Assessing Cyber Risk Using the CISIApro Simulator

Chiara Foglietta, Cosimo Palazzo, Riccardo Santini, Stefano Panzieri

Chapter 19

ASSESSING CYBER RISK USING THE CISIApro SIMULATOR

Chiara Foglietta, Cosimo Palazzo, Riccardo Santini and Stefano Panzieri

Abstract Dependencies and interdependencies between critical infrastructures are difficult to identify and model because their effects appear infrequently with unpredictable consequences. The addition of cyber attacks in this context makes the analysis even more complex. Integrating the consequences of cyber attacks and interdependencies requires detailed knowledge about both concepts at a common level of abstraction.

CISIApro is a critical infrastructure simulator that was created to evaluate the consequences of faults and failures in interdependent infrastructures. This chapter demonstrates the use of CISIApro to evaluate the effects of cyber attacks on physical equipment and infrastructure services. A complex environment involving three interconnected infrastructures is considered: a medium voltage power grid managed by a control center over a SCADA network that is interconnected with a general-purpose telecommunications network. The functionality of the simulator is showcased by subjecting the interconnected infrastructures to an ARP spoofing attack and worm infection. The simulation demonstrates the utility of CISIApro in supporting decision making by electric grid operators, in particular, helping choose between alternative fault isolation and system restoration procedures.

Keywords: Critical infrastructure, simulation, cyber attacks, risk

1. Introduction

Critical infrastructures are vital to modern society. Airports, rail transport, network communications, electric grids, oil refineries and water systems are examples of critical infrastructure assets. Industrial operations adhere to the so-called $N-1$ standard, which refers to the ability to operate without the loss of service after the failure of one key component. Industrial plants also have the ability to operate despite the loss of two key components ($N-2$ standard). However, the $N-2$ standard is inadequate for critical infrastructures because major service outages, coordinated cyber attacks and faults often initiate in other interconnected infrastructures and propagate to the infrastructure of interest. Conditions within the infrastructure of interest as well as the existing infrastructure interdependencies must be considered and evaluated in order to restore services as soon as possible.

For more than fifteen years, researchers have grappled with the problems of modeling interdependencies and predicting the effects of infrastructure failures. The 2003 North American blackout was the first example of cascading effects after a power outage. The blackout, which was due to a software bug in an electric grid control room, impacted water supply, transportation, communications systems and several industries [1]. Another example is Hurricane Katrina, which interrupted oil production, transportation, refining, ocean shipping and exports as well as electric utilities [10].

Critical infrastructures adhere to the $N-1$ standard and they are protected from failures that initiate in their own sectors. In the event of a failure in the power grid, operators can reconfigure the grid to isolate the fault and restore power to customers (some users might still not have power, but the blackout is not complete). The reconfiguration procedure can be automated or executed manually and it depends on the specific topology (the sequence of opening and closing circuit breakers is related to the topology) as well as on other infrastructures, especially the telecommunications network, which is used to send commands to circuit breakers. This procedure is called fault isolation and system restoration (FISR) or power load shedding.

If a cyber event or a failure occurs in the telecommunications network, the procedure for restoring power may fail without any alerts being sent to power grid operators. In this situation, a routine failure can evolve to become a large-scale blackout that lasts for an extended period of time. One of the most famous cyber attacks on a SCADA network was perpetrated by Stuxnet [9]. This chapter focuses on the modeling and assessment of the impacts of cyber events on interconnected critical infrastructures.

The vast reach of telecommunications networks leads to poorly understood situations that can have uncontrolled effects on physical equipment in critical infrastructure assets. However, the problem of detecting cyber anomalies is outside the scope of this research because the approach presented here is independent of anomaly detection techniques. Indeed, the assumption here is that intrusion detection systems and malware protection software are in place to collect data about potential anomalies.

This chapter demonstrates the application of CISIApro to evaluate the effects of cyber attacks on physical equipment and infrastructure services. A complex environment involving three interconnected infrastructures is considered: a medium voltage power grid managed by a control center over a SCADA network that is interconnected with a general-purpose telecommunications network. The functionality of the simulator is illustrated by subjecting the interconnected infrastructures to an ARP spoofing attack to compromise a secure communications channel, which is then used to launch a worm infection. The simulation demonstrates the utility of CISIApro in supporting decision making by electric operators, specifically helping choose between alternative fault isolation and system restoration procedures.

2. Related Work

This section conducts a brief analysis of techniques and tools for modeling and simulating interdependent critical infrastructures, with a focus on evaluating the consequences of cyber attacks.

2.1 Infrastructure Modeling and Simulation

Satumitra and Duenas-Osorio [15] have published an exhaustive survey of the principal methods for critical infrastructure modeling and simulation. Their survey reveals that most of the approaches for dealing with infrastructure interdependencies, cascading system failures and risk mitigation are complementary rather than competing. The modeling approaches include techniques based on game theory, graph theory, risk-based models, Petri nets and Bayesian networks. However, many of the interdependency models are primarily conceptual in nature or are limited to simple or high-level scenarios.

Rahman et al. [13] have developed the Infrastructure Interdependency Simulator (I2Sim) based on the well-known cell-channel model. In this model, infrastructures and their interconnections are represented using cells and channels. A cell is an entity that performs a function. For example, a hospital is a cell that uses input tokens such as electricity, water and medicines, and produces output tokens such as the number of patients served. A channel is a means through which tokens flow from one cell to another. The interdependencies between infrastructures are non-linear relationships that are summarized in the form of human-readable tables. I2Sim helps decision makers optimize resources and prioritize system restoration actions after critical events. I2Sim is the core element of DR-NEP (Disaster Response Network Enabled Platform), an advanced disaster management tool that is based on a web services infrastructure and incorporates domain simulators. The modeling technique has been validated by several case studies, including one involving the Vancouver 2010 Winter Olympics. However, the case studies mainly focus on natural disasters and do not consider the impacts of cyber attacks.

