Application of STPA to ESF-CCS

Dong-Ah Lee, Jang-Soo Lee, Se-Woo Cheon, and Junbeom Yoo

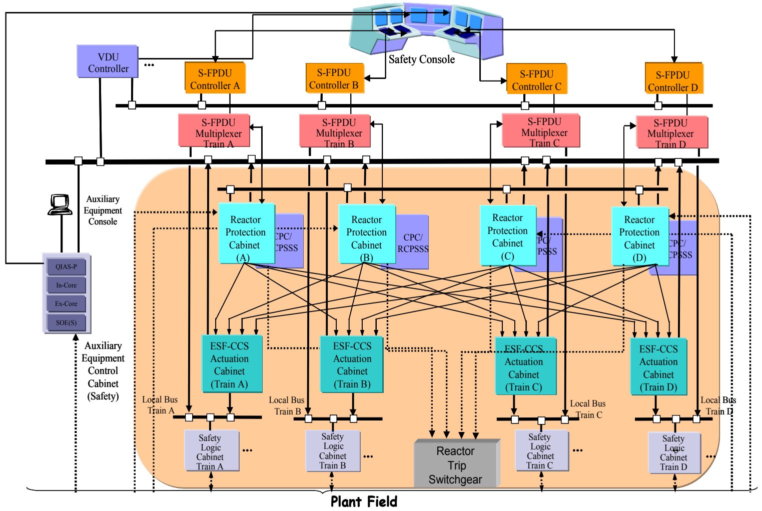
KAERI 한국원자력연구원
Korea Atomic Energy Research Institute

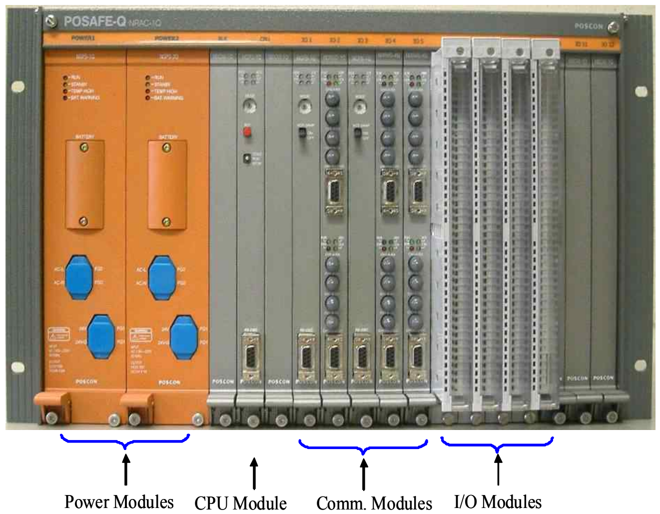
Contents

- Background: KNICS experiences
- Introduction: New HA approach
- Application: Case study of STPA
- Conclusion
- Discussion
  - on a harmonized dependability engineering

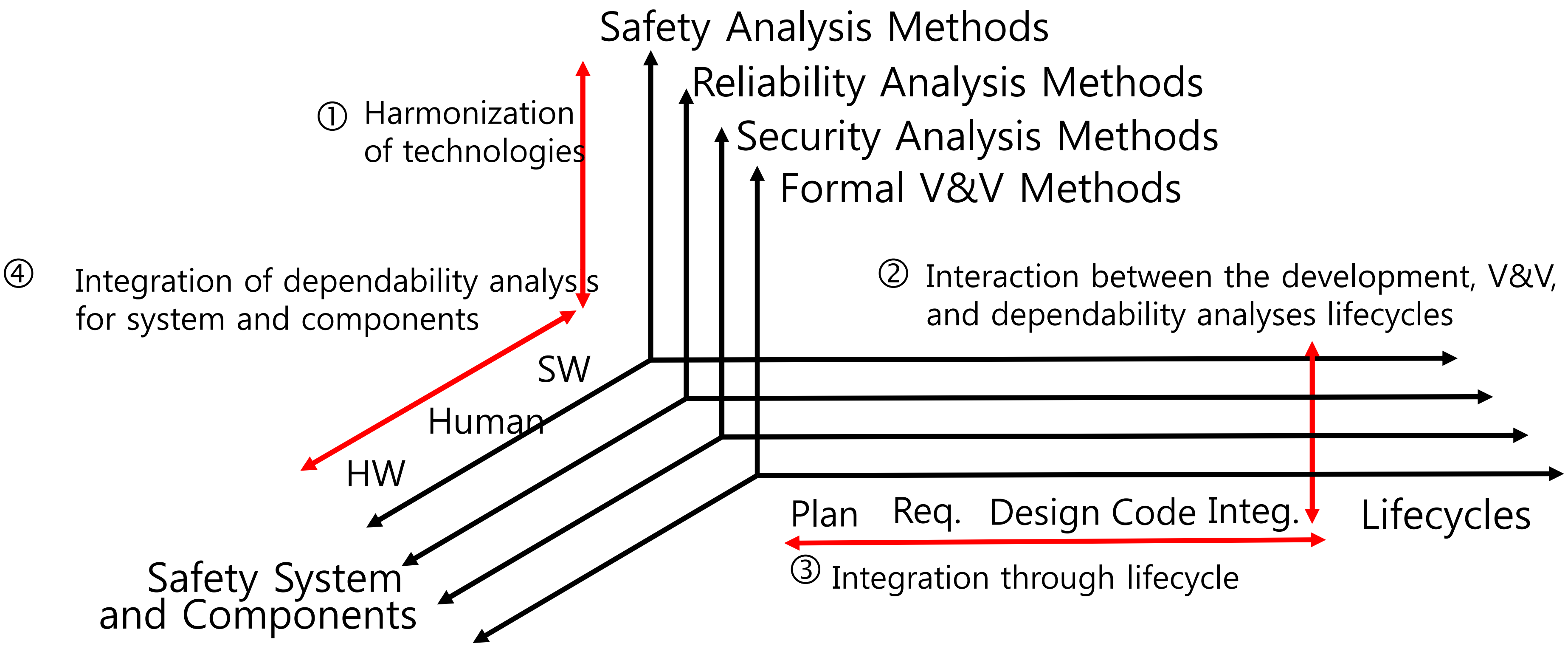
Korea Nuclear I&C System (KNICS)

- Instrumentation and Control (I&C) systems and equipment for APR1400 Nuclear Power Plant (NPP)
- Period: July 2001 ~ April 2008 (7 years)
- Target
  - Fully digitalized I&C systems development for APR1400 (Shin-Ulchin units #1&2)
  - I&C upgrade for existing NPPs

