Comparison of Hazard Analysis Requirements for Instrumentation and Control System of Nuclear Power Plants

Jang Soo Lee[1] and Jun Beom Yoo[2]

1. I&C.HF Division, KAERI, Daejeon, Korea (jslee@kaeri.re.kr)
2. Department of Computer Science, KonKuk University, Seoul, Korea (jbyoo@konkuk.ac.kr)

Abstract: A hazard, in general, is defined as "potential for harm." In this paper, the scope of "harm" is limited to the loss of a safety function in a Nuclear Power Plant (NPP). The Hazard Analysis (HA) of an Instrumentation and Control (I&C) systems is to identify the relationship from the logical faults, error, and failure of I&C systems to the physical harm of the nuclear power plant, and also to find the impact of the external hazard, e.g., tsunami, of the nuclear power plant to the I&C systems. This paper includes the survey of the existing hazard analysis requirements in the nuclear industries. The purpose of the paper is to compare the HA requirements in various international standards in unclear domain, specifically the safety requirements and guidance for the instrumentation and control system for the nuclear power plant from IAEA, IEC, IEEE, and NRC.

Keyword: I&C, Hazard Analysis

1 Introduction

1.1 What is the HA of I&C systems?

A hazard, in general, is defined as "potential for harm." In this paper, the scope of "harm" is limited to the loss of a safety function in an Nuclear Power Plant (NPP).

Hazards analysis (HA), a systems engineering activity, is the application of systematic and replicable methods to identify hazards, their potential adverse effects, their causes, and the changes in system concept or safety requirements needed to meet the overall safety goals of the system.[11]

Although the term "hazard analysis" has been used in many ways in various other publications, in this paper the scope of HA is limited to identify all internal hazards of I&C systems leading to the loss of safety functions of the NPP.

The Hazard Analysis (HA) of an Instrumentation and Control (I&C) systems is to identify the relationship from the logical faults, error, and failure of I&C systems to the physical harm of the nuclear power plant, and also to find the impact of the external hazard, e.g., tsunami, of the nuclear power plant to the I&C systems.

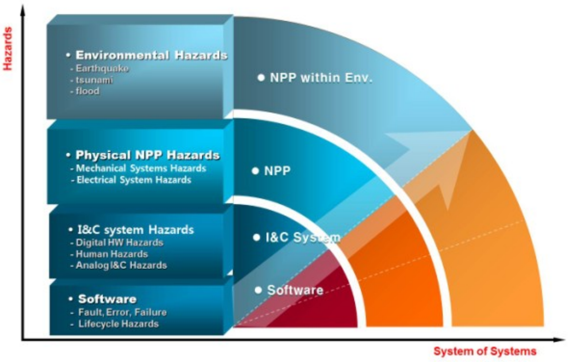

Figure 1. Internal or External Hazards

1.2 Why HA?

The purpose of HA should be

1. To identify the hazard and the contributory hazards of I&C systems of system (SoS).
2. To validate the safety of system, software, hardware, and human through the lifecycle.
3. To provide the solutions for the elimination, control, and mitigation of the hazards.

1.3 How to HA?

There are two sides of HA of I&C systems, one is the performance of the HA and the other side is the evaluation of the HA. The acceptability of HA should be decided through the evaluation of the HA.

There must be a harmonized HA method of System of Systems(SoS), that is, we should decide how deeply conduct the HA of SoS.

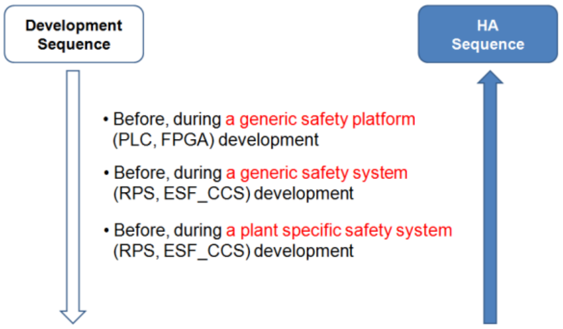
Development Sequence
HA Sequence
• Before, during a generic safety platform (PLC, FPGA) development
• Before, during a generic safety system (RPS, ESF_CCS) development
• Before, during a plant specific safety system (RPS, ESF_CCS) development

Figure 2. When HA should be started?