A survey of the research literature reveals that the majority of simulators employ the agent-based paradigm, in which a population of autonomous interacting agents coordinate their decisions to reach a higher-level global objective. Each infrastructure is modeled as an agent. Interdependencies are modeled as edges between agents. This enables agents to exchange information: each agent receives inputs from other agents and sends its outputs to other agents (see Nieuwenhuijs et al. [12] for further details). The CISIApro (Critical Infrastructure Simulation by Interdependent Agents) simulator [3] used in this research employs the agent-based paradigm, where each agent has a high-level description of the internal dynamics of an infrastructure. The main goal of CISIApro is to study the propagation of faults/attacks and the resulting degradation in performance [6]. Of course, a disadvantage of the approach is the difficulty in acquiring detailed information about the internal dynamics of infrastructures in order to create the agents.

Another recent trend is the use of co-simulation frameworks, where several domain-specific simulators are connected using a well-defined and generic interface (API) for simulation interoperability [16]. The main goal of a co-simulation framework is to reuse existing models in a common context to simulate complex scenarios. The Mosaik ecosystem [16] has been applied to analyze a smart grid scenario in which telecommunications network and power grid simulators are integrated. This work integrated various simulators for the electrical side, including models of electric vehicles in Python, photovoltaic cells in MATLAB/Simulink, residential loads as CSV time series data and two power distribution grids in Python. Mosaik is still at an early stage of development, but it can cope with different temporal resolutions (e.g., continuous, every minute or every fifteen minutes).

2.2 Cyber Attack Impact Assessment

Motivated by Stuxnet, researchers have focused on understanding how cyber attacks can affect physical critical infrastructure assets by leveraging SCADA telecommunications networks. This problem is complex because it requires deep knowledge from different domains – telecommunications and the specific physical infrastructure. Smart grids and power grids, in general, are perfect environments for evaluating the effects of cyber threats. Power grids have detailed analytic models at almost every level of abstraction and they also have well-documented control algorithms.

Lemay et al. [11] have used an industrial control system sandbox for the cyber portion of a cyber-physical system and optimal power flow algorithms for an electrical simulator to replicate the physical portion of an electrical power grid. The ability to model the physical damage caused by cyber attacks enables defenders to accurately evaluate the risk using metrics such as the delivered power and generation costs.

Sgouras et al. [17] have analyzed the impact of denial-of-service and distributed denial-of-service attacks on a smart meter infrastructure. They demonstrated that an attack on a single meter causes a temporary isolation or malfunction, but does not impact the power grid. However, the partial non-availability of the demand-response mechanisms in a large number of smart meters due to a distributed denial-of-service attack could impact load shedding when the grid reaches an unsafe zone close to its maximum capacity. For these reasons, an attacker would prefer to conduct a distributed denial-of-service attack during a peak-use period in order to achieve greater impact.

Dondossola et al. [7] have assessed the impact of malware using a cyber-physical risk index that incorporates a probabilistic interpretation of vulnerability existence, threat occurrence and intrusion success. The basic idea underlying the cyber assessment methodology is to adopt a frequency interpretation of probability; specifically, the probabilities comprising the risk index are translated to their corresponding frequencies.

Another approach is to fuse information from the cyber and physical domains. To accomplish this, Santini et al. [14] have developed a data fusion framework using evidence theory. The data fusion framework was used to identify the cause of a cyber-physical attack (i.e., a denial-of-service attack that caused a breaker in a smart grid to malfunction).

Critical infrastructure operators are especially interested in the quality of the the services provided to their customers. Therefore, it is vital to understand the effects of cyber attacks on physical systems and their services. The CISIApro simulator used in this research is specifically designed to help determine the consequences of cyber attacks on physical equipment and the services they provide.

3. CISIApro Simulator

This section describes the main features of the CISIApro simulator, including its reliance on the mixed holistic reductionist (MHR) approach.

3.1 Mixed Holistic Reductionist Approach

The mixed holistic reductionist approach [5] was created to exploit the advantages of holistic and reductionist methods. In holistic modeling, infrastructures are seen as singular entities with defined boundaries and functional properties. On the other hand, reductionist modeling emphasizes the need to fully understand the roles and behaviors of individual components to comprehend the infrastructure as a whole. Different types of analyses require one or both points of view and their boundaries are lost when complex case studies are considered. In the mixed holistic reductionist approach, the relationships between infrastructures can be viewed at different levels via a top-down or bottom-up approach. Critical infrastructures have specific requirements in terms of the quality of the services delivered to customers. This requires the addition of another layer – the service layer – that describes the functional relationships between components and the infrastructure at different levels of granularity. In the mixed holistic reductionist approach, services provided to customers and to other interconnected infrastructures are explicitly considered as a middle layer between the holistic and reductionist layers.

3.2 Simulator Description

CISIA is an agent-based simulator in which all agents have the same structure (Figure 1). An agent receives resources and failures from other agents. A resource is a good, service or data produced and/or consumed by an agent that is represented in CISIA as an entity. The ability to produce resources is summarized by the concept of an operative level, which depends on the availability of received resources, propagation of faults and functionality of the entity itself.

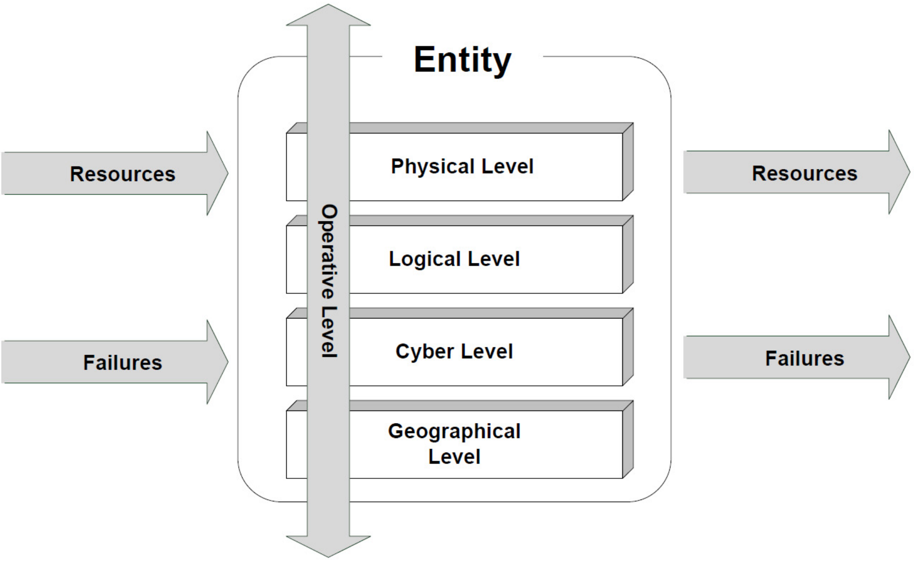


Figure 1. CISIA entity diagram.

