Reliability Engineering and System Safety 96 (2011) 679–686

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

"System-of-systems" approach for interdependent critical infrastructures

Irene Eusgeld, Cen Nan*, Sven Dietz

Laboratory of Safety Analysis, ETH Zurich, Sonneggstr. 3, 8092 Zürich, Switzerland

ARTICLE INFO

Available online 5 January 2011

Keywords:
Critical infrastructure
System-of-Systems (SOS)
High Level Architecture (HLA)
Interdependency study

ABSTRACT

The study of the interdependencies within critical infrastructures (CI) is a growing field of research as the importance of potential failure propagation among infrastructures may lead to cascades affecting all supply networks. New powerful methods are required to model and describe such "systems-of-systems" (SoS) as a whole. An overall model is required to provide security and reliability assessment taking into account various kinds of threats and failures. A significant challenge associated with this model may be to create "what-if" scenarios for the analysis of interdependencies. In this paper the interdependencies between industrial control systems (ICS), in particular SCADA (Supervisory Control and Data Acquisition), and the underlying critical infrastructures to address the vulnerabilities related to the coupling of these systems are analyzed. The modeling alternatives for system-of-systems, integrated versus coupled models, are discussed. An integrated model contains detailed low level models of (sub)systems as well as a high level model, covering all hierarchical levels. On the other hand, a coupled model aggregates different simulated outputs of the low level models as inputs at a higher level. Strengths and weaknesses of both approaches are analyzed and a model architecture for SCADA and the "system under control" are proposed. Furthermore, the HLA simulation standard is introduced and discussed in this paper as a promising approach to represent interdependencies between infrastructures. To demonstrate the capabilities of the HLA standard for the interdependencies study, an exemplary application and some first results are also briefly presented in this paper.

1. Introduction

In this paper we study critical infrastructures, analyzing them at the single system level and the system-of-systems level, and evaluate advanced modeling and simulation techniques that are required to gain a fundamental understanding of the behavior of these types of infrastructures.

Classical reliability theories are well established and widely used to model large complicated systems. Stochastic models, e.g. the Markov and Poisson processes [1], are being applied to predict the behavior of systems that include uncertainties, but these methods lack the capability to completely capture the underlying structure of the system and the ability to adapt to failures of subsystems when strong interdependencies exist [2]. There is a lack of models to capture the interaction of complex adaptive systems, such as the electric power grid and automation systems.

The importance of the dynamics of networks has been evidenced by large scale blackouts in the electric power grid or the internet, showing the evidence of the high degree of coupling between the network and the control systems. A prominent example is the wide-area power outage on the 14th August, 2003, in the Northeastern United States and Canada [3]. Recent theoretical analyses have shown the sensitivity to parameter variations in the dynamic degradation of networks [4–6]. Breakdowns of such complex networks are often the result of relatively slow initial system degradation escalating into a fast avalanche of component failures, potentially leading to a complete loss of service. The nonlinearity of these systems is evident, while the first few outages might even be independent of each other, the causal failure chains usually become more pronounced in the course of the events, ending up in a fully cascading regime. One of the main systems that could react to such events is the SCADA system, allowing the system to adapt to changes. Another relevant vulnerability is related to the control system, as evidenced by the Rome Mini-Blackout of 2004, which

Abbreviations: ABM, Agent-Based Modeling; CI, Critical Infrastructures; DMSO, U.S. Defense Modeling and Simulation Office; EPS, Electric Power Supply; FCD, Field level Control Device; FID, Field level Instrumentation Device; FT, Flow Transducer; HLA, High Level Architecture; ICS, Industrial Control System; ICT, Information and Communication Technology; IRRIS, Integrated Risk Reduction of Information-based Infrastructure Systems; ISE, Integrated Stochastic Exposure; LAN, Local Area Network; MTU, Master Terminal Unit; NRA, Network Reliability Analyzer; RBD, Reliability Block Diagram; RTU, Remote Terminal Unit; RTI, Run Time Infrastructure; SCADA, Supervisory Control and Data Acquisition; SOE, Sequence of Events; SOS, System-Of-Systems; SAT, Stochastic Activity Networks; SuC, System Under Control; WAN, Wide Area Network

* Corresponding author.
E-mail addresses: eusgeld@mavt.ethz.ch (I. Eusgeld), nan@mavt.ethz.ch (C. Nan), dietz@mavt.ethz.ch (S. Dietz).

0951-8320/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2010.12.010

could be a potential source of risk when wrong commands or inappropriate reactions could have an effect on safe operation [7]. A failure in a pipe of the cooling system led to a partial shut-down of parts of the communication system. Stable environmental conditions did not require corrective actions from the SCADA system, but the system was partially blind. The extent of affected infrastructures was not predicted; this is an example of hidden vulnerabilities. These studies need to be supported by an analytical description that captures the extended concepts inherent to complex systems.

One of the main concerns of the reliability analysis of complex systems is to determine the stability and resilience of different infrastructures and analyze the effect of control measures on the adaptiveness to unpredicted changes, maintaining the ability to provide required services. Infrastructures are highly dynamical systems; the capacity of an infrastructure to change in time is crucial for the adaption to failures. The dynamical properties are implicit in the topology of the underlying networks and controlled by the SCADA and/or the process automation system. This analysis allows to identify the behavior and to determine the safety margins needed to avoid cascades and avalanches. The importance of these effects has been acknowledged by the U.S. government by issuing US CODE: Title 42,5195c on "critical infrastructures protection".

