A unified framework for safety and security assessment in critical infrastructures

T. Aoyama, M. Koike, I. Koshijima & Y. Hashimoto
Nagoya Institute of Technology, Japan

Abstract

The appearance of Stuxnet malware changed the idea of security on critical infrastructures greatly. However, in previous studies, cyber security issues have been addressed only from an IT security perspective, with a focus on the detection of malicious activities and the elimination of IT threats. However, these studies missed out the discussion relating to the robustness of the designed plant system. In this research, the relation between information system security and physical plant safety is defined on the basis of a novel framework. This study introduces a preliminary approach which tackles plant safety and security from a more comprehensive point of view. In this context, not only computer security is considered, but also plant availability and robustness. In particular, the presented methodology allows us to understand how unsafe activities and cyber-attacks may propagate throughout the plant system and affect the physical side of the plant.

Keywords: control systems security, plant safety, cyber-terror.

1 Introduction

1.1 Definition of security and safety

The term 'security and safety' are common words which are frequently used in the same context. Their difference, however, is often unclearly stated. Burns *et al.* [1] proposed the following informal definition of the terms safety and security: "A system is not safe if it can harm us; it is not secure if it gives others the means of harming us". Moreover, inside IEC 61508 safety is defined as "Freedom from unacceptable risk ... as a result of damage to property or to the environment [2–4]. In this research, we follow the interpretation given by Furuta *et al*. [5], in

WIT Transactions on The Built Environment, Vol 134, © 2013 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE130071

which safety and security are simultaneously defined on the basis of the intentionality of acts. More precisely, an unsafe status in the plant system could be triggered by two types of acts: unintentional or intentional. The former acts are mainly caused by human errors, such as slips and lapses of the plant operators and are addressed as a safety issue. On the contrary, intentional acts deliberately create violation or sabotage of targeted systems and are considered as a security issue that directly or indirectly links to a certain safety issue.

1.2 Cyber security and safety for critical infrastructures

A violation or sabotage to critical infrastructures can be driven by a physical attack (e.g. disconnection of a cable) or by an indirect attack from the cyberspace and in this paper we focus on the latter. According to the terminology in IEC62443-1-1 [6], cyber security is defined as "actions required to preclude unauthorized use of, denial of service to, modifications to, disclosure of, loss of revenue from, or destruction of critical systems or informational assets". It is important to underline that Information System security and Critical Infrastructures security have different profiles. In Information Systems, the most valuable property is Information, therefore Confidentiality has the highest priority, followed by Integrity and Availability (CIA). On the other hand, failures in Critical Infrastructure threaten public safety and environmental health. Moreover, the failure of services and products can directly cause a loss of profits. Therefore, in the context of Critical Infrastructure, the order of priority changes to AIC, which means that Availability must come first.

2 Problem statement

The reason why IT security approaches are not enough to guarantee Availability, our highest priority, is represented by the fact that a system without vulnerabilities is hard to achieve and new exploit techniques are always available to hackers. Therefore, in order to protect the Availability, we first need to study in detail about Availability robustness. The robustness can be evaluated by assessing the safety and security in the physical side. Accordingly, the connectivity between information systems security and physical infrastructures safety must be clarified in an effective way. To this end, this study proposes a methodology that allows understanding how unsafe activities and cyber-attacks may propagate throughout a critical infrastructure from the IT side to the physical side of the system. In this paper, we focused on modelling of a plant system, which is one of the basic architecture of critical infrastructure.

3 The unified framework

3.1 Plant system decomposition

Devices in a plant system can be decomposed into four categories according to their functionality: plant equipment, field device, control device and office IT

device. Plant equipment is directly involved in the production activity and its usage is mostly limited to its particular function (e.g. tanks, pipes). Field devices are involved in the physical actuation and sensing of the plant equipment (e.g. pump, valve). Control devices are responsible for the control and supervision of the field devices during the production activity (e.g. PLC). The data related to the operation of the plant are gathered and stored in IT servers, which are accessible through the Office IT system, which also supports the intra-office communication. In order to model the interaction between the different components of a plant system, we designed a new framework, inspired by the Open Systems Interconnection (OSI) Reference Model.