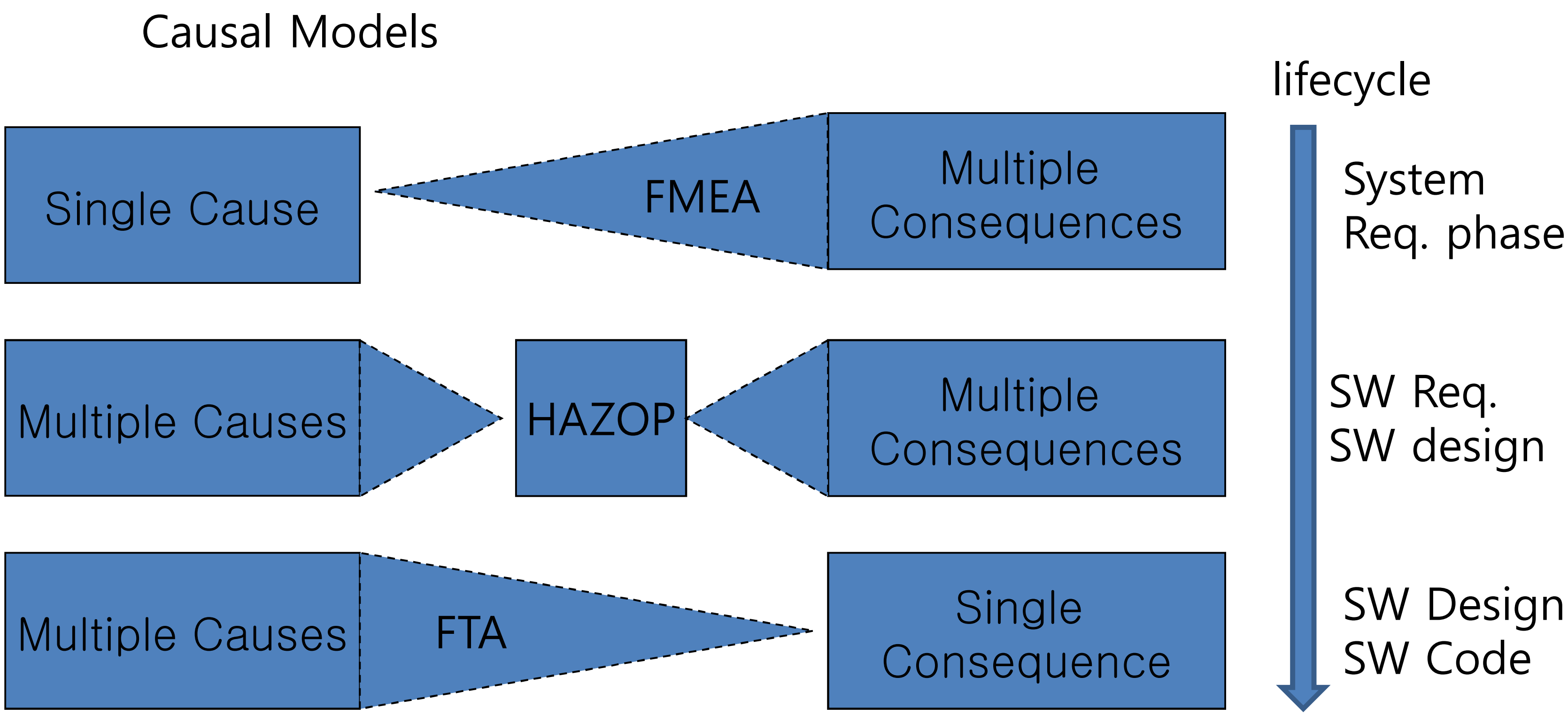




KNICS Dependability Engineering



Hazard Analysis of KNICS



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

Experiences from KNICS project

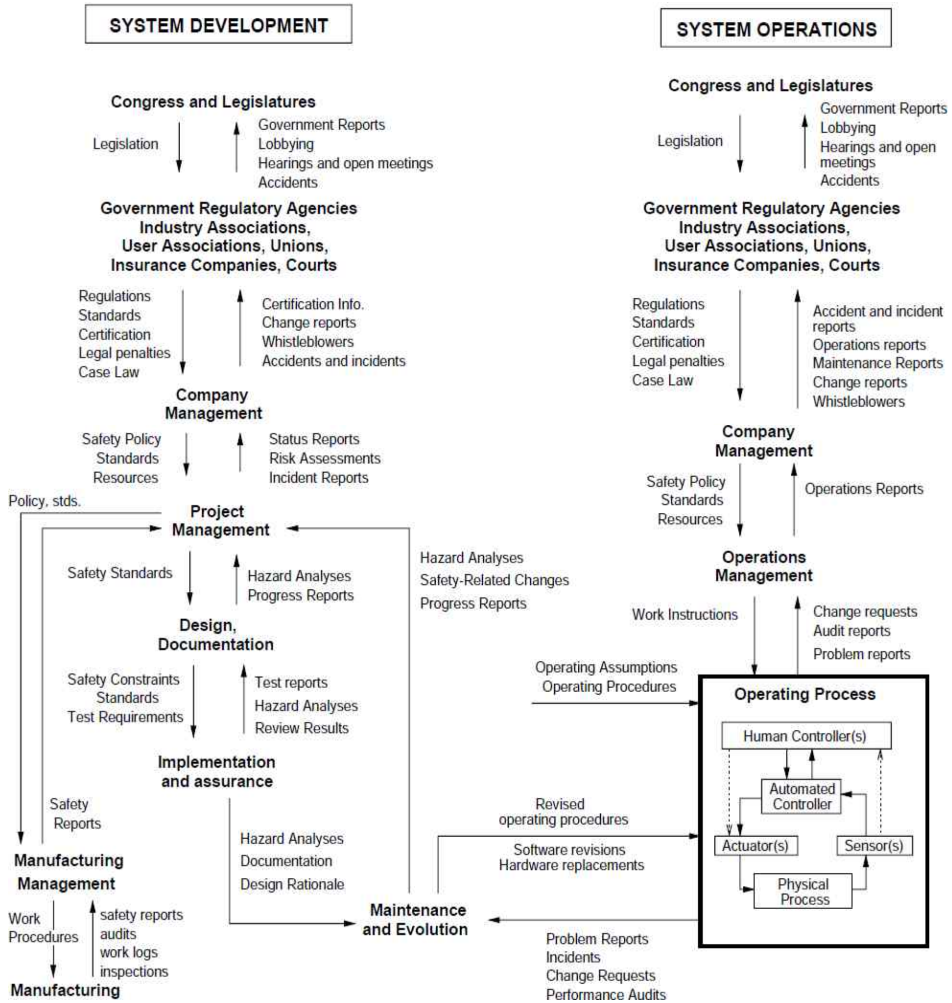
- Safety evidences
  - For developing the I&C system of a nuclear power plant, more than 1000 reports had been produced and had to be traceable through the lifecycle from the system requirements.
- Hazard analysis of complex systems(systems of systems) with traditional methods(FTA, HAZOP) was extremely difficult to justify the safety
- Most hazards came from the wrong interaction of the components (SW, HW, Human)

New Approach

- Traditional hazard analysis techniques, FTA, FMEA, and HAZOP, were not sufficient for modern systems.
  - More complex, software-intensive, socio-technical
- STAMP: a new accident causality model
- STPA: a new hazard analysis technique based on STAMP
- Prof. Nancy Leveson, MIT, “Engineering a Safer World”

