSF	Performance Shaping Factor
PT	Power flow Transducer
RF	Regulating Federate

RISI	Repository of Industrial Security Incidents
RTU	Remote Terminal Unit
RTI	Run Time Infrastructure
OM	Operational Mode
OMT	Object Model Template
SCADA	Supervisory Control and Data Acquisition
SO	Spurious Operation
SOE	Sequence of Events
SOM	Simulate Object Model
SS	Safety System
THERP	Technique for Human Error Rate Prediction
TSO	Transmission System Operator
UDP	User Datagram Protocol
WAN	Wide Area Network

Appendix I-1

LIST OF PUBLICATIONS

1. **Nan, C**. (2011). High Level Architecture, as part of Chapter 6, *Analysis of methods*, in Kröger, W and Zio, E (Eds.): Vulnerable Systems; Springer. ISBN 978-0-85729-654-2.
2. **Nan, C**., and Kröger, W. (2011) Lessons learned from Adopting Distributed Simulation Approach for CI Interdependency Study, in ESRA (European Safety Reliability Association) Newsletter December 2011.
3. Eusgeld, I., **Nan, C**., and Dietz, S. (2011). "System-of-systems" Approach for Interdependent Critical Infrastructures. Journal of Reliability Engineering & System Safety. 96(6): 679-686. ISSN: 09518320
4. **Nan, C** and Eusgeld, I. (2011). Exploring Impacts of Single Failure Propagation between SCADA and SUC, IEEE International Conference on Industrial Engineering and Engineering Management (IEEM) 2011. 1564-1568. ISSN**:** 2157-3611.
5. **Nan, C**., Kröger, W., and Probst, P. (2011). Exploring Critical Infrastructure Interdependency by Hybrid Simulation Approach. In proceedings of Annual European Safety and Reliability Conference (ESREL) 2011. 2483-2491. ISBN 978-0-415-68379-1.
6. **Nan, C** and Kröger, W. (2011). A New Modeling Approach for Resolving CI Interdependency Issues. In proceedings of the 11th International Conference on Applications of Statistics and Probability in Civil Engineering (ICASP11). 1876-1884. ISBN: 978-0-415-68379-1.
7. **Nan, C**., Kröger, W., and Eusgeld, I. (2011). Study of Common Cause Failures of the SCADA System at Substation Level, Scientific report for Swiss Federal Office of Civil Protection.
8. **Nan, C**. (2011). Further Method Development (HLA). Scientific report for Swiss Federal Office of Civil Protection.
9. **Nan, C**., and Eusgeld, I. (2010). Adopting HLA Standard for Interdependency Study. Journal of Reliability Engineering & System Safety. 96(1): 149-159. ISSN: 0951-8320.
10. Kröger, W., **Nan, C**., Trantopoulos, K., Zhou, L., and Eusgeld, I. (2010). Interdependencies between critical infrastructures. Scientific report Swiss Federal Office of Civil Protection.
11. **Nan, C** and Eusgeld, I. (2010). Further Development of Modeling and Simulation to Disclose Vulnerabilities of Interdependent Critical Infrastructures. Scientific report for Swiss Federal Office of Civil Protection.

12. Eusgeld, I and **Nan, C**. (2009). Creating a Simulation Environment for Critical Infrastructure Interdependencies Study. In proceedings of the IEEE International Conference on Industrial Engineering and Engineering Management (IEEM) 2009. 2104-2108. ISBN: 978-1-4244-4869-2.

Appendix I-2

FULL INTERDEPENDENCY TABLE

Table below lists of recently documented incidents whose consequences were worsened due to interdependencies within and among CIs (Based on work done by Kröger et. al in [14], modified by the author)

Incident	Date	Affected area(s)	Primary Cause (Natural of Cause)	Affected Infrastructures	Consequences
1998 Ice Storm Canada	January, 1998	Eastern Ontario, Southern Quebec of Canada and parts of New York and New England of USA	A massive ice storm created a major disaster in areas in Canada and USA. (Natural hazard)	Number of affected CI sectors: 4 Number of affected CI subsectors: 4	*3.6 million people were affected *Economic damage caused by this storm was estimated to be 3 billion U.S dollars.
	Affected Infrastructures (in detail) : Energy(Power supply)->Water and Food (Food supply) Transport(Road transport)-> Water and Food (Food supply) Energy(Power supply)-> Public Safety (Emergency organization)				
2001 Baltimore Howard Street Tunnel Fire	July 18, 2001	Baltimore, USA	A freight train detailed while passing through Howard Street Tunnel in Baltimore and caused the fire explosion due to subsequent ignition of the flammable liquid. (Technical failure)	Number of affected CI sectors: 4 Number of affected CI subsectors: 6	*12 million U.S.dollars associated with incident. *23 bus lines and several train services were suspended or delayed. *Delays of Coal and limestone services. *Extremely heavy road congestion in Baltimore. *14 million gallons of water lost *1,200 Baltimore buildings lost electricity. * Service disruptions for phone/cell phone and slowed internet service.
	Affected Infrastructures (in detail) : Transport (Rail transport)->Water and Food (Drinking water supply) Transport (Rail transport) <-->ICT (Media/radio) Transport (Rail transport)-> Energy(Power supply) Water and Food (Water supply)->ICT (Internet/Telecommunication) Water and Food (Water supply)-> Energy(Power supply)				

2001 World Trade Center Attack	September 11	New York, USA	Terrorist attack with two hijacked planes caused the collapse of WTC, New York . (Social Hazard)	Number of affected CI sectors: 7 Number of affected CI subsectors: 10	*In total 2,993 people were killed, more than 6000 injured. *Loss of power supply in a big area *Loss of gas and steam supply * A lot of phone lines and data lines were damaged. Most communication traffic were rerouted. *New York Stock Exchange closed. International economy was affected * Loss of water supply * All air and subway services were suspended
	Affected Infrastructures (in detail): Energy (Power Supply)<->ICT (Telecommunication) ICT (Telecommunication)-> Finance services (Banks) ICT (Telecommunication)->Public Safety (Emergency organization) Water and Food (Water supply)->Public Safety (Emergency organization) Transport (Rail transport)->Financial services (Banks) Transport (Rail transport)-> Energy (Power Supply) Transport (Rail transport)-> Energy (Oil/Natural gas supply)				
2003 North America Major Power Blackout	August 24, 2003	Northeastern and Midwestern USA and Ontario, Canada.	Eastlake 5 electricity generation unit shut down automatically (USA). (Technical failure)	Number of affected CI sectors: 6 Number of affected CI subsectors: 10	* 4 billion to 10 billion U.S dollars finance losses *11 fatalities * Widespread Water pollutions in many areas * Gasoline price climbed up * Loss of water supply services * Drinking water contamination * Reduced railway services * Hundreds of flights canceled. * Highway traffic problems * Service disruptions for cell phone users
	Affected Infrastructures (in detail): Energy (Power supply)->ICT (Internet/Telecommunication) Energy (Power supply)->Water and Food (Water supply) Energy (Power supply)->Transport(Rail transport/Air transport) Energy (Oil supply)->Transport(Road transport) Energy (Power supply)->Industry (Chemical Industry) Energy (Power supply)->Finance services (Banks)				

2003 Italian Power Blackout	September 28, 2003	Italy and pars of Switzerland	Flashover and shut down of the Lukmanier transmission line causing overload of the San Bernardino line which suffered also from a flashover. (Technical failure)	Number of affected CI sectors: 5 Number of affected CI subsectors: 9	* About 120 million Euro finance losses. * A total of 56 million were affected. * Loss of electricity in the south Switzerland. * Loss of water supply services. * Loss of food supply services. * 110 trains cancelled. * Subway trains loss of service. * All flights in Italy canceled. * Road traffic problems. * Service disruptions for cell phone users
	Affected Infrastructures (in detail): Energy(Power supply) ->ICT (Internet/Telecommunication) Energy(Power supply) ->Transport (Air/Rail/Road) Energy(Power supply) -> Water and Food (Water & Food supply) Transport(Road)-> Public safety (Emergency organizations) Transport(Road/Rail)-> Water and Food (Water & Food supply)				

2005 Hurricane Katrina	August 23-31 , 2005	Gulf coast from Central Florida to Texas, especially in New Orleans, Louisiana	Hurricane Katrina(a category 4 hurricane) (Natural hazard)	Number of affected CI sectors: 6 Number of affected CI subsectors: 8	*Damages cost more than 100 billion U.S dollars. * 1,836 fatalities * 80 percent of New Orleans city flooded * Drinking water contamination * 890,300 customers in Louisiana lost power * 30 oil drilling platform were destroyed or damaged * 24 percent of annual oil production reduced * 18 percent of annual gas production reduced * 3 million customers lost phone lines * 2000 cell sites were out of service * Most of major roads in New Orleans area were damaged * 7 million gallons of oil and 1-2 gallons of gasoline were spilled into southeast Louisiana.
	Affected Infrastructures (in detail) : Energy(Power supply) -> Water and Food (Water supply) ICT (Telecommunication)-> Public safety(emergency organization) ICT (Telecommunication)-> Energy(Power supply) Energy(Power supply) -> ICT (Media/Radio) Transport (Road transport)->Public Health (Medical care and hospitals) Energy (Power supply)->Public Health (Medical care and hospitals) ICT (Radio)->Public Health (Medical care and hospitals)				

A p p e n d i x I I

QUANTITATIVE CCF ANALYSIS STUDY OF SUBSTATION LEVEL COMPONENTS

**** This section is based on the scientific report:***

Nan, C., Kröger, W., and Eusgeld, I. (2011). Study of Common Cause Failures of the SCADA System at Substation Level, Scientific report for Swiss Federal Office of Civil Protection.

Introduction of CCFs (State of the Art)

Techniques to increase reliability and fault tolerance have been adopted to reduce the effects of random hardware failures, e.g. by means of redundancy. Adding redundant elements to the system allows to reduce its failure probability to a minimum as long as failures can be regarded as independent while dependence leads to

P {A and B}>P (A)•P (B)}. (Equation AII-1)

Reality shows that multiple failures, close in time [127], might be caused by a common single event due to, for example,

- common cause initiators (e.g., internal or external events like floods, fires, or earthquakes),
- physical dependencies and interactions (e.g., failure of one component may generate a missile causing failure of another nearby component),
- location/environmental dependencies (e.g., extreme temperatures),
- functional/shared equipment dependencies (e.g., redundant components depend on the same support system),
- dependencies caused by human actions (e.g., design, interventions, maintenance).

There is no generally accepted definition of CCF. Nevertheless, most definitions point to the shared cause of multiple failures and include all the dependences depicted before besides physical interactions causing failure cascades. Common Mode Failures (CMFs) are mostly defined as a subset of CCFs in which redundant components fail in the same way. "Close in time" is also specified differently, while in the nuclear power industry it stands for simultaneity or within a short time interval, aviation refers to the system mission.

Reliability modeling of CCFs was introduced in the nuclear power industry more than 30 years ago within the framework of the so-called Reactor Safety or Wash-1400 study. This industry has a continuous focus on CCFs because of the highly redundant design of safety systems and has been in the forefront regarding development of CCF models, and on collection and analysis of related data. The most outstanding activity in this regards is the "International Common Cause Failure Data Exchange (ICDE)" and evaluation of data organized by the OECD/Nuclear Energy Agency [80], a project allowing multiple countries to collaborate and exchange CCF data to enhance the quality of risk analysis. Furthermore, a qualitative analysis approach is also proposed by the ICDE project for the purpose of identifying CCFs. The aviation industry has also given these failures close attention. The Norwegian offshore industry has, for some 20 years, focused on CCF related to reliability assessment of Safety Instrumented Systems (SISs). More recently, the IEC 61508 standard points to the need to control CCFs in order to maintain the safety integrity level (SIL) of safety functions of instrumented systems (see [127] for further details).

Modeling CCFs

Modeling CCFs/DFs within reliability and risk analysis is still a challenging task mainly due to their complexity and rare occurrence. Two basically different approaches can be applied to model CCFs [128]:

- **Explicit methods** such as logic trees to identify and/or include dependencies among a set of systems or components, e.g., functional dependencies or shared equipments; under the proviso of available data explicit models allow quantification.

- **Implicit methods** to cover so-called unknown or residual causes difficult to model explicitly, i.e. many remaining root causes and coupling factors, currently using parametric modeling based on historical common cause events.

The most widespread implicit method is the "β-factor model" developed by Fleming in 1975 [129]. It may be explained by the following simple example [127]: Consider a system of n identical components each with a constant total failure rate λ, referred to as *channels*. Given that a specific channel has failed, this failure will, with probability β, cause all the n channels to fail, and with probability 1- β, just involve the given channel. The system will then have a CCF rate λ_C= β λ, where all n channels fail. In addition, each channel has a rate of independent failures, λ_I= (1- β) λ. The total failure rate of a channel may be expressed as λ= λ_I + λ_C. The β-factor model may also be regarded as a shock model where shocks occur randomly according to a homogeneous Poisson process with the rate λ_C. Each time a shock occurs, all the channels of the system fail, irrespective of the status of the channels. Each channel may hence fail due to two independent causes; shocks and channel specific (individual) causes. The rate λ_I is sometimes called the rate of individual failures. The parameter β can be interpreted as the mean fraction of all failures of a channel that also affect all other channels of the system. When a failure occurs, the multiplicity of the failure event is either one or n. Intermediate values of the multiplicity are not possible when assuming the β-factor model. Therefore, the β-factor model leads to conservative results for highly redundant systems. Implicit methods like the "β-factor" can be transformed into an explicit model like the fault tree by differentiating failures of multiple components into independent and dependent failures and connecting them by logical OR gate, illustrated in Figure A-II 1. Obviously, the quality of the results gained by following this approach strongly depends on the quality of the data applied.

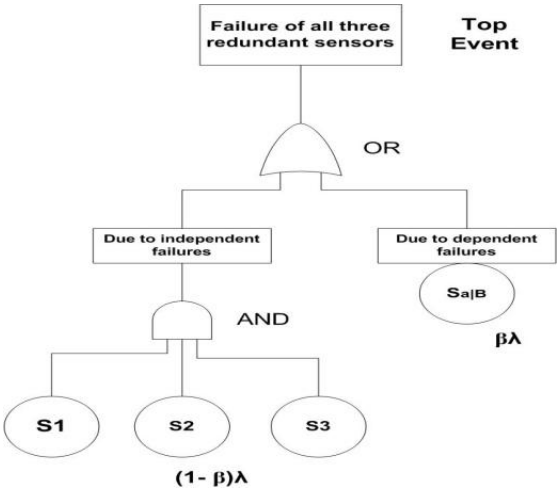


Figure A-II 1 Transformation of implicit β-factor model into a fault tree (assuming same total failure rate λ for all components/sensors).

CCFs can be analyzed qualitatively and quantitatively. One of the objectives of the qualitative CCF analysis is to identify the root causes that could potentially contribute to CCFs and provide engineering arguments to aid the analysis of consequences caused by CCFs. The quantitative CCF analysis extends the qualitative analysis by including failure probabilities of analyzed component(s) and therefore, provides quantitative results such as system service unavailability considering effects induced by CCFs [130]. The quantitative approach to perform a CCF analysis is developed by combining both explicit and implicit CCF modeling methods, according to Figure A-II 1. The fault tree diagram (explicit method) is first constructed to identify all failure causes and combinations as well as dependencies among a set of systems or components (common cause candidates). Then, the β-factor model method (implicit method) is applied at the single component level to quantify the contribution to overall system performance (can use system availability as the measurement) of CCFs.

Quantitative Analysis of CCF

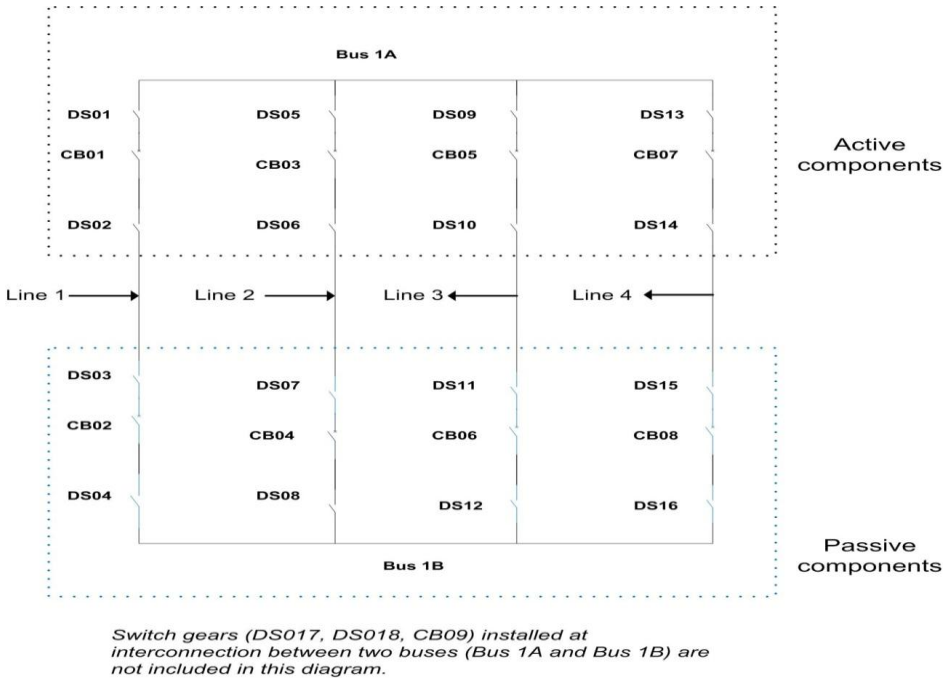


Figure A-II 2 Single line diagram of substation SROBBI [85]

A quantitative approach, which combines both explicit (fault tree diagram) and implicit (β-factor model) CCF modeling methods, is performed to evaluate the effects of CCFs on the reliability of an exemplary substation (It should be noted that parts of contents described in this chapter are based on [85]). The substation analyzed in this chapter is the substation SROBBI, situated in Robbia, Switzerland, which - of all substations studied - was identified as the one with the largest total flow in all case studies [85]. Based on the information from [41], a single line diagram of the substation SROBBI was developed in Figure A-II 2, which shows that a double busbar with a double breaker configuration was assumed for the substation SROBBI. The following lines are connected to the substation SROBBI: Line 1 (SFILIS1A=SROBBI1B, connected to substation SFILIS in FILISUR), Line 2 (SROBBI1A=SYYPUN1A connected to the transmission line between the substations SPRADE in PRADELLA and SFILIS), Line 3 (SROBBI1A=IGORM111 to substation IGORM1 in GORLAGO, Italy) and Line 4 (SROBBI1B=ISFIM111 to substation ISFIM1 in S.FIORANO, Italy). In the following sections, first, a fault tree diagram is constructed to build a reliability model as an application of the explicit CCF model method. The top event of this diagram corresponds to the failure of the substation to realize the predefined

functions. The function of the substation SROBBI is to transfer electrical energy between interconnected lines. According to the report [85], the flow in Line 1 and Line 2 is in the direction of the substation SROBBI (inflow) and the flow in Line 3 and Line 4 is in the direction from the substation (outflow). The following failures of substation were considered during the development of the corresponding fault tree diagram:

- Failure to deliver energy to substation SROBBI from BOTH Line 1 and Line 2.
- Failure to deliver energy to ANY of the Lines 3 and 4.

Fault Tree Diagram of the Substation SROBBI without Considering Effects of CCFs

The fault tree diagram of the substation SROBBI is shown in Figure A-II 3, Figure A-II 4, Figure A-II 5, and Figure A-II 6, and developed using the software of the open FTA. It should be noted that CCFs are not considered in this diagram.

