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.

[b]Department of Nuclear Engineering, Kyung Hee University

**gheo@khu.ac.kr*

Introduction

- Motivation

- The use of digital technology for I&C systems of nuclear power plants (NPPs) and research reactors has been increased.
- As cyber security concerns have become as important as safety, the number of safety and security co-engineering has been increased.

- Objective

- It attempts 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.

Methods and Results

1. Safety and Security

- Safety and Security are similar in terms of dealing with **risk** which is possible to bring system failure.
  → 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).
- Safety considers **hazards**
  → Focus on how the system may harm the environment due to system failure.
  → Hazard means that a potential source of harm (IEC 2008).
- Security considers **threats**
  → Focus on how potential attacks may impact the system's assets and its operation due to vulnerability.
  → Threat is the potential cause of an incident which may result in harm to a system or organi:

2. V-model for Digital I&C Systems

- V-model: One of Verification and Validation (V&V) models (Figure 1).
  Safety-related software of nuclear I&C systems should be required for the V&V process to impr safety and reliability. The V&V process is the process of checking that a software system meets specification and that it fulfills its intended purpose.

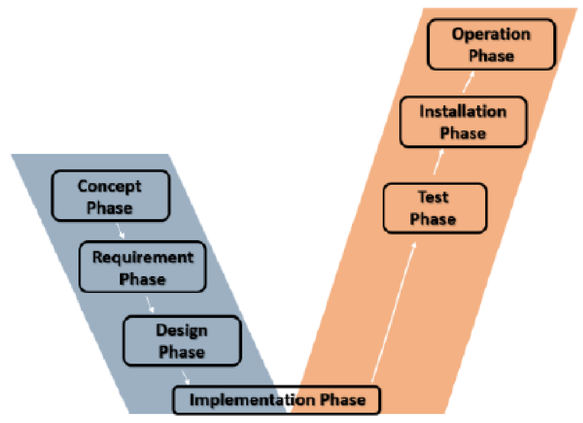
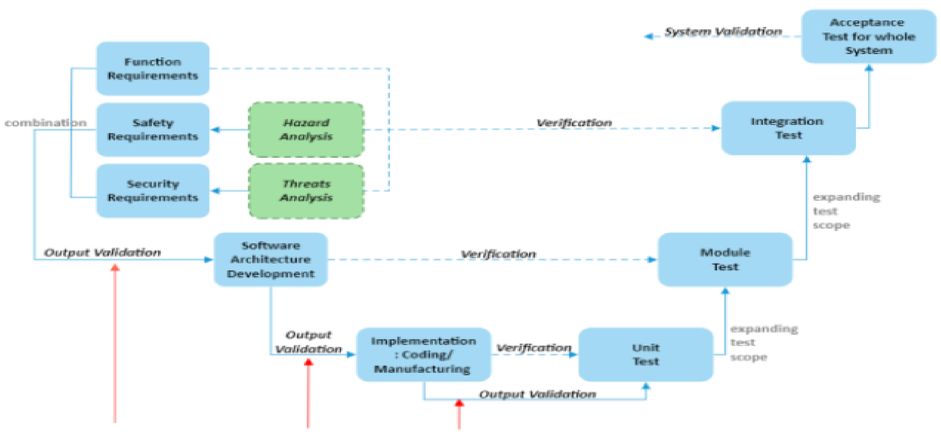


Figure 1. V-model of NPP I&C System



REQUIREMET PHASE	DEVELOPMENT PHASE	IMPLEMENTATION PHASE	TEST PHASE
• Separation of functions • Permitted activity without identification • Obstacle of CDAs • User Identification and Authentication	• Account management • Access control • Data movement control • Least privilege • Connection failure record • System Usage Notice • Previous Logging Notice • Session lock • Access Control Supervision and Review • Network access control • Insecure Protocol Limits • Insecure connection • Log storage capacity • Response when log storage capacity is exceeded • Reduction and Creation of Audit Records • Timestamp • Transmission integrity • Transport Integrity Secure Address Translation Service • Secure Address Translation Service • DNS structure • Session protection • Thin node • Password requirements • Host Based Intrusion Detection System • Monitoring tools and technologies • Information entry restrictions	• Wireless access control • Portable media and mobile device access control • Auditable Emergency Cases • Subject of audit record • Audit record generation • Separation of Application Security Functions • Shared resources • Protection from Denial of Service Attacks • Transmission confidentiality • Trust path • Unauthorized remote service activation • Transmission of Security Parameters • Mobile code • Perform encryption based on encryption module authentication • Remove unnecessary services and programs • Hardware configuration • Install and update operating systems, applications and third party software • Action for error	• Developer security testing • Argument testing

Figure 2. Process of risk analysis for safety and security

3. V-model on Safety and Security

- 50 of 101 security measures which related to V-model for design are selected.
- Relationship between safety and security was investigated on the basis of the V-model framework with the security measures.
- Figure 2 : The detailed processes of mapping the V-model with safety and security. Also it can be used as basic data as it describes safety and security to be considered when designing with nuclear digital I&C.
  - ✓ The output of each phase should be validated with cyber security measurements which means that these measurements were checked during validation process.
  - ✓ After analyzing the cyber vulnerability in the requirements stage, it is important to qualify cyber security according to the analysis.
  - ✓ In addition, it can be seen that it is important to confirm that safety and security are satisfied through a phased test of the system.
  - ✓ Furthermore, as the impact of the requirements stage is large, the designer should invest the most time in the life cycle of the V model to make detailed cybersecurity requirements through vulnerability analysis. These activities can reduce design confusion and errors later in the design phase.

Conclusion

- As the degree of complexity and interconnection among systems have increased, it is important to make balance between safety and security.
- This model 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.

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)