Comparison of Hazard Analysis Requirements of I&C

Jang-Soo Lee

August 26, 2014

ISOFIC

KAERI 한국원자력연구원 Korea Atomic Energy Research Institute

Contents

- Introduction
- Comparison of hazard analysis requirements in nuclear industry
    - IAEA-IEC framework, NRC-IEEE framework
- Challenges and Proposals of HA
- Conclusion

Accidents vs. Hazards

Ship Accident (Ferry Sewol)

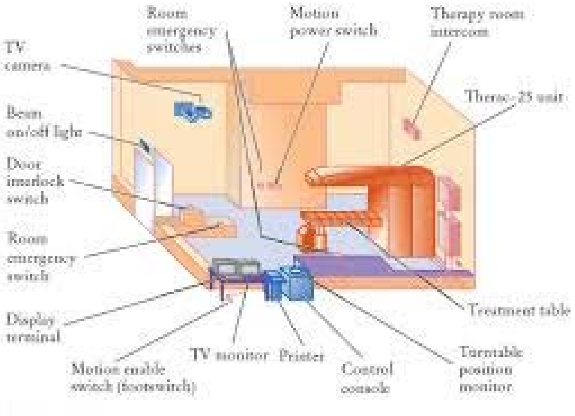


Figure 9 Typical Therac-25 Facility

Medical Device Accident (Therac-25)

NPP Accident (Fukushima)

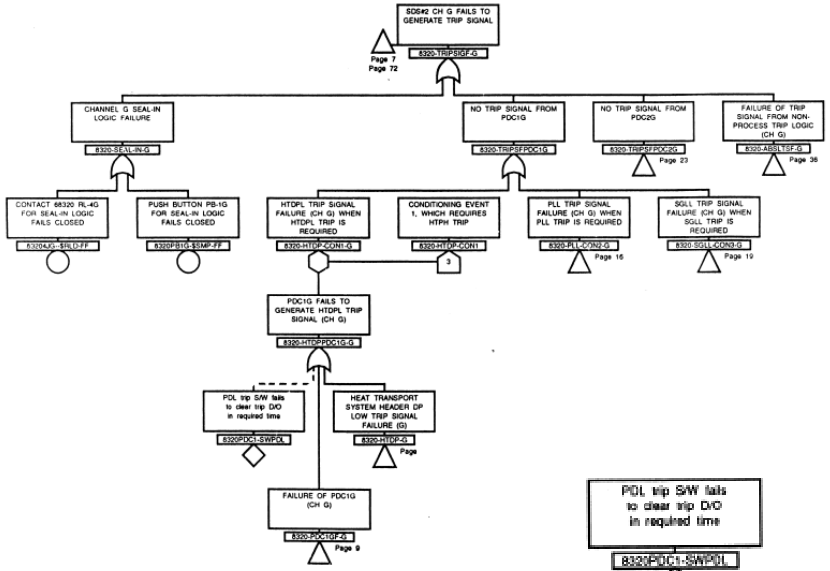
Unintended Acceleration of Car

Software Safety?

- Accident: (IAEA Glossary)
  - Any unintended *event*, including operating errors, equipment *failures* and other mishaps.
- Hazard: (IEC 61508-4)
  - Potential source of accident (harm)
- Software Safety: (IEEE 1228)
  - Freedom from software hazards

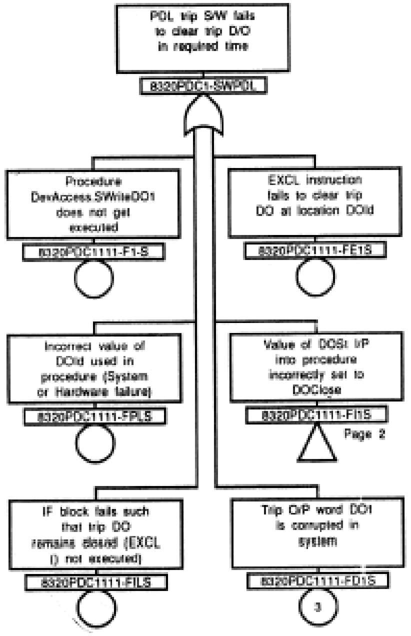
Hazard analysis of digital I&C in Korea

- ‘90: Software Hazard Analysis of SDS, Wolsong 2/3/4 NPPs
  - Software Fault Tree Analysis
  - By AECL, Nancy Leveson



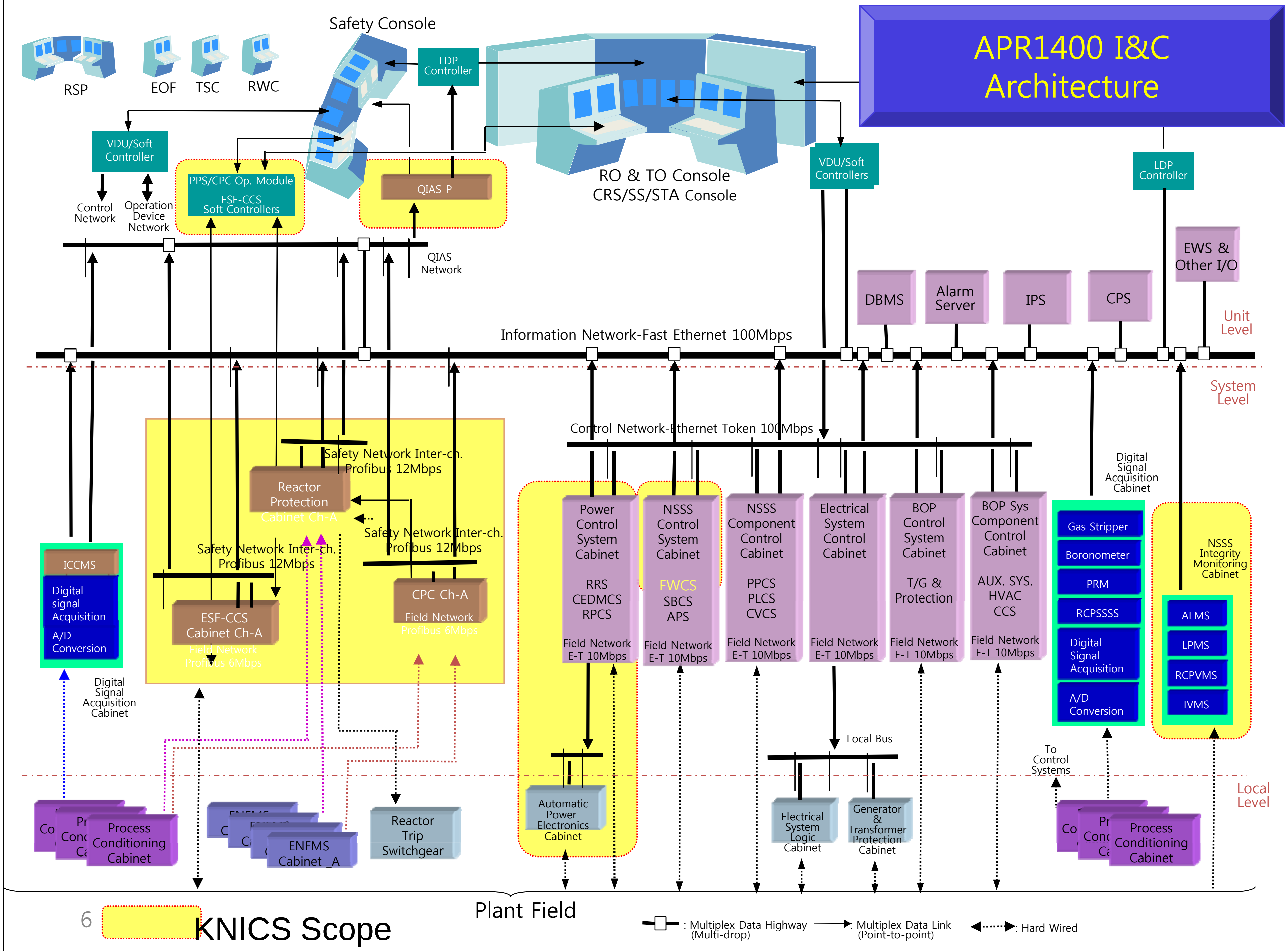
SDS#2 CH G FAILS TO GENERATE TRIP SIGNAL
8320-TRIPSIGF-G
Page 7
Page 72
CHANNEL G SEAL-IN LOGIC FAILURE
8320-SEAL-IN-G
NO TRIP SIGNAL FROM PDC1G
8320-TRIPSFPDC1G
NO TRIP SIGNAL FROM PDC2G
8320-TRIPSFPDC2G
Page 23
FAILURE OF TRIP SIGNAL FROM NON-PROCESS TRIP LOGIC (CH G)
8320-ABSLTSF-G
Page 38
CONTACT 68320 RL-4G FOR SEAL-IN LOGIC FAILS CLOSED
83204JG--$RLD-FF
PUSH BUTTON PB-1G FOR SEAL-IN LOGIC FAILS CLOSED
8320PB1G-$SMP-FF
HTDPL TRIP SIGNAL FAILURE (CH G) WHEN HTDPL TRIP IS REQUIRED
8320-HTDP-CON1-G
CONDITIONING EVENT 1, WHICH REQUIRES HTPH TRIP
8320-HTDP-CON1
3
PLL TRIP SIGNAL FAILURE (CH G) WHEN PLL TRIP IS REQUIRED
8320-PLL-CON2-G
Page 16
SGLL TRIP SIGNAL FAILURE (CH G) WHEN SGLL TRIP IS REQUIRED
8320-SGLL-CON3-G
Page 19
PDC1G FAILS TO GENERATE HTDPL TRIP SIGNAL (CH G)
8320-HTDPPDC1G-G
PDL trip S/W fails to clear trip D/O in required time
8320PDC1-SWPDL
HEAT TRANSPORT SYSTEM HEADER DP LOW TRIP SIGNAL FAILURE (G)
8320-HTDP-G
Page
FAILURE OF PDC1G (CH G)
8320-PDC1GF-G
Page 9

Name of Software Hazards	No	%	Remarks
For construct hazard	4	7	
Initialization hazard	4	7	
IF-THEN-ELSE construct hazard	38	67	
CASE construct hazard	4	7	
Sequence checks hazard	1	2	
Main loop timer hazard	3	4	Hardware related
Wait in the main loop hazard	1	2	
Backup timers hazard	1	2	Hardware related
Common mode failure hazard	1	2	
Summary	57	100	