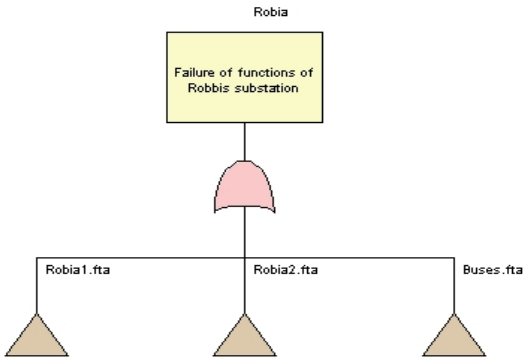


Figure A-II 3 Top gate of the fault tree diagram

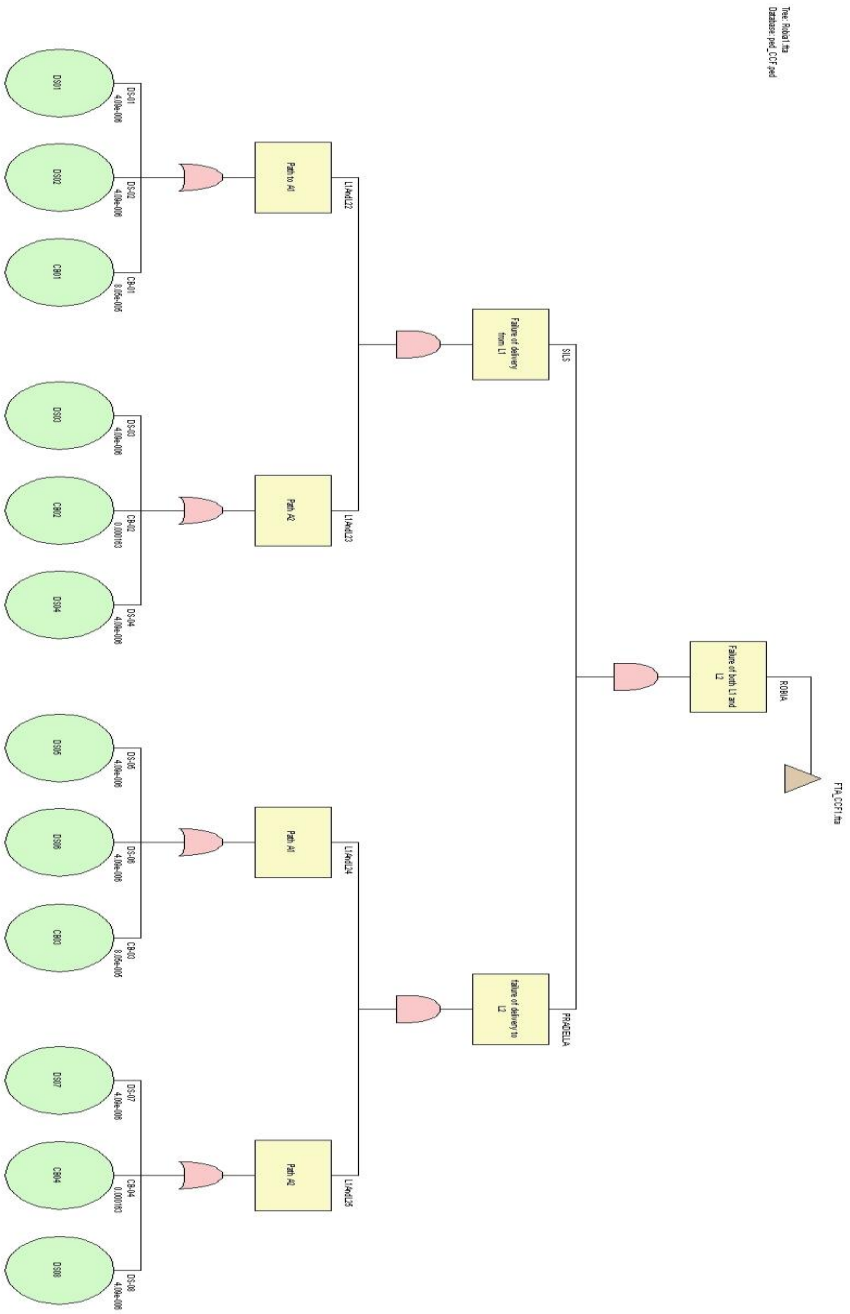


Figure A-II 4 Fault tree diagram of the transfer gate ROBIA-1

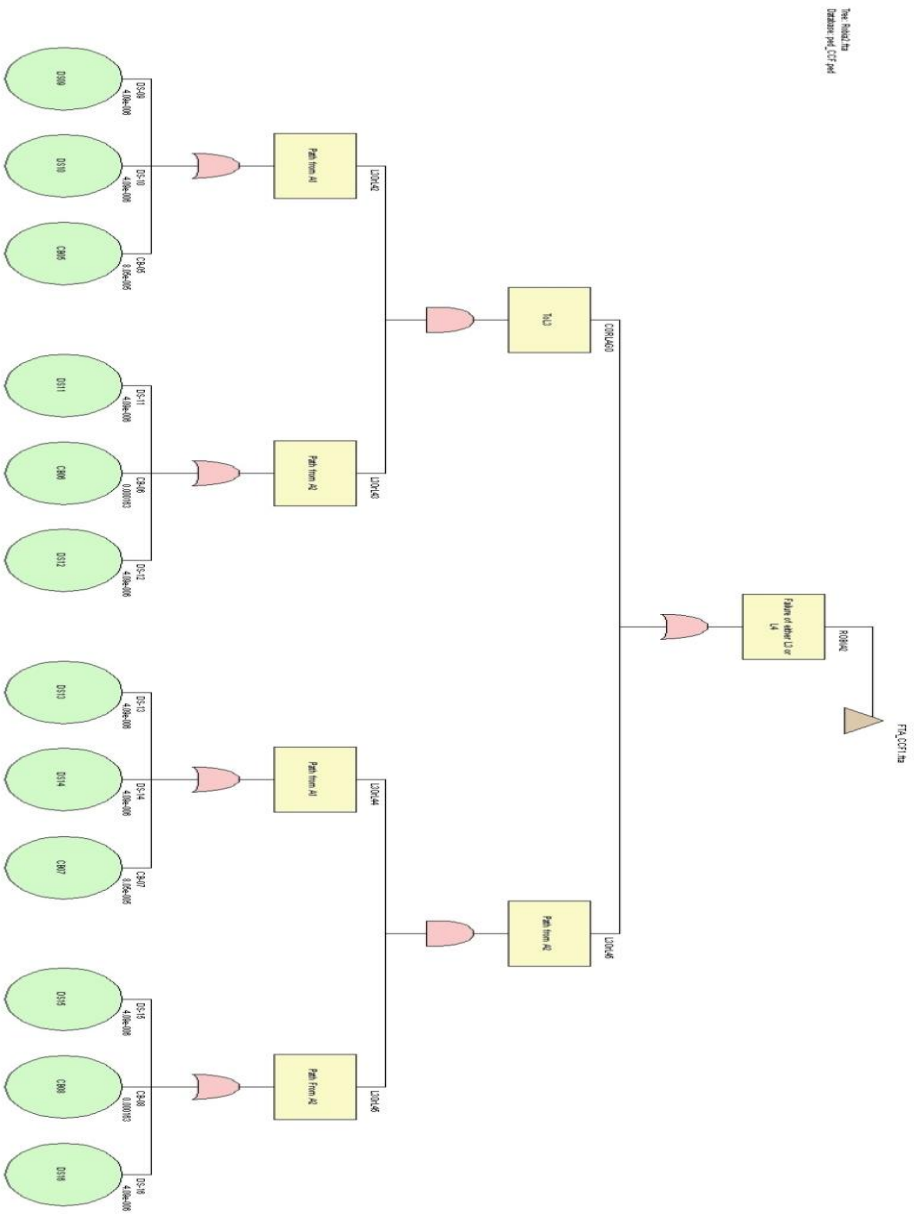


Figure A-II 5Fault tree diagram of the transfer gate ROBIA-2

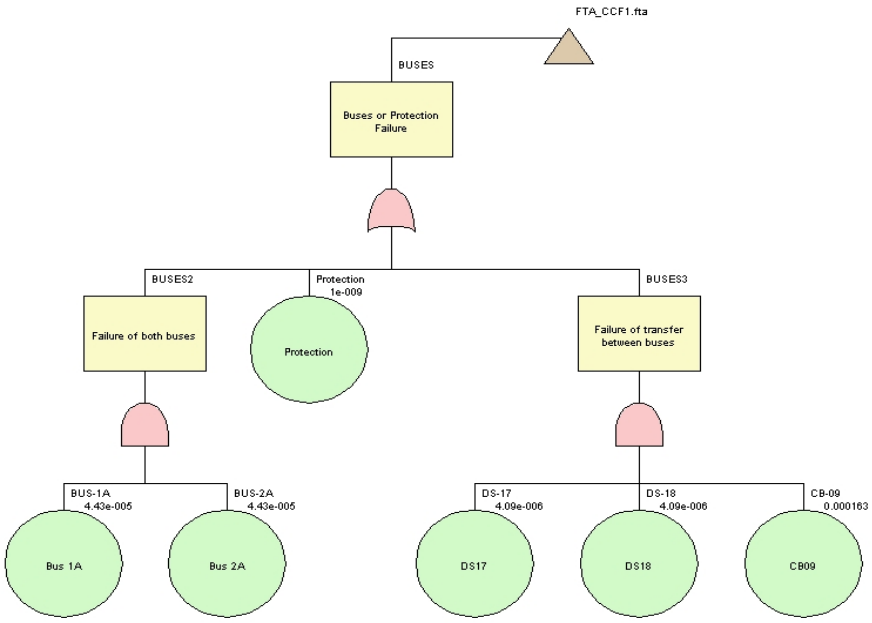


Figure A-II 6 Fault tree diagram of the transfer gate BUSES

The parameters used to construct this fault tree diagram are referred from [85] and are given in Table A-II 1.

Table A-II 1 Parameters used in the analysis

No.	Parameter	Mean unavailability
1	Bus Active	4.43E-5
2	Bus Passive	4.43E-5
3	CB Active	8.05E-5
4	CB Passive	1.63E-4
5	DS Active	4.09E-6
6	DS Passive	4.09E-6
7	Protection	1E-9

After analyzing this fault tree diagram, 102 minimal cut sets are identified. The top event probability is 3.33E-8. According to the analyzed results, 11 components with highest

importance measure are listed in Table A-II 2 and highlighted in Figure A-II 7. As shown in this table, CB-06 and CB-08 contribute to the system reliability more than others. Protection of this substation is also an important component since its importance measure is 3 percent.

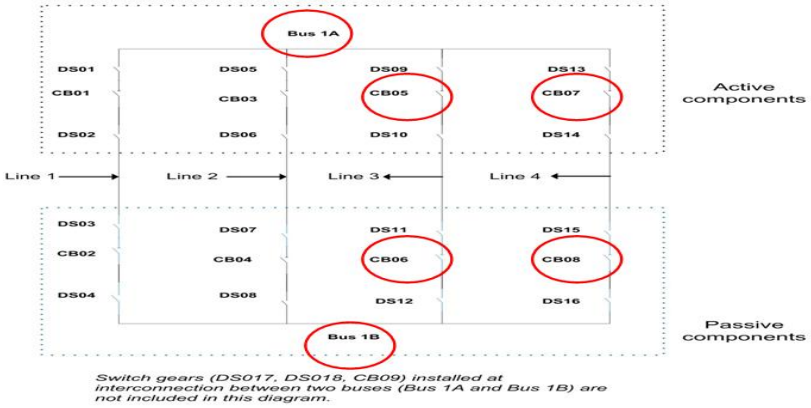


Figure A-II 7 Highlighted important components based on the analysis of the fault tree diagram

Table A-II 2 List of importance measures for components in the fault tree diagram

Component	Failure Contribution	Importance
CB-06	1.4E-8	43.38%
CB-08	1.4E-8	43.38%
CB-05	1.38E-8	41.35%
CB-07	1.38E-8	41.35
Bus-1A	1.96E-9	5.89%
Bus-2A	1.96E-9	5.89%
Protection	1.00E-9	3.00%
DS-09	7.00E-10	2.10%
DS-10	7.00E-10	2.10%
DS-13	7.00E-10	2.10%
DS-14	7.00E-10	2.10%

Fault Tree Diagram of the Substation SROBBI with Considering Effects of CCFs

In this section, another fault tree diagram is constructed to quantify the contribution of CCFs to the reliability of the substation SROBBI by applying the β-factor modeling method at the single component level. Table A-II 3 shows groups of components that are considered as sources of CCFs, due to common producer and similar location.

Table A-II 3 Assumed β-factor value for modeling CCFs [85]

Group of components	**β-factor**
Circuit Breaker (CB)	0.07
Disconnect Switch (DS)	0.05

The fault tree diagram of the substation SROBBI is shown in Figure A-II 8, Figure A-II 9, Figure A-II 10, and developed using the software of the open FTA .

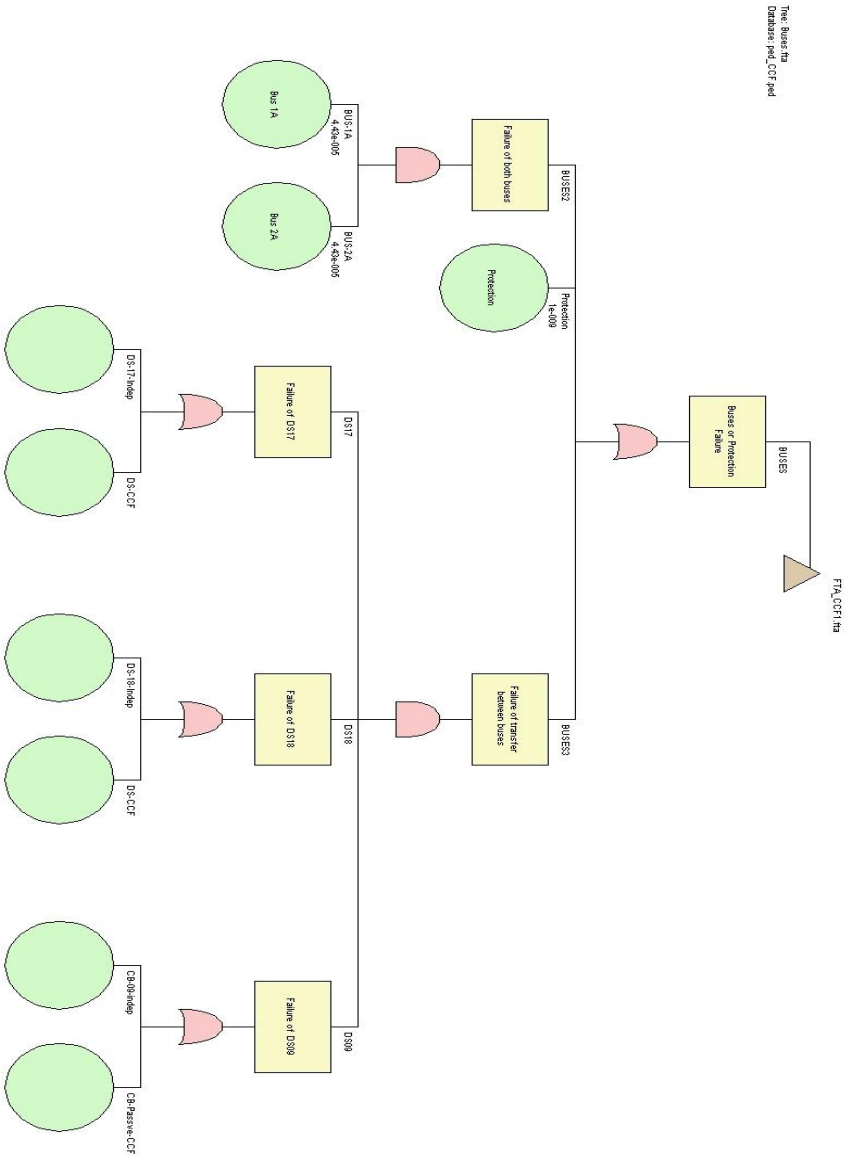


Figure A-II 8 Fault tree diagram of the transfer gate BUSES considering CCFs

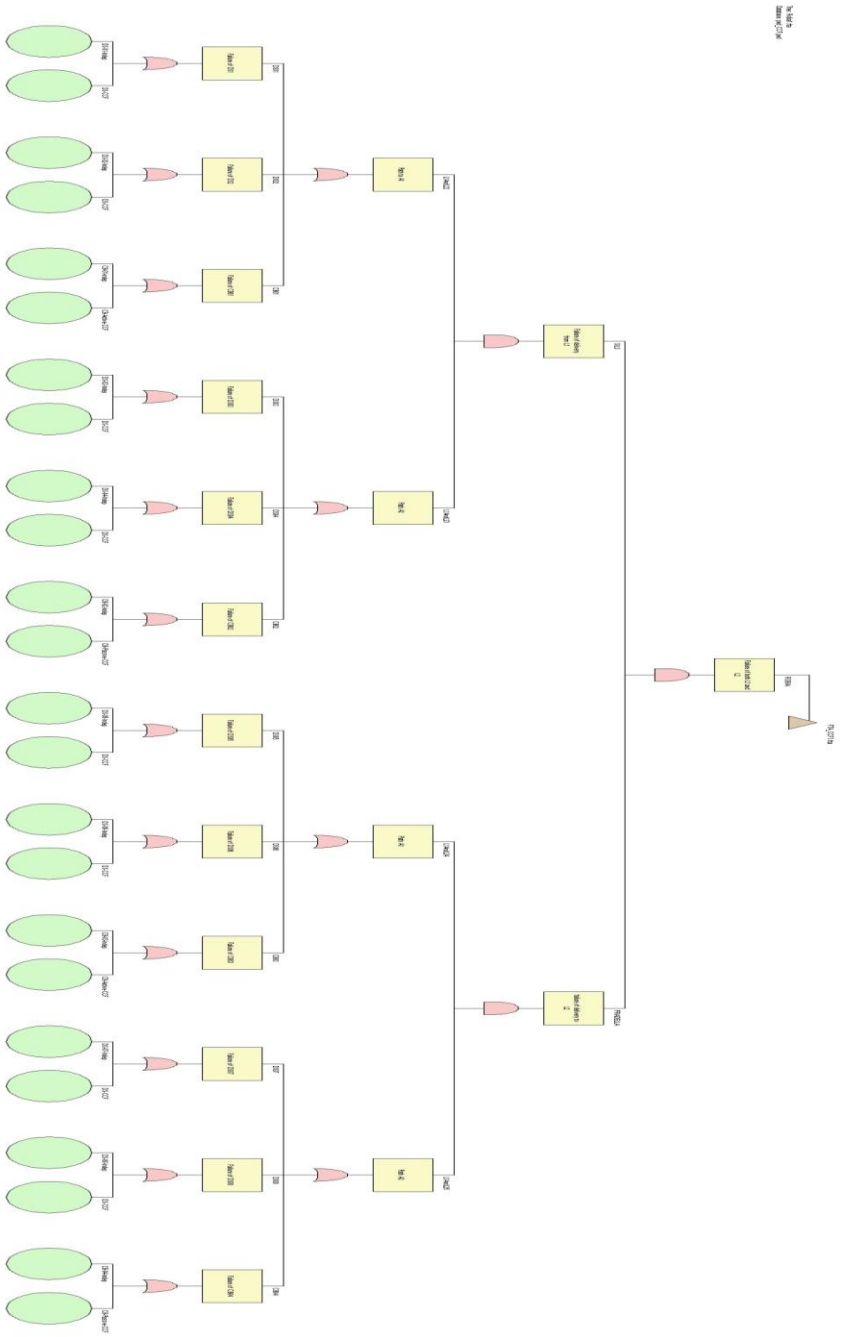


Figure A-II 9 Fault tree diagram of the transfer gate ROBIA-1 considering CCFs

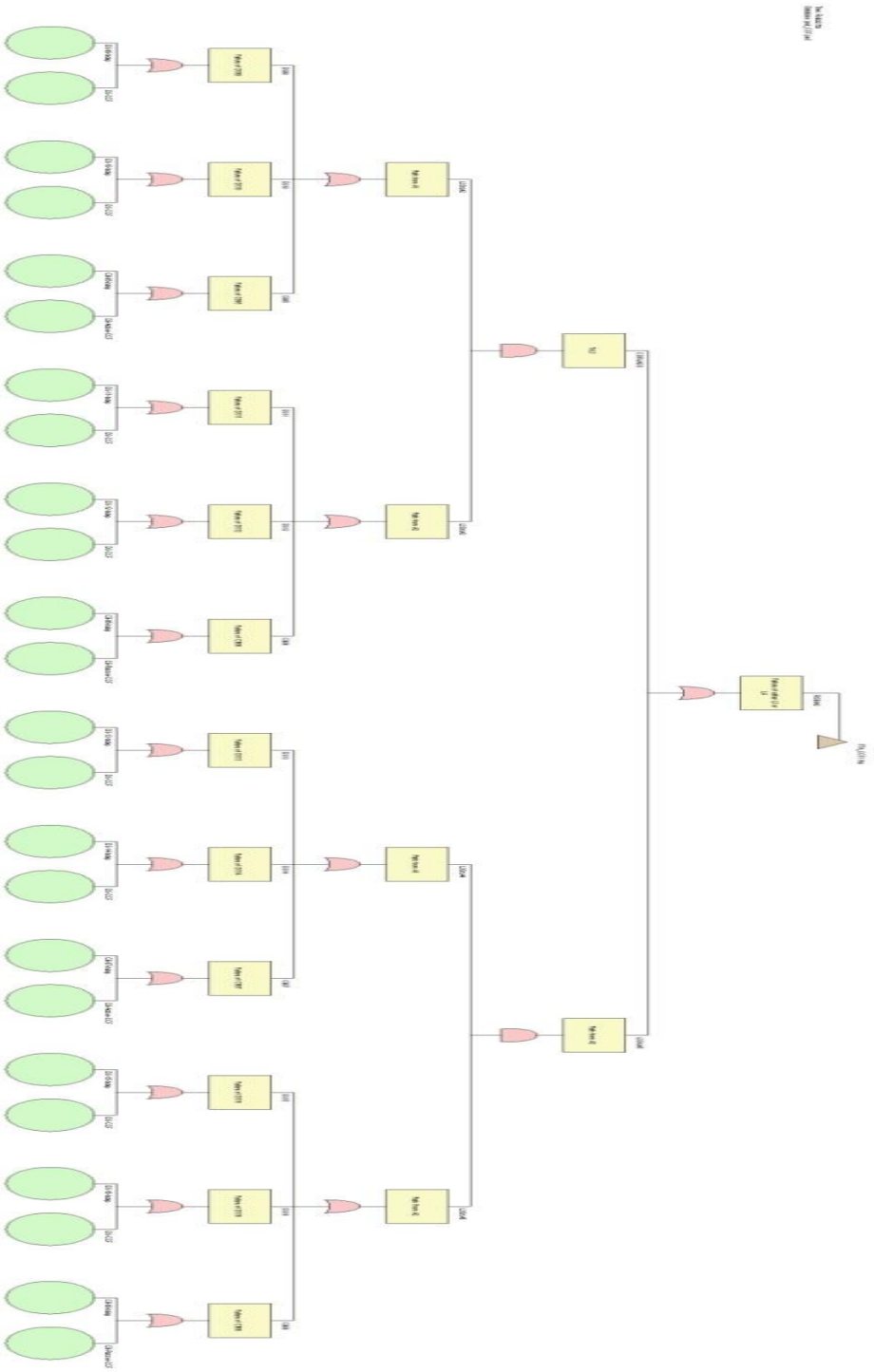


Figure A-II 10 Fault tree diagram of the transfer gate ROBIA-2 considering CCFs

After analyzing this fault tree diagram, 135 minimal cut sets were identified. The top event probability is 2.3E-7, which is higher than the probability calculated without considering CCFs (3.33E-8). According to the calculated important measures, 9 elements with highest importance measures are listed and highlighted in Table A-II 4. As shown in this table, instead of the CB-06 and the CB-08, which were most important components contributing to the reliability of the system without considering CCFs, CCFs related to disconnect switches (DSs) contribute to the system reliability more than other components. Also, CCFs related to circuit breakers contribute much less to the system reliability, compared to disconnect switches (importance measure is 0.78% for CB Active and 0.08% for CB Passive). The protection of this substation contributes less to the system reliability as its importance measure is only 0.43 percent.

