Application of V-model on Safety and Security for Developing Digital I&C Systems

Jiye Jeong [a,b], Gyunyoung Heo [b*]
[a]*Doosan Heavy Industries & Construction Co., Nuclear I&C Dept., 37, Samsung 1-ro 5-gil, Hwaseong-si, Gyeonggi-do 18449, Republic of Korea*
[b]*Department of Nuclear Engineering, Kyung Hee University, 1732 Deogyeong-daero, Giheung-gu, Yongin-si, Gyeonggi-do 17104, Republic of Korea*
[*]*Corresponding author: gheo@khu.ac.kr*

1. Introduction

Utilities are replacing equipment and upgrading certain instrumentation and control (I&C) systems due to obsolescence, increasing maintenance costs, and the lack of qualified spare parts for the equipment and components in operating nuclear power plants (NPPs). These activities generally involve changing from analog to digital technology [1]. Therefore, cyber security concerns have inevitably become as important as safety.

Safety and security are two risk-driven activities that are traditionally tackled separately. It is thus possible to distinguish two communities, each working on their own standards, organizing their own conferences, publishing in their own journals. Since the 9/11 attacks on the Twin Towers in the Aeronautics domain and the discovery of the Stuxnet computer worm in the industrial control systems domain in June 2010 as shown in Figure 1, it is more recognized worldwide that both engineering specialties should be integrated in a more organized manner [2].

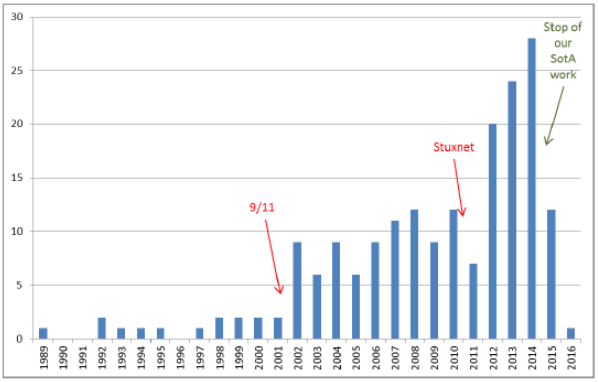

Figure 1. Number of safety and security co-engineering related research publication per year

Similarly, in designing critical systems in an NPP, security and safety are not totally independent. For example, a security threat could trigger an initiating event of a safety hazard, which result in increased risk. Figure 2 shows a motivational example to illustrate how a security threat can initiate a hazard related to a safety component and finally result in a system failure [3]. A security threat source implanted in an operational or control processor exploits a vulnerability in the plant-level network, such as not checking the source of messages sent on the network. By masquerading a signal to indicate that the water level of the Condensate Storage Tank (CST) is too low, a security attack could be successfully initiated. The signal is sent to the Visual Display Units (VDU) first, and then an operator in the main control room triggers another signal via the network to close a valve for water flooding. If the masqueraded signal is sent continuously to the VDU, then a stuck-at-close hazard will occur at the valve [3].

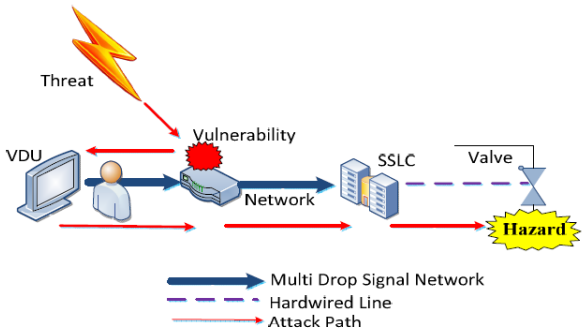

Figure 2. Threat attack initiates hazard occurrences

So, the purpose of this paper is to attempt to bridge the gap between safety and security by using the software verification model, V-model for developing digital I&C systems in an NPP. So far, the V-model has been used to evaluate the completeness, correctness, consistency and accuracy for safety. Therefore, it was focused on the way of considering and accommodating the security on V-model.