PDL trip S/W fails to clear trip D/O in required time
8320PDC1-SWPDL
Procedure DevAccess.SWriteDO1 does not get executed
8320PDC1111-F1-S
EXCL instruction fails to clear trip DO at location DOId
8320PDC1111-FE1S
Incorrect value of DOId used in procedure (System or Hardware failure)
8320PDC1111-FPLS
Value of DOS: I/P into procedure incorrectly set to DOClose
8320PDC1111-FI1S
Page 2
IF block fails such that trip DO remains closed (EXCL () not executed)
8320PDC1111-FILS
Trip O/P word DO1 is corrupted in system
8320PDC1111-FD1S
3

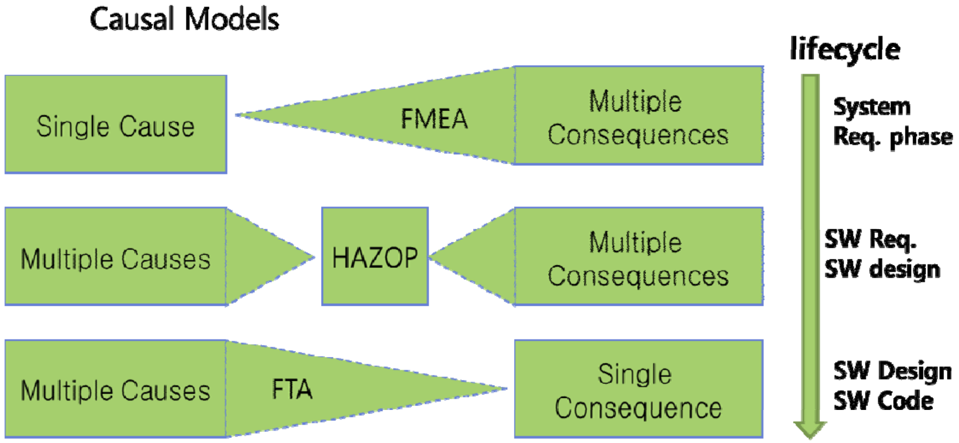
APR1400 I&C Architecture


Safety Console
RSP
EOF
TSC
RWC
LDP Controller
RO & TO Console
CRS/SS/STA Console
VDU/Soft Controller
VDU/Soft Controllers
LDP Controller
PPS/CPC Op. Module
ESF-CCS Soft Controllers
QIAS-P
Control Network
Operation Device Network
QIAS Network
EWS & Other I/O
DBMS
Alarm Server
IPS
CPS
Unit Level
Information Network-Fast Ethernet 100Mbps
System Level
Control Network-Ethernet Token 100Mbps
Safety Network Inter-ch. Profibus 12Mbps
Reactor Protection Cabinet Ch-A
Safety Network Inter-ch. Profibus 12Mbps
Safety Network Inter-ch. Profibus 12Mbps
ESF-CCS Cabinet Ch-A
Field Network Profibus 6Mbps
CPC Ch-A
Field Network Profibus 6Mbps
ICCMS
Digital signal Acquisition
A/D Conversion
Digital Signal Acquisition Cabinet
Power Control System Cabinet
RRS CEDMCS RPCS
Field Network E-T 10Mbps
NSSS Control System Cabinet
FWCS SBCS APS
Field Network E-T 10Mbps
NSSS Component Control Cabinet
PPCS PLCS CVCS
Field Network E-T 10Mbps
Electrical System Control Cabinet
Field Network E-T 10Mbps
BOP Control System Cabinet
T/G & Protection
Field Network E-T 10Mbps
BOP Sys Component Control Cabinet
AUX. SYS. HVAC CCS
Field Network E-T 10Mbps
Digital Signal Acquisition Cabinet
Gas Stripper
Boronometer
PRM
RCPSSSS
Digital Signal Acquisition
A/D Conversion
NSSS Integrity Monitoring Cabinet
ALMS
LPMS
RCPVMS
IVMS
Local Bus
To Control Systems
Local Level
Process Conditioning Cabinet
ENFMS Cabinet _A
Reactor Trip Switchgear
Automatic Power Electronics Cabinet
Electrical System Logic Cabinet
Generator & Transformer Protection Cabinet
Process Conditioning Cabinet
Plant Field
KNICS Scope
: Multiplex Data Highway (Multi-drop)
: Multiplex Data Link (Point-to-point)
: Hard Wired

Hazard Analysis of KNICS

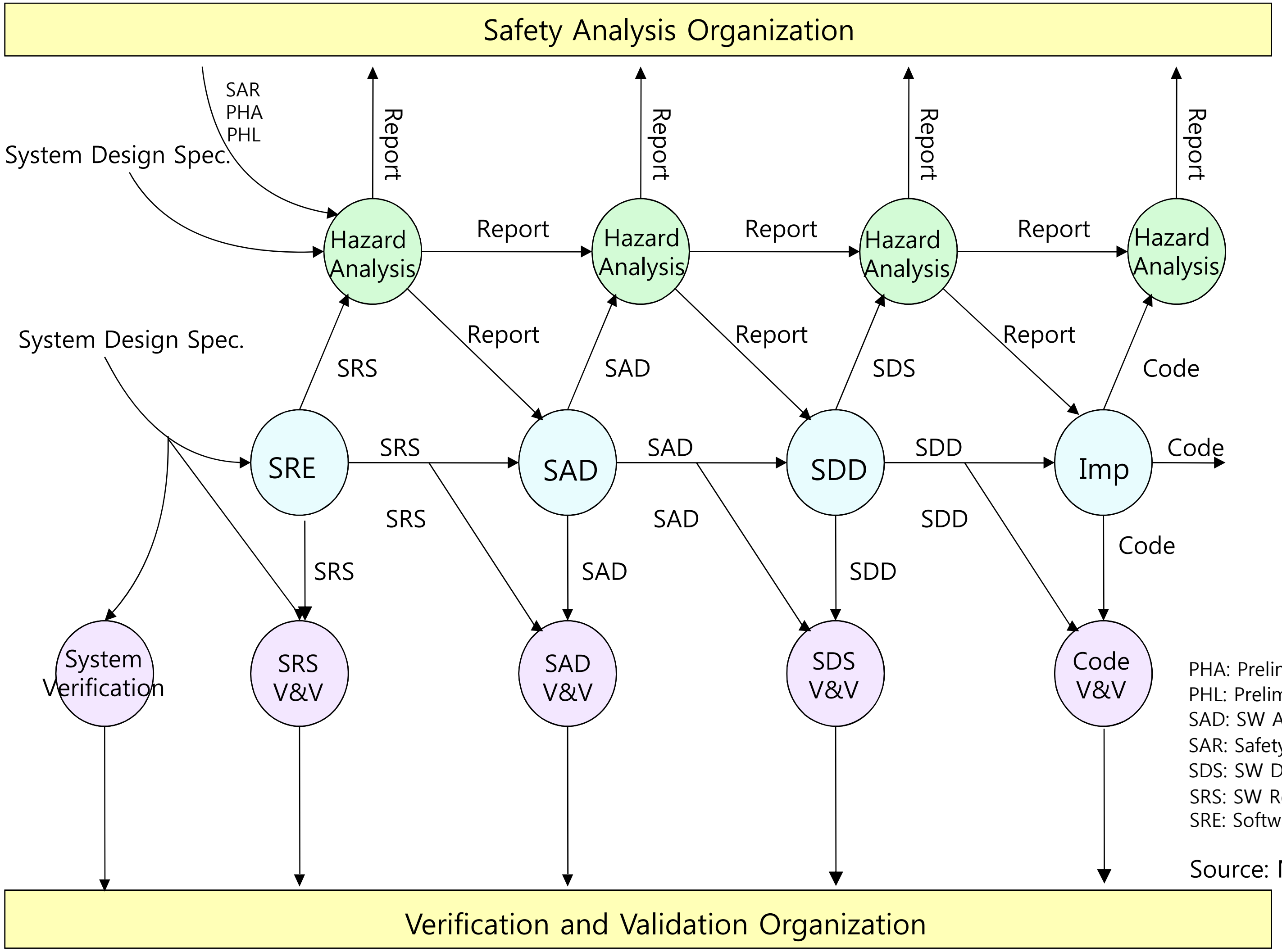
- Korea Nuclear I&C System(KNICS)
- 2001-2004: Develop a combination of FMEA, HAZOP, FTA through lifecycle of system and software
  - Developed FTA template for FBD program
- 2004-2008: KAERI, HA of KNICS

- IEEE 1228,
- SRP BTP14
- IEEE 7-4.3.2 Annex D
- NUREG 6101, 6430



Focused HA through lifecycle (according to NUREG 6430)
Harmonized (top-down and bottom-up) HA
HAZOP checklists with guidewords developed by KAERI and LLNL
FTA templates for FBD program

Software Hazard Analysis Process



PHA: Preliminary Hazard Analysis
PHL: Preliminary Hazard List
SAD: SW Architecture Description
SAR: Safety Analysis Report
SDS: SW Design Spec.
SRS: SW Requirements Spec.
SRE: Software Requirements Eng.

Source: NUREG/CR-6430

	IEC 61508-1 overall safety lifecycle	IEC 61513 overall safety lifecycle
1	Concept	Deriving I&C requirements from the plant safety design base
2	Overall scope definition	
3	Hazard and risk analysis	Outside the scope of this standard, is part of plant design base
4	Overall safety requirements	Overall requirements specification of the I&C system
5	Safety requirements allocation	Design of the I&C architecture and assignment of the I&C functions (There is no Safety Requirements of I&C in IEC 61513)
6	Overall operation and maintenance planning	Overall operation and maintenance plan
7	Overall safety validation planning	No safety validation plan
8	Overall installation and commissioning planning	Overall integration and commissioning plans, QA plan, and security plan
9	E/E/PE safety-related systems: realisation	System safety lifecycle
10	Other technology safety-related systems: realisation	
11	External risk reduction facilities: realisation	
12	Overall installation and commissioning	Overall integration and commissioning
13	Overall safety validation	No safety validation (only system qualification)
14	Overall operation, maintenance and repair	Overall operation and maintenance
15	Overall modification and retrofit	(Implicitly covered)
16	Decommissioning or disposal	
17	Verification	Overall quality assurance programs
18	Functional safety assessment	In the nuclear sector, this assessment depends on the safety bodies and national regulations

NWIP: Hazard Analysis TR

- New Work Item Proposal(NWIP)
  - Proposed at Moscow meeting of IEC SC45A 2013
- Title: Comparison of Hazard Analysis Requirements of I&C
- Purpose
  - To identify the world wide situation of HA requirements for digital I&C
  - To make a technical basis for next revision of IEC SC45A Stds (61513, 60880) if agreed
  - To harmonize IEC and IEEE standards for HA of I&C

Contents of IEC HA TR(Draft)