2. Comparison criteria of HA requirements in the safety industries

Table 1. Comparison Criteria

	Comparison criteria of HA requirements	**HA requirements in the safety standard (Example)**
1	Safety principles (safety model or safety culture)	Nuclear: High energy and radiation release → Protection model Car, Train: High speed on ground → Safe stop model Aircraft: Fly-by-wire → Fail safe model
2	Safety processes	
3	Definition of HA	There must be a definition for: Accident, Harm, Hazard, Failure, Safety, Security,… Hazard Analysis, Hazard Identification Risk Analysis(Assessment), Threat Analysis Reliability, Availability Maintainability, Safety (RAMS) + Security = Dependability Safety Assessment Internal and external hazards Safety Analysis vs. Hazard Analysis Hazard Analysis vs. Failure Analysis Hazard Analysis could be to identify the relationship from faults, error, and failures to harm
4	Purpose of HA	To define the Safety Requirements? To identify the hazard and the contributory hazards of I&C system of systems (SoS). To validate the safety of system, software, hardware, and human through the lifecycle? To provide the solutions for the elimination, control, and mitigation of the hazards.
5	Method of HA	What is the practical HA method and techniques? Maturity of methods? How to measure the acceptability of HA?
6	HA process	When HA should be started, conducted, and finished? When HA of COTS components?
7	Independence of HA (HA organization)	
8	Harmonized HA of SoS	How much HA of SoS?
9	Relationship with other requirements (security, reliability)	Harmonized HA with security and risk analysis? Security Out-to-In Hazard of System External hazard Safety In-to-Out Hazard of System Internal hazard Top-down Analysis Reliability Bottom-up Analysis
10	Discussion (Challenges)	Harmonization of HA requirements for I&C systems, software, hardware, and human HA of SoS HA of COTS products Harmonization of security, safety and reliability requirements for I&C systems What HA should be done according to the safety level?

3 Status of Hazard Analysis Requirements and Guidance for Nuclear Industry

3.1 IAEA Safety Requirements SSR-2/1: Design Safety of NPP

Table 2. Hazard Analysis in IAEA Safety Requirements SSR-2/1

	Comparison criteria of HA requirements	HA requirements in the safety standard (IAEA SSR-2/1: Design Safety of NPP)
1	Safety principles (safety model or safety culture)	**Requirement 17:** Internal and external hazards All foreseeable internal hazards and external hazards, including the potential for human induced events directly or indirectly to affect the safety of the nuclear power plant, shall be identified and their effects shall be evaluated. Hazards shall be considered for determination of the postulated initiating events and generated loadings for use in the design of relevant items important to safety for the plant.
2	Safety processes	None
3	Definition of HA	**Internal hazards** **5.16.** The design shall take due account of internal hazards such as fire, explosion, flooding, missile generation, collapse of structures and falling objects, pipe whip, jet impact and release of fluid from failed systems or from other installations on the site. Appropriate features for prevention and mitigation shall be provided to ensure that safety is not compromised. **External hazards7** **5.17.** The design shall include due consideration of those natural and human induced external events (i.e. events of origin external to the plant) that have been identified in the site evaluation process. Natural external events shall be addressed, including meteorological, hydrological, geological and seismic events. Human induced external events arising from nearby industries and transport routes shall be addressed. In the short term, the safety of the plant shall not be permitted to be dependent on the availability of off-site services such as electricity supply and fire fighting services. The design shall take due account of site specific conditions to determine the maximum delay time by which off-site services need to be available.
4	Purpose of HA	None
5	Method of HA	None
6	HA process	None
7	Independence of HA (HA organization)	None
8	Harmonized HA of SoS	None
9	Relationship with other requirements (security, reliability)	None
10	Discussion	