An entity also receives failures via its upstream interconnections and spreads the failures to downstream entities. The failures propagate different types of faults in different ways. The output of an agent depends on the actual value of the operative level. The classes of interdependencies considered are physical, logical, geographical and cyber. Interested readers are referred to [6] for a detailed description of the CISIA simulator.

Risk is defined as the product of the impact, threat and vulnerability:

$$Risk = Impact \times Threat \times Vulnerability \tag{1}$$

Risk is usually computed as a numeric value from the impact severity, the likelihood of occurrence of the threat and the vulnerability measure. In CISIA applications, the likelihood of occurrence is replaced with the trust of the information. For each entity, a user can also add a vulnerability variable; however, in the case study discussed in this work, it is assumed that the vulnerability depends only on the distance from the source and on the persistence of the attack. The operative level of each agent is associated with a risk level. The risk, which is defined as the amount of harm due to a specific event (e.g., failure), is evaluated as:

$$Risk = 1 - Operative\ Level \tag{2}$$

where 1 represents the maximum value of the operative level. A high operative level corresponds to a low risk.

In 2014, the CISIApro simulator was developed to overcome certain implementation problems associated with CISIA. The main problem was the possibil-

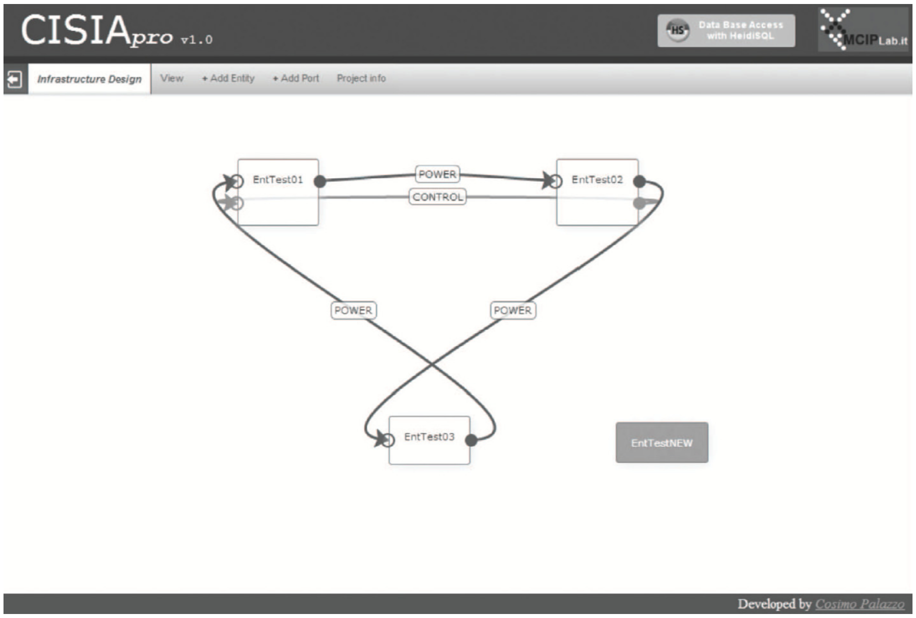


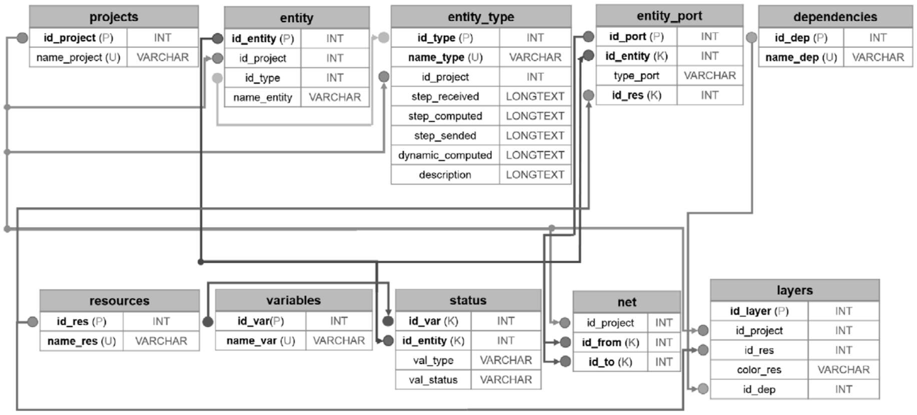
Figure 2. CISIA graphical user interface.

ity of an infinite loop when resources are instantly exchanged between entities. CISIA's main cycle buffers all the information exchanged between entities at each time step. If the exchanges form a cycle, then the simulation time step never ends, which results in an infinite loop. The CISIApro simulator ensures that the information flow is well defined using a maximum execution threshold for a time step; this eliminates infinite loops.

Another disadvantage of CISIA was the extended period of time required to set up and debug the system. In CISIApro, a graphical user interface is provided to create and connect entities and to add the exchanged resources in an efficient manner (Figure 2).

After creating the entities and their interconnections (i.e., interdependencies) and adding the exchanged resources, it is necessary to implement the behavior of each entity. Each entity is composed of four modules that are executed: (i) RECEIVED, which evaluates the received resources and faults; (ii) DYNAMIC COMPUTED, which implements dynamic evolution; (iii) INSTANT COMPUTED, which implements instantaneous evolution; and (iv) SENT, which evaluates the resources that are sent to the downstream entities.