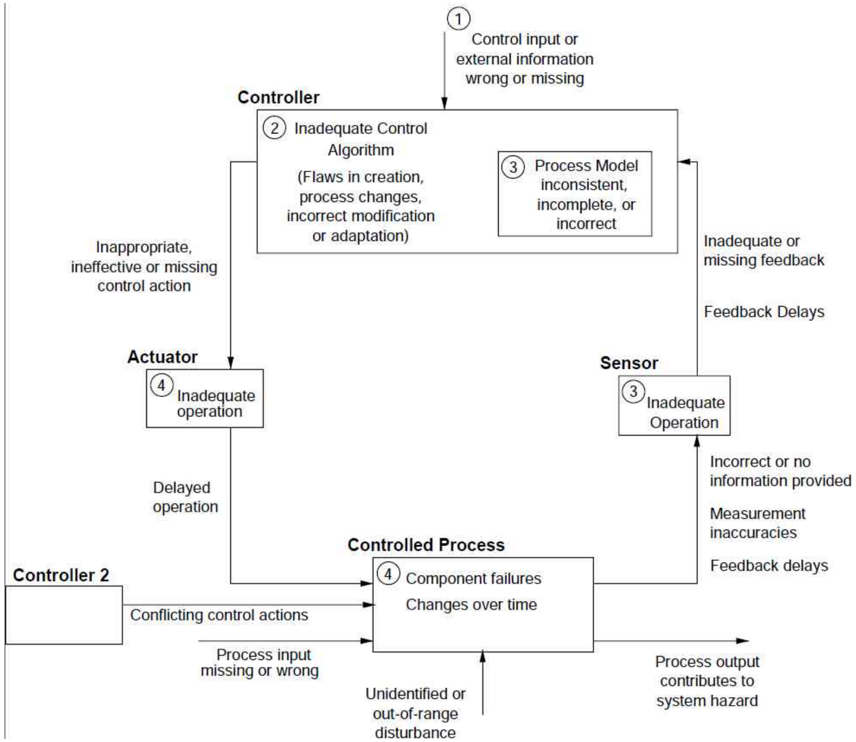
STAMP (System-Theoretic Accident Model and Processes)

- A new accident causality model based on systems theory and systems thinking
- Basic concepts
  - Safety constraints
  - Safety verification
  - Hierarchical safety control structure
  - Safety is trans-scientific issue



STPA(System-Theoretic Process Analysis)

- A new hazard analysis technique based on STAMP
- 4 types of inadequate control actions (Hazards)
  - Not provided
  - Provided
  - Wrong timing
  - Wrong duration



ESF-CCS

- Engineered Safety Features-Components Control System
- To mitigates the consequences of design-basis or loss-of-coolant accident
- 8 operational functions

Function	Description
SIAS	Safety Injection Actuation Signal
CIAS	Containment Isolation Actuation signal
MSIS	Main Stream Isolation Signal
CSAS	Containment Spray Actuation Signal
AFAS	Auxiliary Feed-water Actuation Signal
CREVAS	Control Room Emergency Ventilation Actuation Signal
FHEVAS	Fuel Handling Area Emergency Ventilation Actuation Signal
CPIAS	Containment Purge Isolation Actuation Signal

APPLICATION (0)

- Three functions
  - SIAS, CSAS, and CREVAS
- STPA steps
  1. Identify hazardous states of the system.
  2. Develop the control structure of the system.
  3. Identify the potential for inadequate control of the system that could lead to a hazardous state.
  4. Determine the causal factors of the hazardous control action

APPLICATION (1)

1. Identify hazardous states of the SIAS system.

- Hazard
  - Reactor core is damaged because the SIAS does not operate when the 4 events—LOCA, 2^{nd}HSL, S/WP-Ex, or REA—occur.
- Safety constraint
  - The SIAS must operate when the 4 events—LOCA, 2^{nd}HSL, S/WP-Ex, or REA—occur.

LOCA	Loss Of Coolant Accident
2^{nd}HSL	Second Heat Sink Loss
S/WP-Ex	Steam- and Water-pipe explosion
REA	Rod Ejection Accident

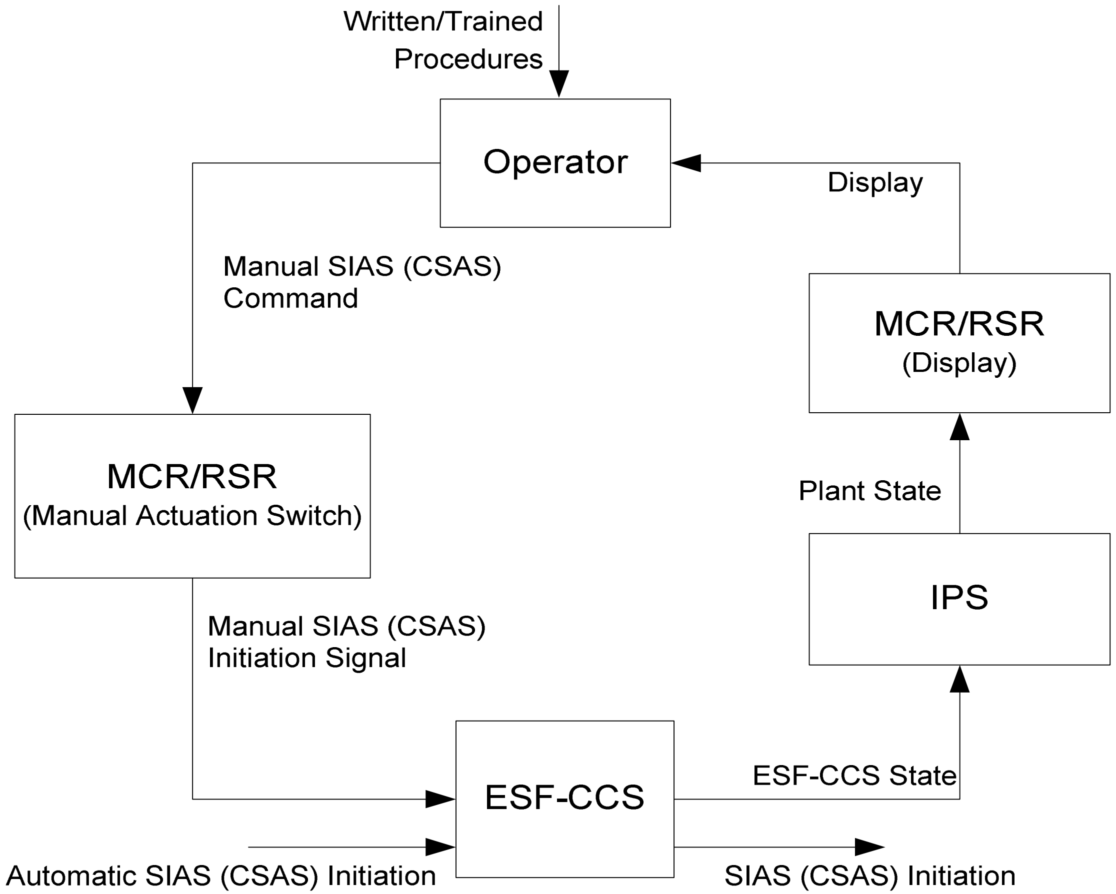
APPLICATION (1)

Hazards and Safety Constraints

Function	Hazard	Safety Constraint
SIAS	Reactor core is damaged because the SIAS does not operate when the 4 events—LOCA, 2^{nd}HSL, S/WP-Ex, or REA—occur.	The SIAS must operate when the 4 events—LOCA, 2^{nd}HSL, S/WP-Ex, or REA—occur.
CSAS	Heat removal and fission clean up fail when the three events—LOCA, S/WP-Ex, or the SIAS—occur.	The CSAS must operate when the three events—LOCA, S/WP-Ex, or the SIAS—occur.
CREVAS	Maintenance of pressure in a main control room fails when the two events—High-level radioactive at air intakes of MCR or the SIAS—occur.	The CREVAS must operate when the two events—High-level radioactive at air intakes of MCR or the SIAS—occur.