Present probabilistic methods for critical infrastructures generally assume randomness and independency of component outages as the additional incorporation of multiple dependent low-probability failures is limited by the enormous computational expenses [2]. However, as the individual components basically are interlinked and interact with each other through the network (e.g. due to actions of protective devices in the electric power grid changing the power flow over the network) the negligence of the mutual influences of failures systematically underestimates their probability of occurrence of cascading failures. It is thus important to identify and model all possible dependencies, including those that are not evident in a first analysis.

The pervasive use of ICT within other infrastructures, e.g., the electric power grid, provides many benefits that become indispensable for the operation of today's interconnected systems, mainly with respect to efficiencies, automation and availability of information. This dependency, however, increases the vulnerability of the analyzed systems to disturbances of the ICT infrastructure. These topics are at an early stage of development [6]. It should be noted that the concept of vulnerability is still evolving and terms are not consensually defined. In this article the vulnerability can be defined as a flaw or weakness in the design, implementation, operation and/or management of an infrastructure system, or its elements that render it susceptible to destruction or incapacitation when exposed to a hazard or threat or reduces its capacity to resume new stable conditions [8].

The propagation of rare and unanticipated but dependent failures in a cascade is not, or only insufficiently, evaluated by conventional assessments [9]. The main reason an accurate sequence of events is difficult to predict is that there is practically an infinite number of possible operating contingencies and system changes, which would have to be considered. With respect to the impact, recovering from a cascade, such as a blackout, is likely to take longer than it would for restoring specific parts of a system, which were disconnected in a controlled manner [10].

2. Problem statement

The necessity to understand qualitatively the behavior of the infrastructure systems on one hand and the SCADA, ICT and control systems on the other is the requirement to assess the risk associated with a particular infrastructure and in this way assess the involved vulnerabilities.

One of the main problems in the application of any method related to the assessment of vulnerability of coupled infrastructures is the availability of data to build a coherent model. Based on this caveat, different methods may provide applicable results to the problem to be analyzed. We clarify this problem on a specific example and then present the advantages of the most promising approaches and the cases when they can be applied.

3. Description and analysis of interdependencies

In this section we extend the concept of the interdependencies introduced by Rinaldi et al. in Ref. [11] (Fig. 1) and look at different systems in more detail. The initial dependencies were described from a system's level and the granularity of the description was suitable to describe basic interdependencies among infrastructures. Here we present a more detailed analysis, where we take a detailed view at the subsystems and identify the mechanisms leading to failure cascades in the system-of-systems.

Below we present a short description of interdependencies as described by different authors and relate the different concepts to the SCADA and critical infrastructures [12]:

- Input
  The SCADA systems require information to be able to perform the functions related to process control and management. In case of a failure of the underlying infrastructure (system under control), the operability of the complete SCADA system is compromised.
- Mutual
  At least one of the operations of any infrastructure is dependent upon each of the other infrastructures. This type is given, when two or more systems, where the output of each system is an input to other systems, are discussed. "This type of interdependency would be said to occur when a power plant uses coal that is shipped by trains that require power from the plant in order to operate". In our case the SCADA is dependent on electrical power for correct operation and the EPS relies on the SCADA for control actions.
- Co-located
  The geographical location of the sensors and actuators for the CI and the SCADA system has an inherent potential to be physically damaged in case of a natural event or an explosion.

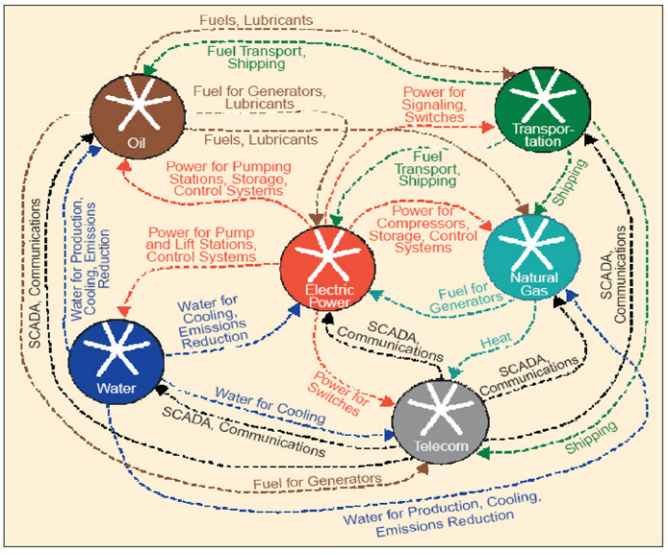

Fig. 1. Interdependencies between infrastructures [11].

These geographical interdependencies are an underlying attribute of the SCADA architecture and cannot be avoided. Mechanisms, such as fault tolerance to data unavailability, have to be implemented to account for this problem. "There were numerous examples of both power lines and fiber optic cables being located in the same manhole, thus creating the possibility that the organizations responsible for these infrastructures would have to coordinate efforts at the manholes. A second example occurred at bridge and tunnel entrances, which also served as the locations for security checks (New York Times Editorial Staff, 2001)."