CISIApro uses a database to capture all the information needed to represent multiple critical infrastructures and their interconnections. Figure 3 shows the database structure. Each entity is an instance of an entity type whose status is expressed using variables. Each entity has ports for exchanging resources and creating the mixed holistic reductionist model layers. Each layer embodies various interdependencies.



projects	
id_project (P)	INT
name_project (U)	VARCHAR

entity	
id_entity (P)	INT
id_project	INT
id_type	INT
name_entity	VARCHAR

entity_type	
id_type (P)	INT
name_type (U)	VARCHAR
id_project	INT
step_received	LONGTEXT
step_computed	LONGTEXT
step_sended	LONGTEXT
dynamic_computed	LONGTEXT
description	LONGTEXT

entity_port	
id_port (P)	INT
id_entity (K)	INT
type_port	VARCHAR
id_res (K)	INT

dependencies	
id_dep (P)	INT
name_dep (U)	VARCHAR

resources	
id_res (P)	INT
name_res (U)	VARCHAR

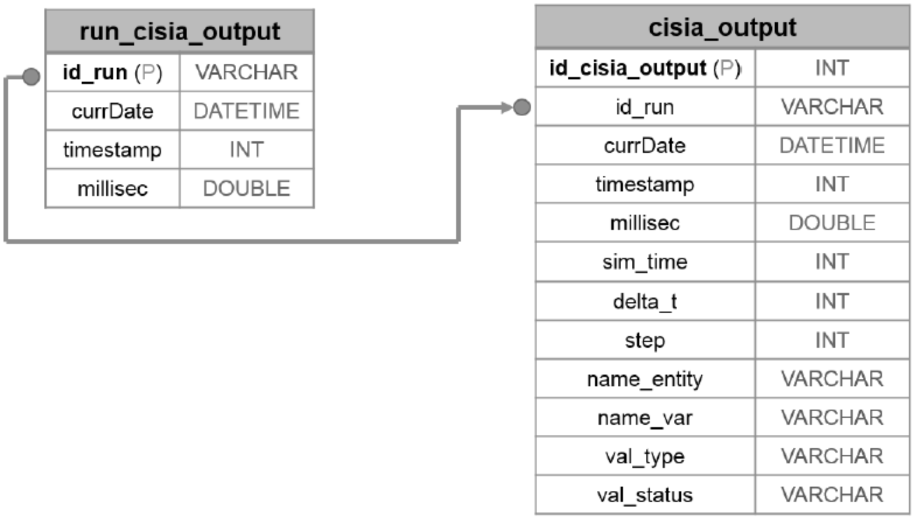
variables	
id_var(P)	INT
name_var (U)	VARCHAR

status	
id_var (K)	INT
id_entity (K)	INT
val_type	VARCHAR
val_status	VARCHAR

net	
id_project	INT
id_from (K)	INT
id_to (K)	INT

layers	
id_layer (P)	INT
id_project	INT
id_res	INT
color_res	VARCHAR
id_dep	INT

Figure 3. CISIApro database representation.



run_cisia_output	
id_run (P)	VARCHAR
currDate	DATETIME
timestamp	INT
millisec	DOUBLE

cisia_output	
id_cisia_output (P)	INT
id_run	VARCHAR
currDate	DATETIME
timestamp	INT
millisec	DOUBLE
sim_time	INT
delta_t	INT
step	INT
name_entity	VARCHAR
name_var	VARCHAR
val_type	VARCHAR
val_status	VARCHAR

Figure 4. CISIApro output database representation.

The CISIApro output is stored in a separate database (Figure 4). This database stores timestamped data for use by operators.

Adjacency matrices that represent interdependencies existing between entities are generated during the design phase. During the simulation, the matrices are represented as queue data structures to speed up computations.

The ability of CISIApro to support operator decision making has been validated by two European Union projects, FACIES [8] and CockpitCI [4]. Figure 5 shows the information flow from input acquisition to operator display. The physical system data is gathered from the SCADA control center and the cyber threat data is obtained from cyber detection systems such as intrusion

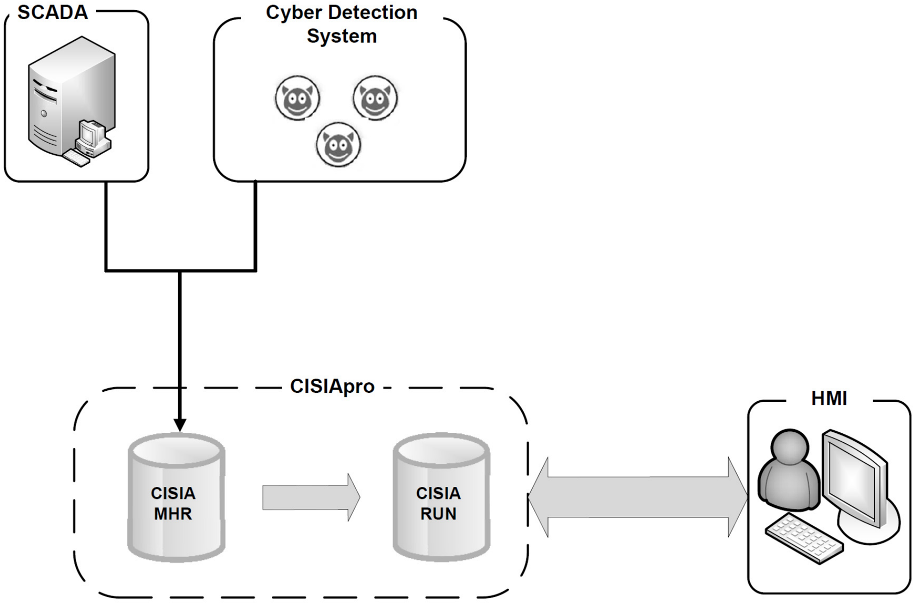


Figure 5. Information flow.

detection systems and anti-virus software. All the information is translated and saved into the CISIApro database (CISIA MHR) and the output is placed in the CISIA RUN database. The CISIApro execution results are displayed to operators via human-machine interfaces (HMIs).