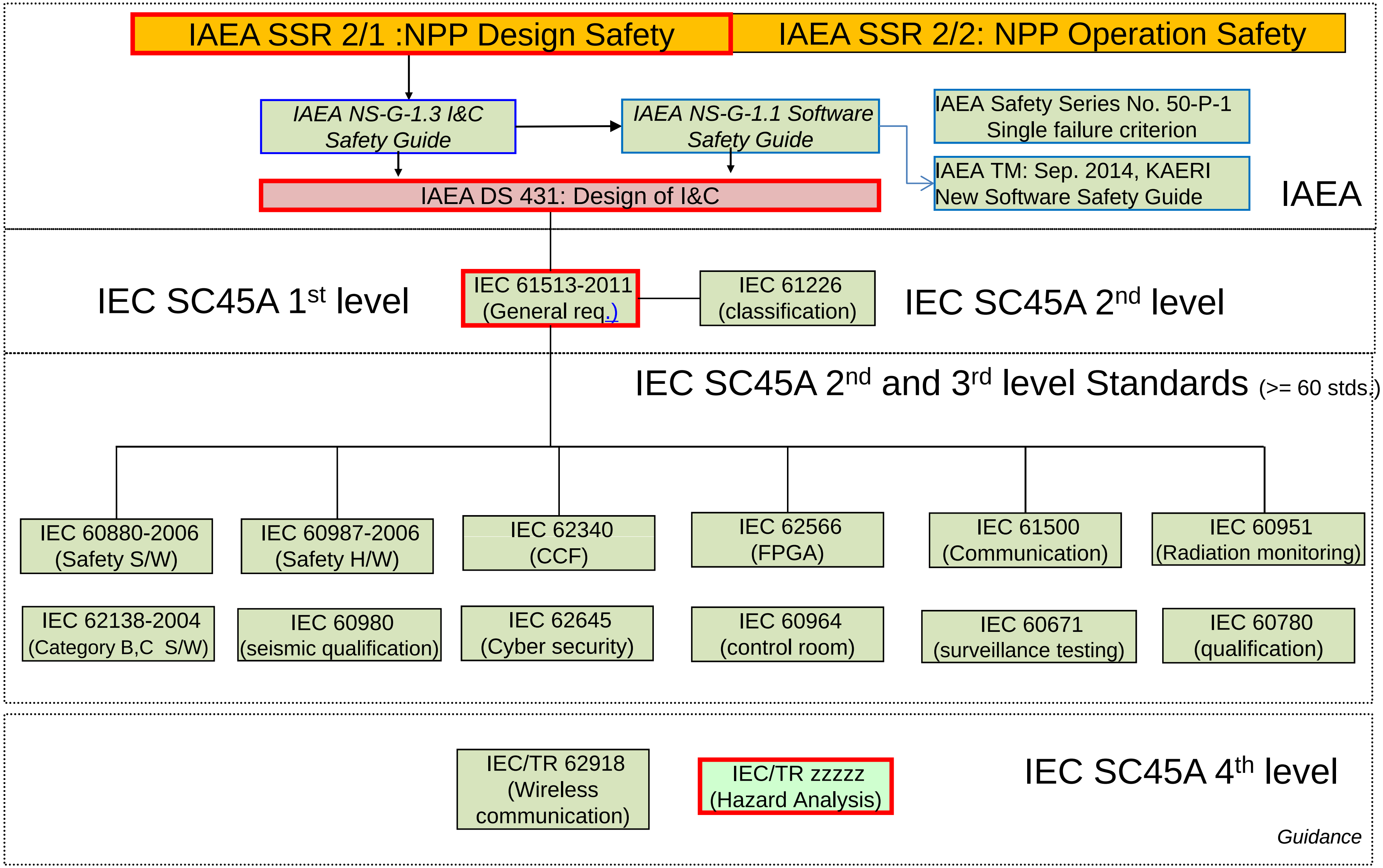
Comparison Template for Nuclear Domain

	Comparison criteria of HA requirements	IAEA SSR 2/1	IAEA DS 431	IEC 61513 -2011	IEEE 603 - 2009	IEEE 7-4.3.2 -2010	IEEE 1012 - 2012	IEEE 1228 - 1994	US NRC DSRS app.A RIL 1101 Reg. Guides
1	Safety principles								
2	Safety processes								
3	Definition of HA								
4	Purpose of HA								
5	Method of HA								
6	HA process								
7	Independence of HA (HA organization)								
8	Harmonized HA of SoS								
9	Relationship with other dependability (security, reliability) requirements								

Comparison Template for other safety industries

	Comparison criteria of HA requirements	(General) IEC 61508	(Aircraft) DO-178C, ARP 4761	(Civil Air) FAA Safety Guide	(space) NASA Safety Guide	(Military) MIL 882E	(Car) ISO 26262	(Railway) IEC 62278	(Medical) IEC 60601
1	Safety principles								
2	Safety processes								
3	Definition of HA								
4	Purpose of HA								
5	Method of HA								
6	HA process								
7	Independence of HA (HA organization)								
8	Harmonized HA of SoS								
9	Relationship with other dependability (security, reliability) requirements								

IAEA-IEC Framework



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 TM: Sep. 2014, KAERI
New Software Safety Guide

IAEA DS 431: Design of I&C

IAEA

IEC SC45A 1st level

IEC 61513-2011
(General req.)

IEC 61226
(classification)

IEC SC45A 2nd level

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)

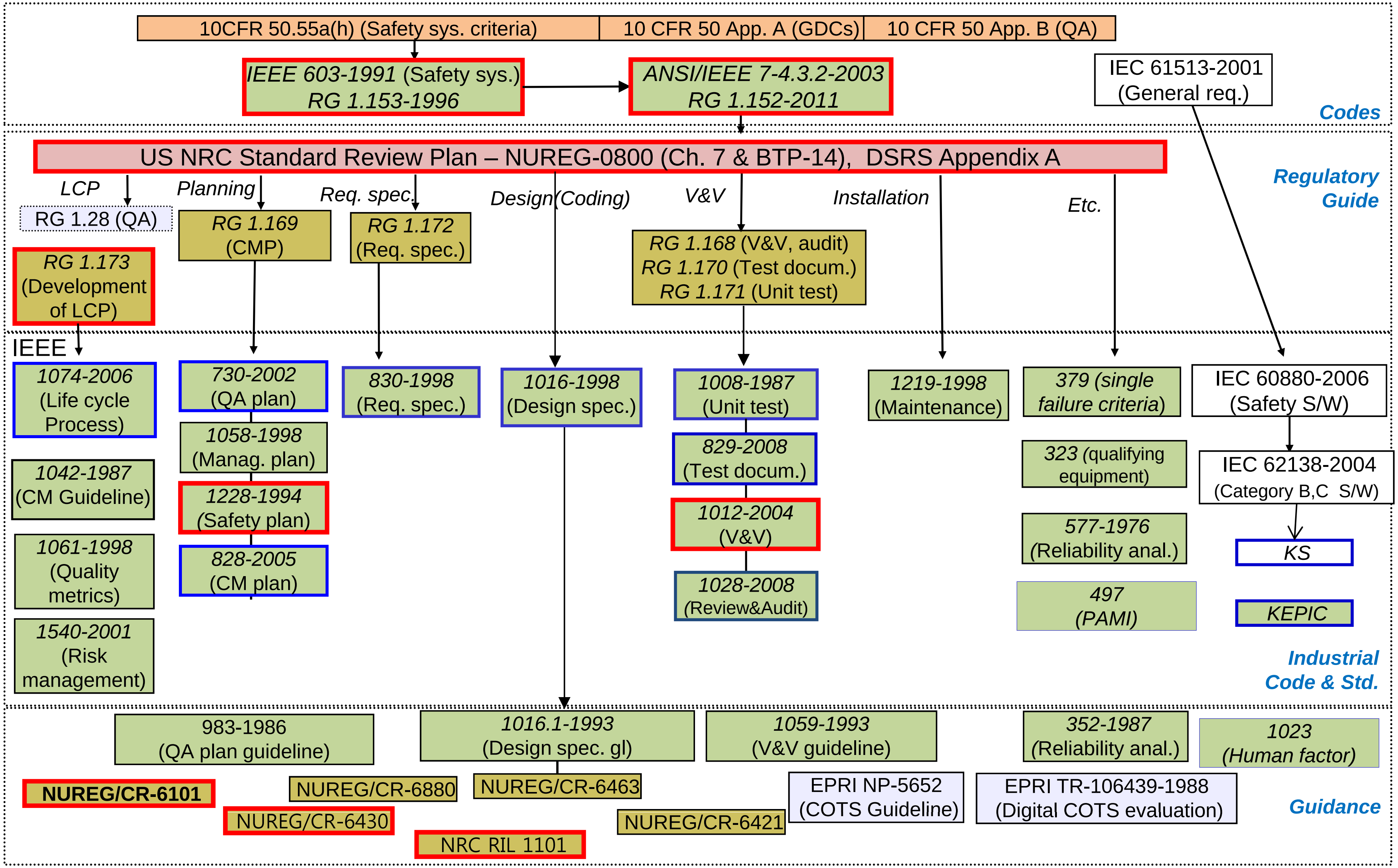
IEC/TR zzzzz
(Hazard Analysis)

IEC SC45A 4th level

Guidance

🟥 :Hazard Analysis related

NRC-IEEE Framework



10CFR 50.55a(h) (Safety sys. criteria)
10 CFR 50 App. A (GDCs)
10 CFR 50 App. B (QA)

IEEE 603-1991 (Safety sys.)
RG 1.153-1996

ANSI/IEEE 7-4.3.2-2003
RG 1.152-2011

IEC 61513-2001
(General req.)

Codes

US NRC Standard Review Plan – NUREG-0800 (Ch. 7 & BTP-14), DSRS Appendix A

LCP
RG 1.28 (QA)
RG 1.173 (Development of LCP)

Planning
RG 1.169 (CMP)

Req. spec.
RG 1.172 (Req. spec.)

Design(Coding)

V&V
RG 1.168 (V&V, audit)
RG 1.170 (Test docum.)
RG 1.171 (Unit test)

Installation

Etc.

Regulatory Guide

IEEE

1074-2006 (Life cycle Process)
1042-1987 (CM Guideline)
1061-1998 (Quality metrics)
1540-2001 (Risk management)

730-2002 (QA plan)
1058-1998 (Manag. plan)
1228-1994 (Safety plan)
828-2005 (CM plan)

830-1998 (Req. spec.)

1016-1998 (Design spec.)

1008-1987 (Unit test)
829-2008 (Test docum.)
1012-2004 (V&V)
1028-2008 (Review&Audit)

1219-1998 (Maintenance)

379 (single failure criteria)
323 (qualifying equipment)
577-1976 (Reliability anal.)
497 *(PAMI)*

IEC 60880-2006
(Safety S/W)

IEC 62138-2004
(Category B,C S/W)

KS

KEPIC

Industrial Code & Std.