3.2 OSI reference model and the unified framework

The original OSI model defines IT network communication protocols by dividing them into seven layers: physical, data-link, network, transport, session, presentation and application layer. These layers were reinterpreted comprehensively, based on the original definition provided by Zimmermann in 1980 [7], in order to include the field equipment, field devices and control devices. This unified framework is necessary to describe the data flow in the plant system. It is important to underline that the concepts of the original OSI model are still used to represent the IT communication protocols of the office IT system.

Detailed explanations of each layer in the unified framework are provided below:

Application layer The application layer provides service applications for the operation of the plant. Some of the entities of this layer allow human operators to manage and supervise the production process (e.g. Operator interface), while other entities communicate with each other in order to control and maintain autonomously the operation of the plant (e.g. loop control program).

Presentation layer The services provided by this layer are supporting the upper layer activities. In particular, it translates information coming from lower layers so that they become meaningful to the application services. For example, supposing that a lower layer entity provides information about temperature in Fahrenheit degrees and an application layer entity requires the same information in form of Celsius degree, the presentation layer handles the translation.

Session layer The session layer models the interaction between presentation entities which are highly interdependent. For example, in the case that those presentation entities such as “Temperature” and “Pressure” are related to a fluid, they must satisfy the law of nature described by the session entity “perfect gas equation of state”.

Transport layer The transport layer entities represent the properties of the information media used in the network layer and they are used to describe and support the equilibrium laws described in the upper layer. In this way, the same transport entity can be used to represent two different materials

of the network layer. For example, the Transport entity "delta-temperature" can be used to characterize both water and gas flow. The prefix delta is used to highlight that these entities are used in the upper layer to define equations representing the natural laws.

Network layer The entities in this layer are the media that support the information flow (e.g. gas stream, water flow).

Data-link layer If a physical connection between devices exists, this doesn't necessarily mean that there is an information flow. In order to model the active flow of a media between devices, we use the Data-link layer. For example, the flow of water from Device 1 to Device 2 and from Device 2 to Device 1 is represented by two different variables. Moreover, if Device 1 and Device 2 are physically connected but there is no flow, then this connection is considered void in the Data-link layer.

Physical layer The physical layer represents the physical connection between devices. Both active and non-active connections must be included in the model. For example if a pipe and a tank are physically connected, but no flow of material exists, their connection is still modelled in the physical layer.

Figure 1 shows the communication flow between Plant equipment and Field devices. This unified framework explains the communication between devices in detail, which is useful for detecting the cause of a failure in a system.

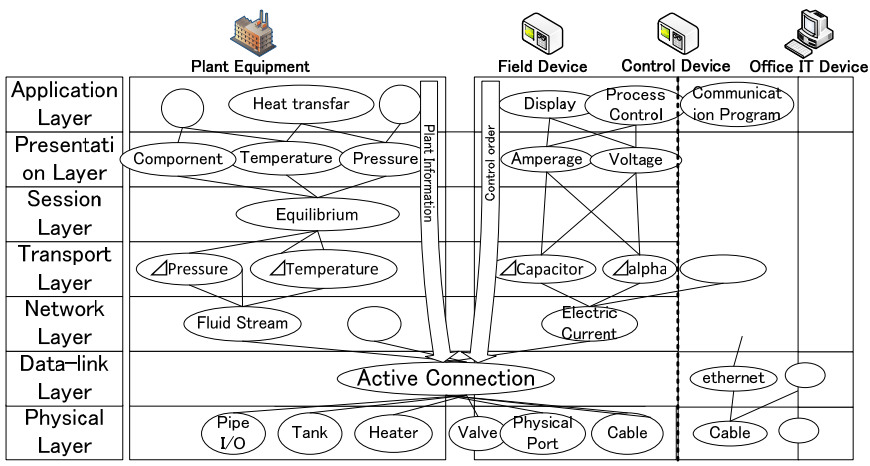


Figure 1: The entire structure in the framework.

4 System implementation based on the framework

One of the goals of this study is to design a unified framework for the modeling of the plant network so that safety and security could be assessed in a unique domain. Still, connectivity scheme obtained from the proposed unified model requires a suitable visualization.