- Shared
  Underlying CI and the SCADA system may require the supply from shared infrastructures such as the electric power supply network. The goal here would be to decouple the shared vulnerabilities by introducing mechanisms such as buffering devices.
- Exclusive-or
  Either one or another of the two infrastructures can be in use during provision of the service.

In Ref. [11] we find a description of the interaction levels within critical infrastructures:

- Physical
  Infrastructures are linked through material output(s). In the case of the EPS, we find that other infrastructures will not have such a direct effect on the SCADA.
- Cyber
  The state of critical infrastructures is affected by the transmission of information. As the SCADA system is usually not dependent on public data lines, this interaction level is not critical for the SCADA.
- Geographic
  An event that affects a region (such as an earthquake or flooding) will affect several infrastructures, or parts of them. Components of the SCADA system and the system under control have to be installed in the same place; this leads to a geographic linkage (equivalent to the co-located type described earlier).
- Logical
  This type is not of the types mentioned above, but follows different rules. In our case no logical dependencies could be identified.

In our case we can see a physical dependency of generators on the supply of gas to produce electricity. On the other hand, the SCADA system controlling the gas supply network will require electricity from the power plants to operate and will affect the transmission network by exchange of information, which constitutes a cyber dependency. We could speak of Physical/Cyber interdependency between these two systems. Many other composed types of interdependencies could be identified between critical infrastructures.

To illustrate the dependencies between subsystems that lead to interdependencies an example of the coupling between the electric power system and the gas transportation network is presented (Fig. 2). Subsystems of the single infrastructures are dependent on the functionality of subsystems of other infrastructures. In this example we see that generators of the EPS are dependent on the delivery of gas supplied from the buffers of the gas transmission systems and that the SCADA system of the gas network relies on the supply of electricity by the electric power system EPS.

A failure of the transmission grid in the EPS will eventually lead to the failure of the SCADA system in the gas supply network, and this will affect the correct operation of the complete gas network. The failure will propagate to the management of buffers, interrupting the supply of carburant to the generators. We see a classical example of interdependencies between infrastructures developing from dependencies of subsystems.

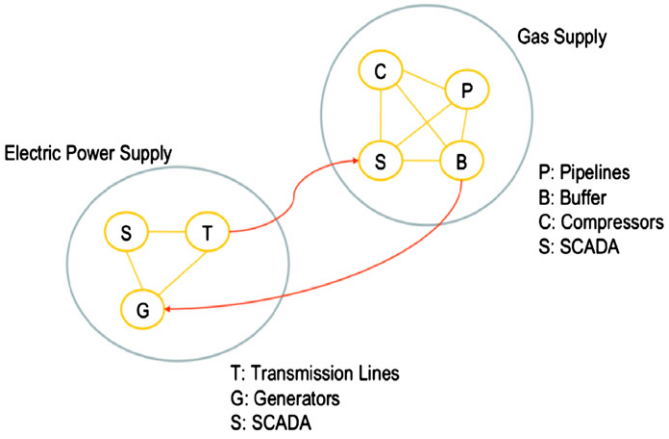

Fig. 2. Zoom-in analysis of systems (decomposition).

4. "System-of-systems" model architecture

We observe CI as complex systems and complex systems can be defined as follow: "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." [13]. Additional characteristics of complex systems are an adaptive emergent behavior 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 highly integrated systems with low dynamic, which can be described with numerous variables. The decomposition of a complicated system for analytical goals is reasonable and common. On the contrary a complex system can never be fully knowable not only due to rapid changes in the system state (high dynamic) and nonlinear behavior, but also interconnections within the system (interdependencies, see section 3).

CI can be seen as so-called "system-of-systems". There is no universally accepted definition of the term "system-of-systems" yet. Numerous definitions vary depending on the application areas and their focus. We focus on the following definition of a system-of-systems: "A system-of-systems (SoS) consists of multiple, heterogeneous, distributed, occasionally independently operating systems embedded in networks at multiple levels, which evolve over time" [14]. Alternatively, system-of-systems can be defined using the term "complex systems": "Systems–of-systems are large scale concurrent and distributed systems that are comprised of complex systems" [1]. The problem is how to deal with the complexity? How to model such systems?

In Ref. [15] a general model architecture is proposed (see Fig. 3). This architecture consists of three hierarchical levels and can be interpreted as follow:

1. The low level: system models of single infrastructure.
2. The middle level: interaction model between single infrastructures (let us call it "local system-of-systems").
3. The high level: global system-of-systems model.