983-1986 (QA plan guideline)
1016.1-1993 (Design spec. gl)
1059-1993 (V&V guideline)
352-1987 (Reliability anal.)
1023 *(Human factor)*

NUREG/CR-6101
NUREG/CR-6880
NUREG/CR-6430
NUREG/CR-6463
NRC RIL 1101
NUREG/CR-6421
EPRI NP-5652 (COTS Guideline)
EPRI TR-106439-1988 (Digital COTS evaluation)

Guidance

□:Hazard Analysis related

Safety Principle

		IEC	IEEE
1	Framework	IAEA-IEC framework	NRC-IEEE framework
2	Risk based qualification	Graded application of quality and reliability features	No graded application
3	Classification	SIL in 61508, Categories in 61226	Class IE, Non1E
4	Safety Process	Safety requirements specification is the main activity in the lifecycle.(IEC 61508)	Safety Analysis in all phases of the lifecycle
5	Safety Principles	Safety shall be met through a thorough engineering. Indirect Qualification	Same approach, but different in direct hazard analysis Indirect Qualification + Direct HA
		1. Simple, separate safety systems design	1. Simple, separate safety systems design
		2. System quality	2. System quality
		- Complete & correct safety requirements	- Complete & correct safety requirements
		- Correct implementation	- Correct implementation
		- Producing quality products	- Producing quality products
		3. Defense-in-Depth & Diversity	3. Defense-in-Depth & Diversity
			4. Hazard avoidance/identification/resolution

Safety Process

	IEC 61513 system safety lifecycle	IEC 60880 software safety lifecycle	IEEE 7-4.3.2 computer system safety lifecycle (Annex D)	IEEE 1228 software safety lifecycle (Annex)
1	System requirements specification (no I&C Safety requirements)	Software requirements specification (No Software safety requirements)	Hazards identification and evaluation plan	Software safety plan
2	System planning	Software QA plan, V&V plan	Safety system hazard identification	Software safety analyses preparation
3	System specification		Computer system hazards identification	
4	System detailed design and implementation		Software requirements hazards identification	Software safety requirements analysis
5	- System architecture	Software design	Software design hazards identification	Software safety design analysis
6	- Design constraint requirements			
7	- Defense against propagation of failures			
8	- System architecture, self-monitoring and tolerance to failures	Implementation of new software in general purpose language		
9	- Selection of equipment	Implementation of new software in application-oriented language	Software implementation hazards identification	Software safety code analysis
10	- Internal behavior of system	Configuration of pre-developed software and devices	Evaluation of hazards in previously developed systems	
11	System integration	Software aspects of integration	Computer system integration testing for hazards conditions	Software safety test analysis
12	System operation plan			
13	System validation	Software aspects of validation	Computer system validation testing	
14	System modification		Maintenance and modification hazard analysis	Software safety change analysis
15	System verification plan			

Summary of HA Comparison

IAEA-IEC Framework

- IAEA SSR 2/1 (NPP Design)
  - Internal and External Hazard Analysis Requirements for NPP Design
- IAEA DS 431 (I&C Design)
  - HA Requirements of I&C
- IAEA NS-G-1 (Software)
  - HA Requirements of Computer
- IEC Generic (61508)
  - Hazard Analysis in early phase to derive Safety Function Requirements
  - Risk Assessment in early phase to derive Safety Integrity Requirements (Safety Integrity Level)
- IEC Nuclear Sector (61513, 60880)
  - Hazard Analysis is outside the scope of IEC 61513
  - Functional Safety Assessment is not required in the standard
  - No Safety Validation Plan

NRC-IEEE Framework

- IEEE1228-1994, Software Safety Plan
  - It defines the software safety analysis in each phase of the software lifecycle
- IEEE 7-4.3.2-2003, Digital Computer in Safety Systems of NPP
  - Annex D. Identification and Resolution of Hazards in each phase of the system lifecycle
- NRC Regulation
  - NUREG-0800-1997, Standard Review Plan, BTP-14, Software Safety Analysis in each phase of the software lifecycle
  - US NRC Design-Specific Review Standard for the mPower Design, Appendix A, 2013, Hazard Analysis through I&C lifecycles
- NRC Guidance
  - NUREG/CR-6430-1995, Software Safety Hazard Analysis in each phase of the software lifecycle
  - US NRC RIL 1101, 2013

Challenge 1: Terminology

- There is no consensus in terminology relate to the hazard analysis.
  1. Accident, Harm, Hazard, Failure, Error, Faults
  2. Safety Analysis vs. Hazard Analysis
  3. Hazard Analysis vs. Failure Analysis
  4. Hazard analysis, Hazard identification
  5. Safety Assessment, Safety Analysis
  6. Internal and external hazards

- ***Safety analysis.*** Evaluation of the potential hazards associated with the conduct of an *activity*. (IAEA Glossary)

- **(IEEE 7-4.3.2) Hazard Analysis:** A process that explores and identifies conditions that are not identified by the normal design review and testing process.

- 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. (RIL 1101, US NRC)

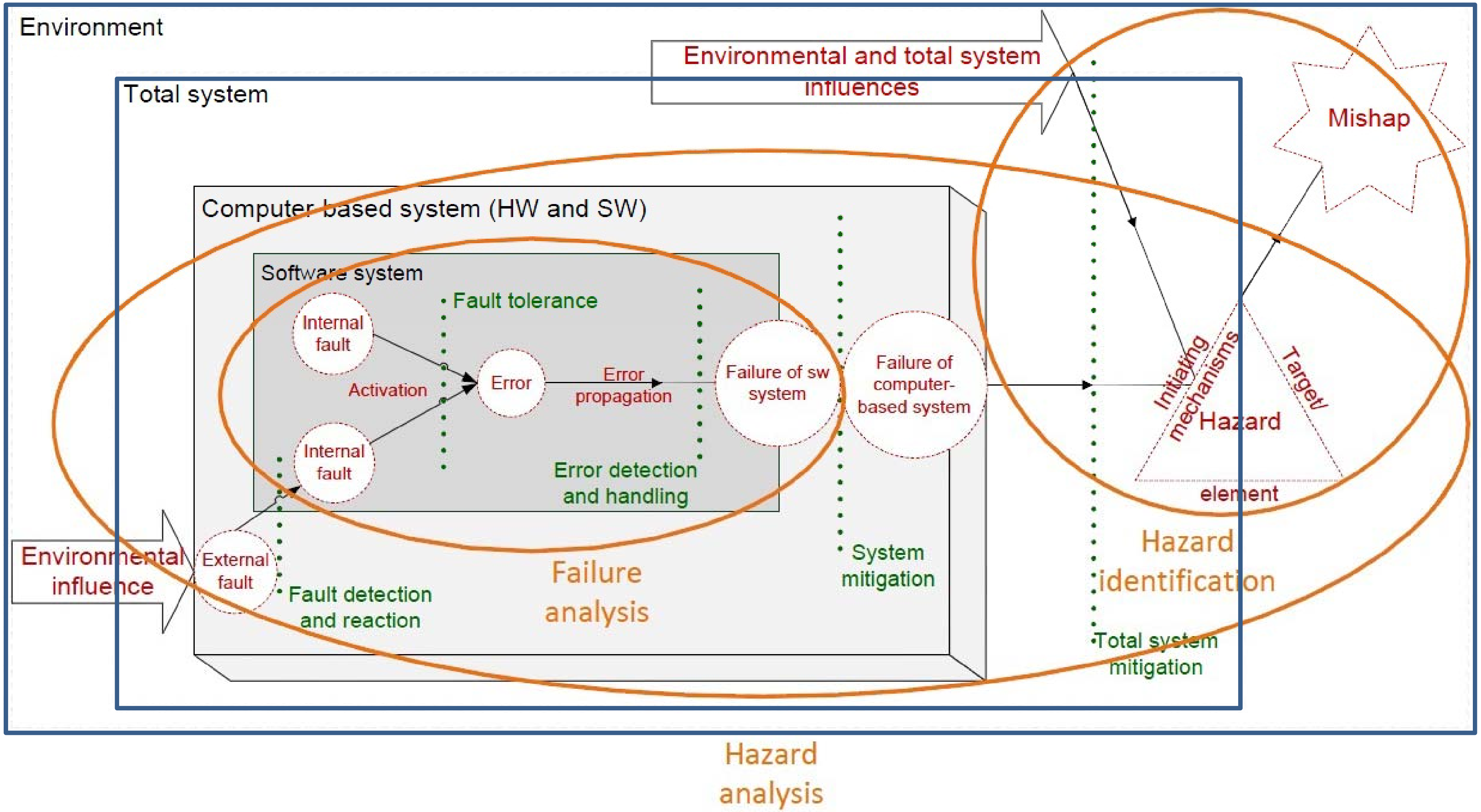
Challenge 2: Purpose of HA

- To define the Safety Requirements (Safety Goal)?
- To identify the hazard and the contributory hazards of I&C system of systems.
- 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.