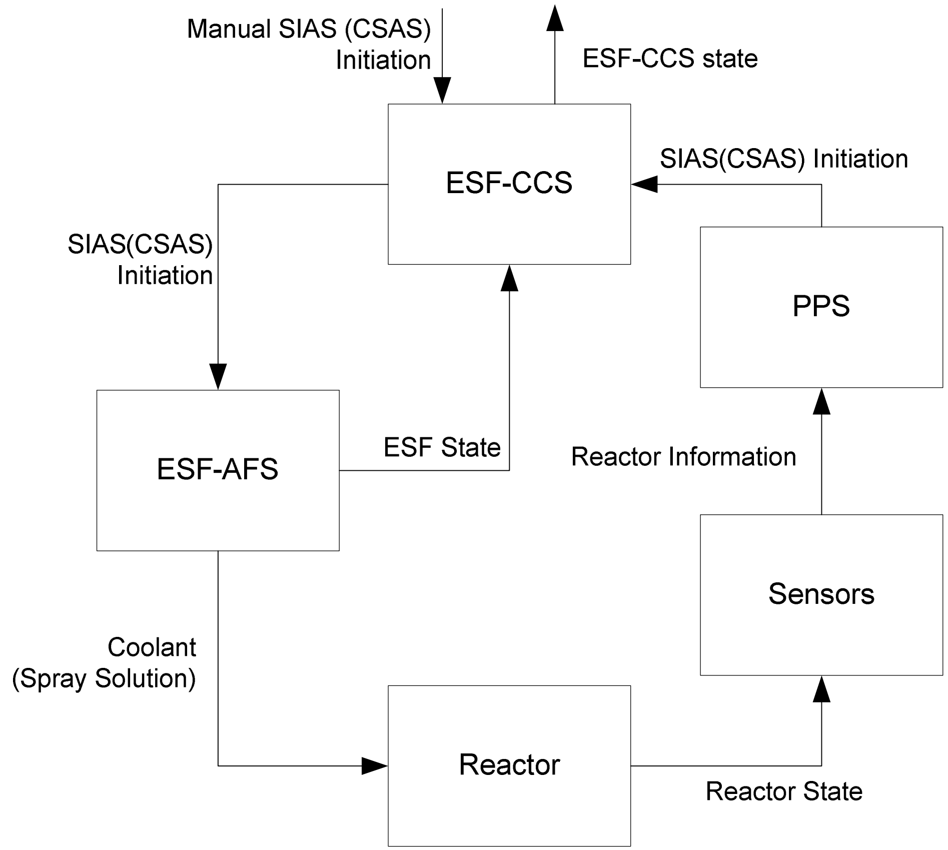
APPLICATION (2)

2. Develop the control structure of the system.



APPLICATION (2)

- Control structure



APPLICATION (3)

3. Identify the potential for inadequate control of the system that could lead to a hazardous state.

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing or Order Causes Hazard	Stopped Too Soon or Applied Too Long
SIAS ON (From ESF-CCS to ESF-AFS)	Not providing SIAS ON when LOCA occurs (a1) Not providing SIAS ON when 2ndHSL occurs (a2) Not providing SIAS ON when S/WP-Ex occurs (a3) Not providing SIAS ON when REA occurs (a4) Not providing SIAS ON when Manual SIAS Initiation occurs (a5)	Not hazardous	When LOCA occurs, ESF-CCS waits too long to turn SIAS ON (c1) When 2ndHSL occurs, ESF-CCS waits too long to turn SIAS ON (c2) When S/WP-Ex occurs, ESF-CCS waits too long to turn SIAS ON (c3) When REA occurs, ESF-CCS waits too long to turn SIAS ON (c4) When Manual SIAS Initiation occurs, ESF-CCS waits too long to turn SIAS ON (c5)	SIAS ON stops before coolant is not provided enough (d1)

APPLICATION (3)