Due to high degree of complexity, we propose at the first step to limit a model to two infrastructures: the SCADA and the System under Control (SuC), which can be Electric Power Supply

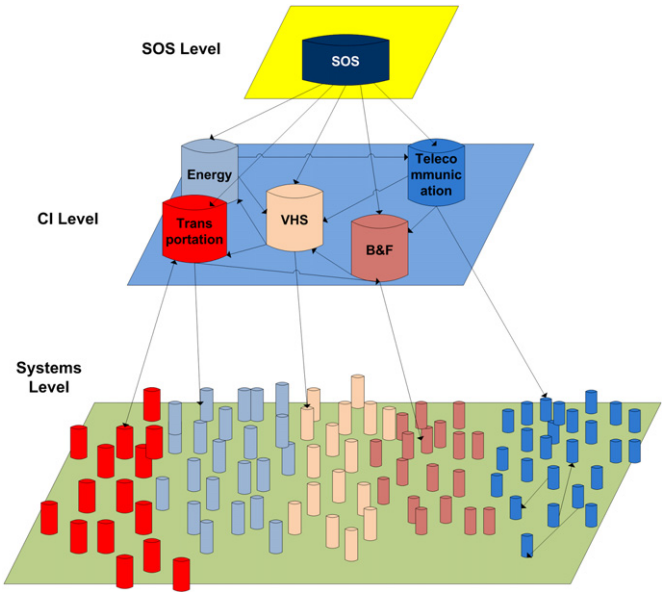

Fig. 3. General model architecture [15].

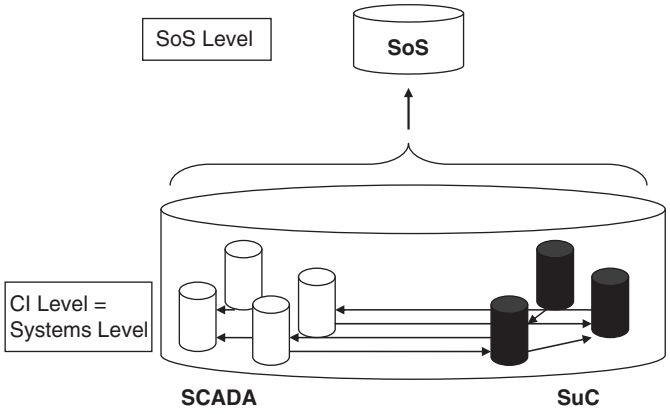

Fig. 4. Model architecture for SCADA and System under Control for an integrated approach.

System or Gas Supply System. For this case our general model is presented in Figs. 4 and 5.

An important question about two main alternative implementations: integrated approach versus coupled approach has to be clarified.

An integrated model contains detailed low level models of (sub)systems as well as a high level model, covering all hierarchical levels. On the other hand, a coupled model aggregates different simulated outputs of the low level models as inputs at a higher level.

As shown in Fig. 4, the a-priori known interdependencies between two systems are modeled directly at low level. The hidden interdependencies will appear during the simulation. System-of-systems level can be understood here as an abstraction that arises through so-called emergence. The CI level is equal to the systems level, because the interaction between two critical infrastructures is modeled directly via low level connections. On this level an analysis of reciprocal impact (e.g. "What is the probability of a blackout, if one transmission line breaks when 10% of the SCADA field devices is down?") can be done. Obviously the integrated model has a big advantage to implement complex emergence behavior in the best, almost "natural" way. Such a model will build the reality in the most appropriate way.

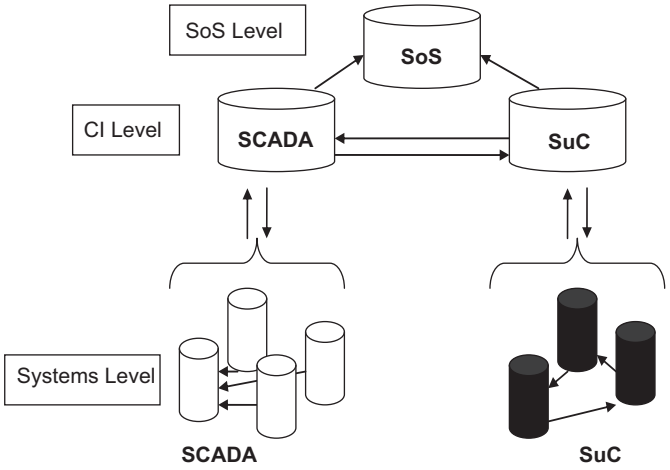

Fig. 5. Model architecture for SCADA and System under Control for a coupled/aggregated approach.

Referring to our previous work, we hypothesize that one of the most appropriated modeling and simulation methods would be the Agent-Based Modeling (or even its modification called the Object-Oriented Modeling) [16].

Agent-based models (ABM) consist of dynamically interacting, rule-based agents [17,18]. ABM has been successfully used in several scientific areas, e.g. economics (supply chain optimization and logistics, consumer behavior, etc.) and informatics (distributed computing, traffic congestion, etc.). Many ABM approaches for modeling and simulation of CI interdependencies, e.g. [19,20] can be found in the literature.

Finally the decision about the best implementation solution depends on the available resources in the broad sense: the integrated model tends to expand to a huge, not transparent formation with extremely long development times [15]. Problems of the data availability to set a great number of model parameters will arise. Very long simulation time and an adequate interpretation of simulation results as well as a nontrivial validation of a model are the unavoidable challenges connected with this approach.

Alternative coupled or aggregated approach requires first a careful decomposition of the given system-of-systems into subsystems, which is a not trivial task due to functional dependencies within the system-of-systems. Other needs encompass reliable interfaces between models, well synchronized simulations of single models due to real-time requirement, clear definition of entry points, aggregation rules, proper emulation of feedback loops, etc.