Challenge 3: Method of HA

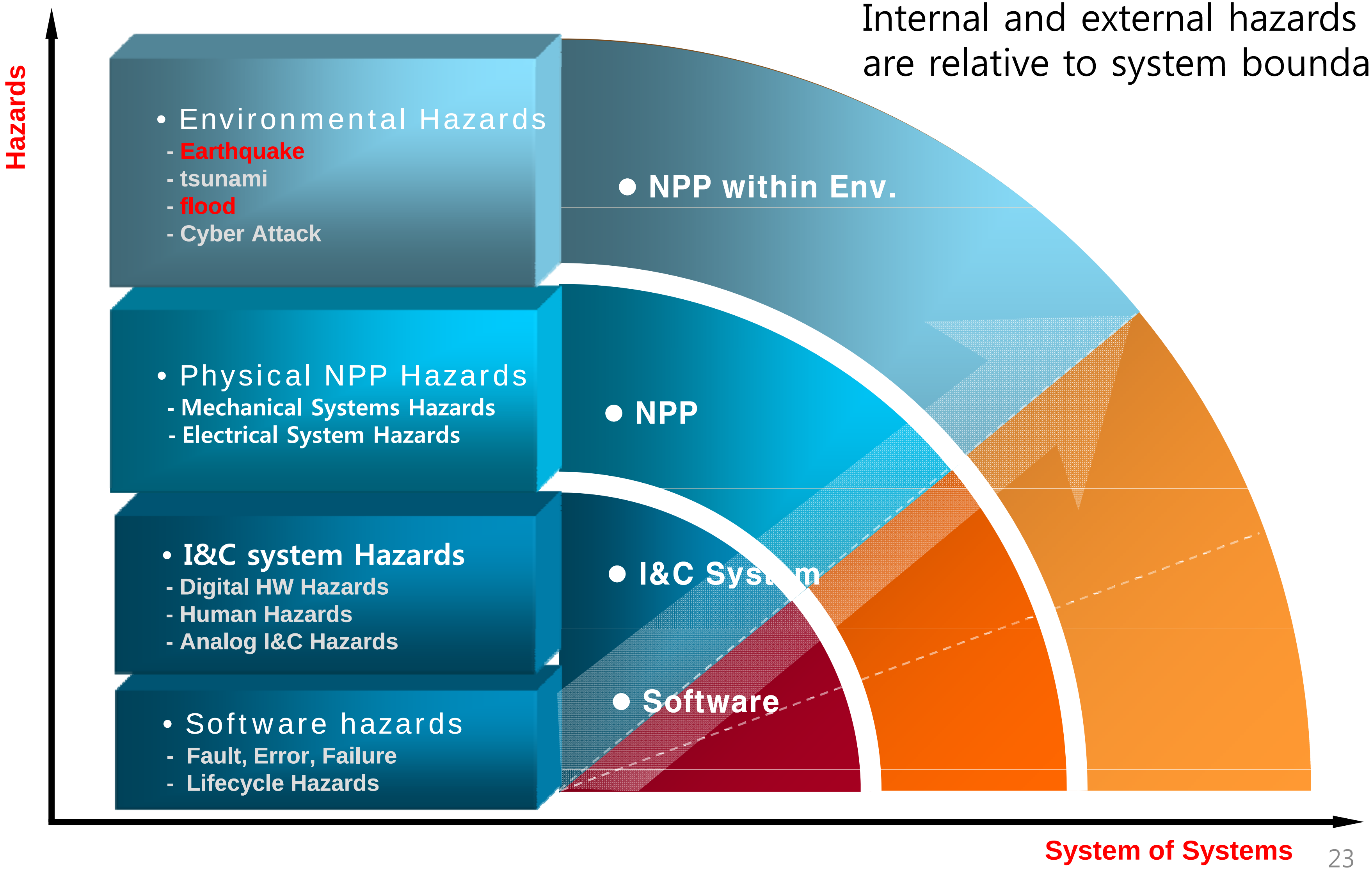
- Practical HA methods and techniques?
- Maturity of methods?
- How to measure the acceptability of HA?
- Harmonized HA with security and risk analysis?
- How much HA of SoS(System of Systems)?

Proposal 1: HA vs. FA



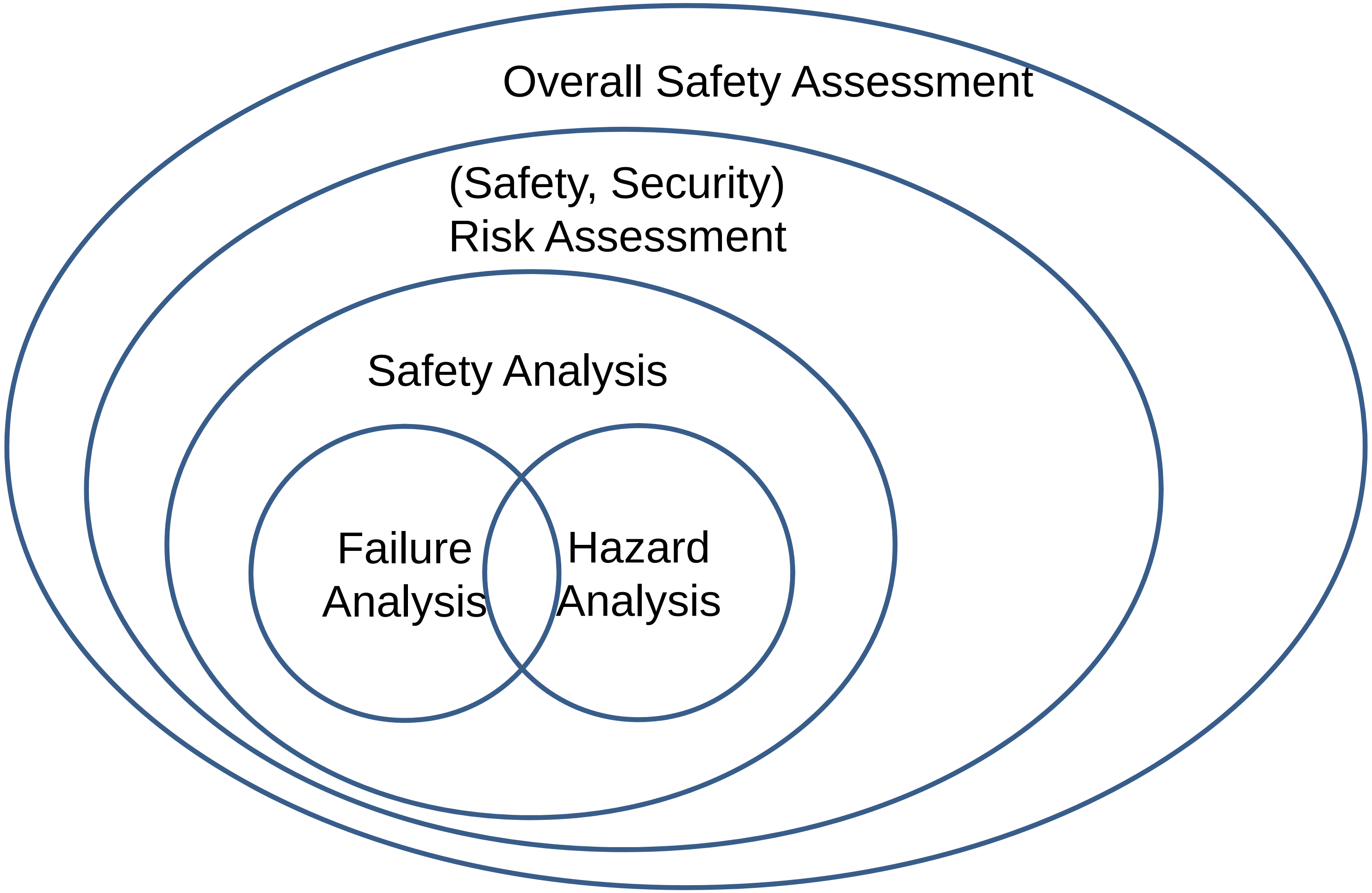
Proposal 2: Internal vs. External Hazards

Internal and external hazards
are relative to system boundary.



Proposal 3: Coverage of Analysis

Assessment = Evaluation of analysis results to judge the acceptability (IAEA Glossary)



Overall Safety Assessment

(Safety, Security)
Risk Assessment

Safety Analysis

Failure
Analysis

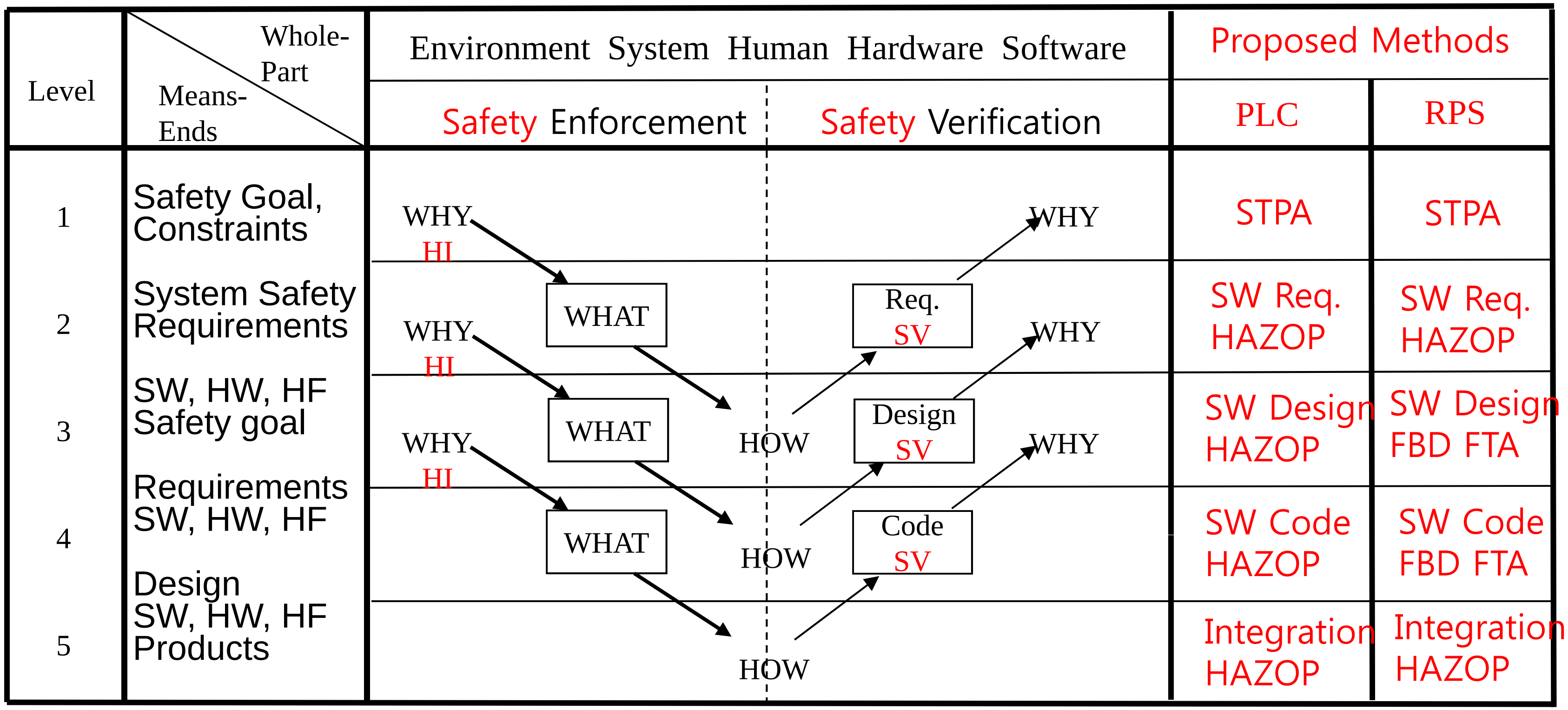
Hazard
Analysis

Proposal 4: Safety Analysis

Safety Analysis = Safety Enforcement + Safety Verification

Design Safety Analysis = Hazard Identification
+ Safety Requirements (to prevent hazard)
+ Safety Verification
+ Hazard Control and Mitigation (D3)