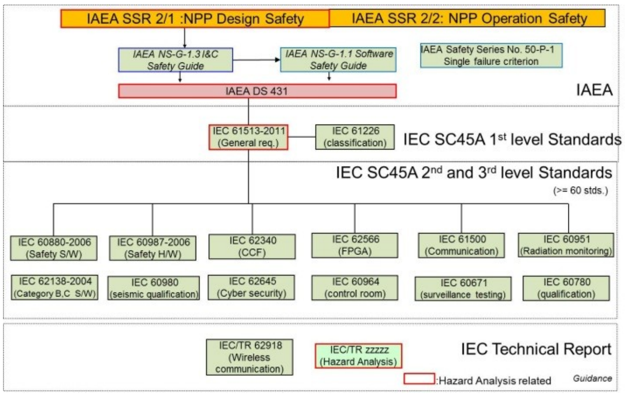
IAEA SSR 2/1 :NPP Design Safety
IAEA SSR 2/2: NPP Operation Safety
IAEA NS-G-1.3 I&C Safety Guide
IAEA NS-G-1.1 Software Safety Guide
IAEA Safety Series No. 50-P-1 Single failure criterion
IAEA DS 431
IAEA
IEC 61513-2011 (General req.)
IEC 61226 (classification)
IEC SC45A 1st level Standards
IEC SC45A 2nd and 3rd level Standards
(>= 60 stds.)
IEC 60880-2006 (Safety S/W)
IEC 60987-2006 (Safety H/W)
IEC 62340 (CCF)
IEC 62566 (FPGA)
IEC 61500 (Communication)
IEC 60951 (Radiation monitoring)
IEC 62138-2004 (Category B,C S/W)
IEC 60980 (seismic qualification)
IEC 62645 (Cyber security)
IEC 60964 (control room)
IEC 60671 (surveillance testing)
IEC 60780 (qualification)
IEC/TR 62918 (Wireless communication)
IEC/TR zzzzz (Hazard Analysis)
IEC Technical Report
:Hazard Analysis related
Guidance

Figure 3. IAEA-IEC Framework of I&C

3.2 IAEA DS 431(Draft) recommendations for I&C system hazard Analysis

Table 3. HA requirements in IAEA DS 431

	Comparison criteria of HA requirements	HA requirements in the safety standard (IAEA DS 431)
1	Safety principles	**2.56.** For the overall I&C

	(safety model or safety culture)	architecture, hazard analysis should be performed to identify conditions that might compromise the defense-in-depth strategy of the plant design. **2.57.** For safety systems, hazards analyses should be performed to identify conditions that might defeat their safety function.
2	Safety processes	None
3	Definition of HA	None
4	Purpose of HA	None
5	Method of HA	**2.58.** Hazards to be considered include internal hazards and external hazards, failures of plant equipment, and I&C failures or spurious operation due to hardware failure or to software errors. **2.59.** I&C system hazard analysis should consider all plant states and operating modes, including transitions between operating modes.
6	HA process	**2.60.** The initial results of the I&C system hazard analysis should be available before the design basis for the overall I&C is completed. **2.61.** The hazard analysis should be updated during the design of the overall I&C architecture, and during the specification of requirements, design, implementation, installation and modification of safety systems. **2.62.** The intent of updating the hazard analysis is to identify hazards that may be caused by specific characteristics of I&C safety systems, by interaction between I&C safety systems and the plant, and by interaction of I&C safety systems with other I&C systems regardless of their safety classification. **2.63.** Measures should be taken to eliminate, avoid, or mitigate the consequences of identified hazards that can defeat safety system functions. **2.64.** Measures to eliminate, avoid, or mitigate the effects of hazards might, for example, take the form of changes to the I&C requirements, design, or implementation or changes to the plant design. **2.65.** The hazard analysis methods should be appropriate for the item being analysed.
7	Independence of HA (HA organization)	None
8	Harmonized HA of SoS	None
9	Relationship with other requirements (security, reliability)	7.105. The failure modes of computer security features and the effects of these failure modes on I&C functions should be known, documented, and considered in system hazard analyses.
	Discussion	TBD

3.3 IEEE 603 requirements for I&C system hazard Analysis

Table 4. HA requirements in IEEE Standard 603-2009

	Comparison criteria of HA requirements	**HA requirements in the safety standard (IEEE Standard 603-2009)**
1	Safety principles (safety model or safety culture)	to protect the public health and safety by functioning to mitigate the consequences of design basis events. Top level safety system design basis related to hazard analysis (interpretation of the abstract requirements in IEEE 603-2009 by NRC experts): h) The conditions having the potential for functional degradation of safety system performance and for which provisions shall be incorporated to retain the capability for performing the safety functions (e.g., missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non-safety-related systems).