Table A-II 4 Importance measures for events in the fault tree diagram considering CCFs

Event	**Failure Contribution**	**Importance**
DS-CCF	2.00E-7	86.45%
CB-06	1.34E-8	5.80%
CB-08	1.34E-8	5.80%
CB-05	1.20E-8	5.21%
CB-07	1.20E-8	5.21%
Bus-1A	1.96E-9	0.85%
Bus-2A	1.96E-9	0.85%
CB Active CCF	1.80E-9	0.78%
Protection	1.00E-9	0.43%

Since the contribution of CCFs of circuit breakers (CBs) is not significant based on the results described above, they can be ignored during following experiments investigating the effects of change of β-factor value on the system reliability, which have been performed by modifying the β-factor value of disconnected switches during the top event probability calculation. Results obtained from these experiments (β-factor modification) are summarized in Table A-II 5 and illustrated in Figure A-II 11 and Figure A-II 12.

Table A-II 5 Summary of results from (DS) β factor modification experiments

β factor value of DS	Top event probability	Importance of DS-CCF
0.01	7.24E-8	56.48%
0.02	1.13E-7	72.27%
0.03	1.51E-7	79.24%
0.04	1.91E-7	83.59%
0.05	2.31E-7	86.45%
0.06	2.81E-7	88.87%
0.07	3.21E-7	90.27%
0.08	3.61E-7	91.35%
0.09	4.01E-7	92.23%
0.1	4.40E-7	92.92%
0.2	8.5E-7	96.38%
0.3	1.26E-6	97.58%

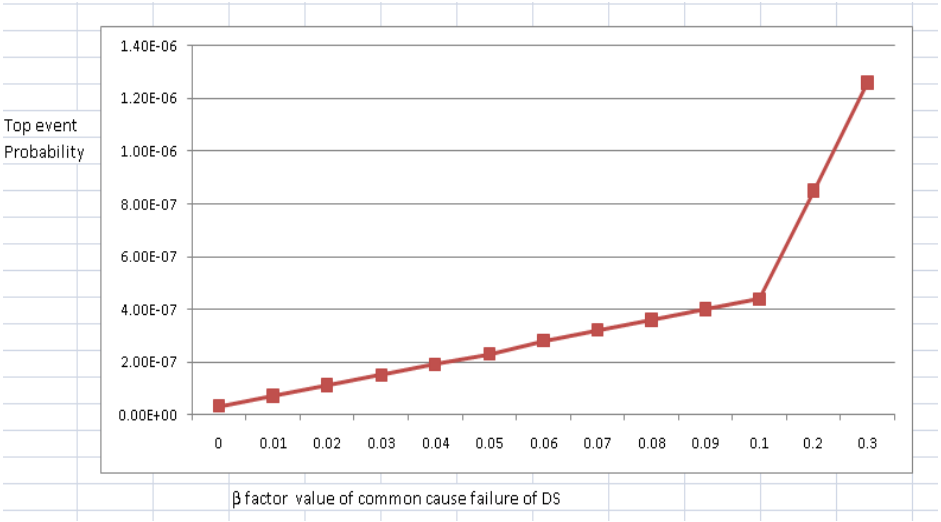


Figure A-II 11 Top event probability vs. DS β factor

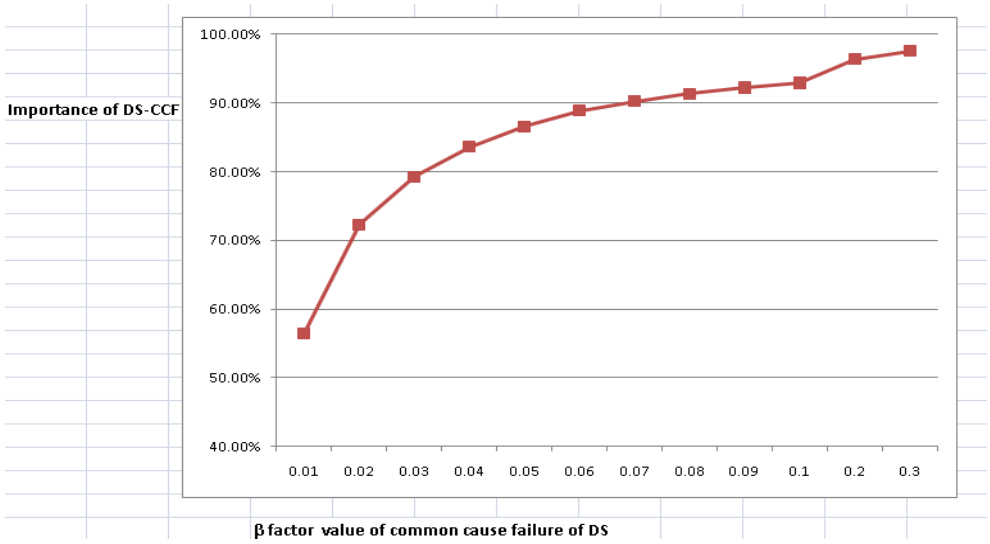


Figure A-II 12 Importance of DS CCFs vs. DS β factor

As shown in the figures above, both top event probability and importance of DS CCFs increase after increasing the β factor value. Top event probability and importance of DS CCFs increase to 1.26E-6 and 97.58 percent if β-factor value of DS is set to 0.3.

Appendix III

INTRODUCTION OF CREAM

CREAM is derived from the method of Contextual Control Model (COCOM), the purpose of which is to provide the conceptual and practical basis for developing operator performance models. In both methods, the cognition is regarded as not only an issue of processing input(s) and producing a reaction, but also an issue of the continuous revision and review of goals/intentions [131]. Therefore, the cognition should not be described as a sequence of steps, but rather a controlled use of available competence and resources [96]. The basic assumption of CREAM is that human performance is an outcome of the controlled use of competence adapted to the requirements of the situation, rather than the result of pre-determined sequences of responses to events.

Four characteristic control modes are defined in the CREAM method and briefly explained below [96]:

- **Scrambled Control Mode:** In this mode, the choice of next action is in practice unpredictable or haphazard, and the situation characterized by this mode is little or no thinking involved in choosing what to do.
- **Opportunistic Control Mode**: In this mode, the next action is determined by the salient features of the current context rather than on more stable intentions or goals.
- **Tactical Control Mode**: In this mode, performance is based on planning, which more or less follows a known procedure or rule.
- **Strategic Control Mode**: In this mode, the human (person) considers the global context, thus using a wider time horizon and looking ahead at higher level goals. Strategic mode provides a more efficient and robust performance.

The relations between control modes and performance reliability is appropriately illustrated in Figure A-III 1.

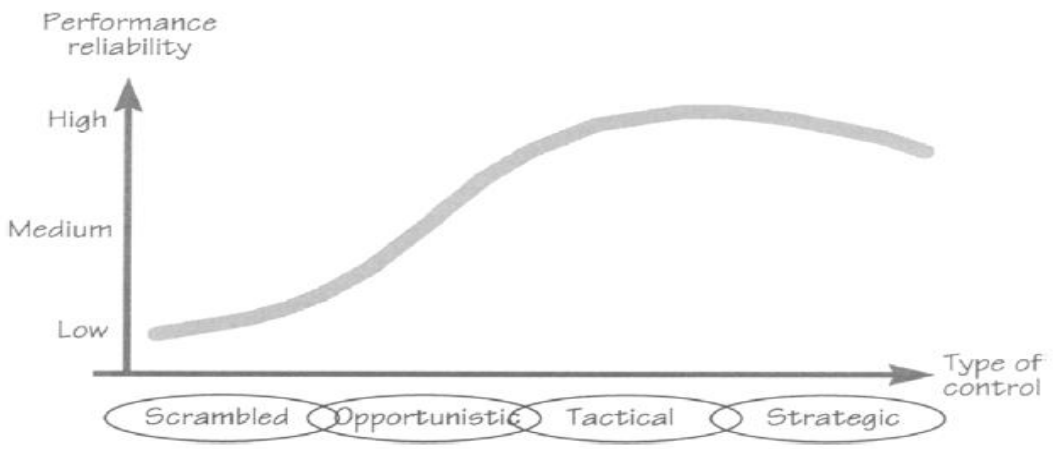


Figure A-III 1 Relation between the control modes and performance reliability [96]

Instead of PSFs, the method of CREAM uses CPCs (Common Performance Conditions) to determine sets of error modes and probable error causes. Total nine CPCs, proposed by Hollnagel, are adopted in this model development including various levels assigned to each CPC, listed in Table A-III 1. The main difference between the CPCs and the PSFs is that the CPCs can be applied at the early stage of the analysis to characterize the context for the task as a whole, rather than a simplified way of adjusting probability values for each event. Therefore, the influence of CPCs is closely linked to the task analysis. Advantage performance conditions such as the level "very efficient" (CPC level) of "Adequacy of organization" may improve the performance reliability, while disadvantage performance conditions such as the level "inefficient" of "Adequacy of organization" may reduce the performance reliability. If the performance reliability is improved, operators could fail less often in their tasks. If the performance reliability is reduced, operators could fail more often. Table A-III 2 summarizes relations between all defined levels of nine CPCs and their expected effects on the performance reliability. It should be noted that relations shown in Table A-III 2, adapted from [96], are based on the author's general human factor knowledge as well as experiences from the HRA discipline, and can be modified for other implementations.

Table A-III 1 Descriptions and corresponding assigned levels of nine CPCs [96]

CPC name	Descriptions/Levels
Adequacy of organization	The quality of the roles and responsibilities of team members, additional support, communication systems, Safety Management System, instructions and guidelines for externally oriented activities, role of external agencies, etc.
	Very efficient / Efficient / Inefficient / Deficient
Working conditions	The nature of the physical working conditions such as ambient lighting, glare on screens, noise from alarms, interruptions from the task, etc.
	Advantaqeous / Compatible / Incompatible
Adequacy of MMI and operational support	The Man-Machine Interface in general, including the information available on control panels, computerised workstations, and operational support provided by specifically designed decision aids.
	Supportive ~Adequate / Tolerable / Inappropriate
Availability of procedures / plans	Procedures and plans include operating and emergency procedures, familiar patterns of response heuristics, routines, etc.
	Appropriate ~Acceptable / Inappropriate
Number of simultaneous goals (tasks)	The number of tasks a person is required to pursue or attend to at the same time (i.e., evaluating the effects of actions, sampling new information, assessing multiple goals etc.).
	Fewer than capacity / Matching current capacity / More than capacity
Available time	The time available to carry out a task and corresponds to how well the task execution is synchronised to the process dynamics.
	Adequate / Temporarily inadequate / Continuously inadequate
Time of day	The time of day (or night) describes the time at which the task is carried out, in particular whether or not the person is adjusted to the current time (circadian rhythm). Typical examples are the effects of shift work. It is a well-established fact that the time of day has an effect on the quality of work, and that performance is less efficient if the normal circadian rhythm is disrupted.
	Day-time (adjusted) / Night-time (unadjusted)
Adequacy of training and experience	The level and quality of training provided to operators as familiarisation to new technology, refreshing old skills, etc. It also refers to the level of operational experience.
	Adequate, high experience /Adequate, limited experience / Inadequate
Crew collaboration quality	The quality of the collaboration between crew members, including the overlap between the official and unofficial structure, the level of trust, and the general social climate among crew members.
	Very efficient / Efficient / Inefficient / Deficient

In most first generation HRA methods, it is always assumed that PSFs are independent. This assumption raises concerns since even a cursory investigation is able to show that it is not possible that all PSFs are independent of each other. This concern has been taken into consideration by most second generation HRA methods. In the method of CREAM, all CPCs have influences on each other. For instance, "Working conditions" (e.g., ambient lighting, noises from alarms, interruptions, etc) have direct impacts on both of "Number of simultaneous goals" and "Available time". Improved "Working conditions" can be assumed to increase "Available time" (+) and decrease "Number of simultaneous goals" (-). The

dependencies between CPCs are summarized in Table A-III 3, showing how the CPCs in the upper row can affect the CPCs in the left hand column. It is very important to take these dependencies into account when applying the CREAM method.

Table A-III 2 Relations between CPCs and performance reliability [96]

CPC name	Level	Expected effect on performance reliability
Adequacy of organisation	Very efficient	Improved
	Efficient	Not significant
	Inefficient	Reduced
	Deficient	Reduced
Working conditions	Advantageous	Improved
	Compatible	Not significant
	Incompatible	Reduced
Adequacy of MMI and operational support	Supportive	Improved
	Adequate	Not significant
	Tolerable	Not significant
	Inappropriate	Reduced
Availability of procedures/plans	Appropriate	Improved
	Acceptable	Not significant
	Inappropriate	Reduced
Number of simultaneous goals (tasks)	Fewer than capacity	Improved
	Match current capacity	Not significant
	More than capacity	Reduced
Available time	Adequate	Improved
	Temperary inadequate	Not significant
	Continuously inadequate	Reduced
Time of day	Day time	Not significant
	Night time	Reduced
Adequacy of training and experience	Adequate, high experience	Improved
	Adequate, limited experience	Not significant
	Inadequate	Reduced
Crew collaboration quality	Very efficient	Improved
	Efficient	Not significant
	Inefficient	Not significant
	Defficient	Reduced

The combined characteristic of all CPCs determines which control mode is chosen. A typical combined CPC score can be calculated by simply counting the number of times where a CPC is expected:

1) to reduce performance reliability ($\sum reduced$)
2) to have no significant effect ($\sum not\ significant$)
3) to improve performance reliability ($\sum improved$)

In general, using the method of CREAM includes two approaches to provide a quantified outcome (HEP): the basic approach and the extended approach. The purpose of the basic approach is to produce an overall assessment of the performance reliability that may be expected for a specific task. This approach can be considered as an initial screening of the analyzed task by providing an overall assessment, which can be performed by determining one of four control modes based on characteristics of all CPCs.

Figure A-III 2 illustrates relations between the CPC scores and the control modes. It should be noted that each control mode has its corresponding probability interval, as shown in Table A-III 4.

Table A-III 3 Dependencies between CPCs [96]

	Adequacy of organisation	Working conditions	Adequacy of MMI and operational	Availability of procedures/	Number of simultaneous goals (tasks)	Available time	Time of day	Adequacy of training and experience	Crew collaboration quality
Adequacy of organisation									
Working conditions	+		+			+	+	+	
Adequacy of MMI and operational support	+								
Availability of procedures/plans	+								
Number of simultaneous goals (tasks)		-	-	-					
Available time		+	+	+	-		+		+
Time of day									
Adequacy of training and experience	+								
Crew collaboration quality	+							+	

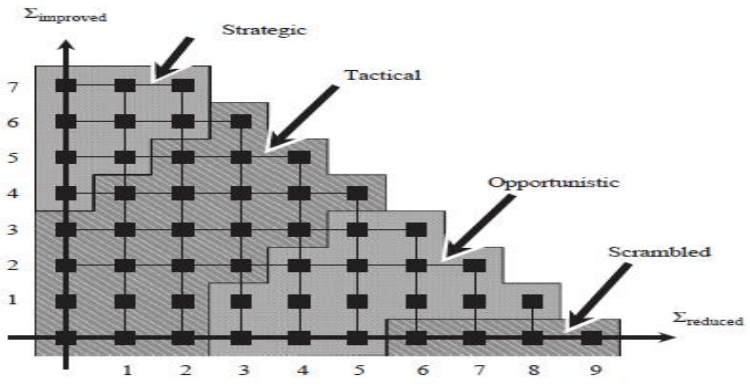


Figure A-III 2. Relations between the CPC scores and the control modes.

Table A-III 4 Control modes and probability interval [96]

Control mode	**Probability interval**
Strategic	0.00005<P<0.01
Tactic	0.001<P<0.1
Opportunistic	0.01<P<0.5
Scambled	0.1<P<1.0

The extended approach can be divided into three steps:

- Identifying the cognitive activities to build a cognitive demands profile,
- Identifying a most likely cognitive function failure for each identified cognitive activity,
- Determining the probability for each identified cognitive activity

Totally 13 generic failure types in various cognitive functions (observation, interpretation, planning and execution) with its own nominal failure probability value have been defined by Hollnagel [96] and shown in Table A-III 5.

Table A-III 5 Nominal values for 13 generic cognitive failure types [96]

Cognitive function	Generic failure type	Basic value
Observation	O1: Wrong object observed	0.001
	O2: Wrong identification	0.07
	O3: Observation not made	0.07
Interpretation	I1: Faulty diagnosis	0.02
	I2: Decision error	0.01
	I3: Delayed interpretation	0.01
Planning	P1: Priority error	0.01
	P2: Inadequate plan	0.01
Execution	E1:Action of wrong type	0.003
	E2: Action at wrong time	0.003
	E3: Action on wrong object	0.0005
	E4: Action out of sequences	0.003
	E5: Missed action	0.003

A p p e n d i x I V

DETAILED DESCRIPTION OF EXPERIMENTS

EXPERIMENT I

FCD FO Mode

As seen from the SOE table of one of the FCD FO tests (Table A-IV 1), line 119 became overloaded and an overload alarm was sent to the RTU. However, the operator failed to respond to this alarm and undertook no further action such as redistribution of the power load. Normally, the safety system installed for this line should be triggered to disconnect the line. However, due to the FO failure mode, line 119 failed to be disconnected. Therefore, line 119 continued to be overloaded and another alarm was generated. At this time, the operator recognized the alarm and the redistribution action was taken. In this test, the consequences seem not very significant since the operator recognized the alarm and redistributed power load, meaning that the negative consequences caused by FCD's FO failure mode could be alleviated by the operator's correct response. Most simulation results observed in FCD FO tests are similar to the results shown in Table A-IV 1. In the case when FCD is in FO failure mode, its controlled line cannot be disconnected and remains connected although it should be disconnected for safety reason. Therefore, the overload alarm will not be handled and the affected transmission line remains overloaded which will trigger the same alarm again. Results collected from all FCD FO tests are shown and summarized in Table A-IV 2 and the average service unavailability after 20 tests is 0.4%.

FCD FC Mode

As seen from the SOE table from one of FCD FC tests (Table A-IV 3), the overload alarm was processed and the line 103 was requested to be connected at a certain time. However, due to the FC failure mode, the FCD device of this line failed to close and line 103 remained disconnected until the FCD device is out of FC failure mode. Most observed results during FCD FC tests are similar to the results shown in Table A-IV 3. In the case

when FCD is in FC failure mode, it often failed to be triggered to connect its controlled line. Therefore, the affected line remains disconnected and service unavailability increases. Results collected from all FCD FC tests are shown and summarized in Table A-IV 4 and the average service unavailability after 20 tests is 2.5 %.