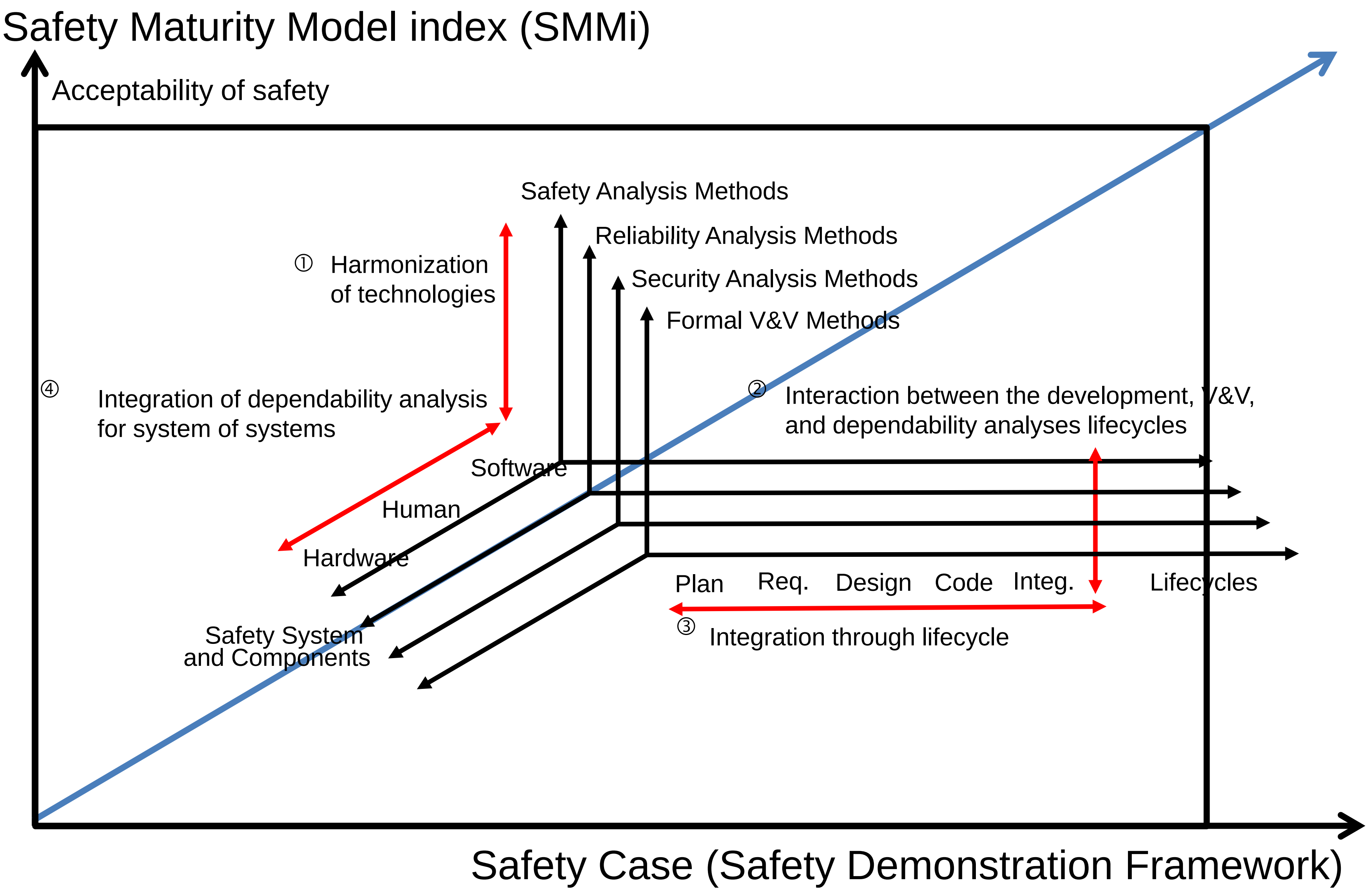
Operation Safety Analysis



Level	Whole-Part / Means-Ends	Environment System Human Hardware Software		Proposed Methods	
		Safety Enforcement	Safety Verification	PLC	RPS
1	Safety Goal, Constraints	WHY HI	WHY	STPA	STPA
2	System Safety Requirements	WHAT WHY HI	Req. SV WHY	SW Req. HAZOP	SW Req. HAZOP
3	SW, HW, HF Safety goal	WHAT HOW WHY HI	Design SV WHY	SW Design HAZOP	SW Design FBD FTA
4	Requirements SW, HW, HF	WHAT HOW	Code SV	SW Code HAZOP	SW Code FBD FTA
5	Design SW, HW, HF Products	HOW		Integration HAZOP	Integration HAZOP

SA: Safety Analysis, HI: Hazard Identification, SV: Safety Verification,

Proposal 5: Safety Assessment


Safety Maturity Model index (SMMi)
Acceptability of safety
Safety Analysis Methods
Reliability Analysis Methods
Security Analysis Methods
Formal V&V Methods
① Harmonization of technologies
④ Integration of dependability analysis for system of systems
② Interaction between the development, V&V, and dependability analyses lifecycles
Software
Human
Hardware
Safety System and Components
Plan
Req.
Design
Code
Integ.
Lifecycles
③ Integration through lifecycle
Safety Case (Safety Demonstration Framework)

Conclusions

- There is a difference of engineering principles between IEC and IEEE.
  - Need to decide whether there should be the HA requirements for I&C level in IEC SC45A Standards.
    - I will discuss on IEC HA TR (Oct., 2014, Las Vegas)
    - There are HA requirements for I&C in IAEA DS 431 and software in IAEA NS-G-1.1.
  - Need to define clearly the HA requirements and their relationship for I&C in IEEE Standards and NRC Reg. Guides
    - IEEE 603, IEEE 7-4.3.2, IEEE 1012, IEEE 1228, IEEE 1074
    - US NRC Reg. Guides, RIL 1101, and DSRS, App. A Hazard Analysis

- Need to make an international consensus on HA

Thank You for Your Attention

감사합니다.

For a safer world

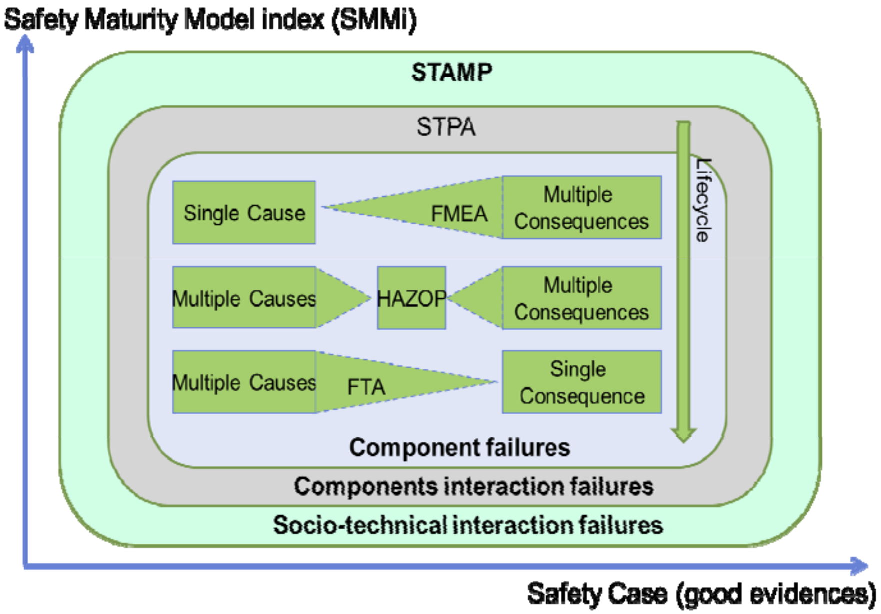
Jang-Soo Lee
(jslee@kaeri.re.kr)

International Efforts

1. IEC SC45A/WG3, Discussion on IEC HA TR
    - Oct., 2014, Las Vegas
2. HRP for "Safety Demonstration Framework"
    - Sep., 2014, EHPG2014
3. US NRC, RIL 1101, DSRS, App. A, Hazard Analysis
    - March, 2014, RIC2014
4. EU Safety Critical Software Task Force
    - Oct. 2014, Munich (EU, US, Canada, Korea)
5. IAEA TM for SW dependability assessment
    - Sep. 2014, KAERI, Korea
6. IEEE NPEC
7. MDEP
8. Safety Critical System Club, Safety Critical Mailing List
    - by Univ. of York (Safety Case)
9. STAMP/STPA by Prof. Nancy Leveson, MIT

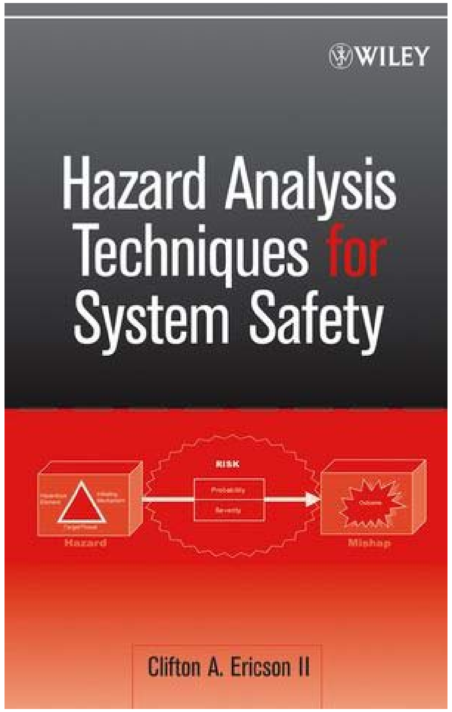
Safety Demonstration Framework

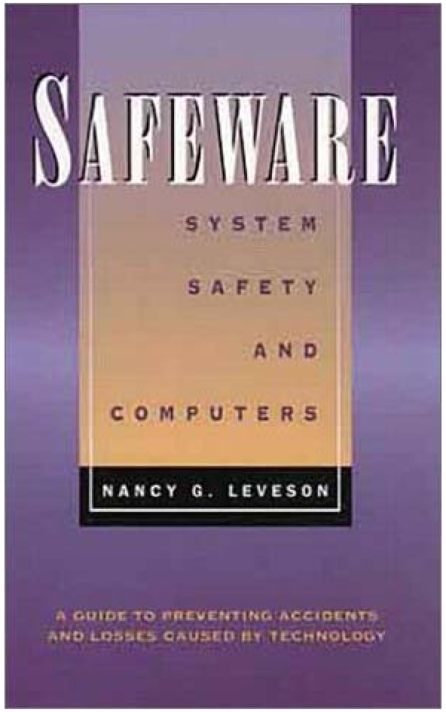
- 2014-2016, on going by KAERI
- Develop a DiD&D I&C to cope with CCF
- Develop a diverse platform with PLC and FPGA
- Study a New HA methodology for the complex I&C (HA of System of systems(SoS))
  - Safety Case, STAMP/STPA, and traditional
  - Safety Demonstration Framework with HRP, Norway