As can be seen in Fig. 5, by this implementation the systems do not interact at the low level, but CI level is involved. CI level is not equal to systems level in this case, but represents an active interface between the systems. We would say that interdependencies proceed on the CI level first, in contrast to the integrated approach.

Modeling and simulation technique for this approach have to be defined for each single model individually. Particularly for the systems level (low level of the model), ABM seems to be a suitable method. Alternatively a System Dynamics approach can be recommended as well. System Dynamics is a method for studying/understanding the behavior and the underlying structure of a complex system over time and represents a fundamentally interdisciplinary top–down approach [21]. Grounded in the theory of nonlinear dynamics and feedback control, System Dynamics method deals with internal feedback processes (loops) and time delays, which influence the whole system [22]. System Dynamics is widely used in environmental modeling, economics and

analysis of infrastructure interdependencies (e.g. Ref. [23]). This approach is also used in modeling and simulation of critical infrastructure systems (e.g. Ref. [24]).

For models related to CI level (local system-of-systems view) High Level Architecture (HLA) seems to be appropriate. HLA is a general architecture for modeling and simulating complex distributed systems. This technique breaks the entire system down into individually operating subsystems. Communication within a "system-of-systems" is managed by a run time infrastructure that represents a very powerful tool [25,26]. HLA has widely been used in the development of military software systems, as well as in multiplicity fields for computer based tool development. One of the main advantages of the approach is the possibility to couple the already developed and benchmarked tools on the low systems level. A combination with self-developed tools is feasible as well.

As a very first step in the direction of the SCADA and the SuC modeling can be seen the approach [7], where the underlining physical and logical interconnected networks (network connections, segments and main elements) are decomposed, and then the service availability of the interconnected network accounting the availability of each network that supports the service is computed. Three subsystems are modeled: (a) Telco network that connects two control centers of the SCADA system, throughout a HDSL (High bit-rate Digital Subscriber Line) connection, (b) Telco emergency power supply that feeds Telco network at different Telco sites, on loss of main power supply and (c) ACEA power distribution grid that provides the main power supply at different Telco sites. The corresponding methods are (a) Reliability Block Diagrams (RBD), wherein independent failures/repairs are assumed, (b) a states model, based on the Stochastic Activity Networks (SAN), an extension of the Stochastic Petri Nets and (c) Network Reliability Analyzer (NRA), which is based on the Binary Decision Diagrams, also under the assumption of independent failures/repairs mechanisms of any grid elements.

Although the model is very simplified and not able to simulate a dynamic interaction between networks, it is based on traditionally well established methods and can be applied for a validation of a more sophisticated system-of-systems model.

5. M&S methods

Implementing models to assess different characteristics of the analyzed system strongly depends on the parameters that are relevant and the questions to be answered. The applicability of a particular method cannot be evaluated at a general level and addressed without a more detailed framing of the problem.

If we are interested in the stability of the system regarding "hidden vulnerabilities" we would be interested in identifying all possible scenarios where the correct functioning of the system is compromised. A possible approach would be to model all components in an ABM and run the simulation under a variation of parameters to try to find scenarios where the correct functioning of the system is no longer given. Different aspects could be included in the model, such as protocol implementation, entry points, reliability of communication lines, reliability of components in the SuC, etc. This requires an enormous amount of data regarding the components and extremely high computational power. Due to the fact that such models have to handle rare events, an exhaustive analysis cannot be guaranteed.

The data requirements for both cases are very different and none of the two approaches would deliver a complete evaluation by themselves. This fact stresses the importance of selecting the right questions to be addressed by the study and the necessity to correctly identify the variables to be taken into consideration to obtain the desired results.

In cases where detailed information about the components of the system is available and the communication between these elements is known, ABM can provide a platform to model the system from a bottom-up approach and even help to identify hidden vulnerabilities. An exact analysis and understanding of the overall function of the system is not absolutely required and, in many cases, not even practical.

In case of unavailable data regarding the components, but in presence of an overall understanding of the basic principles governing the processes that represent critical infrastructures, a Systems Dynamics approach (as mentioned earlier) can provide useful information. In this case, information about the components (and even their physical implementation) is not required and the model is constructed top–down.

The last case we would like to highlight is when partial simulations are already available (such as the EPS and SCADA). Here an integration, as proposed in the High Level Architecture Approach, could provide a powerful framework to integrate existing (and potentially very powerful) tools.

Studying and analyzing interdependent CIs through M&S approaches always involve the development and integration of multiple simulation components since more than one infrastructure system needs to be considered and more cross-infrastructure analyses need to be conducted. These approaches have been challenged by two major technical difficulties: the lack of performance and the lack simulation interoperability, which are mainly due to the increasing complexity of overall simulation environment, continuous consumption of simulation hardware and increasing demands for more accurate simulation validation. One possible solution for these technical difficulties is to distribute different simulation components that could be domain-specific or sector-specific, so as to make the best use of computational resources, by adopting appropriate simulation standards. While several simulation standards do exist for supporting the simulation component distribution, the most widely implemented and applicable one is the HLA simulation standard [5,27].