4. Case Study

The case study considers three interconnected infrastructures: a medium voltage power grid controlled by a SCADA network and connected to a general-purpose telecommunications network. Interested readers are referred to [2] for details about the interconnected infrastructures.

Figure 6 shows a portion of the medium voltage power grid. It consists of two lines fed by two substations that transform current from the high voltage grid. During normal conditions, the two lines are usually disconnected by two circuit breakers that are normally open (Breakers #7 and #8 in Figure 6). Also, Breakers #3 and #5 are open in order to maintain a radial topology.

All the circuit breakers, except for the two located at the substations (not numbered in Figure 6), are controlled from the SCADA control center via a telecommunications network. This proprietary network, which belongs to the power grid owner, uses a protocol compatible with TCP/IP. A remote terminal unit (RTU) is directly connected to each circuit breaker, except for the two breakers located at the substations. The SCADA control center in Figure 7

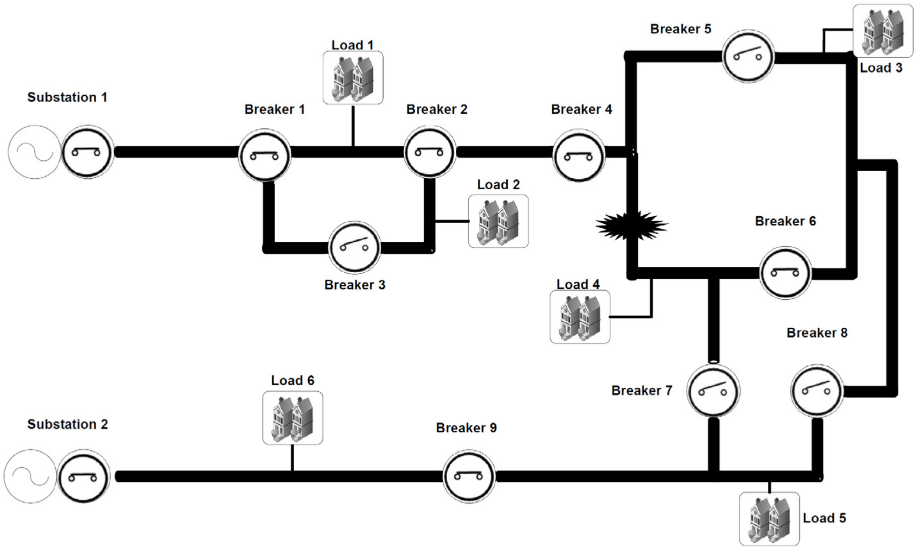


Figure 6. Power grid.

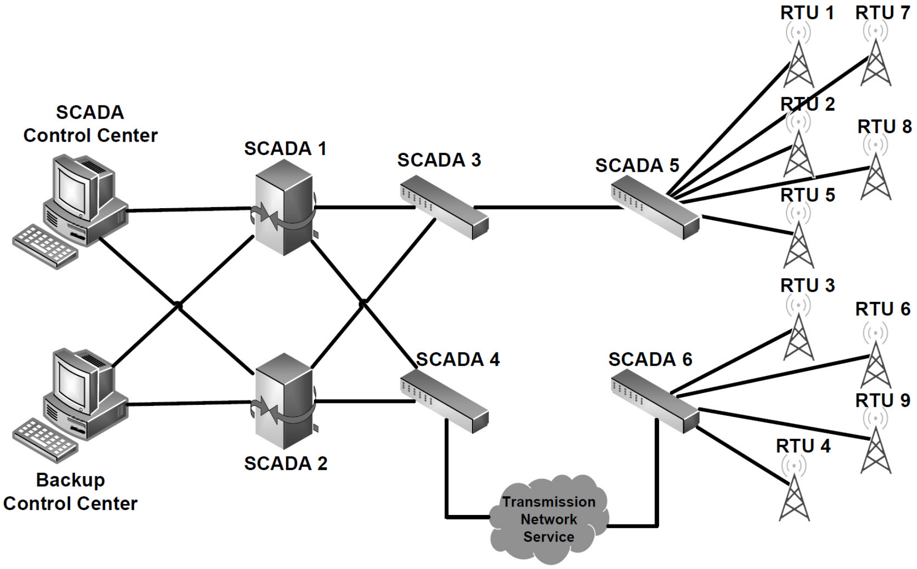


Figure 7. SCADA control center.

sends commands to the remote terminal units to open or close the associated circuit breakers.

Figure 8 shows the general-purpose telecommunications network (i.e., Internet) that is connected to the SCADA system. The network essentially has a

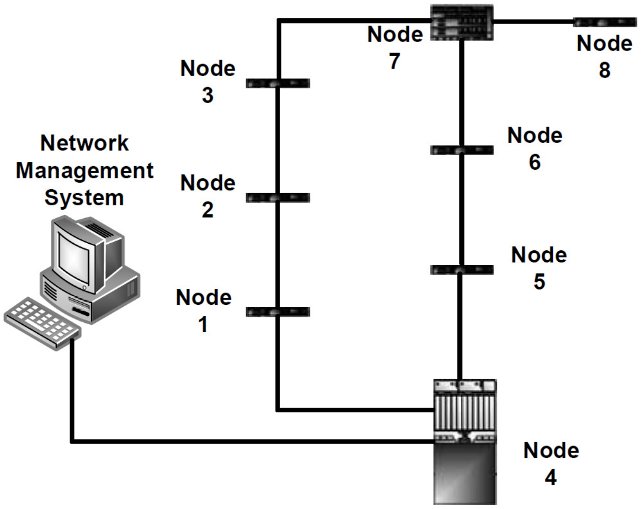


Figure 8. Telecommunications network.

ring topology. In the event of a link failure, network packets are transmitted back to the sending node in order to change the routing protocol.