2	Safety processes	There is not any prescriptive safety analysis process.
3	Definition of HA	There is not definition of HA, but there are requirements to document the safety system design basis in section 4 of IEEE 603.
9	Relationship with other requirements (security, reliability)	Section 4: i) The methods to be used to determine that the reliability of the safety system design is appropriate for each safety system design and any qualitative or quantitative reliability goals that may be imposed on the system design. The performance of a probabilistic assessment of the safety systems may be used to demonstrate that certain postulated failures need not be considered in the application of the criterion. A probabilistic assessment is intended to eliminate consideration of events and failures that are not credible; it shall not be used in lieu of the single-failure criterion. IEEE Std 352-1987 and IEEE Std 577-2004 provide guidance for reliability analysis. Where reasonable indication exists that a design that meets the single-failure criterion may not satisfy all the reliability requirements specified in Clause 4 item i) of the design basis, a probabilistic assessment of the safety system shall be performed. The assessment shall not be limited to single failures. If the assessment shows that the design basis requirements are not met, design features shall be provided or corrective modifications shall be made to ensure that the system meets the specified reliability requirements.
10	Discussion	There are the functional and design requirements to accomplish the safety function in IEEE 603-2009. In order to meet the single-failure criteria and the common cause failure criteria in section 5 of IEEE 603-2009, there must be some analysis like a failure analysis or a hazard analysis. The failures to meet the safety system criteria in section 5 could cause harm by not accomplishing the safety function. There are many questions about IEEE 603-2009: Where is HA of Electrical System? Where is HA of Analog I&C? What's difference between Hazard analysis and Failure analysis by single-failure criterion and CCF criteria?

3.4 IEEE7-4.3.2-2010 requirements for computer based I&C system hazard Analysis

Table 5. HA requirements in IEEE7-4.3.2-2010

	Comparison criteria of HA requirements	**HA requirements in the safety standard (IEEE7-4.3.2-2010)**
1	Safety principles(safety model, safety culture)	HA to meet "5.5.1 Design for computer integrity" requirement The computer shall be designed to perform its safety function when subjected to conditions, external or internal, that have significant potential for defeating the safety function.
2	Safety processes	All initial plant level hazards and safety goal of NPP are already identified.
3	Definition of HA	**3.1.18 hazard:** A condition that is a prerequisite to an accident. Hazards include external events as well as conditions internal to computer hardware or software. (*different definition from IEC 61513 of internal hazard) **3.1.19 hazard analysis:** A process that explores and identifies conditions that are not identified by the normal design review and testing process. The scope of hazard analysis extends beyond

		plant design basis events by including abnormal events and plant operations with degraded equipment and plant systems. Hazard analysis focuses on system failure mechanisms rather than verifying correct system operation. (*different scope from IEC hazard) **3.1.22 safe state:** A state in which potential hazards and operational risks are minimized.
4	Purpose of HA	Appendix D The purpose of a hazard analysis is to explore and identify conditions that are not identified by the normal design review and testing process.
5	Method of HA	None
6	HA process	Annex D. Identification and Resolution of Hazards in each phase of the system lifecycle
7	Independence of HA (HA organization)	None
8	Harmonized HA of SoS	None
9	Relationship with other requirements (security, reliability)	**5.17.1.6 Evaluate computer security** COTS items to be used in safety systems shall provide computer security features as required by 5.9 of this standard. The dedicating entity shall perform an evaluation of the computer security risks and hazards associated with this system, including impacts on hardware, software, interfaces to other systems, and life cycle documentation, as well as plant procedures for the COTS items and the interfacing systems.
10	Discussion	(Question) Why there are not HA requirements in main content of 7-4.3.2? (Answer) in appendix D.2 Discussion **5.5.1 Design for computer integrity** The computer shall be designed to perform its safety function when subjected to conditions, external or internal, that have significant potential for defeating the safety function. (Question) (conditions, external or internal) means hazard? (There are some requirements of HA for COTS. And there is detail HA in Appendix D.) **5.17.1.1 Document the system safety function risks and hazards** **5.17.1.3 Identify the safety function(s) the COTS item shall perform** Appendix D **D.4.5 Evaluation of hazards in previously developed systems** **(**The guidelines of D.4.3 and D.4.4 should be applied to the extent possible,…) **is not clear.** **D.4.7 Preliminary hazard analysis questions** **D.4.2.2 Planning** One may encounter resistance to hazard analyses at the beginning of system development stemming from a desire to keep development costs as low as possible. Real and identifiable hazards do not exist at the start of the design process, so justifying or assigning resources to the hazard analysis process can be difficult to quantify or justify. However, as discussed in D.4.2.1 above, there are significant advantages to incorporating hazard identification into the normal design process early on.