As discussed in section 4, HLA is a general purpose high-level simulation architecture/framework to facilitate the interoperability of multiple-types of models and simulations [5]. Originally, HLA was developed under leadership of the U.S. Defense Modeling and Simulation Office (DMSO) in order to support interoperation of simulations, reuse existing simulators for other purposes and reduce the cost/time required to create a synthetic environment for a new purpose [25]. In 2000, HLA was approved as an open standard by the organization of the Institute of Electrical and Electronic Engineers: IEEE Standard 1516-2000 [28]. Since then, the HLA standard has been revised and improved. A functional view of the HLA is given in Fig. 6.

As an open IEEE standard, HLA has been widely implemented for the purpose of conducting research works in the area of CI interdependency study. In 2007, HLA has been considered an interface solution for trying to connect several individual simulators to study interdependencies between heterogeneous interconnected CI [29]. In 2009, a communication middleware serving other distributed CI simulators was created by a team in a EU research project "Design of an Interoperable European federated Simulation network for critical Infrastructures (DIESIS)" [27]. 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).

6. Implementation

HLA is a simulation standard, and not a modeling method. Combining HLA standard with other modeling method(s) as a

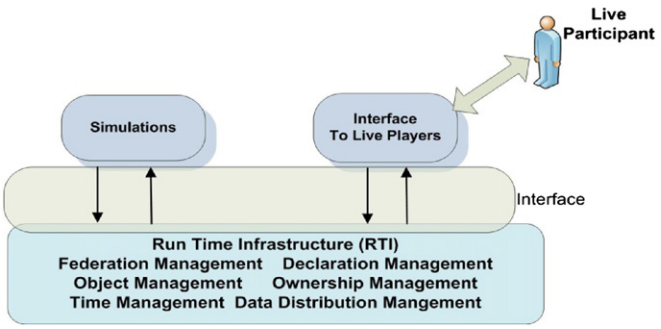

Fig. 6. Functional view of the HLA standard [5].

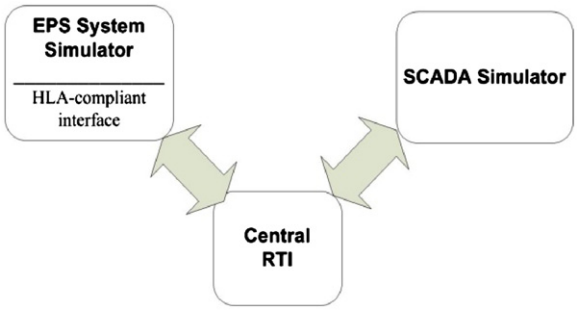

Fig. 7. Architecture of the experimental simulation platform.

hybrid M&S approach can be considered as an applicable method to study interdependent CI. Currently, an HLA-compliant experimental platform, which is part of an ongoing broader-scale project in the area of CI vulnerability and interdependency studies at ETH Zurich, is under development based on the HLA and the ABM for the purpose of studying interdependencies between the SCADA system and the SuC. It should be noted in this experimental platform that the EPS system is used as an example of the SuC. The architecture of this simulation experiment platform is built upon **the coupled approach** of the SOS model architecture, which has been introduced in section 4. The combined approach allows to benefit from M&S potential of the both methods. The ABM is applied at the low level and HLA is used for the communication between two systems. The ABM is capable of exhibiting complex behavior patterns and provides valuable information about the dynamics of its simulated real-world system. The level of details (agents) is flexible and can be defined depending on the task. One of main advantages of the HLA is the possibility to couple the already developed and benchmarked simulation tools that simulate complex distributed systems. The HLA supports the extension of the model through adding more systems or even subsystems to the interface. The weaknesses of this combined approach include the increase in the complexity of overall simulation environment, demands for more accurate validation and requests for more computational resources. More details regarding the structure and introduction of this experimental platform can be found in Refs. [30,31].

Currently, the experimental platform consists of three major simulation components: EPS system simulator, SCADA simulator and Central RTI, which are shown in Fig. 7.

The EPS system simulator is a time-stepped and object-oriented simulator, which has been fully developed using the software of Anylogic 5.5 based on a two-layer object-oriented modeling approach [32]. The SCADA simulator is an event-driven and object-oriented simulator, which is still being developed using the software of Anylogic 6.4. The central RTI acts as the center of the experimental

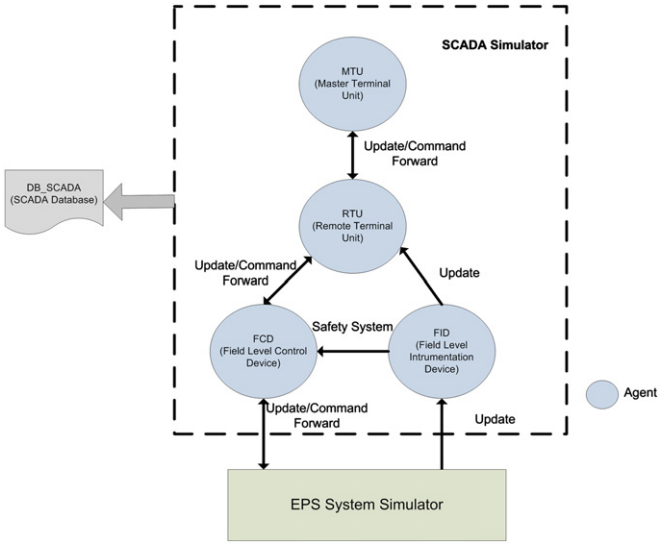

Fig. 8. Simplified model development structure of the experimental simulation platform.

platform and is responsible for simulation synchronization and communication routing between all components.