In the case of a permanent failure in the power grid, the operator executes a fault isolation and system restoration procedure to open or close circuit breakers. This procedure determines where the fault occurred and how to restore power to customers after the damage is repaired. If a cyber fault occurs in the telecommunications network, then the fault isolation and system restoration procedure fails with unpredictable consequences.

The attack scenario considered in this work involves a cyber attacker who attempts to modify the behavior of the power grid using a computer worm to infect the remote terminal units, as in the case of Stuxnet [9]. The attack begins with an ARP spoofing attack that exploits ARP vulnerabilities. The goal is to map the attacker's MAC address to the IP address of a trusted node in the network so that traffic directed at the trusted node is sent to the attacker. The attacker is assumed to be connected to the telecommunications network and uses the connectivity to send the worm to the remote terminal units and their associated circuit breakers.

5. Simulation Results

The simulation, which lasted 40 seconds, is divided into two parts. The first part, lasting from 1 to 10 seconds, involves the attacker performing a man-in-the-middle attack on Node #6 in the telecommunications network (Figure 8). The second part, lasting from 11 to 40 seconds, involves an infection being spread from Node #6 to the remote terminal units and their associated circuit breakers via the SCADA network (Figure 7).

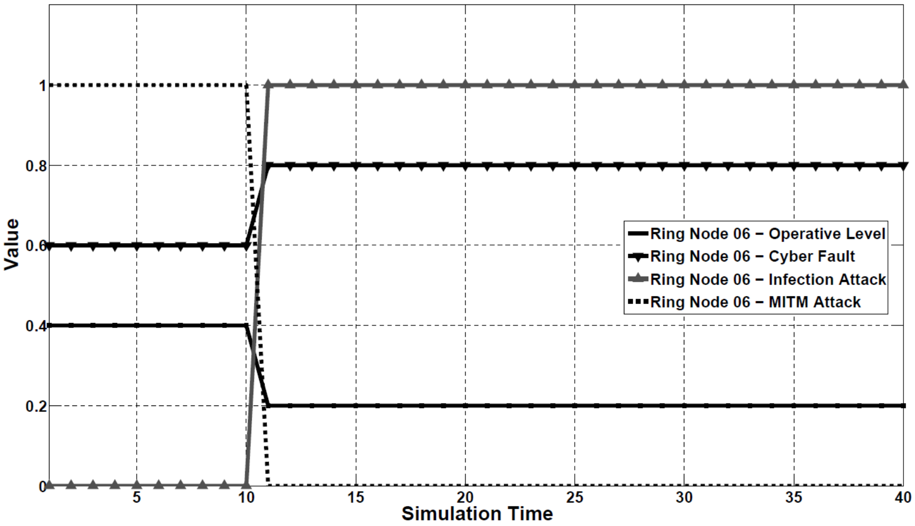


Figure 9. Telecommunications Node #6 simulation results.

The man-in-the-middle attack has a static aspect – no changes occur during the first 10 seconds of the simulation for the involved entities. The spreading of the cyber attack depends on the distance from the infected node: the greater the number of hops needed to reach a node, the lower is the effect of the cyber attack and the lower is the risk of the node malfunctioning. Figure 9 shows the simulation results for Telecommunications Node #6 (Figure 8) whose operative level was 0.4 during the man-in-the-middle attack. The operative level of the downstream SCADA node (Node #6 in Figure 7) was 0.85 as shown in Figure 10. The operative levels of the remote terminal units connected to SCADA Node #6 (in particular, RTUs #3, #4, #6 and #9 on Figure 7) were also 0.92 as shown in Figure 12.

Figure 9 shows that, after the infection is detected at 11 seconds, the telecommunications node (Node #6 in Figure 8) is greatly affected and with high confidence. Note that the SCADA network has two paths for sending information to the remote terminal units; the bottom path in Figure 7 is via the telecommunications network. The CISIApro simulation did not consider the real path over the telecommunications network, but instead, it considered the global evaluation of the service level of the network, which is referred to as the telecommunications network service (TNS) and whose operative level is shown in Figure 11.

As seen in Figure 10, the downstream node of the SCADA network (SCADA Node #6 in Figure 7) is affected by the infection after 12 seconds. Nodes that are further away from the source of the infection are affected after nodes closer to the source node. Therefore, SCADA Node #6 needs more time to become completely unavailable with respect to Telecommunications Node #6. The

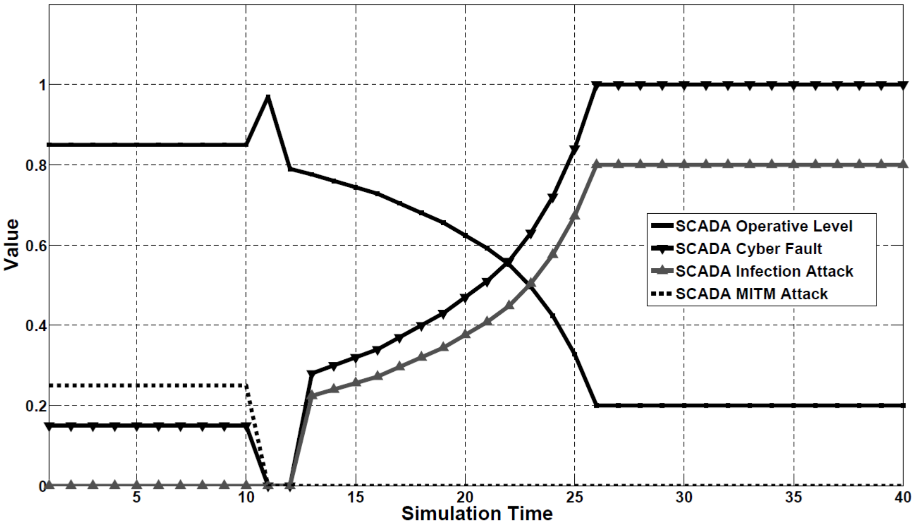


Figure 10. SCADA Node #6 simulation results.