FCD SO Mode

Generally, the overload threshold value for the overload alarm of a FCD device could be increased (SOH) or decreased (SOL). In this experiment, both situations have been considered. However, all the tests related to the increase of overload threshold value show that no negative consequences are observed. For example, as seen from the SOE table from one of FCD SO tests (Table A-IV 5), no overload alarms are observed and service unavailability is zero, Therefore, in this experiment, it is assumed that the overload threshold value of the studied FCD device is modified to a smaller number (SOL). As seen from the SOE table from one of FCD SOL tests (Table A-IV 6), the FCD device of line 103 first was in SO failure mode and its overload threshold value was decreased. The most direct consequence of this failure is that line 103 was considered as overloaded by mistake. Most observed results during FCD FO tests are similar to the results shown in Table A-IV 6. In the case when FCD is in SO failure mode, the overload threshold value of the affected FCD device is modified and its controlled line becomes overloaded although it should not. Results collected from all FCD SO tests are summarized in Table A-IV 7 and the average service unavailability after 20 tests is 5.4 %.

Table A-IV 1 Observed Results from one of FCD FO tests

Stamped Time	Events
3631	Line 119 is overloaded and an alarm has been generated (FID)
3632	119 has been detected and related FCD device gets noticed (FCD)
4508	RTU has processed an alarm from Line 119 and sent it to MTU (RTU)
5832	..Operator fails to make action for Line 119 (MTU)
6825	**********FCD device for 119 is in FO mode ********** (FCD)
6909	**********FCD device fail to be triggered to disconnect 119 due to FO failure mode******* (FCD)
6969	Line 119 is overloaded and an alarm has been generated (FID)
7027	RTU has processed an alarm from Line 119 and sent it to MTU (RTU)
8409	Operator recognize the alarm for Line119 (MTU)
8410	Operator response the problem correctly and distributing algorithm will be taken for line 119 (MTU)

Stamped Time	Events
8492	command has been processed by operator successfully, redistribution command has been sent out (RTU)
11850	overload problem solved and circuit breaker will be closed to connect 103 (FCD)
	Test Summary (SF): unavailability of service: 0

Table A-IV 2 Summary of FCD FO single failure mode tests

Test Number	Service Unavailability (studied substation)	Test Number	Service Unavailability (studied substation)
1	0	**11**	2.4%
2	0	**12**	0
3	0	**13**	2.1%
4	0	**14**	0
5	1.9%	**15**	0
6	0	**16**	0
7	0	**17**	2.5%
8	0	**18**	0
9	0	**19**	0
10	0	**20**	0
Summary: Service unavailability (Average): 0.4% Confidence Interval (CI) [0, 0.8%] where α=0.05			

Table A-IV 3 Observed Results from one of FCD FC tests

Stamped Time	Events
1462	Line 103 is overloaded and an alarm has been generated (FID)
1463	103 has been detected and related FCD device gets noticed (FCD)
1572	RTU has processed an alarm from Line 103 and sent it to MTU (RTU)
1716	..Operator fails to make action for Line 103 (MTU)
4500	FCD device has been triggered to disconnect line 103 (FCD)
6409	**********FCD device for 103 is in FC mode ********** (FCD)
7727	overload problem solved and circuit breaker will be closed to connect 103 (FCD)
7729	********* FCD device fail to be triggered to connect 103 due to its FC failure mode *********

Stamped Time	Events
	(FCD)
11417	**********FCD device for 103 is out of FC mode ********* (FCD)
11419	******* Line 103 been connected after the maintenance********* (FCD)
	Test Summary (SF) unavailability of service: 1.9 %

Table A-IV 4 Summary of FCD FC single failure mode tests

Test Number	Unavailable of Service (studied substation)	Test Number	Unavailable of Service (studied substation)
1	5.9%	**11**	1.9%
2	1.2%	**12**	8.2%
3	1.6%	**13**	2.7%
4	2.9%	**14**	0.7%
5	1.2%	**15**	0.6%
6	1.2%	**16**	7.1%
7	0.5%	**17**	5.2%
8	1%	**18**	2.1%
9	1.4%	**19**	3.1%
10	3.6%	**20**	1%
Summary: Service unavailability (Average): 2.5 % Confidence Interval (CI) [1.4%, 3.6%] where α=0.05			

Table A-IV 5 Observed Results from one of FCD SO (SOL) tests

Stamped Time	Events
1831	Line 103 is overloaded and an alarm has been generated (FID)
1831	103 has been detected and related FCD device gets noticed (FCD)
1963	RTU has processed an alarm from Line 103 and sent it to MTU (RTU)
2037	..Operator fails to make action for Line 103 (MTU)
2376	**********FCD device for 119 is in SO mode ********** (FCD)
2376	119's STE offset has been updated to 4.598210767208476 (FCD)
2700	FCD device has been triggered to disconnect line 103 (FCD)
5882	overload problem solved and circuit breaker will be closed to connect 103 (FCD)
5882	103 has received the command from RTU for connecting the line (FCD)
33594	**********FCD device for 103 is in SO mode ********** (FCD)
33594	103's STE offset has been updated to 7.780126031133754 (FCD)

Stamped Time	Events
	Test Summary (SF)Total Numbers of Overloads: 0 Unavailability of service: 0

Table A-IV 6 Observed Results of one of FCD SO (SOH) tests

Stamped Time	Events
11788	**********FCD device for 103 is in SO mode ********** (FCD)
11788	103's STE offset has been updated to -6.093011696519018 (FCD)
11956	**********FCD device for 119 is in SO mode ********** (FCD)
11956	119's STE offset has been updated to -4.633760378796047 (FCD)
126550	Line 103 is overloaded and an alarm has been generated (FID)
126551	103 has been detected and related FCD device gets noticed (FCD)
126595	RTU has processed an alarm from Line 103 and sent it to MTU (RTU)
126782	Operator recognize the alarm for Line103 (MTU)
126786	Operator response the problem correctly and distributing algorithm will be taken for line 103 (MTU)
126814	command has been processed by operator successfully, redistribution command has been sent out (RTU)
126850	Line 103 is overloaded and an alarm has been generated (FID)
126851	103 has been detected and related FCD device gets noticed (FCD)
126881	RTU has processed an alarm from Line 103 and sent it to MTU (RTU)
127359	Operator recognize the alarm for Line103 (MTU)
127365	Operator response the problem correctly and distributing algorithm will be taken for line 103 (MTU)
127415	command has been processed by operator successfully, redistribution command has been sent out (RTU)
127450	Line 103 is overloaded and an alarm has been generated (FID)
127451	103 has been detected and related FCD device gets noticed (FCD)
127480	RTU has processed an alarm from Line 103 and sent it to MTU (RTU)
127704	Operator recognize the alarm for Line103 (MTU)
127710	Operator response the problem correctly and distributing algorithm will be taken for line 103 (MTU)
127757	command has been processed by operator successfully, redistribution command has been sent out (RTU)
127810	Line 103 is overloaded and an alarm has been generated (FID)
127811	103 has been detected and related FCD device gets noticed (FCD)
127855	RTU has processed an alarm from Line 103 and sent it to MTU (RTU)
127938	Operator recognize the alarm for Line103 (MTU)
127941	Operator response the problem correctly and distributing algorithm will be taken for line 103 (MTU)
127983	command has been processed by operator successfully, redistribution command has been sent out (RTU)
128020	Line 103 is overloaded and an alarm has been generated (FID)
128021	103 has been detected and related FCD device gets noticed (FCD)
128071	RTU has processed an alarm from Line 103 and sent it to MTU (RTU)

Stamped Time	Events
128685	Operator recognize the alarm for Line103 (MTU)
128691	Operator response the problem correctly and distributing algorithm will be taken for line 103 (MTU)
128734	command has been processed by operator sucessfully, redistribution command has been sent out (RTU)
128770	Line 103 is overloaded and an alarm has been generated (FID)
128771	103 has been detected and related FCD device gets noticed (FCD)
128804	RTU has processed an alarm from Line 103 and sent it to MTU (RTU)
130078	Operator recognize the alarm for Line103 (MTU)
130085	Operator response the problem correctly and distributing algorithm will be taken for line 103 (MTU)
130117	command has been processed by operator sucessfully, redistribution command has been sent out (RTU)
130150	Line 103 is overloaded and an alarm has been generated (FID)
130189	RTU has processed an alarm from Line 103 and sent it to MTU (RTU)
130557	..Operator fails to make action for Line 103 (MTU)
155650	Line 119 is overloaded and an alarm has been generated (FID)
155651	119 has been detected and related FCD device gets noticed (FCD)
155697	RTU has processed an alarm from Line 119 and sent it to MTU (RTU)
156999	FCD device has been triggered to disconnect line 103 (FCD)
157824	overload problem solved and circuit breaker will be closed to connect 103 (FCD)
157824	103 has received the command from RTU for connecting the line (FCD)
	Test Summary (SF) Unavailability of service: 5.1%

Table A-IV 7 Summary of FCD SO single failure mode tests

Test Number	Service unavailability (Studied substation)	Test Number	Service unavailability (Studied substation)
1	8%	**11**	6.1%
2	6%	**12**	7.8%
3	8%	**13**	7.7%
4	5.4%	**14**	1.1%
5	6.4%	**15**	2.4%
6	5.9%	**16**	7.1%
7	5.7%	**17**	2.1%
8	5.2%	**18**	3.9%
9	7.2%	**19**	2.1%
10	9%	**20**	2.6%
Summary: Service unavailability (Average): 5.4% Confidence Interval (CI) [4.4%, 6.4%] where α=0.05			

FID FRL Mode

As seen from the SOE table from one of FID FRL tests (Table A-IV 8), no serious events have been observed after the drop of FID's calibration value. Most observed results during FID FRL failure modes tests are similar. After more than 20 tests, service unavailability averages 0.

FID FRH Mode

As seen from the SOE table from one of the FID FRH tests (Table A-IV 9), the FID device for line 119 was in FRH failure mode and its calibration value was modified by increasing its offset. Due to this mistake, line 119 was considered as overloaded by mistake, which can be observed from the table, although it should not. Most observed results during FID FRH tests are similar. In the case when FID is in FRH failure mode, the calibration of the affected device will be modified and its controlled line will become overloaded although it should not. Table A-IV 10 shows observed results from another FRH test, with similar results shown in Table A-IV 9. However, in this test, the affected line, line 119, remained overloaded after the calibration mistake had been corrected.

Table A-IV 8 Observed results from one of FID FRL tests

Stamped Time	Events
105378	**********FID device for 103 is in FRL mode ********** (FID)
105378	******Line 103's FID calibration has been modified, offset is -7.304466344149219********* (FID)
106539	******Line 103's FID calibration problem has been solved...
106539	**********FID device for 103 is out of FRL mode ********* (FID)
189085	**********FID device for 119 is in FRL mode ********** (FID)
189085	******Line 119's FID calibration has been modified, offset is -8.625314461016023********* (FID)
192509	******Line 119's FID calibration problem has been solved...
192509	**********FID device for 119 is out of FRL mode ********* (FID)
231584	**********FID device for 103 is in FRL mode ********** (FID)
231584	******Line 103's FID calibration has been modified, offset is + -4.217143277334121********* (FID)
232284	******Line 103's FID calibration problem has been solved...
232284	**********FID device for 103 is out of FRL mode ********* (FID)
237682	**********FID device for 119 is in FRL mode ********** (FID)
237682	******Line 119's FID calibration has been modified, offset is + -5.017874130566275********* (FID)
238653	******Line 119's FID calibration problem has been solved...
238653	**********FID device for 119 is out of FRL mode ********* (FID)

Stamped Time	Events
	Test Summary (SF) Unavailability of Service: 0.0

Table A-IV 9 Observed Results of one of FID FRH tests

Stamped Time	Events
68446	**********FID device for 119 is in FRH mode ********** (FID)
68446	******Line 119's FID calibration has been modified, offset is 9.315529670315708********* (FID)
70497	Line 119 is overloaded and an alarm has been generated (FID)
70498	119 has been detected and related FCD device gets noticed (FCD)
70605	RTU has processed an alarm from Line 119 and sent it to MTU (RTU)
72340	Operator recognize the alarm for Line119 (MTU)
72344	Operator response the problem correctly and distributing algorithm will be taken for line 119 (MTU)
72401	command has been processed by operator successfully, redistribution command has been sent out (RTU)
72432	Line 119 is overloaded and an alarm has been generated (FID)
72433	119 has been detected and related FCD device gets noticed (FCD)
72510	RTU has processed an alarm from Line 119 and sent it to MTU (RTU)
72614	Operator recognize the alarm for Line119 (MTU)
72618	Operator response the problem correctly and distributing algorithm will be taken for line 119 (MTU)
72683	command has been processed by operator successfully, redistribution command has been sent out (RTU)
72712	Line 119 is overloaded and an alarm has been generated (FID)
72713	119 has been detected and related FCD device gets noticed (FCD)
72750	RTU has processed an alarm from Line 119 and sent it to MTU (RTU)
73342	Operator recognize the alarm for Line119 (MTU)
73347	Operator response the problem correctly and distributing algorithm will be taken for line 119 (MTU)
73422	command has been processed by operator sucessfully, redistribution command has been sent out (RTU)
73452	Line 119 is overloaded and an alarm has been generated (FID)
73453	119 has been detected and related FCD device gets noticed (FCD)
73531	RTU has processed an alarm from Line 119 and sent it to MTU (RTU)
74482	Operator recognize the alarm for Line119 (MTU)
74487	Operator response the problem correctly and distributing algorithm will be taken for line 119 (MTU)
74550	command has been processed by operator successfully, redistribution command has been sent out (RTU)
74900	FCD device has been triggered to disconnect line 119 (FCD)
75312	******Line 119's FID calibration problem has been solved...
75312	**********FID device for 119 is out of FRH mode ********* (FID)
76511	overload problem solved and circuit breaker will be closed to connect 119 (FCD)
76511	119 has received the command from RTU for connecting the line (FCD)

Stamped Time	Events
259200	Test Summary (SF) Unavailability of service: 1.1%

Table A-IV 10 Observed Results of one of FID FRH tests

Stamped Time	Events
37845	**********FID device for 119 is in FRH mode ********** (FID)
37845	******Line 119's FID calibration has been modified, offset is 6.330422875309715********* (FID)
37877	Line 119 is overloaded and an alarm has been generated (FID)
37878	119 has been detected and related FCD device gets noticed (FCD)
37917	RTU has processed an alarm from Line 119 and sent it to MTU (RTU)
39286	Operator recognize the alarm for Line119 (MTU)
39293	Operator response the problem correctly and distributing algorithm will be taken for line 119 (MTU)
39351	command has been processed by operator successfully, redistribution command has been sent out (RTU)
39371	Line 119 is overloaded and an alarm has been generated (FID)
39372	119 has been detected and related FCD device gets noticed (FCD)
39462	RTU has processed an alarm from Line 119 and sent it to MTU (RTU)
39631	******Line 119's FID calibration problem has been solved...
39631	**********FID device for 119 is out of FRH mode ********* (FID)
39717	Operator recognize the alarm for Line119 (MTU)
39722	Operator response the problem correctly and distributing algorithm will be taken for line 119 (MTU)
39802	command has been processed by operator successfully, redistribution command has been sent out (RTU)
39831	Line 119 is overloaded and an alarm has been generated (FID)
39832	119 has been detected and related FCD device gets noticed (FCD)
39870	RTU has processed an alarm from Line 119 and sent it to MTU (RTU)
40039	Operator recognize the alarm for Line119 (MTU)
40046	Operator response the problem correctly and distributing algorithm will be taken for line 119 (MTU)
40144	command has been processed by operator successfully, redistribution command has been sent out (RTU)
40171	Line 119 is overloaded and an alarm has been generated (FID)
40172	119 has been detected and related FCD device gets noticed (FCD)
40216	RTU has processed an alarm from Line 119 and sent it to MTU (RTU)
41829	Operator recognize the alarm for Line119 (MTU)
41838	Operator response the problem correctly and distributing algorithm will be taken for line 119 (MTU)
41903	command has been processed by operator successfully, redistribution command has been sent out (RTU)
41931	Line 119 is overloaded and an alarm has been generated (FID)
42983	Line 103 is overloaded and an alarm has been generated (FID)
42983	103 has been detected and related FCD device gets noticed (FCD)

Stamped Time	Events
43015	RTU has processed an alarm from Line 119 and sent it to MTU (RTU)
43152	..Operator fails to make action for Line 119 (MTU)
43166	FCD device has been triggered to disconnect line 119 (FCD)
43200	FCD device has been triggered to disconnect line 103 (FCD)
45762	overload problem solved and circuit breaker will be closed to connect 119 (FCD)
45762	119 has received the command from RTU for connecting the line (FCD)
48170	overload problem solved and circuit breaker will be closed to connect 103 (FCD)
48170	103 has received the command from RTU for connecting the line (FCD)
126909	**********FID device for 103 is in FRH mode ********** (FID)
126909	******Line 103's FID calibration has been modified, offset is 9.8419555538671963********* (FID)
127007	Line 103 is overloaded and an alarm has been generated (FID)
127008	103 has been detected and related FCD device gets noticed (FCD)
127080	RTU has processed an alarm from Line 103 and sent it to MTU (RTU)
128466	******Line 103's FID calibration problem has been solved...
128466	**********FID device for 103 is out of FRH mode ********* (FID)
128577	..Operator fails to make action for Line 103 (MTU)
128700	FCD device has been triggered to disconnect line 103 (FCD)
131708	overload problem solved and circuit breaker will be closed to connect 103 (FCD)
131708	103 has received the command from RTU for connecting the line (FCD)
	Test Summary (SF) Unavailability of service: 5.9%

RTU FRF Mode

As seen from the SOE table from one of RTU FRF tests (Table A-IV 14), an overload alarm was generated for line 103 and sent to the MTU through its connected RTU device at first. Then the RTU001 lost connection to field devices. At time 2793 seconds, the RTU device received a redistribution command from the MTU, but failed to follow this command due to the lost connection to field devices. At time 3400 seconds, the FCD device of line 103 was automatically triggered, although it should not. The service was interrupted until the affected RTU device connected the field device again, which can be observed at time 73887 seconds. In this test, no overload alarm is generated caused by the RTU FRF mode and unavailability of service caused by FRF mode is 28%. Results collected from all RTU FRF single failure mode tests are summarized in Table A-IV 11 .

RTU FRW Mode

As seen from the SOE table from one of the RTU FRW tests (Table A-IV 15), line 103 first became overloaded and in this case the operator failed to recognize this alarm. The FCD

device for line 103 was first triggered to disconnect the line. Then the hardware of the RTU device failed rendering it unavailable to both the MTU and field devices. Therefore, line 103 could not be connected since no command can be sent from the RTU device to field devices. The affected line, line 103, remained disconnected until the failure had been solved. Table A-IV 16 lists recorded events during another RTU FRW test. During this test, an overload alarm was first lost due to the hardware failure and no further actions were performed by the operator. Line 119. which is connected to line 103, was overloaded and the operator failed to recognize the alarm causing the line to be disconnected by its FCD device. At time 25209, the FCD device tried to connect line 119, but failed due to RTU hardware failure. Therefore, line 119 remained disconnected until the hardware failure was solved. However, line 119 remained overloaded for a certain period. Results collected from all RTU FRW single failure mote tests are summarized in Table A-IV 12.

RTU FRC Mode

In this test, it is assumed that the communication is not stable between the RTU and the MTU. As seen from the SOE table from one of the RTU FRC tests (Table A-IV 17), the RTU001 first received a command from the MTU for redistributing the load. However, the RTU device failed to interpret this command due to communication error, which caused the FCD device of line 103 to be triggered to disconnect the line. Most observed results during RTU FRC tests are similar. In the case when the communication error occurs between MTU and the RTU, the command sent from the MTU to the RTU will be interpreted incorrectly and no further actions will be performed. Results collected from all RTU FRC single failure mode tests are summarized in Table A-IV 13.