Fig. 8 illustrates a simplified model development structure of the experimental platform. Four agents, FCD (Field level Control Device), FID (Field level Instrumentation Device), RTU (Remote Terminal Unit) and MTU (Master Terminal Unit), have been designed and developed in the simulator of SCADA for the purpose of modeling fundamental functionalities of the SCADA system and interacting with the EPS system simulator. FCD is an agent representing switch gears such as disconnector and circuit breaker. FID is an agent representing the instrumentation devices such sensors and transducers. The responsibilities of this agent include data acquisition (measured variable value) from SuC, measured variable monitoring and potential alarm determination. In this experimental platform, both FID agent and FCD agent act as the interface between two simulators. DB_SCADA is a Microsoft Access based database that is linked to the SCADA simulator. The purpose of this database is to trace and record sequential events during abnormal operating situation via its real-time SOE (Sequence of Events) table.

To demonstrate the capabilities of this platform for investigating and representing interdependencies between infrastructures or systems, several experiments have been designed and developed, including feasibility experiment and failure propagation experiment, which are summarized below:

- **Feasibility experiment**: the experiment that mainly studies the capability and applicability of the proposed methodology as an approach to represent interdependencies between CI. More details related to this experiment can be found in Ref. [31].
- **Failure propagation experiment**: the experiment that mainly studied the failure propagation between CI due to the interdependencies. During this experiment, single technical failure or even multiple technical failures are triggered in order to observe and study sequent events possibly caused by the failure of propagation.

The summarized investigation results, shown in Table 1, are collected and analyzed based on both feasibility experiment and failure propagation experiment regarding which type of interdependency can be represented through the experimental platform by observing the propagation of different techniques and

Table 1
Investigation results about interdependency representation.

Types of interdependency	**Input**	**Mutual**	**Co-located**	**Shared**	**Exclusive-or**
Is current experimental platform able to represent this type of interdependency ?	Yes	Yes	No	Yes	No
Types of interdependency	**Physical**	**Cyber**	**Geographic**	**Logic**	
Is current experimental platform able to represent this type of interdependency ?	Yes	Yes	No	No	

Table 2
List of sequential events after incorrect calibration modification of PT_i.

Stamped time (s)	**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's correct response to the problem and distribution of algorithm will be taken (MTU)
212.31	Command has been processed by operator successfully, redistribution command has been sent out (MTU)
223.05	Power flow of line(i) decreases (EPS system simulator)

failures of operator. Since the platform is still under development, some types of interdependency will be able to be represented after completing the platform.

Below is a case study demonstrating the propagation of a technique failure due to the input/physical dependency between SCADA system and EPS system through one of the failure propagation experiment. In this case study, FID is the agent representing a power flow transducer (PT_i) measuring the value of transmitted power flow (in unit of MW) of a selected transmission line ($Line_i$) simulated by the EPS system simulator. It is assumed that PT_i is calibrated incorrectly due to aging of piece part of PT_i, which can be considered as a technique failure. Table 2 shows a list of sequential events after the incorrect modification of PT_i's calibration value recorded by the SOE table of table DB_SCADA during the simulation. The stamped time represents the computer time when a specific event is recorded in the SOE table.

As shown in Table 2, at time 52.43 s, PT_i's calibration is modified incorrectly. As a consequence, the output of PT_i is more than the value its measured variable should be. According to this incorrect measured value, RTU generates a wrong transmission overloading alarm to MTU causing the operator in control room to take a wrong decision to redistribute power flow of transmission line(i). As a result, the amount of power transmitted in line(i) decreases, although it should not. The measured variable from PT_i, as part of the EPS system, acts as the physical input to the SCADA system. This relationship can be considered as **the input/physical interdependency**. The failure of PT_i propagates from EPS system to SCADA system and goes back to EPS system is caused by this interdependency.

7. Conclusion

In this approach the mechanisms leading to interdependencies in critical infrastructures are demonstrated by showing that a detailed view of the subsystems in these infrastructures leads to coupling of the different subsystems. This study has extended the seminal work by Rinaldi et al. [11] and allows to characterize the underlying events and components related to the analysis of interdependencies. As has been shown, a closer look at the components that comprise such a complex system, as a complete infrastructure is necessary, not only to capture the behavior but also to provide models that lead to more quantitative simulation results.

Different approaches to model the interdependencies between the SuC (e.g. EPS) and the SCADA system are presented. With the presented approaches, the selection of the most suitable method can be tackled. A first evaluation indicates that the most promising approaches seem to be ABM, HLA and Hybrid Systems, as well as a combination of methods that allow for the flexibility required to model all aspects of interdependencies related to the SCADA and the CI. The first results of the implementation (which is still under development) have confirmed the ability of our approach to investigate interdependencies between the CI.