3.5 IEEE 1228-1994 requirements for I&C software hazard Analysis

Table 6. HA requirements in IEEE 1228-1994

	Comparison criteria of HA requirements	HA requirements in IEEE 1228-1994 (TBD)
1	Safety principles (safety model or safety culture)	
2	Safety processes	
3	Definition of HA	Accident: An unplanned event or series of events that results in

		death, injury, illness, environmental damage, or damage to or loss of equipment or property Risk: A measure that combines both the likelihood that a system hazard will cause an accident and the severity of that accident Software Hazard: A software condition that is a prerequisite to an accident System hazard: A system condition that is a prerequisite to an accident Software Safety: Freedom from software hazards System Safety: Freedom from System hazards

3.6 IEEE 1012-2012 requirements for system hazard Analysis

There are requirements for hazard analysis for the system, hardware, and software of SIL level 3 and 4 through lifecycle in IEEE 1012-2012.

Table 7. HA requirements in IEEE 1012-2012 (TBD)

	Comparison criteria of HA requirements	HA requirements in IEEE 1012-2012
1	Safety principles (safety model or safety culture)	TBD
2	Safety processes	TBD
3	Definition of HA	hazard: (A) An intrinsic property or condition that has the potential to cause harm or damage. (B) A source of potential harm or a situation with a potential for harm in terms of human injury, damage to health, property, or the environment, or some combination of these. NOTE—For (A), see ISO/IEC/IEEE 24765-2010 [B19]. hazard identification: The process of recognizing that a hazard exists and defining its characteristics. NOTE—For (A), see ISO/IEC/IEEE 24765-2010 [B19].
9	Relationship with other requirements (security, reliability)	Annex J (informative) Hazard, security, and risk analyses
10	Discussion	

3.7 HA Guidance of US NRC

We surveyed the two draft guidance for the hazard analysis from US Nuclear Regulatory Commission (NRC), Draft of Design Specific Review Standard (DSRS) and Draft RESEARCH INFORMATION LETTER (RIL) 1101.

Table 8. DSRS APPENDIX A. Hazard Analysis

	Comparison criteria of HA requirements	**HA requirements in the safety standard (US NRC DSRS FOR mPowerTM iPWR DESIGN Appendix A, Hazard Analysis)**
1	Safety principles (safety model or safety culture)	None
2	Safety processes	None
3	Definition of HA	A hazard analysis (HA) is a process for examining an instrumentation and control (I&C) system throughout its development lifecycle to identify hazards (i.e., factors and causes), and system requirements1 and constraints to eliminate, prevent, or control them.
4	Purpose of HA	to evaluate HAs
5	Method of HA	**B. HA Information to be reviewed** Not different the requirements in 7-4.3.2 … 7. Internal hazards that could be generated by the I&C system. For example, excessive load or demand on resources by the I&C system, such as electric power overload due to a short circuit or communication bus overload. 8. External hazards such as disruption in I&C system conditions and physical conditions in the environment that may impair a safety function, e.g.: 8.1. Water intrusion. 8.2. Uncontrolled transfer of energy into the system. Such energy may take various forms, e.g.: heat; light; vibration; radiation; electromagnetic radiation. …

		C. HA Information to be considered for Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) I&C systems development process contributory hazards Software-related contributory hazards
6	HA process	HA is iterative and should be performed at every phase in the system development lifecycle to identify new hazards that could arise as the design is implemented in software and hardware.
8	Harmonized HA of SoS	None
9	Relationship with other requirements (security, reliability)	None
10	Discussion	TBD

Table 9. Research Information Letter of HA review (US NRC RIL 1101)