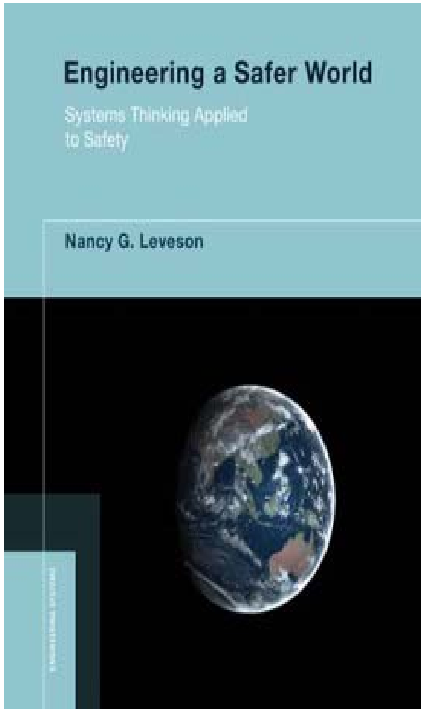


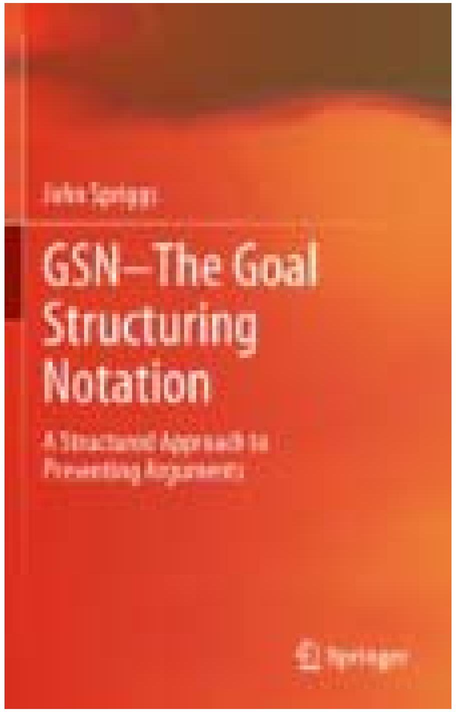
Safety Info.

- Safety Case vs. STPA

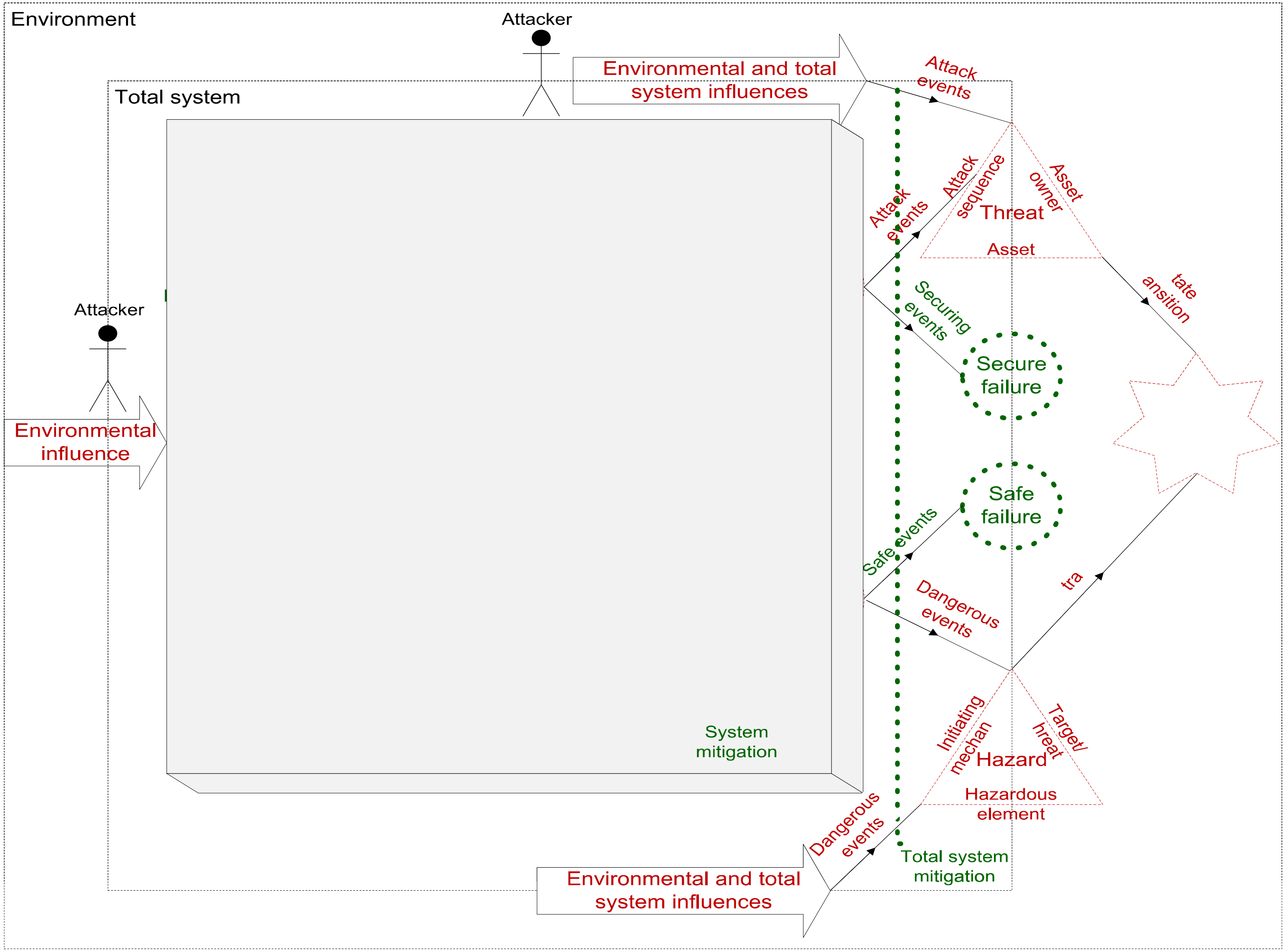



SAFEWARE
SYSTEM SAFETY AND COMPUTERS
NANCY G. LEVESON
A GUIDE TO PREVENTING ACCIDENTS AND LOSSES CAUSED BY TECHNOLOGY




John Spriggs
GSN—The Goal Structuring Notation
A Structured Approach to Presenting Arguments
Springer

Relation of safety and security



<from IFE, Norway Dr. Christian Raspotnig>

Comparison of Terminology

		IAEA-IEC framework	NRC-IEEE framework
1	Accident	(IAEA NS-G-1.3) Deviations from normal operation	(IEEE 1228) An unplanned event or series of events that results in death, injury, illness, environmental damage, or damage to or loss of equipment or property
2	Hazard	(IEC 61508-4) Potential source of harm	(IEEE 7-4.3.2) A condition that is a prerequisite to an accident. Hazards include external events as well as conditions internal to computer hardware or software
3	Risk	(IEC 61508-4) Combination of the probability of occurrence of harm and severity of that harm	(IEEE 1228) A measure that combines both the likelihood that a system hazard will cause an accident and the severity of that accident
4	Safety	(IEC 61508-4) Freedom from unacceptable risk	
5	Software Hazard		(IEEE 1228) A software condition that is a prerequisite to an accident
6	System Hazard		(IEEE 1228) A system condition that is a prerequisite to an accident
7	Software Safety		(IEEE 1228) Freedom from software hazards
8	System Safety		(IEEE 1228) Freedom from system hazards
9	Hazard Analysis	(IEC 61508-0) Hazard Analysis derives Safety Function Requirements (IAEA Glossary2007) No definition	(IEEE 7-4.3.2) Hazard Analysis: A process that explores and identifies conditions that are not identified by the normal design review and testing process. Hazard analysis focuses on system failure mechanisms rather than verifying correct system operation.
10			(NUREG-CR 6430) Hazard Analysis is the process of identifying and evaluating the hazards of a system, and then either eliminating the hazard or reducing its risk to an acceptable level.
11	Risk Assessment	(IEC 61508-0) Risk Assessment derives Safety Integrity Requirements	No definition

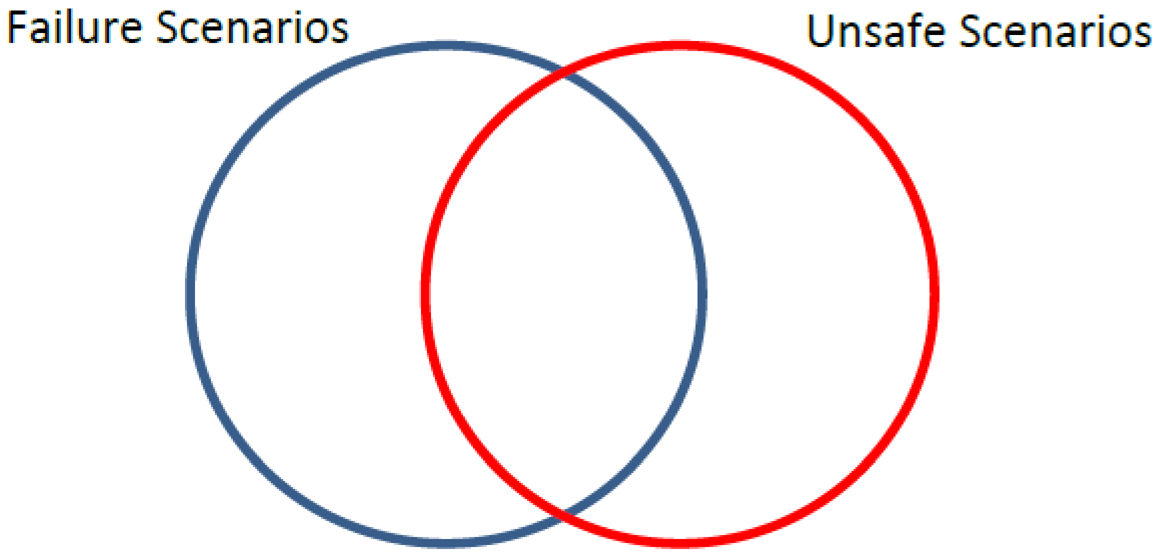


Figure 6.1: Failure scenarios vs. unsafe scenarios

From the Book "Engineering a Safer World", by Prof. Nancy Leveson

	Comparison criteria of HA requirements	HA requirements in the safety standard (IAEA SSR-2/1: Design Safety of NPP)
	Title	**Safety of Nuclear Power Plants: Design**
	Scope	for land based stationary nuclear power plants with water cooled reactors designed for electricity generation
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. IAEA-IEC Framework