References

[1] Kotov V. Systems-of-systems as communicating structures, Hewlett Packard Computer Systems Laboratory Paper, HPL-97-124, 1997.
[2] Birolini A. Reliability Engineering Theory and Practice. 5th ed.. Berlin: Springer; 2007.
[3] 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.
[4] Johansson J, Hassel H. An approach for modelling interdependent infrastructures in the context of vulnerability analysis. Reliability Engineering and System Safety 2010;95(12):1335–44.
[5] Pederson P, Dudenhoeffer D, Hartly S, et al. Critical Infrastructure Interdependency Modeling: A Survey of U.S and International Research. Idaho National Laboratory; 2006.
[6] Carreras BA, Lynch VE, Dobson I, et al. Critical points and transitions in an electric power transmission model for cascading failure blackouts. Chaos 2002;12(4):985–94.
[7] Bonanni G, Ciancamerla E, Minichino M, et al. Exploiting stochastic indicators of interdependent infrastructures: the service availability of interconnected networks. Safety, Reliability and Risk Analysis: Theory, Methods and Applications 2009;1–4:2501–9.
[8] Kröger W, Nan C. Vulnerability analysis of interdependent critical infrastructures. Invited contribution to special issue on "Risk Analysis of Critical Infrastructures" of IJRAM, in preparation.
[9] Schläpfer M, Dietz S, Kaegi M. Stress induced degradation dynamics in complex networks. In: Proceedings of the first international conference on infrastructure systems and services: building networks for a brighter future (INFRA 2008). 2008. p. 5.
[10] Schläpfer M, Shapiro JL. Modeling failure propagation in large-scale engineering networks. In: Zhou J, editor. Complex Sciences, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Berlin Heidelberg: Springer; 2009. p. 2127–38.

[11] Rinaldi SM, Peerenboom JP, Kelly TK. Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine 2001;21(6):11–25.
[12] Mendonca D, Wallace WA. Impacts of the 2001 World Trade Center attack on New York City critical infrastructures. Journal of Infrastructure Systems 2006;12(4):260–70.
[13] Jamshidi M. Large-Scale Systems—Modeling and Control. New York, NY: North-Holland Publishing Company; 1983.
[14] DeLaurentis D. Role of humans in complexity of a system-of-systems. In: Duffy VG, editor. Digital Human Modeling. Berlin: Springer-Verlag; 2007. p. 363–71.
[15] Schmitz W, Neubecker KA. Architecture of an Integrated Model Hierarchy, vol. Final Report, ACIP, 2003.
[16] Eusgeld I, Kröger W. Comparative evaluation of modeling and simulation technique for interdependent critical infrastructures. In: Proceedings of the ninth international probabilistic safety assessment conference. Hong Kong, 2008. p. 49–57.
[17] D'Inverno M, Luck M. Understanding Agent System. Berlin: Springer; 2004.
[18] Wooldridge M, Jennings N. Intelligent agents: theory and practice. Knowledge Engineering Review 1995;10(2):115–52.
[19] Barton DC, Stamber KL. An Agent-Based Microsimulation of Critical Infrastructure Systems. 2000.
[20] Panzieri S, Setola R, Ulivi G. An Agent-Based Simulator for Critical Interdependent Infrastructures. In: Proceedings of the conference on securing critical infrastructures. Grenoble, 2004.
[21] Kirkwood CW. System Dynamics Methods: A Quick Introduction. College of Business, Arizona State University; 1998.
[22] Sterman JD. Systems dynamics modeling: tools for learning in a complex world. IEEE Engineering Management Review 2002;30(1):42.
[23] LeClaire RJ, O'Reilly G. Leveraging a high fidelity switched network model to inform system dynamics model of the telecommunications infrastructure. In: Proceedings of the 23rd international conference of the system dynamics society. Boston, 2005.
[24] Conrad SH, LeClaire RJ, O'Reilly GP, et al. Critical national infrastructure reliability modeling and analysis. Bell Labs Technical Journal 2006;11(3):57–71.
[25] Dahmann JS, Fujimoto RM, Weatherly RM. The department of defense high level architecture. In: Proceedings of the 29th conference on winter simulation. Atlanta, Georgia, United States, 1997. p. 142–9.
[26] Seliger G, Krützfeldt D, Lorenz P. On the HLA and Internet Based Coupling Commercial Simulation Tools for Production Networks. Berlin: Technical University of Berlin; 1999.
[27] Gorbil G, Gelenbe E. Design of a mobile agent-based adaptive communication middleware for federations of critical infrastructure simulations. In: Proceedings of the CRITIS, 2009.
[28] IEEE. IEEE Standard for Modeling and Simulation High Level Architecture (HLA)—Framework and Rules. IEEE Std. 1516-2000. 2000. p. i-22.
[29] Duflos S, Diallo AA, Grand GL. An overlay simulator for interdependent critical information infrastructures. In: Proceedings of the 2nd international conference on dependability of computer systems. 2007. p. 27–34.
[30] Eusgeld I, Nan C. Creating a simulation environment for critical infrastructure interdependencies study. In: Proceedings of the IEEE international conference on Industrial Engineering and Engineering Management, IEEM. 2009. p. 2104–8.
[31] Nan C, Eusgeld I. Adopting HLA standard for interdependency study. Reliability Engineering and System Safety 2011;96(1):149–59.
[32] Schläpfer M, Kessler T, Kröger W. Reliability analysis of electric power systems using an object-oriented hybrid modeling approach. In: Proceedings of the 16th power systems computation conference, Glasgow, 2008.