	Comparison criteria of HA requirements	**HA requirements in the safety standard (US NRC RIL 1101)**
1	Safety principles(safety model, safety culture)	Contributory Hazard, systemic cause are focusing on the process HA, not product HA.
2	Safety processes	None
3	Definition of HA	**Hazard** Potential for harm **Contributory hazard** Factor contributing to potential for harm. AviationGlossary.com, “Contributory Hazard,” <http://aviationglossary.com/aviation-safety-terms/contributory-hazard/>, October 15, 2012. Hazard analysis (HA) is the process of examining a system throughout its lifecycle to identify inherent hazards and contributory hazards, and requirements and constraints to eliminate, prevent, or control them. “Hazard identification” part of HA includes the identification of losses (harm) of concern.
10	Discussion	Contributory Hazard, systemic cause, dependency are tightly related with the design process. So it looks design analysis or V&V. If the concept of contributory hazard from FAA system safety handbook, the concept of it in RIL1101 looks too much expanded to systemic cause of the development process. “Deviations are malfunctions, degradation, errors, failures, faults, and system anomalies. They are unsafe conditions and/or acts with the potential for harm. These are termed *contributory hazards* in this FAA System Safety Handbook. ”

4 Harmonization of HA requirements for I&C system of systems (SoS), software, hardware, and human

Hazard analysis process for I&C systems should be integrated with I&C system development process. Hazard analysis should support and drive the activities related to system development by evaluating the functions and the design of I&C system and its parts (i.e. subsystems, elements including software and hardware) to identify the hazardous/failure conditions, and requirements to address those conditions.

For an integrated system constituting several parts as well as several interfaces to the environment (i.e. other systems including humans), an integrated hazard analysis process is important to identify hazardous conditions, establish appropriate requirements, identify integrity levels, apportion requirements and integrity levels to the parts of the system, and identify lower-level conditions related to the parts of the systems causing the system-level conditions. Due to the iterative nature of the development process, the changes made to the functions and design of the system can introduce new hazardous conditions. Therefore, at each phase of development lifecycle, the respective product or the result of the phase should be analyzed to identify new hazardous conditions, and new or derived requirements to address the conditions. Such a hazard analysis performed throughout the system development lifecycle is required to ensure that the system as a whole achieves the overall safety objectives. Moreover, hazard analysis is fundamental to demonstration of safety of the system, by providing the required evidence on the achievement of overall system safety.

There should be a clear description of the activities related to hazard analysis, input information for each activity, and the deliverable output. The communication, i.e. information flow, between the activities of hazard analysis and system development should be clearly defined. It should be planned (probably described through a safety or qualification plan) how hazard analysis activities along with the system development activities provide evidence to the demonstration of system safety.

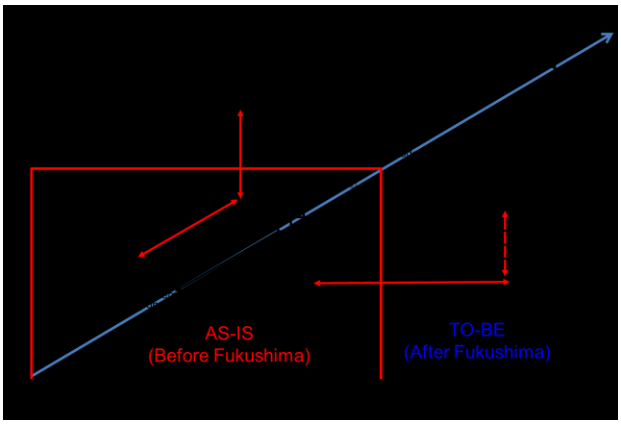

Figure 4. Harmonization of HA requirements for I&C system of systems

5 HA Requirements harmonized with security and reliability requirements for I&C systems

Security requirements are similar to safety requirements, as they state what or how to avoid unwanted behavior or aspects of a system. Whereas safety is concerned with avoiding hazards leading to accidental harm, security is about considering responses to threats in order to avoid intentional harm. Accidental and intentional harm can both be damage and injury to *humans*, *property* or the *environment*, in which case safety and security will be closely related.[12]

A hazard analysis process for an I&C system resembles the threat analysis process that have to be undertaken for the same system. In both cases the system has to be examined through the complete lifecycle in order to identify potential harm (hazards and threats) and their causes (both inherent and contributory), in order to identify requirements and constrains to eliminate, prevent or control the potential harm. These requirements and constraints can either be related to each other, e.g., in conflict, reinforcing or dependent on each other, or unrelated. If related, it is important to analyze them and resolve conflicts or take advantage of reinforcement.