2. Safety and Security

Safety and security are quite similar from the fact that they deal with risk. According to ISO31004, risk is defined as “the effect of uncertainty on objectives, regardless of the domain or circumstances, therefore an event or a hazard (or any other risk source) should not be described as a risk. Risk should be described as the combination of the likelihood of an event (or hazard or source of risk) and its consequence.” [4] Normally, security is concerned with the risk originating from the environment and potentially impacting the system, whereas safety deals with the risk arising from the system and potentially impacting the environment. This means that safety considers hazards that focus on how the system may harm the environment due to system failure

and security considers threats that focus on how potential attacks may impact the system's assets and its operation due to vulnerability [5, 6]. According to Figure 3, the concept of hazards, threats and failures is associated with some parts of a total system. Hazard means that a potential source of harm (IEC 2008), threat is the potential cause of an incident which may result in harm to a system or organization (ISO, 2005), and failure is a termination of the ability of a functional unit to provide a required function or operation of functional unit in any way other that as required (IEC, 2008) [7]. So, as approaching to the I&C system in an NPP, it is necessary to figure out hazards and threats to make failures.

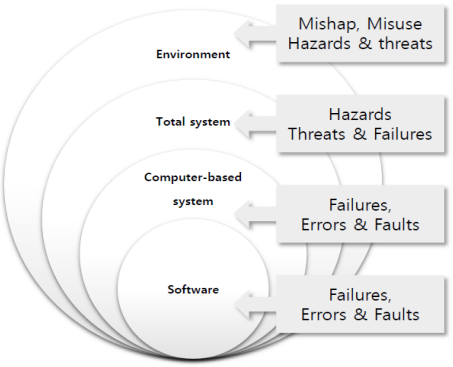

Figure 3. Comparing risk identification for safety and security

3. V-model for Digital I&C Systems

The V-model is one of the efficient methods of evaluating the quality for software. In addition, it is benefited to improve the verification and validation (V&V) process and to appraise the software development processes and products [8]. The V&V process is the steps of checking that a software system meets specifications and that it fulfills its intended purpose. The V-model has been selected for designing digital I&C of Korean NPPs as a V&V tool. The V-model consists of seven phases described Table 1. This would be a reference standard to apply V-model on safety and security in the next section.

4. V-model on Safety and Security

Authors analyzed the cyber security activities at each phase of V-model in a previous study [10]. Based on the activities, the life cycle, V-model for safety and security was developed in this section.

Table 1. Summary of V&V activities of V-model

Phase	Description
Concept	Define the features, constraints and goals with the users.
Requirement	Define how the systems work by identifying input data, processing contents and output data.
Design	Logically determine how to perform the function defined in previous phase. From this phase, the V&V process should be divided into hardware and software.
Implementation	Draw for outline and assembly in detail, and purchase components for hardware. Coding for the control and monitoring software.
Testing	This step is to improve the completeness by finding out errors and whether the developed system meets the requirements. The test range should begin with small and gradually widens such as unit tests, module tests and integrated system tests.
Installation	After installing the system in the field, check that there is no abnormality by test run.
Operation & Maintenance	This period is after commercial operation and the longest in the software life cycle. If the systems should be revised, the previous phases must be implemented.

Firstly, the security measures, which are recommend by the Korean regulatory guides, were connected to each phase of V-model. The security measures incorporate technical security measures, operational security measures, and management security measures. The fifty cyber security measures were selected, which could directly affect system design. The others were mostly related to policies or periodic activities of audit or secure operation environment during development of systems. Moreover, during installation phase and operation & maintenance phase, the activities of cyber security were not related to develop the cyber security systems.

And then, the relationship between safety and security was investigated on the basis of the V-model framework with the security measures shown as Figure 4. This way is to improve the overall area of safety and security for evaluating and ensuring the safety of digital I&C systems basically.

The detailed processes of mapping the V-model with safety and security can be summarized: In view of system design, security and safety risk assessment should be analyzed in the concept phase. As the definition of safety and security as described in section 2, hazard analysis for safety requirements and threats analysis for security requirements are conducted in the concept phase. Figure 4 shows the process of the analysis in an abstract level.

The output of each phase should be validated with cyber security measurements described in Figure 4. This means that these measurements were checked during validation process.

Moreover, the output should be tested as expending the scope for verification such as unit test, module test and integration test.