4.1 Model implementation into DSM

The DSM (Design Structure Matrix) [8] can be used as a networking model to embody the idea of the unified framework. By applying the DSM paradigm, it is possible to visualize all the available paths in the overall system. In particular, the focus is on possible horizontal inter-device connections at each layer of the unified framework. On the other hand there is no need to analyze the vertical communication between layers because it is mainly caused in an intra-device activity. As a result, connectivity matrices for each layer are designed in seven matrices. Also, as one of the extended usage of DSM, the reachability from one node to the other can be calculated. According to the unified framework, physical connectivity is considered as the universal protocol in the physical layer. Therefore, the physical static structure of the entire plant system is represented by the static DSM of the first layer. On the other hand, unlike the first layer, for each of the layers from the second to the seventh (upper layers), the DSM represents the information flow. For this reason, it is possible to describe the vectors of the protocol flow by the input-output relationship of the dynamic DSM. By using this approach, each upper layer contains fragments of the entire information flow. These upper layers matrices are used for finding information linkages.

4.2 Safety and security assessment methodology

At this point, the plant risk analysis based on the DSM obtained from the unified framework is presented. The achieved model was used to perform two types of risk analysis: FTA (Fault Tree Analysis) and HAZOP (hazard and operability study). The FTA is used for assessing system vulnerabilities based on a priori knowledge, while the HAZOP is used for potential danger which is not known in advance, nor predictable. By combining both methodologies, event probability of both external fault and internal fault could be achieved.

4.2.1 Adapting HAZOP to the unified framework

In corresponding context of the presented unified framework, a HAZOP parameter is equivalent to unique media (e.g. water flow) supporting each entity in the layers of the framework. Therefore, since the DSM represents the input-output relationship between two devices at a given layer, HAZOP analysis can be applied to each cell of each DSM matrix of the model. The process of eliciting HAZOP deviations from the DSM is shown in Figure 2 and explained below.

1. **To generate the fundamental DSM**: As previously mentioned, the DSM which is plotted by the first layers linkage shows the physical structure of the entire network. From this DSM the fundamental information for generating HAZOP deviations is obtained.
2. **To select the parameters:** Devices of a system have HAZOP parameters representing their features. These parameters can be found according to the profile of the devices in the perspective of the framework, so that the found parameters are added to columns. For example, the heater has the

parameters "temperature" in Presentation Layer and "electric flow" in Network Layer. The combination of devices and parameters are plotted so as to form multi domain matrix (MDM) beneath the DSM.

3. **To connect the parameters and guide words:** Guide words are defined as "word or phrase which expresses and defines a specific type of deviation from an element's design intent" [9]. Their role is to stimulate imaginative thinking, to focus the study and to elicit ideas and discussion, thereby maximizing the chances of study completeness. Here, all possible combinations of the guide words and parameters is plotted so as to form a matrix next to the generated MDM. Since the relation between HAZOP parameters and the guide words does not change, this matrix is a universal matrix, and is independent from the DSM generated from the objective network.
4. **To elicit the deviation:** By combining the parameters and the guide words, causes of deviation from the design intent can be found [10] (e.g. Higher-Temperature, Lower-Temperature). At this point also, the device element should also be combined (e.g. Heater – High – Temperature, Tank – Higher – Temperature). In this way, all the possible deviations in a given network are elicited.