As the processes of hazard analysis and threat analysis can be closely related, it is of importance to align them. Both processes should be integrated with the I&C system development process, and they are then likely to have overlapping activities during the various phases of the development lifecycle. The overlap can be related to stakeholders involved in analysis, the product that is subject to the analysis, techniques and tools used, or the resulting outcome of a phase. Some of the activities from the hazard and threat analysis might be performed sequentially or even combined.

Reliability requirements are describing a system's ability to function correct under certain conditions for a certain time. This is related to hazard analysis requirements, as certain functions of a system are critical to safety and can lead to hazardous events if not functioning correct under the given conditions at a given time period.

6 Plan for the New Standard for Hazard Analysis of I&C for NPP

A hazard analysis (HA) is a process for examining an instrumentation and control (I&C) system throughout its development lifecycle to identify hazards (i.e., factors and causes), and system requirements1 and constraints to eliminate, prevent, or control them. Hazard analyses examine safety related I&C systems, subsystems, and components, their interrelationships and their interactions with other systems, subsystems, and components to identify unintended or unwanted I&C system operation including the impairment or loss of the ability to perform a safety function.[10]
A hazard analysis shall provide a consistent, comprehensive, and systematic way to address the potential hazards associated with the I&C systems in a unified framework.[10] In the IEC Technical Report,

we will propose the following HA requirements for the I&C safety systems

- HA requirements for the digital I&C systems
- HA requirements for the analog I&C systems
- HA requirements for the digital I&C platform, component, device, and equipment
- HA requirements for the analog I&C platform, component, device, and equipment
- HA of electrical systems
- HA of I&C system by external systems hazards and environmental hazards

7 Conclusion

We surveyed the status on the hazard analysis requirements for the instrumentation and control(I&C) systems important to safety in nuclear industry.

The hazard analysis(HA) requirements in IAEA, IEC, IEEE standards for the nuclear industry, and the HA recommendation in US NRC guidance have been compared by the nine comparison criteria, the safety principle, safety process, definitions, purposes, methods, HA process, independence of HA, HA of system of systems, harmonized requirements among safety, security, and reliability.

Acknowledgement

This research was supported, in part, by a grant from the Korea Ministry of Science, ICT and Future Planning, under the development of the integrated framework of I&C dependability assessment, sustainable monitoring, and emergency response for nuclear facilities.

References

[1] IAEA Safety Standards, Safety of Nuclear Power Plants: Design, Specific Safety Requirements No. SSR-2/1. 2012.

[2] IAEA Safety Standards, Draft Safety Guide, DS-431, "Design of Instrumentation and Control Systems for Nuclear Power Plants," 2013.

[3] IEEE Standard 603-2009, "IEEE standard criteria for safety systems for nuclear power generating stations" 2009.

[4] IEEE Standard 7-4.3.2-2010, "IEEE standard criteria for Digital Computers in safety systems for nuclear power generating stations" 2010.

[5] IEC 61508, "Functional Safety of electrical/ electronic/ programmable electronic safety-related systems, Part1: General requirements," 2010.

[6] IEC 60880 Ed. 2.0 "Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions," 2006.

[7] IEC 60987 Ed. 2.0 "Nuclear power plants - Instrumentation and control important to safety - Hardware design requirements for computer-based systems," 2007.

[8] IEC 61226 Ed. 3.0 "Nuclear power plants - Instrumentation and control important to safety - Classification of instrumentation and control functions," 2009.

[9] IEC 61513 Ed. 2.0 "Nuclear power plants - Instrumentation and control important to safety - General requirements for systems," 2011.

[10] Draft of Design Specific Review Standard, Appendix A. Hazard Analysis, US NRC, 2014.

[11] Draft RESEARCH INFORMATION LETTER (RIL) 1101: Technical basis to review hazard analysis of digital safety systems, US NRC, August, 2013.

[12] Christian Raspotnig, Andreas Opdahl, "Comparing risk identification techniques for safety and security requirements," The Journal of Systems and Software, Vol 86, pp. 1124– 1151, 2013.