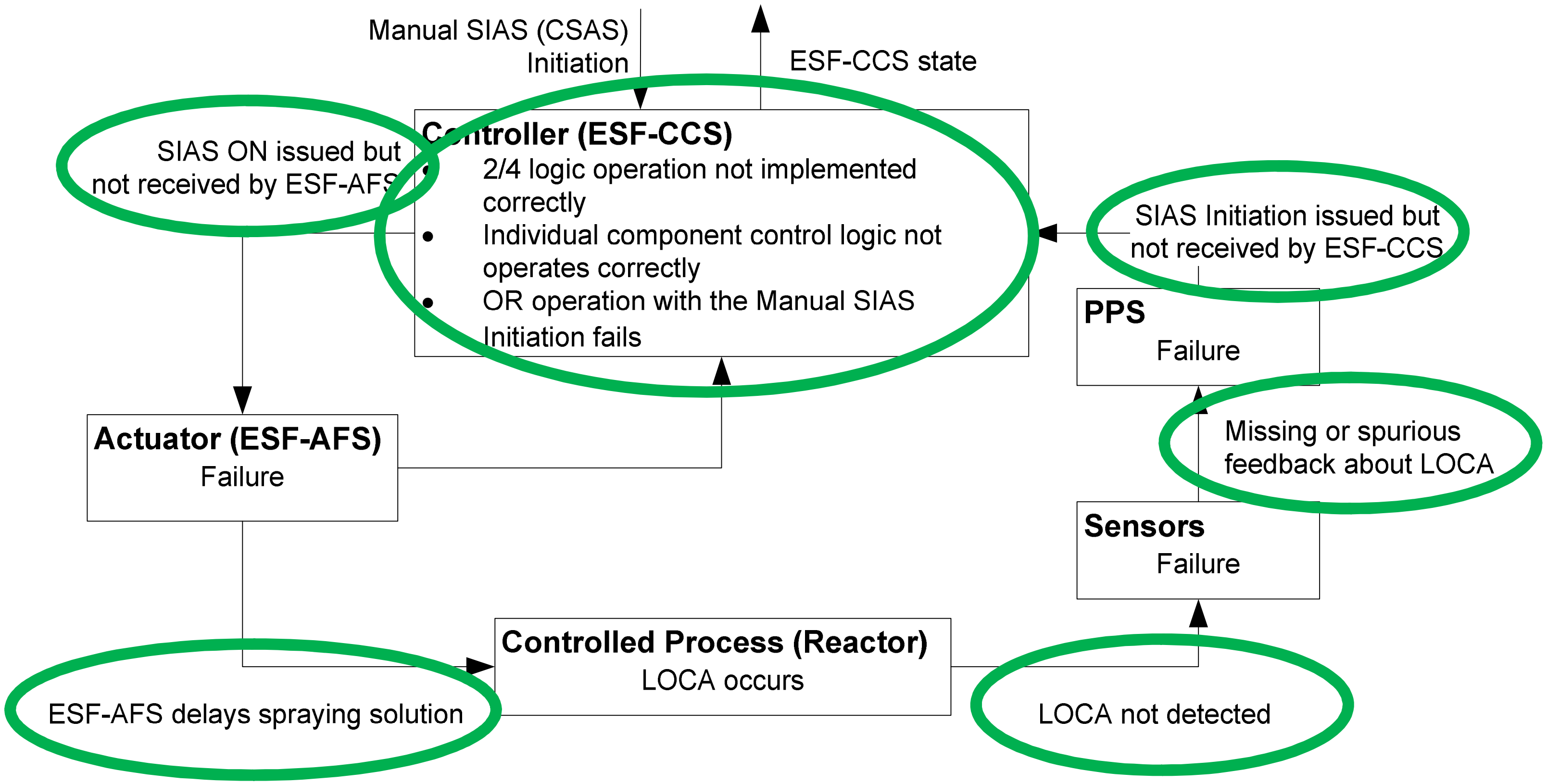
Hazardous behaviour of the SIAS

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing or Order Causes Hazard	Stopped Too Soon or Applied Too Long
SIAS ON (From ESF-CCS to ESF-AFS)	Not providing SIAS ON when LOCA occurs (a1) Not providing SIAS ON when 2ndHSL occurs (a2) Not providing SIAS ON when S/WP-Ex occurs (a3) Not providing SIAS ON when REA occurs (a4) Not providing SIAS ON when Manual SIAS Initiation occurs (a5)	Not hazardous	When LOCA occurs, ESF-CCS waits too long to turn SIAS ON (c1) When 2ndHSL occurs, ESF-CCS waits too long to turn SIAS ON (c2) When S/WP-Ex occurs, ESF-CCS waits too long to turn SIAS ON (c3) When REA occurs, ESF-CCS waits too long to turn SIAS ON (c4) When Manual SIAS Initiation occurs, ESF-CCS waits too long to turn SIAS ON (c5)	SIAS ON stops before coolant is not provided enough (d1)
SIAS OFF (From ESF-CCS to ESF-AFS)	Not hazardous	Providing SIAS OFF when LOCA occurs (b1) Providing SIAS OFF when 2ndHSL occurs (b2) Providing SIAS OFF S/WP-Ex occurs (b3) Providing SIAS OFF REA occurs (b4) Providing SIAS OFF when Manual SIAS Initiation occurs (b5)	SIAS OFF is provided before the temperature decrease enough (c6)	Not hazardous
Manual SIAS ON (From Operator to MCR/RSR)	Not providing SIAS ON when LOCA occurs (a6) Not providing SIAS ON when 2ndHSL occurs (a7) Not providing SIAS ON when S/WP-Ex occurs (a8) Not providing SIAS ON when REA occurs (a9)	Not hazardous	When LOCA occurs, ESF-CCS waits too long to turn SIAS ON (c7) When 2ndHSL occurs, ESF-CCS waits too long to turn SIAS ON (c8) When S/WP-Ex occurs, ESF-CCS waits too long to turn SIAS ON (c9) When REA occurs, ESF-CCS waits too long to turn SIAS ON (c10)	Not hazardous

APPLICATION (4)

4. Determine the causal factors of the hazardous control action

Hazard: Not providing SIAS ON when LOCA occur (a1)



Need to create requirements specification without control flaws

APPLICATION (4)

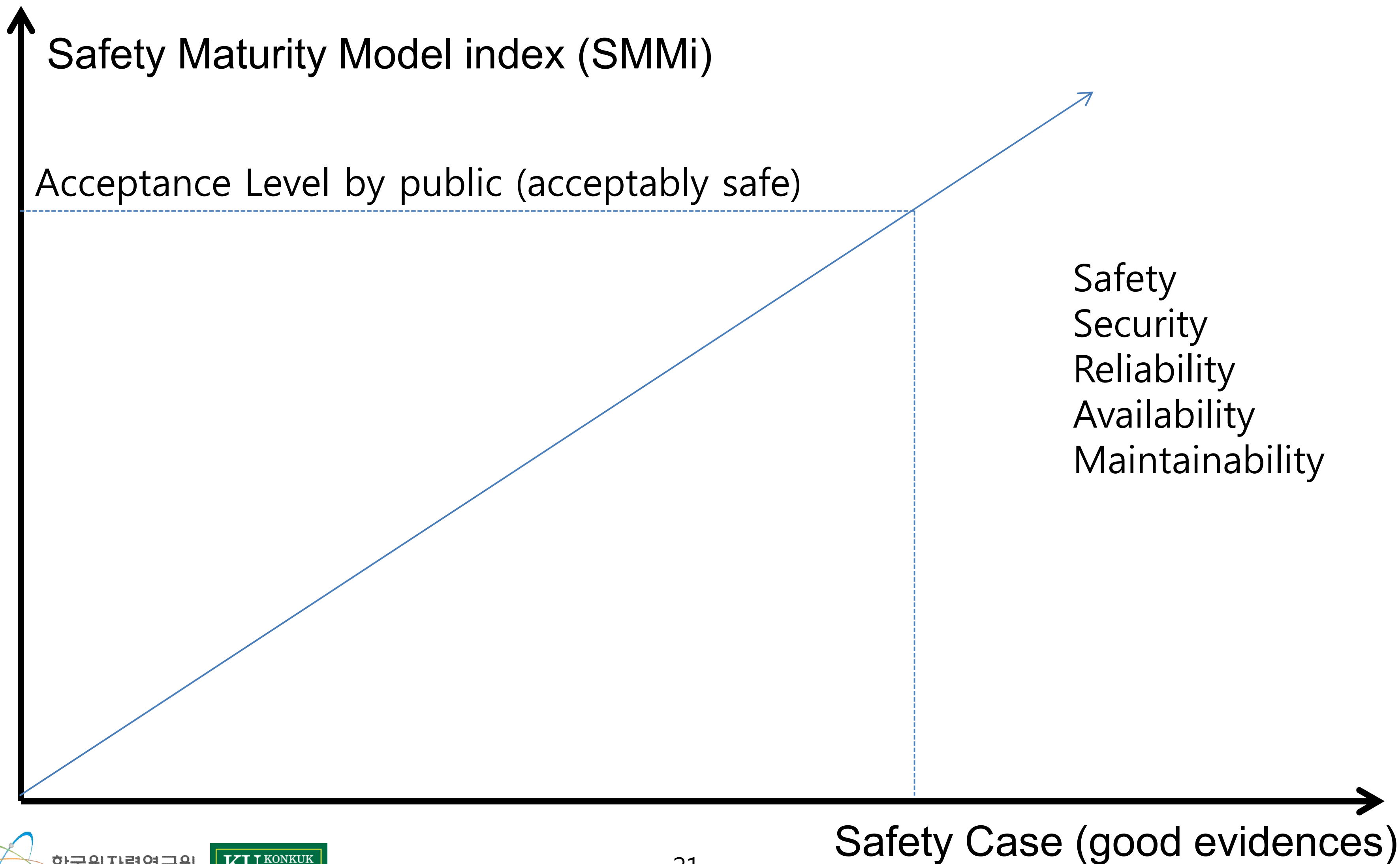
Causal factors of unsafe control actions of SIAS (a1-a9)