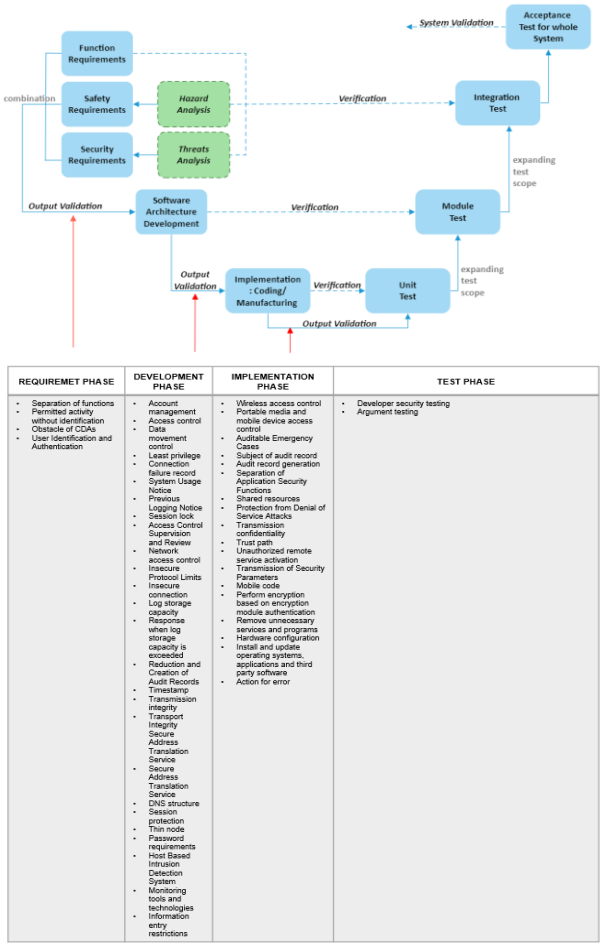

Figure 4. Process of risk analysis for safety and security

As it is possible to verify the output of each stage of the development lifecycle when the successful implementation of the input stage is achieved, this could be a structural and systematic model incorporating the phase of the development of digital I&C systems.

5. Conclusions

Safety and security aspects are currently often evaluated independently using separate assessments and specific methods that are performed by specialized experts at different system design phases in accordance with recognized security and safety standards [11]. As the degree of complexity and interconnection among systems have increased, it is important to make balance between safety and security. This means that it should be developed in a way that avoids contradictory situations of safety and security requirements and can evaluate the system for accident systems even if such a situation occurs.

Sharing such motivation, this study attempted to suggest a kind of design processes to system developers or software designers for digital I&C systems. When the V-model applies to an NPP, it is necessary to consider all the specific details, including the interference of various I&C properties and the characteristics of all technologies used. Also, this should be done in both top-down and down-up way because NPP I&C systems consist of interactions based on different technologies with different functions.

Acknowledgement

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIP: Ministry of Science, ICT and Future Planning) (No. 2017M2B2B1072806) and the Korea Institute of Energy Technology Evaluation and Planning(KETEP) and the Ministry of Trade, Industry & Energy(MOTIE) of the Republic of Korea (No. 20171510102100).

REFERENCES

[1] M. Chiramal. Application of commercial-grade digital equipment in nuclear power plant safety systems, Proceedings 20th IEEE Symposium on Reliable Distributed Systems

[2] Merge safety & security(ITEA (Information Technology for European Advancement), Recommendations for Security and Safety Co-engineering (Release 3).

[3] Yean-Ru Chen, Sao-Jie Chen, Hsin Chou, Pao-Ann Hsiung. Unified Security and Safety Risk Assessment -A Case Study on Nuclear Power Plant, 2014 International Conference on Trustworthy Systems and their Applications

[4] Risk management - guidance for the implementation of ISO 31000. ISO/TR31004:2013

[5] Siwar Kriaa, Ludovic Pietre, Marc Bouissou, Yoran Halgand. A survey of approaches combining safety and security for industrial control systems, Reliability Engineering and System Safety 139(2015)156–178

[6] Kornecki A, Liu M. Fault tree analysis for safety/security verification in aviation software. Electronics 2013;2(1):41–56.

[7] Christian Raspotnig, Andres Opdahl. Compareing risk identification techniques for safety and security requirements. (Jan 2013)

[8] Peng-Fei Gu, Zhe-Ming Liu, Hui-Hui Liang, Wei-Hua Chen, and Feng Gao. Evaluation Measures About Software V&V of the Safety Digital I&C System in Nuclear Power Plant

[9] T. Novak, A. Gerstinger. Safety- and Security-Critical Services in Building Automation and Control Systems. IEEE Trans. Ind. Electron., vol. 57, no. 11, pp. 3614 - 3621, 2010

[10] Jiye Jeong, Gyunyoung Heo. Cyber Security Evaluation for Nuclear I&C Systems Corresponding to V-Model, Transactions of the Korean Nuclear Society Spring Meeting Jeju, Korea, July 9-10, 2020

[11] Nikolaos Papakonstantinou. Early Hybrid Safety and Security Risk Assessment Based on Interdisciplinary Dependency Models, VTT Technical Research Centre of Finland