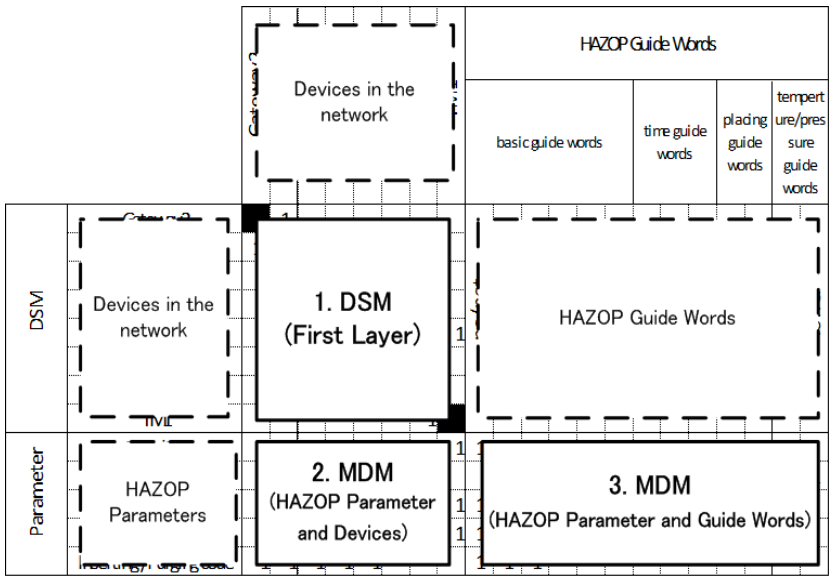


Figure 2: The process for eliciting HAZOP deviations from the DSM.

For instance, from the point of view of security, packets, which are media of IT protocols, can be treated as HAZOP parameters. In this case, by applying the guide words (e.g. "More – Quantitative increase" [11]), security issues might be highlighted (e.g. buffer overflow). It should be noted that according to the basic idea of layering, each layer adds value to services provided by the set of lower

layers in such a way that from the highest layer set of services is offered as to run distributed applications. Thus, the layering divides the total problem into small pieces [7]. Therefore, the HAZOP analysis should be applied in detail to each layer, in order to specifically locate a cause of an anomaly.

4.2.2 To apply FTA to the unified framework

The FTA analysis is adopted to perform a risk analysis on the basis of a provided framework. In particular, the determination of a device contributing to an event is derived easily by tracing back reachable paths from the DSM of the unified framework. This is because, in this context, the contribution to an event is considered as a reachability matter. The reachable paths enable systematic and logical determination of all contributors to a particular event.

As the contributors to the critical event are found from the reachable paths, the lower-level event related to the contributors should be analyzed to identify realistic causes. At this point the HAZOP analysis can be performed easily. The parameter of a selected contributor is derived from the framework, and then, by combining HAZOP guide words with the parameter, potential deviations are specified. Their causes are categorized in human errors, equipment failure, and external events, from the perspective of cyber security.

5 Illustrative example

In this section, a part of our cyber security testbed is analysed as an example (pictures of the testbed in Figure 3). In 2012, a testbed for ICS security was developed in the Nagoya Institute of Technology (NIT). The design of the specifications of the testbed is based on the requirements of those who are concerned with control systems security (e.g. vendors, researchers, users etc.).

From the requirement analysis, the purpose of the testbed was decided as follows:

a. **Training for gaining public awareness:** the testbed will be used as an educational training tool, in order to show the importance of cyber security and the threat of cyber attacks.
b. **Intrusion detection:** the testbed is used to test the intrusion detection tool under development.
c. **Improvement of plant resiliency:** data obtained from the testbed by simulating plant operation will be analysed, for the research on the effectiveness of security and safety measures.

From this testbed, the example work only focuses on a simple control process which is illustrated in Figure 4. In detail, the temperature information of Tank 1 is sensed by TM1, and the data is gathered to a controller (“UT35A (TC1)”). At this point, the controller uses the temperature information in order to send a command to a heater. The controller communicates with an OPC data server and the information of the operation is stored in the server. Meanwhile, a human operator will observe and handle the operation using SCADA. The gateway is not directly connected to the Internet; however it is connected to the office area, which is in turn connected.

(a) (b)

Figure 3: The plant side (a) and the operator side (b) of the testbed.

Devices and applications used in this control process are listed below;

- M-SYSTEM SCADALINXpro OPC DA2.0 on WindowsXP Professional SP2 as OPC data server (OPC1)
- M-SYSTEM SCADALINXpro on WindowsXP Professional SP2 as SCADA system (SCADA1)
- Yokogawa UT35A/UT32A Digital Indicating Controllers as controller (UT35A (TC1)).