UCAs	A part of the safety control structure	Causal Factors
(a1-a4)	ESF-CCS	2/4 logic operation not implemented correctly
		Individual component control logic not operates correctly
		OR operation with the Manual SIAS Initiation fails
	SIAS On(ESF-CCS to ESF-AFS)	SIAS ON issued but not received by ESF-AFS
	ESF-AFS	ESF-AFS fails to implement its function
	Release Coolant (ESF-AFS to Reactor)	ESF-AFS delays spraying solution
	Sensing (Reactor to Sensor)	The 4 events is not detected by Sensor
	Sensor	Sensor fails
	Reactor's state (Sensor to PPS)	Sensor provides spurious feedback
	PPS	PPS received the feedback correctly but does not issue SIAS Initiation
	SIAS Initiation (PPS to ESF-CCS)	SIAS Initiation issued but not received by ESF-CCS
(a5)	ESF-CCS	OR operation with the SIAS Initiation of PPS fails
	SIAS On(ESF-CCS to ESF-AFS)	SIAS ON issued but not received by ESF-AFS
	ESF-AFS	ESF-AFS fails to implement its function
	Release Coolant (ESF-AFS to Reactor)	ESF-AFS delays spraying solution
(a6-a9)	Operator	Judgement fails about the 4 events
		Misunderstanding about state of Safety Injection operation
	Manual SIAS (Operator to MCR/RSR)	SIAS Initiation issued but not received by MCR/RSR
	MCR/RSR (Manual Actuation Switch)	Manual Actuation Switch fails
	Manual SIAS Initiation Signal (MCR/RSR to ESF-CCS)	Manual SIAS Initiation Signal issued but not received by ESF-CCS
	ESF-CCS State (ESF-CCS to IPS)	ESF-CCS provides spurious information about Safety Injection
		Information about Safety Injection issued but not received by IPS
	MCR/RSR (Display)	MCR/RSR fails to display information
	Display (MCR/RSR to Operator)	Information of the 4 events issued but not received by Operator
		MCR/RSR displays spurious information about the 4 events and Safety Injection

CONCLUSION

- STPA provides analysts with a systematic method to analyse hazards with a global view.
- However, development of safety control structures and identification of causal factors of hazards were still subjective, depending on the domain-knowledge of analyst.
- Future Works to be objective HA
  - Need an automatic STPA based on a process model of system
  - STPA based on a formal(NuSCR) model
  - Need to find an optimized framework for safety demonstration(STPA, Safety Case, and traditional causal-chain methods)

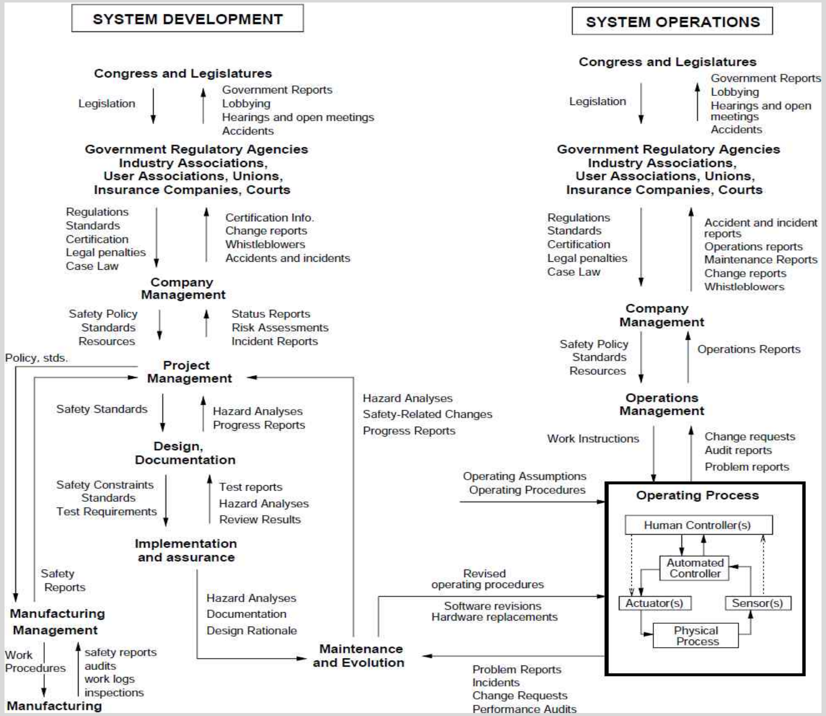
Discussion: Harmonized Dependability?



Discussion: A Harmonized Safety Analyses

Safety Maturity Model index (SMMi)

STAMP



Socio-technical interaction failures

Safety Case (good evidences)

한국원자력연구원 KAERI Korea Atomic Energy Research Institute

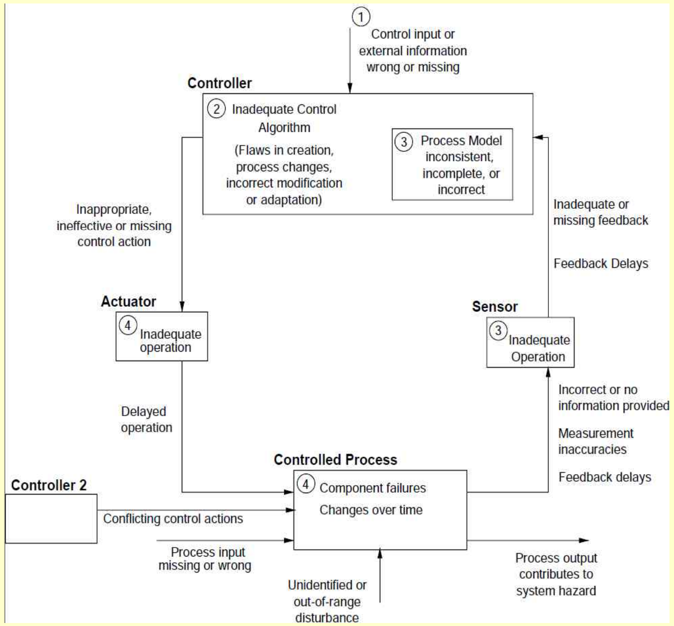
KU KONKUK UNIVERSITY

Discussion: A Harmonized Safety Analyses

Safety Maturity Model index (SMMi)