Table A-IV 11 Summary of RTU FRF single failure mode tests

Test Number	Service unavailability (Studied substation)	Test Number	Service unavailability (Studied substation)
1	16%	**11**	14%
2	17%	**12**	21%
3	38%	**13**	34%
4	26%	**14**	46%
5	28%	**15**	9.6%

6	34%	**16**	15%
7	9.7%	**17**	10%
8	40%	**18**	43%
9	47%	**19**	11%
10	37%	**20**	22%
Summary: Service unavailability (Average): 26 % Confidence Interval (CI) [21%, 34%] where α=0.05			

Table A-IV 12 Summary of RTU FRW single failure mode tests

Test Number	Service unavailability (Studied substation)	Test Number	Service unavailability (Studied substation)
1	1.5%	11	4.2%
2	1.8%	12	4.6%
3	2.3%	13	4.5%
4	2.7%	14	5.3%
5	2.9%	15	5.5%
6	3%	16	6.1%
7	3.1%	17	6.4%
8	3.6%	18	6.6%
9	4.1%	19	7.4%
10	1.5%	20	7.7%
Summary: Service unavailability (Average): 4.3% Confidence Interval (CI) [3.3%, 5.1%] where α=0.05			

Table A-IV 13 Summary of RTU FRC single failure mode tests

Test Number	Service unavailability (Studied substation)	Test Number	Service unavailability (Studied substation)
1	1.1%	**11**	3.8%
2	1.5%	**12**	4.9%
3	1.7%	**13**	5.7%
4	2.4%	**14**	5.8%
5	2.7%	**15**	6.7%

6	2.8%	**16**	9.2%
7	2.9%	**17**	4.4%
8	3%	**18**	3.3%
9	3.5%	**19**	4.8%
10	3.6%	**20**	1.5%
Summary: Service unavailability (Average): 3.8% Confidence Interval (CI) [2.8%, 4.8%] where α=0.05			

Table A-IV 14 Observed Results of one of RTU FRF tests

Stamped Time	Events
2425	Line 103 is overloaded and an alarm has been generated (FID)
2426	103 has been detected and related FCD device gets noticed (FCD)
2464	RTU has processed an alarm from Line 103 and sent it to MTU (RTU)
2518	**********RTU device: RTU-001 is in FRF mode ********** (RTU)
2518	*********Warning: RTU device RTU-001 lost connection to field devices********** (RTU)
2757	Operator recognize the alarm for Line103 (MTU)
2761	Operator response the problem correctly and distributing algorithm will be taken for line 103 (MTU)
2793	*********Warning: RTU device RTU-001 receives command from MTU , but unable to process it due to connection lost to field devices (RTU)
3400	FCD device has been triggered to disconnect line 103 (FCD)
5663	******* circuit breaker is not able to be closed to connect 103 due to RTU failure (FCD)
73887	RTU connection lost to field devices is solved
73887	**********RTU device: RTU-001 is out of FRF mode ********** (RTU)
75218	overload problem solved and circuit breaker will be closed to connect 103 (FCD)
75218	103 has received the command from RTU for connecting the line (FCD)
	Test Summary (SF) Unavailability of service: 28%

Table A-IV 15 Observed Results of one of RTU FRW tests

Stamped Time	Events
2466	Line 103 is overloaded and an alarm has been generated (FID)
2467	103 has been detected and related FCD device gets noticed (FCD)
2521	RTU has processed an alarm from Line 103 and sent it to MTU (RTU)
2700	FCD device has been triggered to disconnect line 103 (FCD)
5633	**********RTU device: RTU-001 is in FRW mode ********** (RTU)
5633	Warning: RTU hardware fails (RTU)
9750	******* circuit breaker is not able to be closed to connect 103 due to RTU failure (FCD)
13873	RTU hardware failure solved
13873	**********RTU device: RTU-001 is out of FRW mode ********** (RTU)
16420	overload problem solved and circuit breaker will be closed to connect 103 (FCD)

Stamped Time	Events
16420	103 has received the command from RTU for connecting the line (FCD)
	Test Summary (SF)Unavailability of service: 5.5%

Table A-IV 16 Observed events during one of RTU FRW tests.

Stamped Time	Events
1536	**********RTU device: RTU-001 is in FRW mode ********** (RTU)
1536	Warning: RTU hardware fails (RTU)
1666	Line 103 is overloaded and an alarm has been generated (FID)
1668	********Warning : An alarm has been lost due to hardware failure ******(RTU)
7550	RTU hardware failure solved
7550	**********RTU device: RTU-001 is out of FRW mode ********** (RTU)
18261	Line 119 is overloaded and an alarm has been generated (FID)
18262	119 has been detected and related FCD device gets noticed (FCD)
18364	RTU has processed an alarm from Line 119 and sent it to MTU (RTU)
19826	..Operator fails to make action for Line 119 (MTU)
19941	**********RTU device: RTU-001 is in FRW mode ********** (RTU)
19941	Warning: RTU hardware fails (RTU)
21600	FCD device has been triggered to disconnect line 119 (FCD)
25209	******* circuit breaker is not able to be closed to connect 119 due to RTU failure (FCD)
28229	******* circuit breaker is not able to be closed to connect 119 due to RTU failure (FCD)
28611	RTU hardware failure solved
28611	**********RTU device: RTU-001 is out of FRW mode ********** (RTU)
31161	overload problem solved and circuit breaker will be closed to connect 119 (FCD)
31161	119 has received the command from RTU for connecting the line (FCD)
32425	Line 119 is overloaded and an alarm has been generated (FID)
32426	119 has been detected and related FCD device gets noticed (FCD)
32472	RTU has processed an alarm from Line 119 and sent it to MTU (RTU)
34400	Operator recognize the alarm for Line119 (MTU)
34405	Operator response the problem correctly and distributing algorithm will be taken for line 119 (MTU)
34453	command has been processed by operator successfully, redistribution command has been sent out (RTU)
34485	Line 119 is overloaded and an alarm has been generated (FID)
34486	119 has been detected and related FCD device gets noticed (FCD)
34519	RTU has processed an alarm from Line 119 and sent it to MTU (RTU)
34693	Operator recognize the alarm for Line119 (MTU)
34698	Operator response the problem correctly and distributing algorithm will be taken for line 119 (MTU)
34796	command has been processed by operator successfully, redistribution command has been sent out (RTU)
259200.001	Test Summary (SF) Unavailability of service : 4.1%

Table A-IV 17 Observed results from one of RTU FRC tests

Stamped Time	Events
1559	Line 103 is overloaded and an alarm has been generated (FID)
1560	103 has been detected and related FCD device gets noticed (FCD)
1620	RTU has processed an alarm from Line 103 and sent it to MTU (RTU)
1857	Operator recognize the alarm for Line103 (MTU)
1862	Operator response the problem correctly and distributing algorithm will be taken for line 103 (MTU)
1892	**********RTU device: RTU-001 is in FRC mode ********** (RTU)
1918	**********Communication error from MTU to RTU is assumed**********
1923	RTU fails to interpret command for Line103from MTU due to data lost (RTU)
2065	FCD device has been triggered to disconnect line 103 (FCD)
9003	overload problem solved and circuit breaker will be closed to connect 103 (FCD)
9003	103 has received the command from RTU for connecting the line (FCD)
	Test Summary (SF) Unavailability of service: 2.8%

Experiment II

Table A-IV 18 Summary of FCD FO normal tests

Test Number	The number of overload alarms	The number of affected SUC components	The number of affected SCADA components	ASSAI/Vulnerability
1	2	0	0	1
2	3	1	0	1
3	2	0	0	1
4	2	0	0	1
5	2	0	0	1
6	2	0	0	1
7	2	0	0	1
8	2	0	0	1
9	2	0	0	1
10	2	0	0	1
Average				
	2	**0**	**0**	**1**

Table A-IV 19 Observed Results from one of FCD FO normal tests

Stamped Time	Events
40634	Line 127 is overloaded (373.21 MW)and an alarm has been generated (FID)
40635	**********FCD device for 127 is in FO mode ********** (FCD)
40643	RTU has processed an alarm from Line 127 and sent it to MTU (RTU)
40714	..Operator fails to make action for Line 127 (MTU)
42324	**********FCD device fail to be triggered to disconnect 127 due to FO failure mode******* (FCD)
43226	Line 127 is overloaded (374.94 MW)and an alarm has been generated (FID)
43246	RTU has processed an alarm from Line 127 and sent it to MTU (RTU)
43312	..Operator fails to make action for Line 127 (MTU)
46015	**********FCD device for 127 is out of FO mode ********* (FCD)
432001	**Test Summary ASSAI is : 1.0 Total Numbers of Overloads: 2**

Table A-IV 20 Observed results from one of FCD FO worse-case tests

Stamped Time	Events
41424	Line 127 is overloaded (373.56 MW)and an alarm has been generated (FID)
41425	**********FCD device for 127 is in FO mode ********** (FCD)
41436	RTU has processed an alarm from Line 127 and sent it to MTU (RTU)
41500	..Operator fails to make action for Line 127 (MTU)
42506	**********FCD device fail to be triggered to disconnect 127 due to FO failure mode******* (FCD)
44128	Line 127 is overloaded (374.53 MW)and an alarm has been generated (FID)
44140	RTU has processed an alarm from Line 127 and sent it to MTU (RTU)
44200	..Operator fails to make action for Line 127 (MTU)

Stamped Time	Events
46941	**********FCD device for 127 is out of FO mode ********* (FCD)
86401	Test Summary ASSAI is : 1.0 Test Summary (Total)Total Numbers of Overloads: 2

Table A-IV 21 Observed Results from one of FCD FC normal tests

Stamped Time	Events
40571	Line 127 is overloaded (373.5 MW)and an alarm has been generated (FID)
40593	RTU has processed an alarm from Line 127 and sent it to MTU (RTU)
40653	..Operator fails to make action for Line 127 (MTU)
42526	FCD device has been triggered to disconnect line 127 (FCD)
42527	**********FCD device for 127 is in FC mode ********** (FCD)
43400	Line 194 is overloaded (-778.78 MW)and an alarm has been generated (FID)
43401	Line 66 is overloaded (563.77 MW)and an alarm has been generated (FID)
43420	RTU has processed an alarm from Line 194 and sent it to MTU (RTU)
43498	Operator recognize the alarm for Line194 (MTU)
44101	Operator response the problem correctly and distributing algorithm will be taken for line 194 (MTU)
44120	command has been processed by operator successfully, redistribution command has been sent out (RTU)
44162	Operator recognize the alarm for Line66 (MTU)
44164	Operator response the problem correctly and distributing algorithm will be taken for line 66 (MTU)
44186	command has been processed by operator successfully, redistribution command has been sent out (RTU)

Stamped Time	Events
44817	overload problem solved and circuit breaker will be closed to connect 127 (FCD)
44817	********* FCD device fail to be triggered to connect 127 due to its FC failure mode ********* (FCD)
45439	**********FCD device for 127 is out of FC mode ********* (FCD)
45439	******* Line 127 been connected after the maintance********* (FCD)
432001	Test Summary ASSAI is : **0.9995** Test Summary (Total)Total Numbers of Overloads:**3**

Table A-IV 22 Summary of FCD FC normal tests

Test Number	The number of overload alarms	The number of affected SUC components	The number of affected SCADA components	ASSAI / Vulnerability
1	3	2	0	0.9995
2	3	2	0	0.9997
3	4	3	0	0.9997
4	3	2	0	0.9995
5	3	2	0	0.9996
6	3	2	0	0.9995
7	4	3	0	0.9996
8	3	2	0	0.9998
9	3	2	0	0.9996
10	3	2	0	0.9996
Average				
	3.2	**2.2**	**0**	**0.9996**

Table A-IV 23 Observed results of one of FCD FC worse-case tests

Time (s)	Events
40588	Line 127 is overloaded (373.62 MW)and an alarm has been generated (FID)
40605	RTU has processed an alarm from Line 127 and sent it to MTU (RTU)
41408	..Operator fails to make action for Line 127 (MTU)
43312	FCD device has been triggered to disconnect line 127 (FCD)
43312	**********FCD device for 127 is in FC mode ********** (FCD)
44241	Line 66 is overloaded (563.29 MW)and an alarm has been generated (FID)
44241	Line 194 is overloaded (-779.11 MW)and an alarm has been generated (FID)
44249	RTU has processed an alarm from Line 66 and sent it to MTU (RTU)
44341	..Operator fails to make action for Line 66 (MTU)
47729	overload problem solved and circuit breaker will be closed to connect 127 (FCD)
47729	********* FCD device fail to be triggered to connect 127 due to its FC failure mode ********* (FCD)
47767	FCD device has been triggered to disconnect line 194 (FCD)
47829	Line 62 is overloaded (352.7 MW)and an alarm has been generated (FID)
47829	Line 184 is overloaded (-1133.86 MW)and an alarm has been generated (FID)
47833	RTU has processed an alarm from Line 184 and sent it to MTU (RTU)
47854	RTU has processed an alarm from Line 62 and sent it to MTU (RTU)
47921	..Operator fails to make action for Line 184 (MTU)
48609	..Operator fails to make action for Line 62 (MTU)
48648	Line 187 is overloaded (-1220.0 MW)and an alarm has been generated (FID)
48671	RTU has processed an alarm from Line 187 and sent it to MTU (RTU)
49502	Line 64 is overloaded (350.34 MW)and an alarm has been generated (FID)
49521	RTU has processed an alarm from Line 64 and sent it to MTU (RTU)
49604	FCD device has been triggered to disconnect line 184 (FCD)
49605	..Operator fails to make action for Line 187 (MTU)
49634	**********FCD device for 127 is out of FC mode ********* (FCD)
49634	******* Line 127 been connected after the maintance********* (FCD)
50501	FCD device has been triggered to disconnect line 62 (FCD)
50502	..Operator fails to make action for Line 64 (MTU)
51423	overload problem solved and circuit breaker will be closed to connect 194 (FCD)
52227	Line 127 is overloaded (541.13 MW)and an alarm has been generated (FID)
52240	RTU has processed an alarm from Line 127 and sent it to MTU (RTU)
52261	overload problem solved and circuit breaker will be closed to connect 66 (FCD)
52261	66 has received the command from RTU for connecting the line (FCD)
52407	Line 137 is overloaded (320.01 MW)and an alarm has been generated (FID)
53117	RTU has processed an alarm from Line 137 and sent it to MTU (RTU)
53269	overload problem solved and circuit breaker will be closed to connect 184 (FCD)
53269	184 has received the command from RTU for connecting the line (FCD)
54109	overload problem solved and circuit breaker will be closed to connect 62 (FCD)
54109	62 has received the command from RTU for connecting the line (FCD)
54163	Line 194 is overloaded (-994.68 MW)and an alarm has been generated (FID)
54904	RTU has processed an alarm from Line 194 and sent it to MTU (RTU)
55109	FCD device has been triggered to disconnect line 127 (FCD)
55111	..Operator fails to make action for Line 127 (MTU)
56711	Line 66 is overloaded (542.56 MW)and an alarm has been generated (FID)

Time (s)	Events
56723	RTU has processed an alarm from Line 66 and sent it to MTU (RTU)
56808	FCD device has been triggered to disconnect line 186 (FCD)
56809	..Operator fails to make action for Line 137 (MTU)
57669	FCD device has been triggered to disconnect line 191 (FCD)
57671	..Operator fails to make action for Line 186 (MTU)
58541	FCD device has been triggered to disconnect line 137 (FCD)
58542	..Operator fails to make action for Line 194 (MTU)
58613	Line 184 is overloaded (-1041.85 MW)and an alarm has been generated (FID)
58613	Line 62 is overloaded (347.91 MW)and an alarm has been generated (FID)
58629	RTU has processed an alarm from Line 184 and sent it to MTU (RTU)
58632	RTU has processed an alarm from Line 62 and sent it to MTU (RTU)
58710	FCD device has been triggered to disconnect line 194 (FCD)
58712	..Operator fails to make action for Line 66 (MTU)
59439	overload problem solved and circuit breaker will be closed to connect 127 (FCD)
59439	127 has received the command from RTU for connecting the line (FCD)
59534	FCD device has been triggered to disconnect line 66 (FCD)
59535	..Operator fails to make action for Line 184 (MTU)
60483	overload problem solved and circuit breaker will be closed to connect 186 (FCD)
60483	186 has received the command from RTU for connecting the line (FCD)
61269	FCD device has been triggered to disconnect line 64 (FCD)
61270	..Operator fails to make action for Line 62 (MTU)
61271	FCD device has been triggered to disconnect line 62 (FCD)
61348	overload problem solved and circuit breaker will be closed to connect 191 (FCD)
61373	Line 127 is overloaded (537.76 MW)and an alarm has been generated (FID)
61403	RTU has processed an alarm from Line 127 and sent it to MTU (RTU)
62117	FCD device has been triggered to disconnect line 184 (FCD)
62155	..Operator fails to make action for Line 127 (MTU)
62192	overload problem solved and circuit breaker will be closed to connect 137 (FCD)
62192	137 has received the command from RTU for connecting the line (FCD)
63037	overload problem solved and circuit breaker will be closed to connect 194 (FCD)
63037	194 has received the command from RTU for connecting the line (FCD)
63211	overload problem solved and circuit breaker will be closed to connect 66 (FCD)
63211	66 has received the command from RTU for connecting the line (FCD)
64910	overload problem solved and circuit breaker will be closed to connect 64 (FCD)
64910	64 has received the command from RTU for connecting the line (FCD)
64912	overload problem solved and circuit breaker will be closed to connect 62 (FCD)
64912	62 has received the command from RTU for connecting the line (FCD)
65717	overload problem solved and circuit breaker will be closed to connect 184 (FCD)
65717	184 has received the command from RTU for connecting the line (FCD)
65737	FCD device has been triggered to disconnect line 127 (FCD)
65738	..Operator fails to make action for Line 186 (MTU)
65746	Line 194 is overloaded (-1007.11 MW)and an alarm has been generated (FID)
65763	RTU has processed an alarm from Line 194 and sent it to MTU (RTU)
66610	**********RTU device: RTU-038 lost power ********** (RTU)

Time (s)	Events
66692	**********RTU device: RTU-038 resume power ********** (RTU)
66776	Line 66 is overloaded (542.17 MW)and an alarm has been generated (FID)
66777	66 has been detected and related FCD device gets noticed (FCD)
66798	RTU has processed an alarm from Line 66 and sent it to MTU (RTU)
66806	**********RTU device: RTU-037 lost power ********** (RTU)
67652	**********RTU device: RTU-037 resume power ********** (RTU)
68482	FCD device has been triggered to disconnect line 186 (FCD)
68483	..Operator fails to make action for Line 191 (MTU)
68568	overload problem solved and circuit breaker will be closed to connect 127 (FCD)
68568	127 has received the command from RTU for connecting the line (FCD)
68659	..Operator fails to make action for Line 194 (MTU)
69496	FCD device has been triggered to disconnect line 194 (FCD)
69497	..Operator fails to make action for Line 66 (MTU)
69567	Line 184 is overloaded (-1076.57 MW)and an alarm has been generated (FID)
69567	Line 62 is overloaded (358.56 MW)and an alarm has been generated (FID)
70216	RTU has processed an alarm from Line 184 and sent it to MTU (RTU)
70224	RTU has processed an alarm from Line 62 and sent it to MTU (RTU)
70306	FCD device has been triggered to disconnect line 66 (FCD)
70307	..Operator fails to make action for Line 184 (MTU)
70499	Line 64 is overloaded (338.03 MW)and an alarm has been generated (FID)
71117	RTU has processed an alarm from Line 64 and sent it to MTU (RTU)
71303	overload problem solved and circuit breaker will be closed to connect 186 (FCD)
71303	186 has received the command from RTU for connecting the line (FCD)
71338	Line 127 is overloaded (550.21 MW)and an alarm has been generated (FID)
71339	127 has been detected and related FCD device gets noticed (FCD)
71363	RTU has processed an alarm from Line 127 and sent it to MTU (RTU)
72023	FCD device has been triggered to disconnect line 62 (FCD)
72024	..Operator fails to make action for Line 62 (MTU)
72199	FCD device has been triggered to disconnect line 184 (FCD)
72200	..Operator fails to make action for Line 64 (MTU)
72924	overload problem solved and circuit breaker will be closed to connect 194 (FCD)
72924	194 has received the command from RTU for connecting the line (FCD)
73103	overload problem solved and circuit breaker will be closed to connect 66 (FCD)
73103	66 has received the command from RTU for connecting the line (FCD)
74018	Line 186 is overloaded (-1331.24 MW)and an alarm has been generated (FID)
74019	186 has been detected and related FCD device gets noticed (FCD)
74042	RTU has processed an alarm from Line 186 and sent it to MTU (RTU)
74708	RTU has processed an alarm from Line 191 and sent it to MTU (RTU)
74842	overload problem solved and circuit breaker will be closed to connect 62 (FCD)
74843	62 has received the command from RTU for connecting the line (FCD)
74932	FCD device has been triggered to disconnect line 127 (FCD)
74934	..Operator fails to make action for Line 127 (MTU)
75652	overload problem solved and circuit breaker will be closed to connect 184 (FCD)
75652	184 has received the command from RTU for connecting the line (FCD)