	Comparison criteria of HA requirements	HA requirements in the safety standard for I&C (IAEA DS 431: Design of I&C System for NPP)
1	Safety principles (safety model)	2.56. For the overall I&C 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.
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. 2.64. 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.
		IAEA-IEC Framework

	Comparison criteria of HA requirements	HA requirements in the safety standard for I&C (IEC 61513-2011)
	Title	**Nuclear power plants – Instrumentation and control important to safety – General requirements for systems**
1	Safety principles (safety model)	(The safety principles of I&C system in IEC 61513 are based on the premise that all hazards are defined in plant level, and are input for the I&C.) (in IEC 61513) The IEC SC 45A standards series consistently implements and details the principles and basic safety aspects provided in the IAEA code on the safety of NPPs and in the IAEA safety series, in particular the requirements document NS-R-1, establishing safety requirements related to the design of nuclear power plants, and the safety guide NS-G-1.3 dealing with instrumentation and control systems important to safety in nuclear power plants.) (IAEA NS-G-1.3 is now being changed to DS431 with HA requirements.) (There is a HA requirements for computer system in IAEA NS-G-1.1) (However, there is no hazard analysis Requirements for I&C in IEC 61513.)
3	Definition of HA	3.25 Hazard event having the potential to cause injury to plant personnel or damage to components, equipment or structures. Hazards are divided into internal hazards and external hazards NOTE 1 Internal hazards are, for example, fire and flooding. Internal hazards may be also a consequence of a PIE (for example, loss of coolant accident, steam-line break). NOTE 2 External hazards are, for example, earthquake and lightning. IAEA-IEC Framework

	Comparison criteria of HA requirements	HA requirements in the safety standard for I&C (IEEE Standard 603-2009)
	Title	**IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations**
	Scope	for the power, instrumentation, and control portions of safety systems for nuclear power generating stations.
1	Safety principles (safety model or safety culture)	(There is no explicit HA requirements for I&C and power system) 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 no definition of HA, but there are requirements to document the safety system design basis in section 4 of IEEE 603.
10	Discussion	Where is HA requirements of Electrical System? Where is HA requirements of Analog I&C? NRC-IEEE Framework

	Comparison criteria of HA requirements	HA requirements in the safety standard for digital computer (IEEE 7-4.3.2-2010)
	Title	**IEEE Standard Criteria for Digital Computers in safety Systems of Nuclear Power Generating Stations**
1	Safety principles (safety model)	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.
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 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. (*different definition and scope from IEC)
6	HA process	Annex D. Identification and Resolution of Hazards in each phase of the system lifecycle NRC-IEEE Framework

	Comparison criteria of HA requirements	HA guidance for NRC staff (US NRC RIL 1101)
	Title	**Technical basis to review hazard analysis of digital safety systems**
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: “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.” 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. NRC-IEEE Framework

	Comparison criteria of HA requirements	HA requirements in the military safety standard (MIL 882 E, 2012)
	Title	**DEPARTMENT OF DEFENSE STANDARD PRACTICE** **SYSTEM SAFETY**
	Scope	Systems Engineering (SE) approach to eliminating hazards, where possible, and minimizing risks where those hazards cannot be eliminated. This Standard covers hazards as they apply to systems / products / equipment / infrastructure (including both hardware and software) throughout design, development, test, production, use, and disposal.
1	Safety principles	To provides a standard, generic method for the identification, classification, and mitigation of hazards.
2	Safety processes	HTS(Hazard Tracking System) is used for safety demonstration through lifecycle The safety(risk) assessment are conducted in system and software level separately.
3	Definition of HA	3.2.44 System safety engineering. An engineering discipline that employs specialized knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify hazards and then to eliminate the hazards or reduce the associated risks when the hazards cannot be eliminated.
4	Purpose of HA	The use of a system safety approach to identify hazards and manage the associated risks. Comparison Template for other safety industries

5	Method of HA	TASK SECTION 100 - MANAGEMENT TASK 101 HAZARD IDENTIFICATION AND MITIGATION EFFORT USING THE SYSTEM SAFETY METHODOLOGY TASK 102 SYSTEM SAFETY PROGRAM PLAN TASK 103 HAZARD MANAGEMENT PLAN TASK 104 SUPPORT OF GOVERNMENT REVIEWS/AUDITS TASK 105 INTEGRATED PRODUCT TEAM/WORKING GROUP SUPPORT **TASK 106 HAZARD TRACKING SYSTEM** TASK 107 HAZARD MANAGEMENT PROGRESS REPORT TASK 108 HAZARDOUS MATERIALS MANAGEMENT PLAN TASK SECTION 200 - ANALYSIS TASK 201 PRELIMINARY HAZARD LIST TASK 202 PRELIMINARY HAZARD ANALYSIS TASK 203 SYSTEM REQUIREMENTS HAZARD ANALYSIS TASK 204 SUBSYSTEM HAZARD ANALYSIS TASK 205 SYSTEM HAZARD ANALYSIS TASK 206 OPERATING AND SUPPORT HAZARD ANALYSIS TASK 207 HEALTH HAZARD ANALYSIS TASK 208 FUNCTIONAL HAZARD ANALYSIS **TASK 209 SYSTEM-OF-SYSTEMS HAZARD ANALYSIS** TASK 210 ENVIRONMENTAL HAZARD ANALYSIS TASK SECTION 300 - EVALUATION TASK 301 SAFETY ASSESSMENT REPORT TASK 302 HAZARD MANAGEMENT ASSESSMENT REPORT TASK 303 TEST AND EVALUATION PARTICIPATION TASK 304 REVIEW OF ENGINEERING CHANGE PROPOSALS, CHANGE NOTICES, DEFICIENCY REPORTS, MISHAPS, AND REQUESTS FOR DEVIATION/WAIVER TASK SECTION 400 - VERIFICATION TASK 401 SAFETY VERIFICATION TASK 402 EXPLOSIVES HAZARD CLASSIFICATION DATA TASK 403 EXPLOSIVE ORDNANCE DISPOSAL DATA Comparison Template for other safety industries

	Comparison criteria of HA requirements	HA requirements in the car safety standard (ISO 26262)
	Title	**Road vehicles — Functional safety**
1	Safety principles (safety model or safety culture)	Safety issues are intertwined with common function-oriented and quality-oriented development activities and work products. ISO 26262 addresses possible hazards caused by malfunctioning behaviour of E/E safety-related systems, including interaction of these systems.
2	Safety processes	Safety lifecycle provides an automotive safety lifecycle (management, development, production, operation, service, decommissioning) and supports tailoring the necessary activities during these lifecycle phases;
3	Definition of HA	Hazard Analysis and Risk Assessment (26262-1) :method to identify and categorize hazardous events (1.59) of items (1.69) and to specify safety goals (1.108) and ASILs (1.6) related to the prevention or mitigation of the associated hazards in order to avoid unreasonable risk (1.136)
		Comparison Template for other safety industries

4	Purpose of HA	The objective of the hazard analysis and risk assessment is to identify and to categorise the hazards that malfunctions in the item can trigger and to formulate the safety goals related to the prevention or mitigation of the hazardous events, in order to avoid unreasonable risk.
5	Method of HA	7.4.2.2 Hazard identification 7.4.2.2.1 The hazards shall be determined systematically by using adequate techniques. NOTE Techniques such as brainstorming, checklists, quality history, FMEA and field studies can be used for the extraction of hazards at the item level. 7.4.2.2.2 Hazards shall be defined in terms of the conditions or behaviour that can be observed at the vehicle level. 7.4.2.2.3 The hazardous events shall be determined for relevant combinations of operational situations and hazards. 7.4.2.2.4 The consequences of hazardous events shall be identified.
6	HA process	7.4.2.1 Situation Analysis 7.4.2.2 Hazard Identification 7.4.2.3 Classification of Hazardous events 7.4.4 Determination of ASIL and safety goals Comparison Template for other safety industries

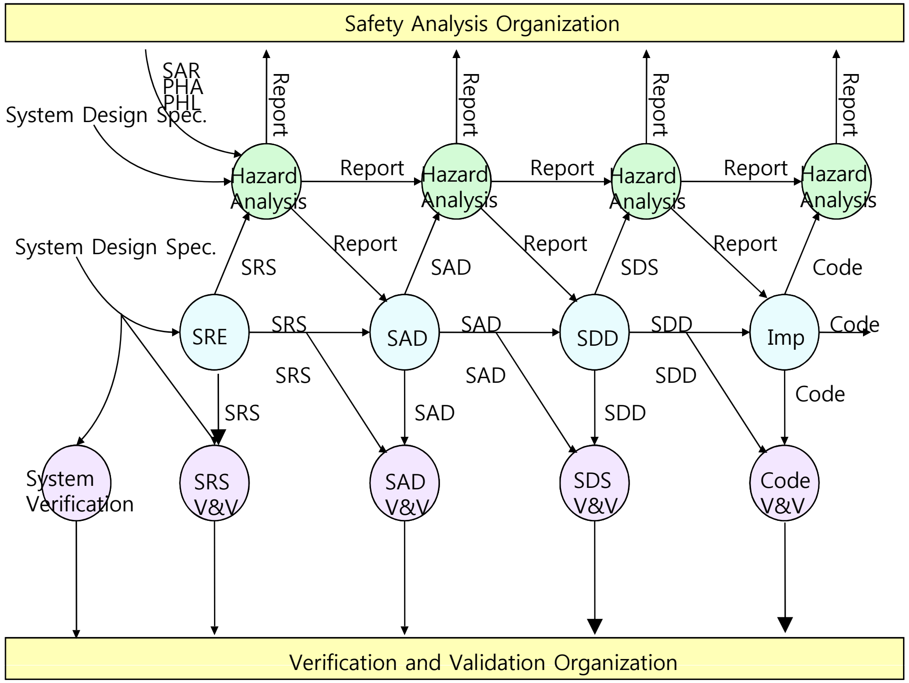
Challenge3: When HA?

HA sequence

Development sequence

- Before, during a plant specific safety system (RPS, ESF_CCS) development
- Before, during a generic safety system (RPS, ESF_CCS) development
- Before, during a generic safety platform (PLC, FPGA) development
- COTS products

- When HA of COTS components?


Safety Analysis Organization
SAR
PHA
PHL
System Design Spec.
Report
Report
Report
Report
Hazard Analysis
Report
Hazard Analysis
Report
Hazard Analysis
Report
Hazard Analysis
System Design Spec.
SRS
Report
SAD
Report
SDS
Report
Code
SRE
SRS
SAD
SAD
SDD
SDD
Imp
Code
SRS
SAD
SDD
Code
SRS
SAD
SDD
System Verification
SRS V&V
SAD V&V
SDS V&V
Code V&V
Verification and Validation Organization