STAMP

STPA by control loops



Components interaction failures

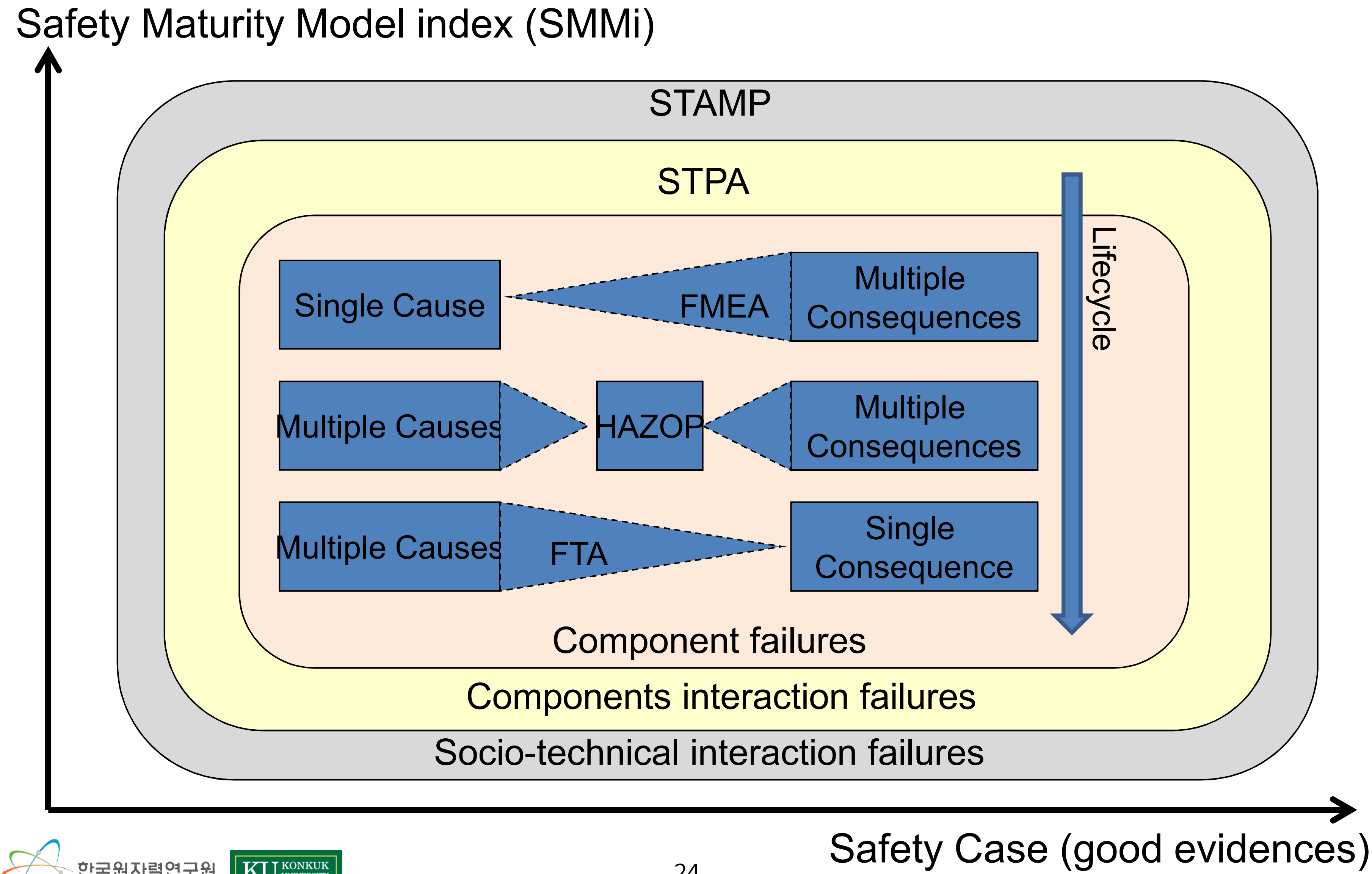
Socio-technical interaction failures

Safety Case (good evidences)

한국원자력연구원 KAERI Korea Atomic Energy Research Institute

KU KONKUK UNIVERSITY

Suggestion: A Harmonized Safety Analyses



THANK YOU

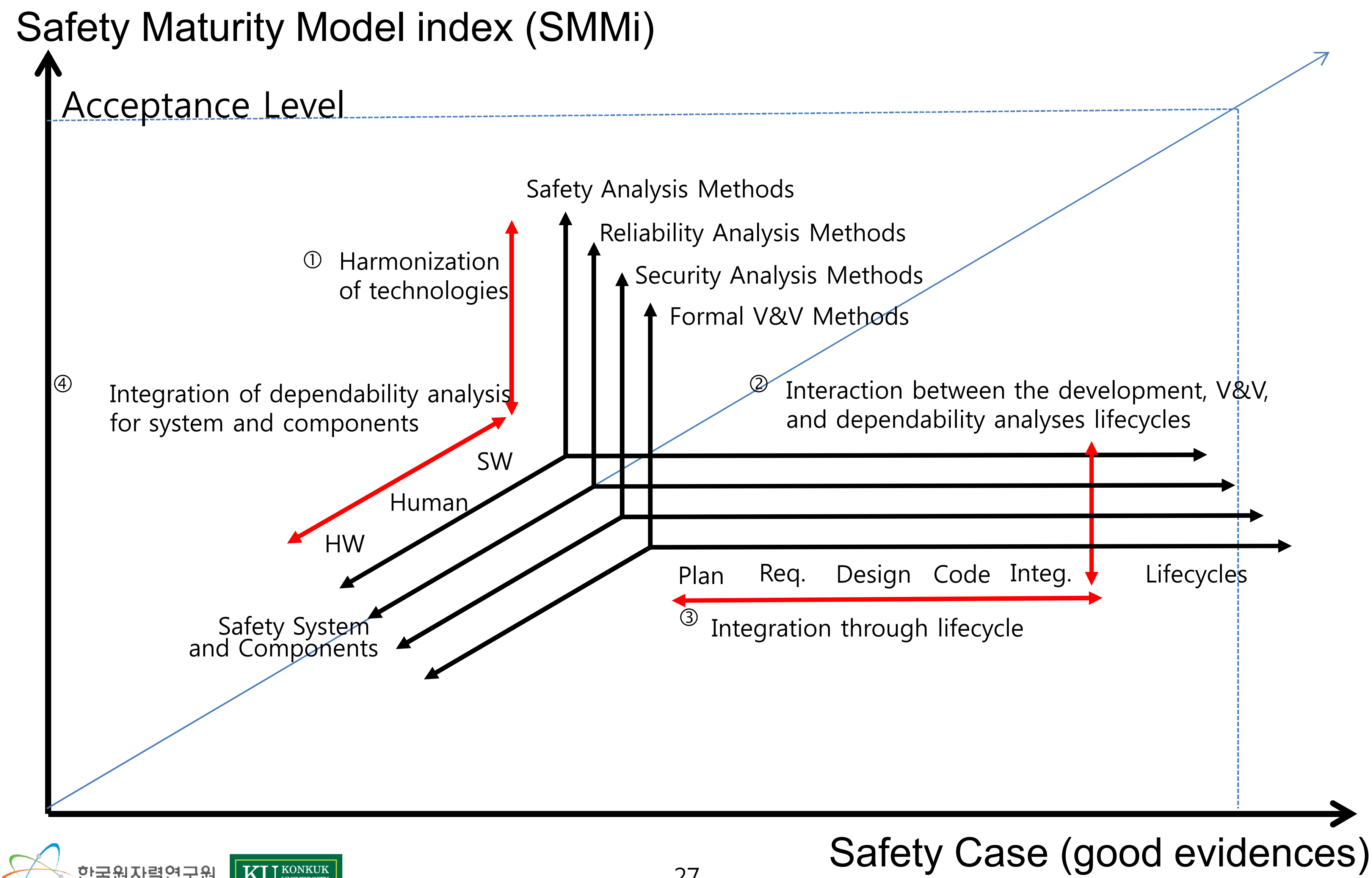
For a Safer World

jslee@kaeri.re.kr

한국원자력연구원
Korea Atomic Energy Research Institute
KU KONKUK UNIVERSITY

APPENDIX

Goal: A Harmonized Dependability Engineering?