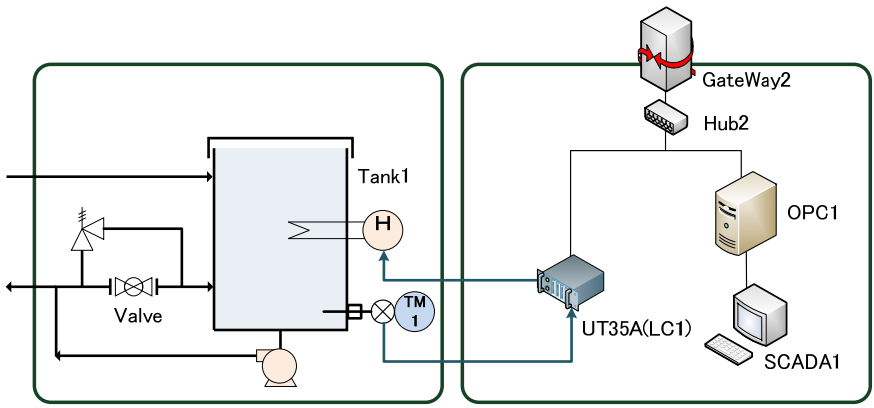


Figure 4: Part of the control process through the testbed.

A given network is translated into a DSM of the first layer (Figure 5). The matrix is sequenced to form two sequences; an information system area and a plant system area. It is noted that the controller ("UT35A (TC1)") is functioning as a connector between the two areas.

		1	2	3	4	5	6	7	8
		Gateway2	Hub1	OPC1	SCADA1	UT32A(TC1)	Heater	Tank1	TM1
1	Gateway2		1						
2	Hub1	1		1		1			
3	OPC1		1		1				
4	SCADA1			1					
5	UT32A(TC1)		1				1		
6	Heater							1	
7	Tank1								1
8	TM1					1			

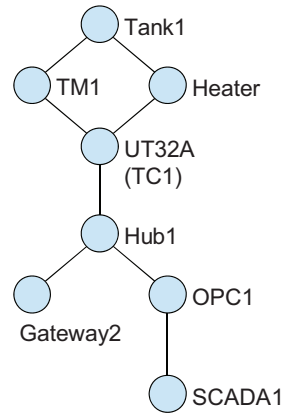


Figure 5: DSM of the first layer, and its translation into the digraph to identify the flow of contributors.

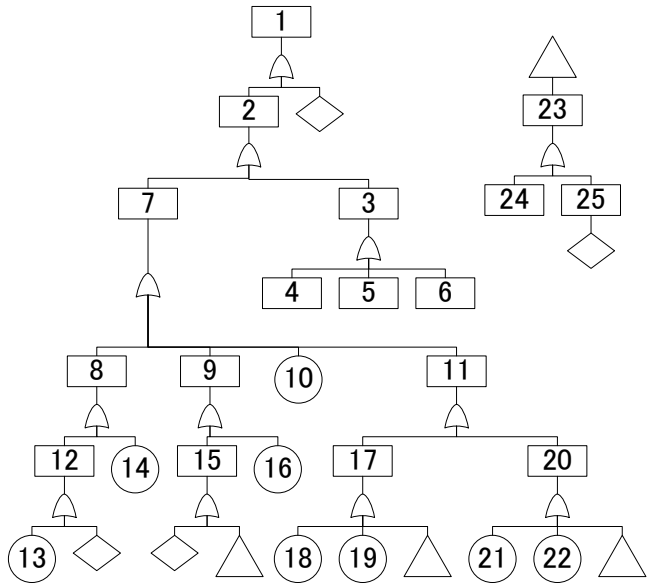
As previously mentioned, the reachability path is found in the DSM by applying the FTA. In this way, elements to be analysed due to a potential effect can be detected easily. For instance, the DSM can be visualized as a simple digraph as shown in Figure 5, which explains reachability to the Tank 1. In this way, the contributors to the event are defined.

		Gateway2	Hub2	OPC1	SCADA	UT32A(TC1)	H	Tank1	TM1	HAZOP Guide Words												
										basic guide words						time guide words			placing guide words		temperature pressure guide	
DSM	Gateway2		1							no/not	more	less	part of	reverse	other than	sooner	later	other than	where else	other than	higher	lower
	Hub2	1		1		1																
	OPC1		1		1																	
	SCADA			1																		
	UT32A(TC1)		1						1													
	H					1																
	Tank1						1															
	TM1							1														
Parameter	Sampling					1			1	1		1					1		1			
	temperature						1	1								1	1				1	1
	electric flow	1	1	1	1	1	1		1	1	1	1		1		1	1		1			
	protocol flow	1	1	1	1	1			1	1	1	1		1		1	1		1			
	Inserting code	1	1	1	1	1				1	1	1										

Figure 6: Determine HAZOP deviations by applying HAZOP Guide Words on DSM.