Time (s)	Events
75674	Line 194 is overloaded (-999.16 MW)and an alarm has been generated (FID)
75675	194 has been detected and related FCD device gets noticed (FCD)
75680	RTU has processed an alarm from Line 194 and sent it to MTU (RTU)
76704	Line 66 is overloaded (534.42 MW)and an alarm has been generated (FID)
76705	66 has been detected and related FCD device gets noticed (FCD)
77408	RTU has processed an alarm from Line 66 and sent it to MTU (RTU)
78323	FCD device has been triggered to disconnect line 186 (FCD)
78324	..Operator fails to make action for Line 186 (MTU)
78519	FCD device has been triggered to disconnect line 191 (FCD)
78520	..Operator fails to make action for Line 191 (MTU)
79223	overload problem solved and circuit breaker will be closed to connect 127 (FCD)
79223	127 has received the command from RTU for connecting the line (FCD)
79355	FCD device has been triggered to disconnect line 194 (FCD)
79356	..Operator fails to make action for Line 194 (MTU)
80112	Line 62 is overloaded (343.72 MW)and an alarm has been generated (FID)
80127	RTU has processed an alarm from Line 62 and sent it to MTU (RTU)
80172	Line 184 is overloaded (-1020.8 MW)and an alarm has been generated (FID)
80173	184 has been detected and related FCD device gets noticed (FCD)
80199	RTU has processed an alarm from Line 184 and sent it to MTU (RTU)
80228	FCD device has been triggered to disconnect line 66 (FCD)
80229	..Operator fails to make action for Line 66 (MTU)
81984	FCD device has been triggered to disconnect line 62 (FCD)
81985	FCD device has been triggered to disconnect line 64 (FCD)
82020	overload problem solved and circuit breaker will be closed to connect 186 (FCD)
82020	186 has received the command from RTU for connecting the line (FCD)
82089	Line 127 is overloaded (536.14 MW)and an alarm has been generated (FID)
82090	127 has been detected and related FCD device gets noticed (FCD)
82103	RTU has processed an alarm from Line 127 and sent it to MTU (RTU)
82164	FCD device has been triggered to disconnect line 184 (FCD)
82174	..Operator fails to make action for Line 127 (MTU)
82998	overload problem solved and circuit breaker will be closed to connect 194 (FCD)
82998	194 has received the command from RTU for connecting the line (FCD)
83815	overload problem solved and circuit breaker will be closed to connect 66 (FCD)
83815	66 has received the command from RTU for connecting the line (FCD)
84735	FCD device has been triggered to disconnect line 127 (FCD)
84791	..Operator fails to make action for Line 191 (MTU)
84807	overload problem solved and circuit breaker will be closed to connect 62 (FCD)
84807	62 has received the command from RTU for connecting the line (FCD)
84808	overload problem solved and circuit breaker will be closed to connect 64 (FCD)
84808	64 has received the command from RTU for connecting the line (FCD)
84839	Line 194 is overloaded (-972.74 MW)and an alarm has been generated (FID)
84863	RTU has processed an alarm from Line 194 and sent it to MTU (RTU)
85602	overload problem solved and circuit breaker will be closed to connect 184 (FCD)
85602	184 has received the command from RTU for connecting the line (FCD)

Time (s)	Events
85814	Line 66 is overloaded (522.56 MW)and an alarm has been generated (FID)
85815	66 has been detected and related FCD device gets noticed (FCD)
86401	Test Summary ASSAI is : 0.9568 Test Summary : Total Numbers of Overloads: 32

Table A-IV 24 Summary of FCD FC worse-case tests

Test Number	The number of overload alarms	The number of affected SUC components	The number of affected SCADA components	ASSAI / Vulnerability
1	36	6	2	0.9533
2	41	7	3	0.9561
3	37	8	1	0.9569
4	37	8	2	0.9562
5	35	8	2	0.9575
6	32	8	2	0.9568
7	39	10	1	0.959
8	29	9	2	0.9736
9	35	9	4	0.9487
10	33	7	2	0.9589
Average				
	35	**8.1**	**2.1**	**0.9604**

Table A-IV 25 Observed results of one of FCD SO normal tests

Stamped Time	Events
20790	**********FCD device for 127 is in SO mode ********** (FCD)
20790	127's STE offset has been updated to -17.482913439808414 (FCD)
22631	Line 127 is overloaded (358.49 MW)and an alarm has been generated (FID)
22640	RTU has processed an alarm from Line 127 and sent it to MTU (RTU)
22715	..Operator fails to make action for Line 127 (MTU)
25306	FCD device has been triggered to disconnect line 127 (FCD)
26141	Line 194 is overloaded (-777.89 MW)and an alarm has been generated (FID)
26142	194 has been detected and related FCD device gets noticed (FCD)
26158	RTU has processed an alarm from Line 194 and sent it to MTU (RTU)

Stamped Time	Events
26201	Line 66 is overloaded (544.21 MW)and an alarm has been generated (FID)
26202	66 has been detected and related FCD device gets noticed (FCD)
26219	RTU has processed an alarm from Line 66 and sent it to MTU (RTU)
26257	Operator recognize the alarm for Line194 (MTU)
26259	Operator response the problem correctly and distributing algorithm will be taken for line 194 (MTU)
26283	command has been processed by operator sucessfully, redistribution command has been sent out (RTU)
27056	Operator recognize the alarm for Line66 (MTU)
27058	Operator response the problem correctly and distributing algorithm will be taken for line 66 (MTU)
27081	command has been processed by operator sucessfully, redistribution command has been sent out (RTU)
27951	overload problem solved and circuit breaker will be closed to connect 127 (FCD)
27951	127 has received the command from RTU for connecting the line (FCD)
28853	**********FCD device for 127 is out of SO mode ********** (FCD)
28853	127's STE (Set up point) has been corrected (FCD)
	Test Summary ASSAI is : **0.9998** Total Numbers of Overloads: **3**

Table A-IV 26 Summary of FCD SO normal tests

Test Number	The number of overload alarms	The number of affected SUC components	The number of affected SCADA components	ASSAI/Vulnerability
1	3	2	0	0.9998
2	3	2	0	0.9998
3	3	2	0	0.9998
4	3	2	0	0.9995
5	3	2	0	0.9998
6	3	2	0	0.9998
7	4	3	0	0.9998
8	3	2	0	0.9998
9	3	2	0	0.9998
10	3	2	0	0.9997
Average				
	3.1	2	0	0.9998

Table A-IV 27 Observed results of one of FCD SO worse-case tests

Stamped Time	Events
27939	**********FCD device for 127 is in SO mode ********** (FCD)
27939	127's STE offset has been updated to -24.234428688620245 (FCD)
28876	Line 127 is overloaded (368.91 MW)and an alarm has been generated (FID)
28877	127 has been detected and related FCD device gets noticed (FCD)
28892	RTU has processed an alarm from Line 127 and sent it to MTU (RTU)
28970	..Operator fails to make action for Line 127 (MTU)
31507	FCD device has been triggered to disconnect line 127 (FCD)
32454	Line 66 is overloaded (556.57 MW)and an alarm has been generated (FID)
32454	Line 194 is overloaded (-781.43 MW)and an alarm has been generated (FID)
32501	RTU has processed an alarm from Line 66 and sent it to MTU (RTU)
34345	..Operator fails to make action for Line 66 (MTU)
35164	overload problem solved and circuit breaker will be closed to connect 127 (FCD)
35185	FCD device has been triggered to disconnect line 194 (FCD)
35279	Line 62 is overloaded (357.92 MW)and an alarm has been generated (FID)
35279	Line 184 is overloaded (-1148.93 MW)and an alarm has been generated (FID)
35296	RTU has processed an alarm from Line 62 and sent it to MTU (RTU)
35299	RTU has processed an alarm from Line 184 and sent it to MTU (RTU)
36027	..Operator fails to make action for Line 184 (MTU)
36058	FCD device has been triggered to disconnect line 66 (FCD)
36060	..Operator fails to make action for Line 62 (MTU)
36120	Line 187 is overloaded (-1220.0 MW)and an alarm has been generated (FID)
36131	RTU has processed an alarm from Line 187 and sent it to MTU (RTU)
36988	Line 64 is overloaded (351.56 MW)and an alarm has been generated (FID)
36989	64 has been detected and related FCD device gets noticed (FCD)
37003	RTU has processed an alarm from Line 64 and sent it to MTU (RTU)
37073	FCD device has been triggered to disconnect line 184 (FCD)
37075	..Operator fails to make action for Line 187 (MTU)
37887	Line 127 is overloaded (558.44 MW)and an alarm has been generated (FID)
37903	RTU has processed an alarm from Line 127 and sent it to MTU (RTU)
37951	FCD device has been triggered to disconnect line 62 (FCD)
37953	..Operator fails to make action for Line 64 (MTU)
38802	overload problem solved and circuit breaker will be closed to connect 194 (FCD)
38802	194 has received the command from RTU for connecting the line (FCD)
38805	FCD device has been triggered to disconnect line 187 (FCD)
38806	..Operator fails to make action for Line 127 (MTU)
39694	overload problem solved and circuit breaker will be closed to connect 66 (FCD)
39694	66 has received the command from RTU for connecting the line (FCD)
41403	overload problem solved and circuit breaker will be closed to connect 184 (FCD)
41403	184 has received the command from RTU for connecting the line (FCD)
41533	FCD device has been triggered to disconnect line 127 (FCD)
41559	overload problem solved and circuit breaker will be closed to connect 62 (FCD)
41559	62 has received the command from RTU for connecting the line (FCD)
42355	Line 194 is overloaded (-1220.0 MW)and an alarm has been generated (FID)

Stamped Time	Events
42356	194 has been detected and related FCD device gets noticed (FCD)
42426	overload problem solved and circuit breaker will be closed to connect 187 (FCD)
42427	187 has received the command from RTU for connecting the line (FCD)
42430	..Operator fails to make action for Line 191 (MTU)
42536	**********RTU device: RTU-037 lost power ********** (RTU)
42572	**********RTU device: RTU-037 resume power ********** (RTU)
43261	Line 66 is overloaded (563.6 MW)and an alarm has been generated (FID)
43287	RTU has processed an alarm from Line 66 and sent it to MTU (RTU)
45009	FCD device has been triggered to disconnect line 191 (FCD)
45011	..Operator fails to make action for Line 66 (MTU)
45031	overload problem solved and circuit breaker will be closed to connect 127 (FCD)
45031	127 has received the command from RTU for connecting the line (FCD)
45188	FCD device has been triggered to disconnect line 194 (FCD)
45934	Line 62 is overloaded (364.63 MW)and an alarm has been generated (FID)
45935	62 has been detected and related FCD device gets noticed (FCD)
45949	RTU has processed an alarm from Line 62 and sent it to MTU (RTU)
45994	Line 184 is overloaded (-1163.27 MW)and an alarm has been generated (FID)
45995	184 has been detected and related FCD device gets noticed (FCD)
46010	RTU has processed an alarm from Line 184 and sent it to MTU (RTU)
46028	..Operator fails to make action for Line 62 (MTU)
46048	FCD device has been triggered to disconnect line 66 (FCD)
46089	..Operator fails to make action for Line 184 (MTU)
46114	Line 187 is overloaded (-1220.0 MW)and an alarm has been generated (FID)
46115	187 has been detected and related FCD device gets noticed (FCD)
46131	RTU has processed an alarm from Line 187 and sent it to MTU (RTU)
46964	FCD device has been triggered to disconnect line 64 (FCD)
46966	..Operator fails to make action for Line 187 (MTU)
46967	FCD device has been triggered to disconnect line 62 (FCD)
86401	**Test Summary ASSAI is : 0.9483** **Test Summary Total Numbers of Overloads: 46**

Table A-IV 28 Summary of FCD SO worse-case tests

Test Number	The number of overload alarms	The number of affected SUC components	The number of affected SCADA components	ASSAI/Vulnerability
1	38	5	2	0.9525
2	49	9	3	0.9275
3	47	9	3	0.9251

4	49	5	4	0.9302
5	41	7	2	0.9489
6	46	8	1	0.9483
7	42	10	3	0.9259
8	46	8	3	0.9305
9	53	9	4	0.9245
10	41	6	2	0.9443
Average				
	45	**7.6**	**2.7**	**0.9357**

Table A-IV 29 Observed Results from one of FID FRL normal tests

TMMS	Events
34267	**********FID device for 127 is in FRL mode ********** (FID)
34267	******Line 127's FID calibration has been modified, offset is -24.629097414870106********* (FID)
47924.	******Line 127's FID calibration problem has been solved...
47924	**********FID device for 127 is out of FRL mode ********* (FID)
131553	Line 127 is overloaded (375.42 MW)and an alarm has been generated (FID)
131563	RTU has processed an alarm from Line 127 and sent it to MTU (RTU)
132310	..Operator fails to make action for Line 127 (MTU)
134124	FCD device has been triggered to disconnect line 127 (FCD)
135023	Line 66 is overloaded (553.32 MW)and an alarm has been generated (FID)
135024	66 has been detected and related FCD device gets noticed (FCD)
135023	Line 194 is overloaded (-775.18 MW)and an alarm has been generated (FID)
135069	RTU has processed an alarm from Line 194 and sent it to MTU (RTU)
135096	RTU has processed an alarm from Line 66 and sent it to MTU (RTU)
135122	Operator recognize the alarm for Line191 (MTU)
135139	command has been processed by operator sucessfully, redistribution command has been sent out (RTU)
135185	Operator recognize the alarm for Line66 (MTU)
135187	Operator response the problem correctly and distributing algorithm will be taken for line 66 (MTU)
135200	command has been processed by operator sucessfully, redistribution command has been sent out (RTU)
135248	Operator recognize the alarm for Line194 (MTU)
135250	Operator response the problem correctly and distributing algorithm will be taken for line 194 (MTU)
135266	command has been processed by operator sucessfully, redistribution command has been sent out (RTU)
135762	overload problem solved and circuit breaker will be closed to connect 127 (FCD)
135762	127 has received the command from RTU for connecting the line (FCD)
.	**Test Summary ASSAI is : 0.9996** **Total Numbers of Overloads: 3**

Table A-IV 30 Results of FID FRL normal tests

Test Number	The number of overload alarms	The number of affected SUC components	The number of affected SCADA components	ASSAI/Vulnerability
1	3	3	0	0.9996
2	3	2	0	0.9998
3	5	3	0	0.9996
4	3	2	0	0.9998
5	4	3	0	0.9998
6	3	3	0	0.9996
7	3	3	0	0.9996
8	4	3	0	0.9998
9	3	3	0	0.9996
10	3	2	0	0.9998
Average				
	3.4	**2.7**	**0**	**0.9997**

Table A-IV 31 Observed Results from one of FID FRH normal tests

Stamped Time	Events
32575	**********FID device for 127 is in FRH mode ********** (FID)
32575	******Line 127's FID calibration has been modified, offset is 18.231372008610972********* (FID)
34293	Line 127 is overloaded (390.0 MW)and an alarm has been generated (FID)
34305	RTU has processed an alarm from Line 127 and sent it to MTU (RTU)
34387	..Operator fails to make action for Line 127 (MTU)
36200	FCD device has been triggered to disconnect line 127 (FCD)
37117	Line 194 is overloaded (-778.65 MW)and an alarm has been generated (FID)
37118	Line 66 is overloaded (559.04 MW)and an alarm has been generated (FID)
37124	RTU has processed an alarm from Line 66 and sent it to MTU (RTU)
37848	RTU has processed an alarm from Line 194 and sent it to MTU (RTU)
37866	Operator recognize the alarm for Line66 (MTU)
37869	Operator response the problem correctly and distributing algorithm will be taken for line 66 (MTU)
37991	Operator recognize the alarm for Line194 (MTU)
37992	Operator response the problem correctly and distributing algorithm will be taken for line 194 (MTU)

Stamped Time	Events
38015	command has been processed by operator sucessfully, redistribution command has been sent out (RTU)
38372	overload problem solved and circuit breaker will be closed to connect 127 (FCD)
38372	127 has received the command from RTU for connecting the line (FCD)
39050	******Line 127's FID calibration problem has been solved...
39050	**********FID device for 127 is out of FRH mode ********* (FID)
39189	Line 66 is overloaded (366.96 MW)and an alarm has been generated (FID)
39211	RTU has processed an alarm from Line 66 and sent it to MTU (RTU)
39312	Operator recognize the alarm for Line66 (MTU)
39314	Operator response the problem correctly and distributing algorithm will be taken for line 66 (MTU)
39337	command has been processed by operator sucessfully, redistribution command has been sent out (RTU)
43200	Test Summary ASSAI is : **0.9998** Total Numbers of Overloads: **5**

Table A-IV 32 Summary of FID FRH normal tests

Test Number	**The number of overload alarms**	**The number of affected SUC components**	**The number of affected SCADA components**	**ASSAI / Vulnerability**
1	3	2	0	0.9998
2	3	2	0	0.9998
3	5	3	0	0.9998
4	4	2	0	0.9998
5	3	2	0	0.9998
6	4	3	0	0.9998
7	4	3	0	0.9996
8	4	3	0	0.9998
9	4	3	0	0.9997
10	3	2	0	0.9998
Average				
	3.7	**2.5**	**0**	**0.99977**

Table A-IV 33 Summary of FID FRH worse-case tests

Test Number	The number of overload alarms	The number of affected SUC components	The number of affected SCADA components	ASSAI / Vulnerability
1	44	10	3	0.9281
2	49	10	3	0.9089
3	43	7	2	0.9507
4	49	10	4	0.9459
5	51	9	3	0.9363
6	48	9	3	0.9316
7	53	10	3	0.933
8	51	10	3	0.9312
9	48	9	3	0.9318
10	46	8	3	0.944
Average				
	48	**9.2**	**3**	**0.9358**

Table A-IV 34 Observed Results from one of RTU FRF normal tests

Stamped Time	Events
40551	Line 127 is overloaded (373.41 MW)and an alarm has been generated (FID)
40563	RTU has processed an alarm from Line 127 and sent it to MTU (RTU)
40655	..Operator fails to make action for Line 127 (MTU)
43237	FCD device has been triggered to disconnect line 127 (FCD)
43238	**********RTU device: RTU-034 is in FRF mode ********** (RTU)
43238	*********Warning: RTU device RTU-034 lost connection to field devices********** (RTU)
44135	Line 66 is overloaded (565.74 MW)and an alarm has been generated (FID)
44136	Warning : An alarm has been lost due to wire cut between RTU and Field device (FID)
44135	Line 194 is overloaded (-778.02 MW)and an alarm has been generated (FID)
44136	Warning : An alarm has been lost due to wire cut between RTU and Field device (FID)
46132	******* circuit breaker is not able to be closed to connect 127 due to RTU failure (FCD)
49712	******* circuit breaker is not able to be closed to connect 127 due to RTU failure (FCD)
140581	******* circuit breaker is not able to be closed to connect 127 due to RTU failure (FCD)
143275	RTU connection lost to field devices is solved

Stamped Time	Events
143275	**********RTU device: RTU-034 is out of FRF mode ********** (RTU)
144156	overload problem solved and circuit breaker will be closed to connect 127 (FCD)
144156	127 has received the command from RTU for connecting the line (FCD)
213355	Line 127 is overloaded (373.82 MW)and an alarm has been generated (FID)
213356	127 has been detected and related FCD device gets noticed (FCD)
213375	RTU has processed an alarm from Line 127 and sent it to MTU (RTU)
213442	Operator recognize the alarm for Line127 (MTU)
213442	Operator response the problem correctly and distributing algorithm will be taken for line 127 (MTU)
213462	command has been processed by operator sucessfully, redistribution command has been sent out (RTU)
432001	Test Summary ASSAI is : **0.9943** Total Numbers of Overloads: **3**

Table A-IV 35 Summary of RTU FRF normal tests

Test Number	**The number of overload alarms**	**The number of affected SUC components**	**The number of affected SCADA components**	**ASSAI / Vulnerability**
1	2	2	0	0.9962
2	2	2	0	0.9982
3	3	3	0	0.9976
4	3	3	0	0.9943
5	2	2	0	0.9988
6	2	2	0	0.9968
7	2	2	0	0.9988
8	3	2	0	0.9995
9	2	2	0	0.9926
10	3	3	0	0.9998
Average				
	2.4	**2**	**0**	**0.9970**

Table A-IV 36 Observed Results from one of RTU FRF worse-case tests

Stamped Time	Events
41476	Line 127 is overloaded (373.27 MW)and an alarm has been generated (FID)
41487	RTU has processed an alarm from Line 127 and sent it to MTU (RTU)
41584	..Operator fails to make action for Line 127 (MTU)
44134.	FCD device has been triggered to disconnect line 127 (FCD)
44136	**********RTU device: RTU-034 is in FRF mode ********** (RTU)
44136	*********Warning: RTU device RTU-034 lost connection to field devices********** (RTU)
44362	Line 194 is overloaded (-777.96 MW)and an alarm has been generated (FID)
44363	Warning : An alarm has been lost due to wire cut between RTU and Field device (FID)
44362	Line 66 is overloaded (564.15 MW)and an alarm has been generated (FID)
44363	Warning : An alarm has been lost due to wire cut between RTU and Field device (FID)
47007	******* circuit breaker is not able to be closed to connect 127 due to RTU failure (FCD)
61204	******* circuit breaker is not able to be closed to connect 127 due to RTU failure (FCD)
63211	RTU connection lost to field devices is solved
63211	**********RTU device: RTU-034 is out of FRF mode ********** (RTU)
64145	overload problem solved and circuit breaker will be closed to connect 127 (FCD)
64145	127 has received the command from RTU for connecting the line (FCD)
	Test Summary ASSAI is : **0.9953** Total Numbers of Overload alarms: **1**

Table A-IV 37 Summary of RTU FRF worse case tests

Test Number	The number of overload alarms	The number of affected SUC components	The number of affected SCADA components	ASSAI / Vulnerability
1	2	2	0	0.9969
2	1	2	0	0.9976
3	1	2	0	0.9858
4	1	2	0	0.9905
5	1	2	0	0.9984
6	1	2	0	0.991
7	1	2	0	0.9953
8	1	2	0	0.9937
9	1	2	0	0.9929
10	1	2	0	0.9950

