Advancing Software V&V for European and Domestic System V&V Compliance

Dongil Lee [a*], Han Gyu Kim [a]
[a]*KHNP, Central Research Institute, 70, 1312-gil, Yuseong-daero, Yuseong-gu, Daejeon, 34101, South Korea*
[*]Corresponding author: diturtle@khnp.co.kr

***Keywords : Software V&V, System V&V, IEC, IEEE**

1. Introduction

In modern high-reliability industries such as nuclear power plant (NPP), aviation, and railway, software has evolved beyond simple control functions to become a critical factor determining the safety and performance of the entire system. Consequently, there is a growing emphasis on System Verification and Validation (V&V), which encompasses not only the verification of isolated software modules but also their interactions with hardware and the overall system. This paper examines the future direction of conventional Software V&V to meet the System V&V requirements of both European and domestic markets. In particular, it proposes a harmonized approach integrating IEC 61508, the international standard for functional safety, and IEEE 1012-2012, the standard for system, software, and hardware V&V.

2. Domestic Status of Software V&V

Currently, the domestic software V&V is predominantly focused on the software development life cycle (SDLC). While high levels of achievement have been made in ensuring Software Quality Assurance (SQA) refer to the American Society of Mechanical Engineers (ASME) Nuclear Quality Assurance-1 (NQA-1), there remains a gap regarding the 'system-level safety function' demanded by global markets, including Europe. The bidirectional traceability management—where system requirements are allocated to software and hardware, and then integrated and verified—along with a systematized integrated verification process, is still in a stage that requires structural refinement [1].

3. Trends in System V&V: IEEE and IEC Technical Standards

The global market already evaluates safety from a unified system perspective rather than separating software and hardware. In high-reliability sectors, this unified approach is increasingly mandated by regulatory bodies to ensure that complex architectures operate without critical failures.

3.1.IEC 61508

This standard defines the safety lifecycle of the entire system and requires the system to possess the capability to avoid and control faults based on the Safety Integrity Level (SIL) derived from hazard analysis. It provides stringent guidelines for managing both random hardware failures and systematic software failures. For instance, achieving stringent targets such as SIL 3 and SIL 4 in safety-critical nuclear power plant systems requires comprehensive adherence to this safety framework to guarantee functional safety [2].

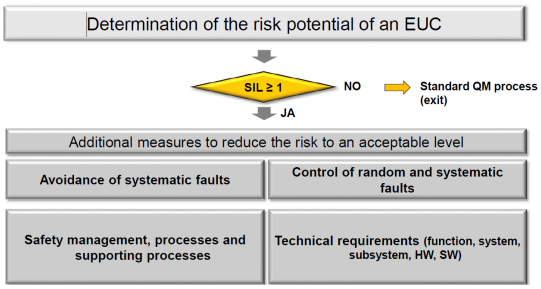


Fig. 1. Risk Reduction Framework in IEC 61508

3.2.IEEE 1012-2012

This standard expands the scope of traditional software V&V to include system and hardware domains. It mandates specific V&V activities for the system, software, and hardware according to their Integrity Levels, explicitly requiring strict management of interactions and traceability among these elements. By establishing distinct, independent verification tasks across the entire development lifecycle, it ensures that every allocated requirement is rigorously tested and validated [3].

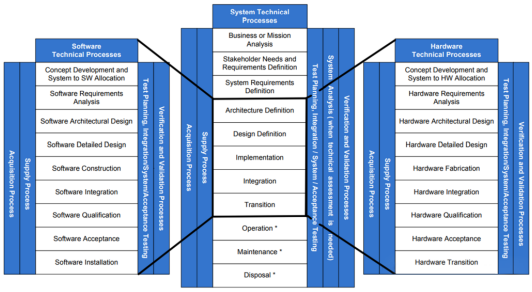


Fig. 2. System, Software, and Hardware V&V Life Cycle Processes in IEEE 1012-2012

These two standards are highly complementary. While IEC 61508 provides a comprehensive safety framework defining 'what' must be achieved (safety goals and SIL), IEEE 1012-2012 offers the practical methodology on 'how' to verify it (specific V&V activities and deliverables).

Furthermore, the practical application of these harmonized standards often intersects with domain-specific regulatory frameworks, such as the USNRC Regulatory Guides, which increasingly emphasize rigorous lifecycle verification processes. To establish a robust software platform for safety-critical systems, it is essential to seamlessly map the integrity levels of IEEE 1012 to the corresponding IEC 61508 SILs.

4. Preparation for Applying System V&V

To comply with European and domestic System V&V regulations through the harmonization of these standards, the following preparations are essential.

First, the integration of the entire lifecycle from requirements to integration testing is necessary. Recognizing the differing development cycles of software and hardware, organizations must design system-level integration verification points at key milestones.

Second, organizations must establish a consistent integrated verification process and deliverable guidelines by mapping the SIL ratings of IEC 61508 to the Integrity Levels of IEEE 1012.

5. Conclusions

While past V&V efforts focused on preventing malfunctions in unit software, future V&V must focus on proving that the entire system can achieve its safety objectives. For domestic industries to meet the system V&V demands of the global market, including Europe, they must combine the rigorous safety lifecycle management of IEC 61508 with the integrated V&V execution methodologies of IEEE 1012-2012. To achieve this, it is essential to secure verification capabilities based on a system architecture that encompasses both software and hardware.

REFERENCES

[1] ISO/IEC/IEEE 12207, Systems and software engineering — Software life cycle processes, 2017.
[2] IEC 61508, Functional Safety of Electrical / Electronic / Programmable Electronic Safety-related Systems, 2010.
[3] IEEE Std 1012, IEEE Standard for System, Software, and Hardware Verification and Validation, 2012.