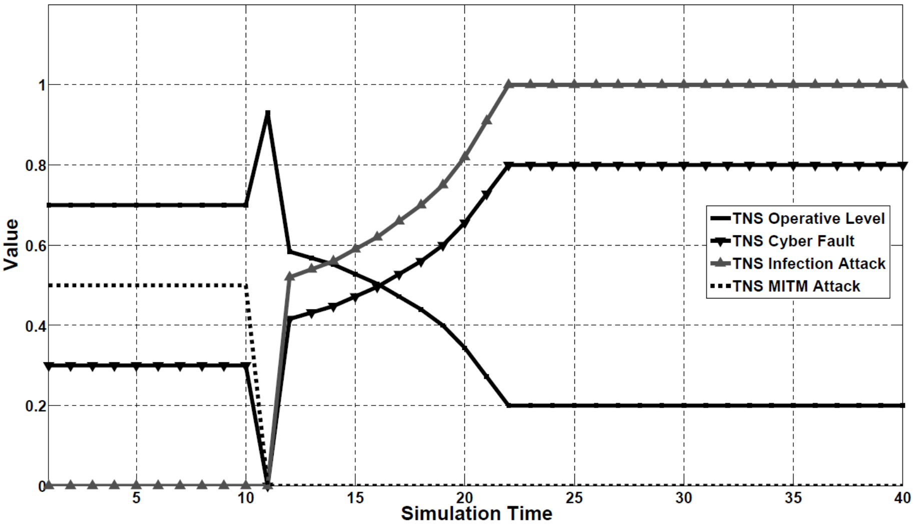


Figure 11. Telecommunications network service simulation results.

remote terminal units (RTUs #3, #4, #6 and #9) that are linked to SCADA Node #6 exhibit similar trends, with delays of one time step (Figure 12).

The CISIApro simulator is designed to enhance operator decision making. The reconfiguration of a power grid is a task that requires the consideration of the interconnected infrastructures. Assume that the fault in the power grid shown in Figure 6 is the result of an explosion. Then, two alternative fault isolation and system restoration (FISR) procedures may be considered:

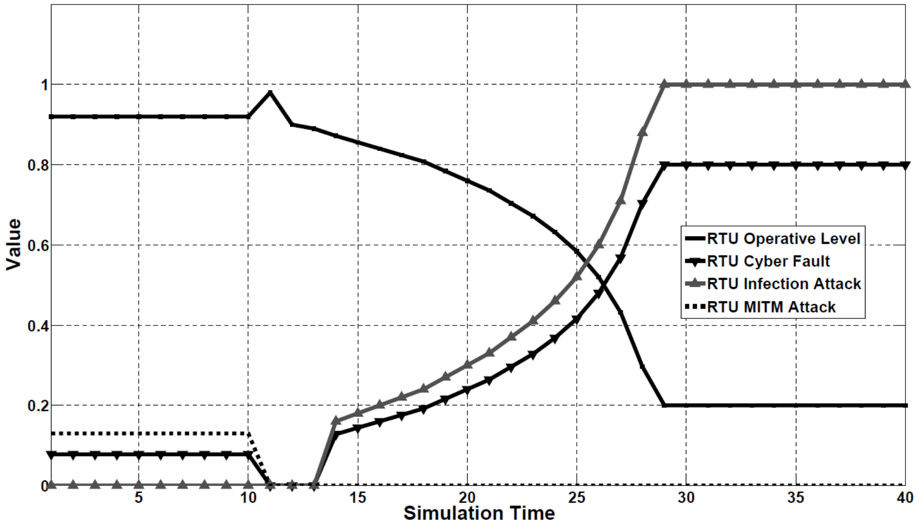


Figure 12. Simulation results for RTUs #3, #4, #6 and #9.

- **FISR #01:** Open Breakers #4 and #6. Close Breaker #8. Breakers #5 and #7 are already open due to the initial configuration. Only Customer #4 is disconnected. Load #3 is fed by Substation #2.

- **FISR #02:** Open Breakers #4 and #6. Customers #3 and #4 are isolated.

Figure 13 shows the trends for the two fault isolation and system restoration procedures. The graphs show that the two procedures yield different results because of the manner in which the infection spreads. Note that the first procedure is less risky than the second procedure.

6. Conclusions

The CISIApro simulator advances the earlier CISIA simulator by providing a convenient graphical interface for modeling infrastructure entities and their interconnections and interdependencies. The simulator helps evaluate the impacts of cyber attacks on interdependent infrastructures; the attacks include ARP spoofing, SYN flooding and worm infections. CISIApro has been validated using complex case studies involving approximately 70 entities that exchange around twelve distinct resources. The case study described in this chapter involves three interconnected infrastructures: a medium voltage power grid managed by a control center over a SCADA network that is interconnected with a general-purpose telecommunications network. The real-time simulation involving an ARP spoofing attack and worm infection demonstrates the utility of the CISIApro for supporting decision making by electric grid operators, in partic-

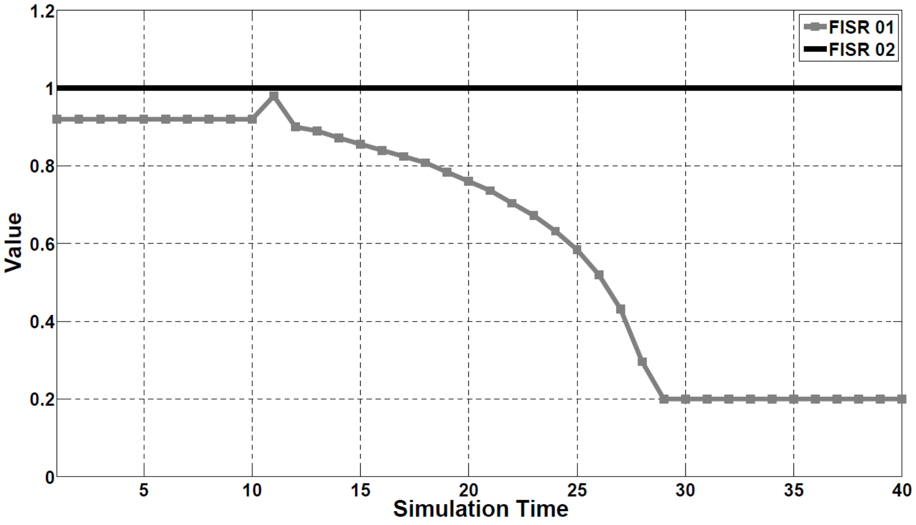


Figure 13. Simulation trends for different FISR procedures.

ular, helping choose between alternative fault isolation and system restoration procedures to reduce the attack impact and enhance system recovery.