As the next step, a cause of a top event (failure) should be defined. To this end, the MDM introduced in the previous chapter is generated (Figure 6).

Possible HAZOP deviations of the contributor are added beneath the contributing events, as lower level contributing events. As a result a fault tree is generated in the way explaining the intrusion path of a cyber attack to the system (Figure 7).



No.	*Fault Event Name*	9	Failure in Program	18	Operator Human Error
1	Overheating in Tank1	10	UT32A Mechanical Failure	19	Protocol Failure
2	Failure/ Deviation in Heater	11	Deviation in Program parameter	20	Failure/ Deviation in SCADA
3	Heater Mechanical Failure	12	Failure/ Deviation in Sampling	21	Protocol Failure
4	Higher Temperture	13	Sensor Mechanical Failure	22	Operator Human Error
5	Longer Heating	14	TM1 Mechanical Failure	23	Malicious code executed
6	Stronger Heating	15	Program Overwritten	24	Physically Incerted
7	Failure/ Deviation in UT32A	16	Missprograming	25	Infected via network
8	Failure/ Deviation in TM1	17	Failure/ Deviation in OPC1		

Figure 7: HAZOP based FTA generated from the control process path.

6 Concluding remarks

The authors just take the very first step of a research towards the combination of safety and cyber security in plant systems. Through this research, we proposed a framework for applying a uniform analysis method for safety and security simultaneously. The research was, although, limited to theoretical study due to in sufficient amount of real-world data to practically assess SIL (Safety Integrity Level) and SAL (Security Assurance Level) using the FTA. This is caused by the difficulty in collecting data of incidents in cyber crimes, since disclosure of a

certain data tends to be avoided. Therefore, future works will be devoted at filling the gap between our present theoretical study and its possible applications in real infrastructures. The presented framework is an attempt to provide a comprehensive and general methodology for retrieving risk information related to a critical infrastructure. This could be beneficial for organizations and companies in their decision making process, which must include risk control.

Acknowledgement

This research was partially supported by the Ministry of Education, Science, Sports and Culture, Grant-in-Aid for Scientific Research (B), No. 24310119 (2012) and (B), No. 25282101 (2013).

References

[1] A. Burns, J. McDermid, and J. Dobson. On the meaning of safety and security. The Computer Journal, 35(1):3–15, 1992.
[2] IEC 61511-1-1: 2003: Functional safety – safety instrumented systems for the process industry sector – part 1-1: Framework, definitions, system, hardware and software requirements, Jan 2003.
[3] IEC 61508 – functional safety of electrical / electronic / programmable electronic safety-related systems (7 parts). Available as BS IEC 61508 from BSI, Milton Keynes, UK, or from the IEC, Geneva (www.iec.ch).
[4] DHS. National cyber incident response plan. Draft, September 2010.
[5] K. Furuta, S. Nagasaki, Introduction to Safety, Nikkagiren, 2007 (in Japanese).
[6] IEC/TS 62443-1-1: 2009: Industrial communication networks – network and system security – part 1-1: Terminology, concepts and models, July 2009.
[7] H. Zimmermann. OSI reference model – the ISO model of architecture for open systems interconnection. Communications, IEEE Transactions on, 28(4):425–432, 1980.
[8] S.D. Eppinger and T.R. Browning. Design Structure Matrix Methods and Applications. Engineering Systems. MIT Press, 2012.
[9] International Electrotechnical Commission *et al*. IEC 61882. Hazard and Operability Studies, (HAZOP Studies) Application Guide, 2001.
[10] International Electrotechnical Commission *et al*. IEC 60050-191 International Electrotechnical vocabulary. International Electrotechnical Commission, Geneva, 1990.
[11] G. Baradits and J. Abonyi. A new software-based HAZOP study development methodology. In 8th International Symposium of Hungarian Researchers, November, pages 15–17, 2007.