Average				
	1	**2**	**0**	**0.9940**

Table A-IV 38 Observed Results from one of RTU FRW normal tests

Stamped Time	Events
40570	Line 127 is overloaded (374.14 MW)and an alarm has been generated (FID)
40577	RTU has processed an alarm from Line 127 and sent it to MTU (RTU)
40661	..Operator fails to make action for Line 127 (MTU)
43269	FCD device has been triggered to disconnect line 127 (FCD)
43270	**********RTU device: RTU-034 is in FRW mode ********** (RTU)
43270	Warning: RTU hardware fails (RTU)
44159	Line 66 is overloaded (564.31 MW)and an alarm has been generated (FID)
44161	Line 194 is overloaded (-778.13 MW)and an alarm has been generated (FID)
44165	********Warning : An alarm has been lost due to hardware failure ******(RTU)
44167	********Warning : An alarm has been lost due to hardware failure ******(RTU)
46845	******* circuit breaker is not able to be closed to connect 127 due to RTU failure (FCD)
47902	RTU hardware failure solved
47902	**********RTU device: RTU-034 is out of FRW mode ********** (RTU)
50435	overload problem solved and circuit breaker will be closed to connect 127 (FCD)
50435	127 has received the command from RTU for connecting the line (FCD)
129831	Line 127 is overloaded (375.69 MW)and an alarm has been generated (FID)
129848	RTU has processed an alarm from Line 127 and sent it to MTU (RTU)
130575	Operator recognize the alarm for Line127 (MTU)
130577	Operator response the problem correctly and distributing algorithm will be taken for line 127 (MTU)
130585	command has been processed by operator sucessfully, redistribution command has been sent out (RTU)
	Test Summary ASSAI is : **0.9996** Total Numbers of Overloads: **2**

Table A-IV 39 Summary of RTU FRW normal tests

Test Number	The number of overload alarms	The number of affected SUC components	The number of affected SCADA components	ASSAI / Vulnerability
1	2	2	0	0.9996
2	2	2	0	0.9996
3	2	2	0	0.9996

4	3	3	0	0.9996
5	2	2	0	0.9998
6	3	3	0	0.9995
7	3	2	0	0.9998
8	2	3	0	0.9996
9	2	3	0	0.9992
10	4	3	0	0.9998
Average				
	2.1	**2.5**	**0**	**0.9996**

Table A-IV 40 Observed Results from one of RTU FRW worse-case tests

Stamped Time	Events
44180	Line 127 is overloaded (374.95 MW)and an alarm has been generated (FID)
44199	RTU has processed an alarm from Line 127 and sent it to MTU (RTU)
44268	..Operator fails to make action for Line 127 (MTU)
46110	FCD device has been triggered to disconnect line 127 (FCD)
46112	**********RTU device: RTU-034 is in FRW mode ********** (RTU)
46112	Warning: RTU hardware fails (RTU)
46999	Line 194 is overloaded (-774.65 MW)and an alarm has been generated (FID)
46999	Line 66 is overloaded (552.32 MW)and an alarm has been generated (FID)
47004	********Warning : An alarm has been lost due to hardware failure ******(RTU)
47005	********Warning : An alarm has been lost due to hardware failure ******(RTU)
49650	******* circuit breaker is not able to be closed to connect 127 due to RTU failure (FCD)
50643	RTU hardware failure solved
50643	**********RTU device: RTU-034 is out of FRW mode ********** (RTU)
53217	overload problem solved and circuit breaker will be closed to connect 127 (FCD)
53217	127 has received the command from RTU for connecting the line (FCD)
	Test Summary ASSAI is : 0.9978 Total Numbers of Overloads: 1

Table A-IV 41 Results from all RTU FRW worse-case tests

Test Number	The number of overload alarms	The number of affected SUC components	The number of affected SCADA components	ASSAI / Vulnerability
1	1	2	0	0.9988

2	1	2	0	0.997
3	1	2	0	0.998
4	1	2	0	0.9988
5	1	2	0	0.9978
6	1	2	0	0.9957
7	1	2	0	0.9988
8	1	2	0	0.9983
9	1	2	0	0.9988
10	1	2	0	0.9975
Average				
	1	**2**	**0**	**0.9980**

Table A-IV 42 Observed Results from one of RTU FRC normal tests

Stamped Time	Events
40535	Line 127 is overloaded (373.51 MW)and an alarm has been generated (FID)
40535	**********RTU device: RTU-034 is in FRC mode ********** (RTU)
40548	RTU has processed an alarm from Line 127 and sent it to MTU (RTU)
40632	Operator recognize the alarm for Line127 (MTU)
40634	Operator response the problem correctly and distributing algorithm will be taken for line 127 (MTU)
40651	**********Communication error from MTU to RTU is assumed**********
40652	RTU fails to interpret command for Line127from MTU due to data lost (RTU)
41532	**********RTU device: RTU-034 is out of FRC mode ********** (RTU)
42484	FCD device has been triggered to disconnect line 127 (FCD)
43346	Line 66 is overloaded (564.02 MW)and an alarm has been generated (FID)
43360	RTU has processed an alarm from Line 66 and sent it to MTU (RTU)
43406	Line 194 is overloaded (-779.05 MW)and an alarm has been generated (FID)
43417	RTU has processed an alarm from Line 194 and sent it to MTU (RTU)
43425	Operator recognize the alarm for Line66 (MTU)
43427	Operator response the problem correctly and distributing algorithm will be taken for line 66 (MTU)
44104	command has been processed by operator sucessfully, redistribution command has been sent out (RTU)
44212	Operator recognize the alarm for Line194 (MTU)
44214	Operator response the problem correctly and distributing algorithm will be taken for line 194 (MTU)
44228	command has been processed by operator sucessfully, redistribution command has been sent

Stamped Time	Events
	out (RTU)
44724	overload problem solved and circuit breaker will be closed to connect 127 (FCD)
44724	127 has received the command from RTU for connecting the line (FCD)
45426	Line 66 is overloaded (366.64 MW)and an alarm has been generated (FID)
45427.	66 has been detected and related FCD device gets noticed (FCD)
45455	RTU has processed an alarm from Line 66 and sent it to MTU (RTU)
45522	Operator recognize the alarm for Line66 (MTU)
45525	Operator response the problem correctly and distributing algorithm will be taken for line 66 (MTU)
45551	command has been processed by operator sucessfully, redistribution command has been sent out (RTU)
	Test Summary ASSAI is : **0.9998** Total Numbers of Overloads: **5**

Table A-IV 43 Results of all RTU FRC normal tests

Test Number	**The number of overload alarms**	**The number of affected SUC components**	**The number of affected SCADA components**	**ASSAI / Vulnerability**
1	5	3	0	0.9998
2	4	3	0	0.9998
3	3	2	0	0.9998
4	3	2	0	0.9998
5	5	4	0	0.9998
6	3	2	0	0.9998
7	3	2	0	0.9998
8	5	4	0	0.9998
9	3	2	0	0.9998
10	3	2	0	0.9998
Average				
	3.7	**2.6**	**0**	**0.9998**

Experiment III

Table A-IV 44 Summary of the Test No.1

#	Number of lost alarms	Number of affected SUC components	Number of affected SCADA components	ASSAI / Vulnerability	Degree of impact
1	0	20	1, RTU 21	0.9905	30 Strong
2	0	17	1, RTU 21	0.9916	30 Strong
3	0	18	2, RTU 124/21	0.9913	34 Strong
4	0	19	1, RTU 21	0.9899	34 Strong
5	0	18	2, RTU 21 / 124	0.9920	34 Strong
6	0	19	1, RTU 21	0.9905	30 Strong
7	0	18	2, RTU 21/124	0.9908	34 Strong
8	0	19	2, RTU 21/ 124	0.9910	34 Strong
9	0	19	2, RTU 21/ 124	0.9911	34 Strong
10	0	18	2, RTU 21/124	0.9910	34 Strong
Average					
	0	18	2	0.9910	34 Strong

Table A-IV 45 Summary of the Test No.2

#	Number of lost alarms	Number of affected SUC components	Number of affected SCADA components	ASSAI / Vulnerability	Degree of impact
1	0	0	0	0.9996	14 Weak
2	0	0	0	0.9996	14 Weak
3	0	0	0	0.9996	14 Weak
4	0	0	0	0.9996	14 Weak
5	0	0	0	0.9996	14 Weak
6	0	0	0	0.9996	14 Weak

7	0	0	0	0.9996	14 Weak
8	0	0	0	0.9996	14 Weak
9	0	0	0	0.9996	14 Weak
10	0	0	0	0.9996	14 Weak
Average					
	0	0	0	0.9996	14 Weak

Table A-IV 46 Summary of Test No.3

#	Number of lost alarms	Number of affected SUC components	Number of affected SCADA components	ASSAI / Vulnerability	Degree of impact
1	1, Line 200	3	0	0.9952	20 Middle
2	1,Line 200	3	0	0.9953	20 Middle
3	1, Line 200	3	0	0.9953	20 Middle
4	1,Line 200	3	0	0.9953	20 Middle
5	1,Line 200	3	0	0.9953	20 Middle
6	1,Line 200	3	0	0.9953	20 Middle
7	1,Line 200	3	0	0.9953	20 Middle
8	1,Line 200	3	0	0.9952	20 Middle
9	1,Line 200	3	0	0.9953	20 Middle
10	1,Line 200	3	0	0.9952	20Middle
Average					
	1	2	0	0.9953	20 Middle

Table A-IV 47 Summary of Test No.4

#	Number of lost alarms	Number of affected SUC components	Number of affected SCADA components	ASSAI / Vulnerability	Degree of impact
1	0	0	0	0.9962	18 weak
2	0	0	0	0.9962	18 weak

3	0	0	0	0.9962	18 weak
4	0	0	0	0.9962	18 weak
5	0	0	0	0.9962	18 weak
6	0	0	0	0.9962	18 weak
7	0	0	0	0.9962	18 weak
8	0	0	0	0.9962	18 weak
9	0	0	0	0.9962	18 weak
10	0	0	0	0.9962	18 weak
Average					
	1	2	0	0.9962	18 Weak

Table A-IV 48 Summary of Test No.5

#	Number of lost alarms	Number of affected SUC components	Number of affected SCADA components	ASSAI /Vulnerability	Degree of impact
1	0	28	4, RTU 114/124/37/139	0.9775	42 Very Strong
2	0	27	4, RTU 21/114/18/17	0.9785	42 Very Strong
3	0	27	5,RTU 21/114/17/18/128	0.9783	42 Very Strong
4	0	29	3, RTU 114/124/139	0.9731	38 Strong
5	0	28	4,RTU 21/114/17/18	0.9789	42 Very Strong
6	0	28	4,RTU 21/114/17/18	0.9777	42 Very Strong
7	0	30	4,RTU 21/128/16/20	0.9740	42 Very Strong
8	0	26	4, RTU 21/114/17/18	0.9800	42 Very Strong
9	0	29	5,RTU 21/114/17/18/128	0.9793	42 Very Strong
10	0	28	4, RTU 21/114/17/18	0.9784	42 Very Strong
Average					
	0	28	4	0.9776	42 Very Strong

Table A-IV 49 Summary of Test No.6

#	Number of lost alarms	Number of affected SUC components	Number of affected SCADA components	ASSAI / Vulnerability	Degree of impact
1	0	0	0	0.9991	14 Weak
2	0	0	0	0.9992	14 Weak
3	0	0	0	0.9991	14 Weak
4	0	0	0	0.9991	14 Weak
5	0	0	0	0.9991	14 Weak
6	0	0	0	0.9992	14 Weak
7	0	0	0	0.9991	14 Weak
8	0	0	0	0.9991	14 Weak
9	0	0	0	0.9991	14 Weak
10	0	0	0	0.9992	14 Weak
Average					
	0	0	0	0.9991	14 Weak

Table A-IV 50 Summary of Test No.7

#	Number of lost alarms	Number of affected SUC components	Number of affected SCADA components	ASSAI / Vulnerability	Degree of impact
1	2, 200/117	10	0	0.9888	28 Middle
2	2, 200/117	10	0	0.9890	28 Middle
3	2, 200/117	10	0	0.9890	28 Middle
4	2, 200/117	10	0	0.9890	28 Middle
5	2, 200/117	10	0	0.9889	28 Middle
6	2, 200/117	10	0	0.9890	28 Middle
7	2, 200/117	10	0	0.9889	28 Middle
8	2, 200/117	10	0	0.9888	28 Middle
9	2, 200/117	10	0	0.9888	28 Middle

10	2, 200/117	10	0	0.9888	28 Middle
Average					
	2	10	0	0.9889	28 Middle

Table A-IV 51 Summary of Test No.8

#	Number of lost alarms	Number of affected SUC components	Number of affected SCADA components	ASSAI / Vulnerability	Degree of impact
1	0	0	0	0.9923	18 Weak
2	0	0	0	0.9923	18 Weak
3	0	0	0	0.9923	18 Weak
4	0	0	0	0.9923	18 Weak
5	0	0	0	0.9923	18 Weak
6	0	0	0	0.9923	18 Weak
7	0	0	0	0.9923	18 Weak
8	0	0	0	0.9923	18 Weak
9	0	0	0	0.9923	18 Weak
10	0	0	0	0.9923	18 Weak
Average					
	0	0	0	0.9923	18 Weak

References

[1] Erster Bericht an den Bundesrat zum Schutz kritischer Infrastrukturen. Bevölkerungsschutz Bf, editor.2007.
[2] Zio E & Kröger W. IEEE Reliability Society 2009 Annual Technology Report: VULNERABILITY ASSESSMENT OF CRITICAL INFRASTRUCTURES.2009.
[3] COMMISSION OF THE EUROPEAN COMMUNITIES. Critical Infrastructure Protection in the fight against terrorism. COM(2004) 702 final. Brussels. 2004.
[4] DHS US. National Infrastructure Protection Plan (NIPP): Partnering to enhance protection and resiliency. p. 188. 2009.
[5] FOCP. The Swiss Programme on Critical Infrastructure Protection. In: FOCP SFOfCP, editor. Bern, Switzerland. p. 4. 2010.
[6] Eusgeld I, Kröger W, Sansavini G, Schläpfer M and Zio E. The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures. Reliability Engineering and System Safety.94: p.954-963.2009.
[7] Kröger W. Critical infrastructure at risk: A Need For A New Conceptual Approach and Extended Analytical Tools. Reliability Engineering and System Safety. 93:1781-1787. 2008.
[8] Jamshidi M. Large-Scale Systems - Modeling and Control. New York, NY: North-Holland Publishing Company; 1983.
[9] DeLaurentis D. Role of Humans in Complexity of a System-of-Systems V.G. Duffy (Ed.): Digital Human Modeling. Berlin: Springer-Verlag.2007.
[10] Kotov V. Systems of Systems as Communicating Structures. p. 1-15.1997.
[11] Amrine JM. The Command of Space: A National Vision for American Prosperity and Security. Base USMAF.2000.
[12] Railroad Accident Brief: Accident (DCA-01-MR-004). NTSB report. 2004.
[13] Report on the blackout in Italy on 28 September 2003. SFOE Report. 2003.
[14] Kröger W, Nan C, Trantopoulos K, Zhou L and Eusgeld I. Report: Interdependencies. Lab for Safety Analysis, ETH Zurich; p. 56. 2009.
[15] Kerry M, Kelk G, Etkin D, Burton I and Kalhok S. Glazed Over: Canada Copes with the Ice Storm of 1998. Environment: Science and Policy for Sustainable Development. 41:p. 6-11. 1999.
[16] The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States. p. 585. 2004.
[17] Report K. A FAILURE OF INITIATIVE: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina. Washington. 2006.
[18] Rinaldi SM, Peerenboom JP and Kelly TK. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Magazine;21:p.11-25. 2001.
[19] U.S - Canada Power System Outage Task Force. Final Report on the August 14,2003 Blackout in the United States and Canada : Causes and Recommendations. 2004.
[20] Christansson H & Luiijf E. Creating a European SCADA Security Testbed. IFIP International Federation for Information Processing. Boston: Springer; p. 237-247. 2007.
[21] Terje A. On how to define, understand and describe risk. Reliability Engineering and System Safety. 95:p. 623-31.2010.

[22] Eusgeld I & Kröger W. Comparative Evaluation of Modeling and Simulation Technique for Interdependent Critical Infrastructures. Proceedings of the Ninth International Probabilistic Safety Assessment Conference. Hong Kong. p. 49-57.2008.
[23] Weichselgartner J. Disaster mitigation: the concept of vulnerability revisited. Disaster Prevention and Management. 10:p.85-95.2001.
[24] Haimes YY. On the Definition of Vulnerabilities in Measuring Risks to Infrastructures. Risk Analysis. 26:p. 293-296.2006.
[25] Kröger W & Zio E. Vulnerable Systems: Springer;2011.
[26] Johansson J, Jonsson H and Johansson H. Analysing the vulnerability of electric distribution systems: a step towards incorporating the societal consequences of disruptions. International Journal of Emergency Management. 4:p.4-17.2007.
[27] Bouchon S. The Vulnerability of Interdependent Critical Infrastructures Systems: Epistemological and Conceptual State-of-the-Art. EUR-report: Joint Research Centre; 2006.
[28] Schläpfer M, Dietz S and Kaegi M. Stress Induced Degradation Dynamics in Complex Networks. Proceedings of 2008 First International Conference on Infrastructure Systems and Services: Building Networks for a Brighter Future (INFRA 2008). p. 1-5.2008.
[29] Bloomfield R, Chozos N and Nobles P. Infrastructure interdependency analysis: Introductory research review.2009.
[30] Eusgeld I & Kröger W. Towards a Framework for Vulnerability Analysis of Interconnected Infrastructures. Proceedings of 9th International Probabilistic Safety Assessment & Management Conference (PSAM 09). Hong Kong.2008.
[31] Boyer SA. SCADA supervisory control and data acquisition. 3rd ed. Research Triangle Park: ISA; 2004.
[32] Richardson BT & Chavez L. National SCADA Test Bed Consequence Modeling Tool. Sandia National Laboratories; p. 23. 2008.
[33] Pfander JP, Baumann R and Amitirigala R. New SCADA/EMS concept of the Swiss Federal Railways. Proceedings of Fourth International Conference on Power System Control and Management. p. 231-239.1996.
[34] Kaneda K, Tamura S, Fujiyama N, Arata Y and Ito H. IEC61850 based Substation Automation System. Proceedings of Power System Technology and IEEE Power India Conference. p. 1-8. 2008.
[35] Giani A, Karsai G, Roosta T, Shah A, Sinopoli B and Wiley J. A testbed for secure and robust SCADA systems. SIGBED Rev.5:1-4.2008.
[36] Stouffer K, Falco J and Scarfone K. Guide to Industrial Control Systems (ICS) Security. National Institute of Standards and Technology;2008.
[37] Igure VM, Laughter SA and Williams RD. Security Issues in SCADA Networks. Computers and Security. 25:p.498-506.2006.
[38] Venkatraman A. SCADA Systems Security.2004.
[39] Balducelli C, Bologna S, Lavalle L and Vicoli G. Safeguarding information intensive critical infrastructures against novel types of emerging failures. Reliability Engineering and System Safety. 92:p.1218-1229.2007.
[40] Nai Fovino I, Carcano A, Masera M and Trombetta A. An experimental investigation of malware attacks on SCADA systems. International Journal of Critical Infrastructure Protection.2:p.139-145.2009.
[41] SWISSGRID: Die Nationale Netzgesellschaft.2007.
[42] Stuxnet: rumours increase, infections spread. Network Security. p.1-2.2010.