Future research will evaluate the impacts of cyber attacks on other critical infrastructures such as water distribution networks and gas pipelines; the goal is to enhance the CISIApro library of cyber attacks and the understanding of their outcomes. Additionally, research will focus on the detailed modeling and simulation of telecommunications networks to better understand attack propagation and to devise approaches for measuring and reducing the impacts of failures within the telecommunications infrastructure as well as failures that propagate from other interdependent infrastructures.

Acknowledgement

This research was partially supported by the DG Home Affairs under the Prevention, Preparedness and Consequence Management of Terrorism and Other Security Related Risks CIPS Grant Action 2013 (HOME/2013/CIPS/AG 2013) (URANIUM – Unified Risk Assessment Negotiation via Interoperability Using Multi-Sensor Data (`uranium.theorematica.it`)).

References

[1] G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca, R. Schulz, A. Stankovic, C. Taylor and V. Vittal, Causes of the 2003 major grid blackouts in North America and Europe and recommended means to improve system dynamic performance, *IEEE Transactions on Power Systems*, vol. 20(4), pp. 1922–1928, 2005.

[2] E. Ciancamerla, C. Foglietta, D. Lefevre, M. Minichino, L. Lev and Y. Shneck, Discrete event simulation of QoS of a SCADA system interconnecting a power grid and a telco network, in *What Kind of Information Society? Governance, Virtuality, Surveillance, Sustainability, Resilience*, J. Berleur, M. Hercheui and L. Hilty (Eds.), Springer, Heidelberg, Germany, pp. 350–362, 2010.

[3] CISIApro Project, CISIApro: Interdependency Modeling and Simulation Made Easy for Critical Infrastructures, University of Roma Tre, Rome, Italy (`cisiapro.dia.uniroma3.it`).

[4] CockpitCI Project, CockpitCI, Selex Systems Integration, Rome, Italy (`www.cockpitci.eu`).

[5] S. De Porcellinis, S. Panzieri and R. Setola, Modeling critical infrastructure via a mixed holistic reductionistic approach, *International Journal of Critical Infrastructures*, vol. 5(1/2), pp. 86–99, 2009.

[6] S. De Porcellinis, S. Panzieri, R. Setola and G. Ulivi, Simulation of heterogeneous and interdependent critical infrastructures, *International Journal of Critical Infrastructures*, vol. 4(1/2), pp. 110–128, 2008.

[7] G. Dondossola, F. Garrone and J. Szanto, Cyber risk assessment of power control systems – A metrics weighed by attack experiments, *Proceedings of the IEEE Power and Energy Society General Meeting*, 2011.

[8] FACIES Project, FACIES: Online Identification of Failures and Attacks on Interdependent Critical Infrastructures, University of Roma Tre, Rome, Italy (`facies.dia.uniroma3.it`).

[9] N. Falliere, L. O'Murchu and E. Chien, W32.Stuxnet Dossier, Version 1.4, Symantec, Mountain View, California, 2011.

[10] A. Kwasinski, P. Chapman, P. Krein and W. Weaver, Hurricane Katrina Damage Assessment of Power Infrastructure for Distribution, Telecommunications and Back-Up, CEME-TR-06-05, UILU-ENG-2006-2511, Grainger Center for Electric Machinery and Electromechanics, Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, Urbana, Illinois, 2006.

[11] A. Lemay, J. Fernandez and S. Knight, Modeling physical impact of cyber attacks, *Proceedings of the Workshop on Modeling and Simulation of Cyber-Physical Energy Systems*, 2014.

[12] A. Nieuwenhuijs, E. Luiijf and M. Klaver, Modeling dependencies in critical infrastructures, in *Critical Infrastructure Protection*, E. Goetz and S. Shenoi (Eds.), Boston, Massachusetts, pp. 205–213, 2008.

[13] H. Rahman, M. Armstrong, D. Mao and J. Marti, I2Sim: A matrix-partition based framework for critical infrastructure interdependencies simulation, *Proceedings of the Electric Power Conference*, 2008.

[14] R. Santini, C. Foglietta and S. Panzieri, Evidence theory for cyber-physical systems, in *Critical Infrastructure Protection VIII*, J. Butts and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 95–109, 2014.

[15] G. Satumitra and L. Duenas-Osorio, Synthesis of modeling and simulation methods in critical infrastructure interdependencies research, in *Sustainable and Resilient Critical Infrastructure Systems*, K. Gopalakrishnan and S. Peeta (Eds.), Springer-Verlag, Berlin Heidelberg, Germany, pp. 1–51, 2010.

[16] S. Schutte, S. Scherfke and M. Troschel, Mosaik: A framework for modular simulation of active components in smart grids, *Proceedings of the First IEEE International Workshop on Smart Grid Modeling and Simulation*, pp. 55–60, 2011.

[17] K. Sgouras, A. Birda and D. Labridis, Cyber attack impact on critical smart grid infrastructures, *Proceedings of the IEEE Power and Energy Society Innovative Smart Grid Technologies Conference*, 2014.

[18] A. Singh, K. Srivastava and J. Marti, Reduction techniques in modeling critical infrastructures under the infrastructure interdependencies simulator framework, *International Journal of Critical Infrastructures*, vol. 9(3), pp. 173–189, 2013.