[43] Johnson RE. Survey of SCADA security challenges and potential attack vectors. Internet Technology and Secured Transactions (ICITST) 2010. p. 5. 2010.
[44] Slay J & Miller M. LESSONS LEARNED FROM THE MAROOCHY WATER BREACH. IFIP International Federation for Information Processing.253:p.73–82.2008.
[45] Zhou L. Forcal Report: Vulnerability Analysis of Industrial Control Systems - Part C: Good practices, Important lessons.BABS Report for FOCP. LSA ETH Zurich; 2011.
[46] Xin YZ. Cyber Security Assessment of Power System. 2004.
[47] Stamp J, Campbell P, DePoy J, Dilinger J and Young W. Sustainable security for infrastructure SCADA. Sandia National Laboratories. 2003.
[48] Zhou L. Forcal Report: Vulnerability Analysis of Industrial Control Systems - Part B: Statistics and analysis of industrial security incidents, Challenges of ICS security research. BABS Report for FOCP. LSA ETH Zurich; 2011.
[49] Zhou L, Kröger W, Probst P and Mock R. Workshop Report: Third Workshop on Critical Information and Communication Networks: Security and Vulnerability of Industrial Control Systems. BABS Report for FOCP. LSA ETH Zurich; 2010.
[50] Brand K-P, Lohmann V and Wimmer W. Substation automation handbook: Utility Automation Consulting Lohmann; 2003.
[51] Northcote-Green J and Wilson R. Control and Automation of Electrical Power Distribution Systems: CRC Press : Taylor & Francis Group; 2006.
[52] Bailey D and Wright E. Practical SCADA for industry Elektronische Daten. Oxford: Newnes; 2003.
[53] Swissgrid annual report 2008. Laufenburg, Switzerland. p. 66. 2009.
[54] Griot C. Modelling and simulation for critical infrastructure interdependency assessment: a meta-review for model characterisation. International Journal of Critical Infrastructure. 6(4): p.363-379. 2010.
[55] Pederson P, Dudenhoeffer D, Hartly S and Permann M. Critical Infrastructure Interdependency Modeling: A Survey of U.S and International Research. Idaho National Laboratory; 2006.
[56] Johansson J & Hassel H. An approach for modelling interdependent infrastructures in the context of vulnerability analysis. Reliability Engineering and System Safety.95:p.1335-1344.2010.
[57] Zimmerman R. Decision-making and the vulnerability of interdependent critical infrastructure. Proceedings of 2004 IEEE International Conference on Systems, Man and Cybernetics. 5:p. 4059-4063.2004.
[58] IRGC. Policy Brief: Managing and reducing social vulnerabilities from coupled critical infrastructures. Geneva, Switzerland: IRGC; 2007.
[59] Rahman HA, Beznosov K and Marti JR. Identification of sources of failures and their propagation in critical infrastructures from 12 years of public failure reports. International Journal of Critical Infrastructures.5:p.220-244.2009.
[60] Zimmerman R & Restrepo CE. The next step: quantifying infrastructure interdependencies to improve security. International Journal of Critical Infrastructures. 2: p.215-30.2006.
[61] Steen MV. Graph Theory and Complex Networks: An Introduction. 1 ed: Maarten van Steen; 2010.
[62] Ouyang M, Hong L, Mao Z-J, Yu M-H and Qi F. A methodological approach to analyze vulnerability of interdependent infrastructures. Journal of Simulation Modelling Practice and Theory.17:p. 817-828.2009.

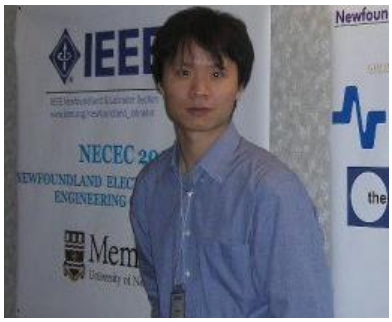
[63] Apostolakis GE & Lemon DM. A Screening Methodology for the Identification and Ranking of Infrastructure Vulnerabilities Due to Terrorism. Journal of Risk Analysis. 25:p.361-376.2005.
[64] Dobson I, Carreras BA, Lynch VE and Newman DE. Complex Systems Analysis of Series of Blackouts: Cascading Failure, Criticality, and Self-organization. Bulk Power System Dynamics and Control - VI. 2004.
[65] Bompard E, Napoli R and Xue F. Analysis of structural vulnerabilities in power transmission grids. International Journal of Critical Infrastructure Protection.2:p.5-12.2009.
[66] Solé RV, Rosas-Casals M, Corominas-Murtra B and Valverde S. Robustness of the European power grids under intentional attack. Physical Review E. 2008.
[67] Leontief WW. Input-output economics. 2nd Ed ed: Oxford University Press, New York; 1986.
[68] Setola R, De Porcellinis S and Sforna M. Critical infrastructure dependency assessment using the input-output inoperability model. International Journal of Critical Infrastructure Protection.2:p.170-178.2009.
[69] Haimes YY, Horowitz BM, Lambert JH, Santos JR, Lian C and Crowther KG. Inoperability Input-Output Model for Interdependent Infrastructure Sectors. I: Theory and Methodology. Journal of Infrastructure Systems.11:p.67-79.2005.
[70] Haimes YY, Horowitz BM, Lambert JH, Santos J, Crowther K and Lian C. Inoperability Input-Output Model for Interdependent Infrastructure Sectors. II: Case Studies. Journal of Infrastructure Systems.11:p.80-92.2005.
[71] Aung Z & Watanabe KA. Framework for Modeling Interdependencies in Japan's Critical Infrastructures. In: Palmer C, Shenoi S, editors. Critical Infrastructure Protection III: Springer Boston;p. 243-257.2009.
[72] Sultana S and Chen Z. Modeling infrastructure interdependency among floodplain infrastructures with extended Petri-Net. Proceedings of the 16th IASTED International Conference on Applied Simulation and Modelling. Palma de Mallorca, Spain: ACTA Press; p. 104-109. 2007.
[73] Klein R, Rome E, Beyel C, Linnemann R and Reinhardt W. Information Modelling and Simulation in large interdependent Critical Infrastructures in IRRIIS.IRRIS Report.2007.
[74] S.Buschi. MIA Report Version 4. 2010.
[75] Schläpfer M, Kessler T and Kröger W. Reliability Analysis of Electric Power Systems Using an Object-oriented Hybrid Modeling Approach. Proceedings of the 16th power systems computation conference. Glasgow. p. 1-7. 2008.
[76] Panzieri S, Setola R and Ulivi G. An Agent Based Simulator for Critical Interdependent Infrastructures. Securing Critical Infrastructures.Grenoble.2004.
[77] Cardellini V, Casalicchio E and Galli E. Agent-based modeling of interdependencies in critical infrastructures through UML. Proceedings of the 2007 spring simulation multiconference:Volume 2.Norfolk, Virginia: Society for Computer Simulation International; p. 119-126. 2007.
[78] Casalicchio E, Galli E and Tucci S. Federated Agent-based Modeling and Simulation Approach to Study Interdependencies in IT Critical Infrastructures. Proceedings of the 11th IEEE International Symposium on Distributed Simulation and Real-Time Applications. p. 182-189.2007.
[79] Eusgeld I & Nan C.Creating a simulation environment for critical infrastructure interdependencies study. Proceedings of IEEE International Conference on Industrial Engineering and Engineering Management. p.2104-2108.2009.

[80] INTERNATIONAL COMMON-CAUSE FAILURE DATA EXCHANGE ICDE GENERAL CODING GUIDELINES - TECHNICAL NOTE. In: INSTALLATIONS NEACOTSON, editor.2004.
[81] Gentile M & Summers E. Random, Systematic, and Common Cause Failure: How Do You Manage Them ? Journal of Process Safety Progress.25(4):p.331-337.2006.
[82] Nan C, Kröger W and Eusgeld I. Focal Report: Study of Common Cause Failures of SCADA System at Substation Level. BABS Report for FOCP. LSA ETH Zurich. 2011.
[83] Caretta Cartozo C. Complex networks: from biological applications to exact theoretical solutions: EPFL Doctoral Thesis No.4462.2009.
[84] Gallos LK, Cohen R, Argyrakis P, Bunde A and Havlin S. Stability and Topology of Scale-Free Networks under Attack and Defense Strategies. Physical Review Letters. 94(18):p. 188701-1-188701-4.2005.
[85] Volkanovski A. Focal Report: Five Parameter Model. BABS Report for FOCP. LSA ETH Zurich. 2010.
[86] Eusgeld I, Nan C and Dietz S. "System-of-systems" Approach for Interdependent Critical Infrastructures. Reliability Engineering and System Safety.96:p.679-686.2011.
[87] DoD. U.S. Department of Defense Directive : Interoperability and Supportability of Information Technology (IT) and National Security Systems (4603.05).2007.
[88] Nai Fovino I, Guidi L, Masera M and Stefanini A. Cyber security assessment of a power plant. Electric Power Systems Research.81:p.518-526.2011.
[89] Lachs WR. Transmission-line overloads: real-time control. Generation, Transmission and Distribution, IEE Proceedings C.134:p.342-347.1987.
[90] Swain AD. Comparative evaluation of methods for human reliability analysis. Institute for Reactor Safety;1989.
[91] Konstandinidou M, Nivolianitou Z, Kiranoudis C and Markatos N. A fuzzy modeling application of CREAM methodology for human reliability analysis. Reliability Engineering and System Safety.91:p.706-716.2006.
[92] Kyriakidis M. Focal Report: A study regarding human reliability within power system control rooms. BABS Report for FOCP. LSA ETH Zurich; 2009.
[93] Ingenieure VD. Methods for quantitative assessment of human reliability.2003.
[94] Kyriakidis M. A scoping method for human performance integrity and reliability assessment in process industries. ETH Zurich.2009.
[95] Forester J, Kolackowski A, Cooper S, Bley D and Lois E. ATHEANA User's Guide: Final Report. U.S.Nuclear Regulatory Research.2007.
[96] Hollnagel E. Cognitive Reliability and Error Analysis Method CREAM: Elsevier; 1998.
[97] He X, Wang Y, Shen Z and Huang X. A simplified CREAM prospective quantification process and its application. Reliability Engineering and System Safety.93:p.298-306. 2008.
[98] Zadeh LA. Fuzzy logic. Journal of IEEE Compute.21:p.83-93.1998.
[99] Marcellus RL. Evaluation of a nonstationary policy for statistical process control. Proceedings of the 6th Annual Industrial Engineering Research Conference.p.89-94.1997.
[100] Harris CJ, Hong X and Gan Q. Adaptive Modeling Estimation and Fusion from Data. New York: Springer; 2002.
[101] Lachs WR. Transmission-line overloads: real-time control IEE Proceedings.134 (C):p.342-347.1987
[102] El-Shal SM & Morris AS. A fuzzy expert system for fault detection in statistical process control of industrial processes. IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews.;30:p.281-289.2000.

[103] Gorbil G & Gelenbe E. Design of a Mobile Agent-Based Adaptive Communication Middleware for Federations of Critical Infrastructure Simulations.Proceedings of CRITIS 2009. 2009.
[104] Lecture notes from California State University Chico. 2003.
[105] DoD. Department of Defense (DOD): High Level Architecture Run-Time Interface Programmers Guide.2000.
[106] DoD. Department of Defense (DOD):High Level Architecture Interface Specification. 1998.
[107] IEEE. IEEE Standard for Modeling and Simulation High Level Architecture (HLA) - Framework and Rules. IEEE Std 1516-2000.p.i-22.2000.
[108] Dahmann JS, Fujimoto RM and Weatherly RM. The Department of Defense High Level Architecture.Proceedings of the 29th conference on Winter simulation.IEEE Computer Society; p.142-149.1997.
[109] Hopkinson KM, Giovanini R and Wang XR. EPOCHS: Integrated Commercial Off-the-Shelf Software For Agent-based Electric Power and Communication Simulation. Proceedings of the 2003 Winter Simulation Conference.p.1158-1166.2003.
[110] Rehtanz C. Autonomous systems and intelligent agents in power system control and operation: Springer; 2003.
[111] Kim IK, Ma YB and Lee JS. Adaptive Quantization-based Communication Data Management for High-Performance Geo-computation in Grid Computing. Proceedings Fifth International Conference on Grid and Cooperative Computing Workshops. p.470-476.2006.
[112] Lees M, Logan B and Theodoropoulos G. Distributed Simulation of Agent-based Systems with HLA. ACM Transactions on Modeling and Computer Simulation.17(3).p.1-11.2007.
[113] Zhao Z, Albada DV and Sloot P. Agent-Based Flow Control for HLA Components. Simulation.81:p.487-501.2005.
[114] Beeker ER & Page EH. A Case Study of the Development and Use of a MANA-Based Federation for Studying U.S. Border Operations. Proceedings of the 38th Conference on Winter Simulation.p.841-847.2006.
[115] Lieshout FV, Cornelissen F and Neuteboom J. Simulating Rail Traffic Safety Systems using HLA 1516. Atos Origin Technical Automation.2008.
[116] Ezell BC. Infrastructure Vulnerability Assessment Model (I-VAM). Risk Analysis. 27:p.571-583.2007.
[117] Möller B, Löfstrand B, Lindqvist J, Backlund A, Waller B and Virding R. Gaming and HLA 1516 Interoperability within the Swedish Defense.2005 Fall Simulation Interoperability Workshop.2005.
[118] Zacharewicz G, Alix T, Vallespir B. Services Modeling and Distributed Simulation DEVS / HLA Supported. Proceedings of the Winter Simulation Conference (WSC) 2009. p. 3023-3035.2009.
[119] Duflos S, Diallo AA and Grand GL. An Overlay Simulator for Interdependent Critical Information Infrastructures.Proceedings of the 2nd International Conference on Dependability of Computer Systems: IEEE Computer Society. p. 27-34.2007.
[120] IEEE. IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems. IEEE Std 493-2007 (Revision of IEEE Std 493-1997)2007. p. 1-383.2007.

[121] Psounis K, Pan R, Prabhakar B and Wischik D.The scaling hypothesis: simplifying the prediction of network performance using scaled-down simulations. SIGCOMM Comput Commun Rev.33:p.35-40.2003.
[122] Wiedemann A. Development and application of a cellular system simulator for an evaluation of signaling performance and efficiency. Essen, Germany: The University of Duisburg-Essen; 2007.
[123] Chillarege R and Bowen NS. Understanding large system failures-a fault injection experiment. Proceedings of 19th International Symposium on Fault-Tolerant Computing. p.356-63.1989.
[124] Hsueh M-C, Tsai TK and Iyer RK. Fault Injection Techniques and Tools. University of Illinois at Urbana-Champaign; 1997.
[125] Fovino IN, Masera M, Guidi L and Carpi G. An experimental platform for assessing SCADA vulnerabilities and countermeasures in power plants. Proceedings of 3rd Conference on Human System Interactions (HSI).p. 679-686.2010.
[126] Queiroz C, Mahmood A, Jiankun H, Tari Z and Xinghuo Y. Building a SCADA Security Testbed. Proceedings of 09 Third International Conference on Network and System Security. p.357-364.2009.
[127] Hokstad P & Rausand M. Common Cause Failure Modeling: Status and Trends Handbook of Performability Engineering. In: Misra KB, editor.: Springer London; p.621-640.2008.
[128] Mohaghegh Z, Modarres M. Common Cause Failure Modelling Using Probabilistic Physics-Of-Failure (POF) Analysis: A Mechanistic Approach. Proceedings of the International Topical Meeting on Probabilistic Safety Assessment and Analysis (PSA 2011).USA. 2011.
[129] Fleming K. A reliability model for common mode failures in redundant safety systems. San Dieago, CA, U.S.A: General Atomic Company; 1975.
[130] Heising CD, Rasmussen NC and Mak CH. Common cause analysis : a review and extension of existing methods. Energy Laboratory, MIT; 1982.
[131] Bainbridge L. Building up behavioural complexity from a cognitive processing element: London: University College; 1993.

PERSONAL INFORMATION



Name: Cen Kelvin Nan
E-Mail: cennan@gmail.com
Citizenship: Canadian

EDUCATION

2009.03-Present **Dr.-Ing.** in Process and Mechanical Engineering
Thesis: `A Hybrid Modeling/Simulation Approach for Identifications of Vulnerabilities due to Interdependencies Between and Among Critical Infrastructures`
Department of Process and Mechanical Engineering, ETH Zürich, Switzerland

2005.09-2007.05 **M. Eng** in Oil and Gas Engineering
Thesis: ` Safety Instrumented System for Process Operation based on Real-time Monitoring`
Department of Engineering and Applied Science, Memorial University of Newfoundland, Canada

2002.01-2005.05 **B. Eng** in Computer Engineering
Department of Engineering and Applied Science, Memorial University of Newfoundland, Canada

PROFESSIONAL ACTIVITIES

2009.03-Present **Research Assistant** (ETH Fellow)
Main participant of Swiss Federal Office of Civil Protection project on `Risk analysis of Critical Infrastructures`.
Lab for Safety Analysis, ETH Zürich, Switzerland

2007.06-2008.12 **Field Engineer**
Supervised the operations of MWD (Measuring While Drilling) and LWD (logging while drilling) tools at well site. Provided expertise to directional drillers for the purpose of steering well to a target zone. Generated petro physical well log.
SCLUMBERGER D&M, Canada

2005.09-2007.05 **Research Assistant**
Main participant of a Vale Inco sponsored project ` Development of *Predicable Process Safety System `.*
Department of Engineering and Applied Science, Memorial University of Newfoundland, Canada

AWARDS

2009 -Present	ETH Zürich Research Grant
2008	ENG-1 Top of Class, Schlumberger
2007	Fellow of School of Graduate, Memorial University of Newfoundland
2005 - 2007	Resource Development Scholarship, Memorial University of Newfoundland

COMPUTER SKILLS

Operating System	WINDOWS, MAC OS and UNIX
Language	Sound knowledge of C++, Java, MATLAB, Visual Basic, SQL, C
Others	Word, Excel, Power Point, and etc

LANGUAGE SKILLS

Chinese	Mother tongue
English	Fluent in speaking, writing and listening
German	Beginner Level

MISCELLANEOUS

Affiliations	Student Member of the Institute of Electrical and Electronics Engineers (IEEE)
	Member of European Safety and Reliability Association (ESRA)

Interests	Culture, Novels, Traveling, Sports (Swimming, badminton, hiking, jogging), Classic music.

List of Publications

I. Book Chapters

[1] **Nan, C**. (2011) High Level Architecture, as part of Chapter 6, *Analysis of methods*, in Kröger, W and Zio, E (Eds.): Vulnerable Systems; Springer. ISBN 978-0-85729-654-2

II. Article in Newsletter

[1] **Nan, C**., and Kröger, W. (2011) Lessons learned from Adopting Distributed Simulation Approach for CI Interdependency Study, in ESRA (European Safety Reliability Association) Newsletter December, 2011.

III. Articles in Refereed Publications

[1] Eusgeld, I., **Nan, C**., and Dietz, S. (2011) "System-of-systems" Approach for Interdependent Critical Infrastructures. Journal of Reliability Engineering & System Safety. 96(6): 679-686. ISSN 09518320

[2] **Nan, C**., and Eusgeld, I. (2010) Adopting HLA Standard for Interdependency Study. Journal of Reliability Engineering & System Safety. 96(1): 149-159. ISSN: 0951-8320.

[3] **Nan**, **C**., Khan, F., and Iqbal, M.T. (2008) Real time Fault Diagnosis using Knowledge-based Expert System. Journal of Process Safety and Environmental Protection. 86(1): 55-71. ISSN 0957-5820.

IV. Published Contributions to Academic Conferences

[1] **Nan, C** and Eusgeld, I. (2011) Exploring Impacts of Single Failure Propagation between SCADA and SUC. In proceedings of IEEE International Conference on Industrial Engineering and Engineering Management (IEEM) 2011. 1564-1568. ISSN: 2157-3611.

[2] **Nan, C**., Kröger, W., and Probst, P. (2011) Exploring Critical Infrastructure Interdependency by Hybrid Simulation Approach. In proceedings of Annual European Safety and Reliability Conference (ESREL) 2011. 2483-2491. ISBN 978-0-415-68379-1.

[3] **Nan, C** and Kröger, W. (2011) A New Modeling Approach for Resolving CI Interdependency Issues. In proceedings of the 11th International Conference on Applications of Statistics and Probability in Civil Engineering (ICASP11). 1876-1884. ISBN 978-0-415-68379-1.

[4] Eusgeld, I and **Nan, C**. (2009) Creating a Simulation Environment for Critical Infrastructure Interdependencies Study. In proceedings of the IEEE International Conference on Industrial Engineering and Engineering Management (IEEM) 2009. 2104-2108. ISBN 978-1-4244-4869-2.

[5] **Nan**, **C**., Khan, F., and Iqbal, M.T. (2007) Abnormal Process Condition Prediction (Fault Diagnosis) using G2 Expert System. In proceedings of 20th IEEE Canadian Conference on Electrical and Computer Engineering. 1507-1510. ISSN 0840-7789.

V. Technical/ Scientific reports:

[1] **Nan, C**., Kröger, W., and Eusgeld, I. (2011) Study of Common Cause Failures of the SCADA System at Substation Level, Scientific report for Swiss Federal Office of Civil Protection.
[2] **Nan, C**. (2011) Further Method Development (HLA). Scientific report for Swiss Federal Office of Civil Protection.
[3] Kröger, W., **Nan, C**., Trantopoulos, K., Zhou, L., and Eusgeld, I. (2010) Interdependencies between critical infrastructures. Scientific report Swiss Federal Office of Civil Protection.
[4] **Nan, C** and Eusgeld, I. (2010) Further Development of Modeling and Simulation to Disclose Vulnerabilities of Interdependent Critical Infrastructures. Scientific report for Swiss Federal Office of Civil Protection.

VI. Oral Presentations:

[1] **Nan, C** and Eusgeld, I. (2011) Building a Distributed Simulation Environment. Presented at the technical workshop at Institute of Automation and Information Systems in Technical University of Munich (TUM-AIS).
[2] Kröger, W and **Nan, C.** (2010) Vulnerability Analysis of Interdependent Critical Infrastructure. Presented at final MIA conference 2010.
[3] **Nan**, **C**., Iqbal, M.T., and Khan, F. (2006) Modeling and Simulating a Micro Steam Power Unit by G2 Real-Time Expert System. Presented at 16th Annual Newfoundland ECE Conference.