한국원자력연구원 Korea Atomic Energy Research Institute KAERI
KU KONKUK UNIVERSITY

Discussion:

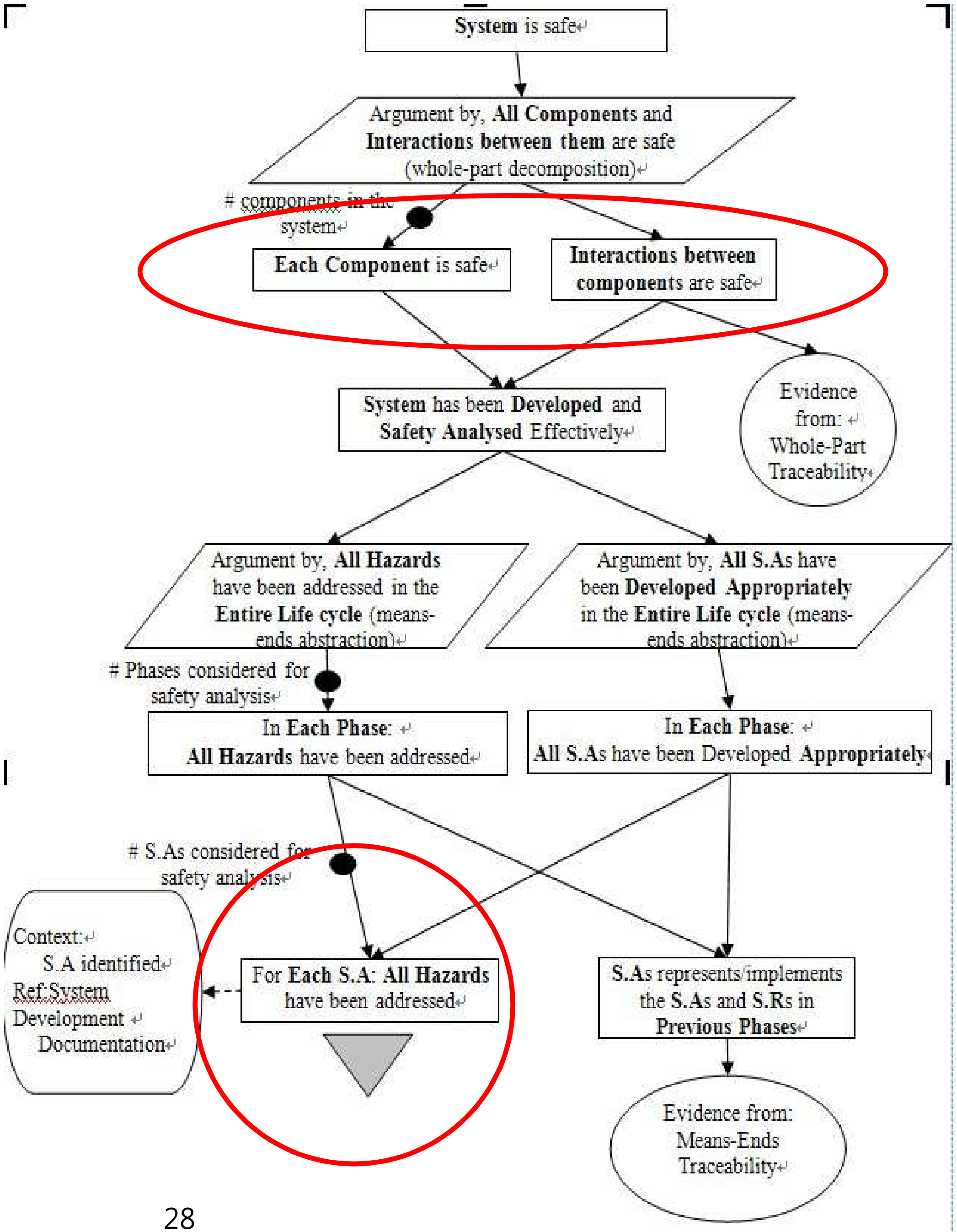
Building Safety Case through means-ends and whole-part traceability

Whole-Part Traceability –

Traceability between S.As and safety analysis results belonging to different abstractions

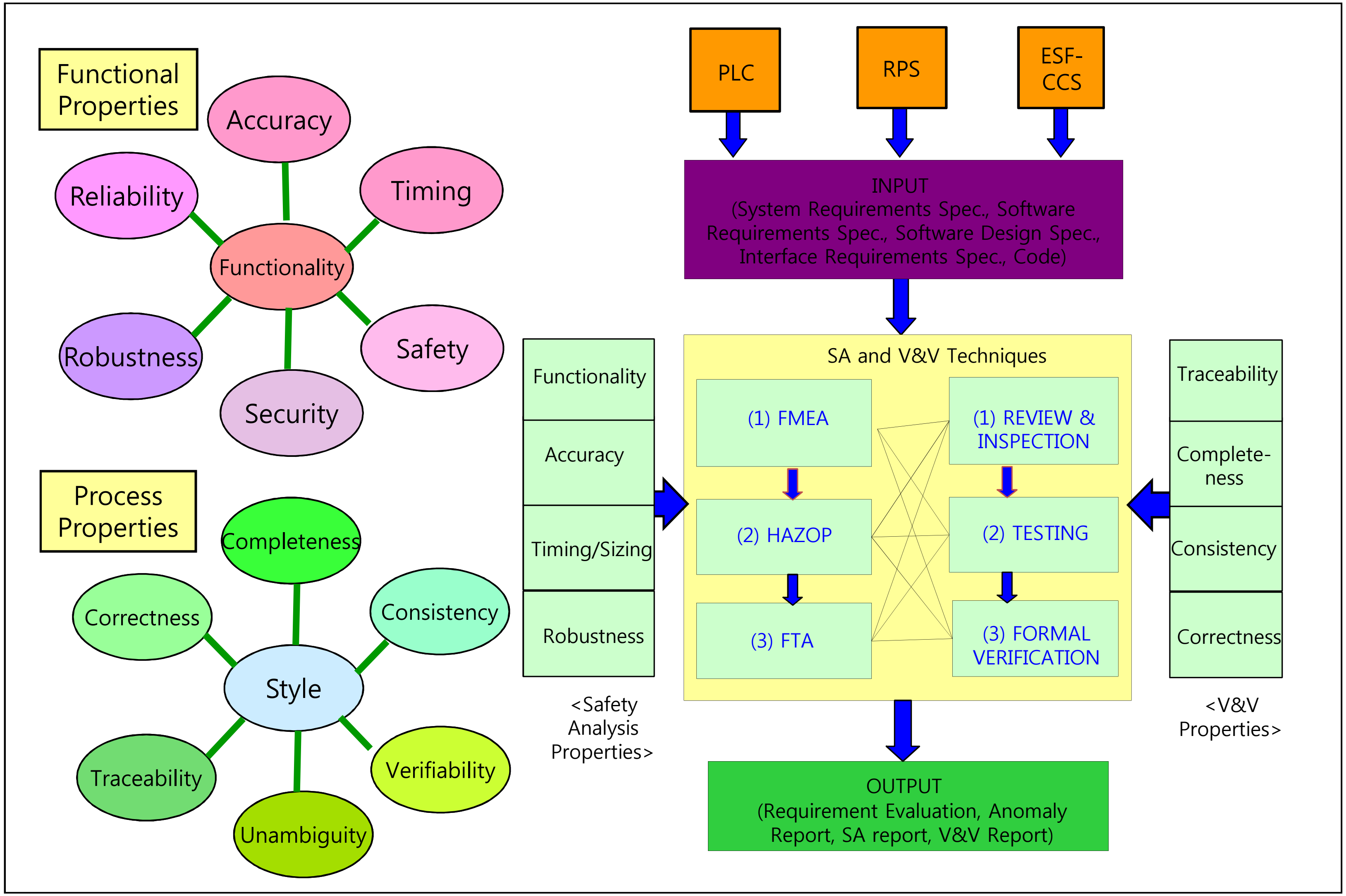
Means-Ends Traceability –

Traceability between S.As and safety analysis results belonging to different phases



Background:

Safety Analysis and V&V



Means-Ends and Whole-Part Safety Analysis

Safety Enforcement

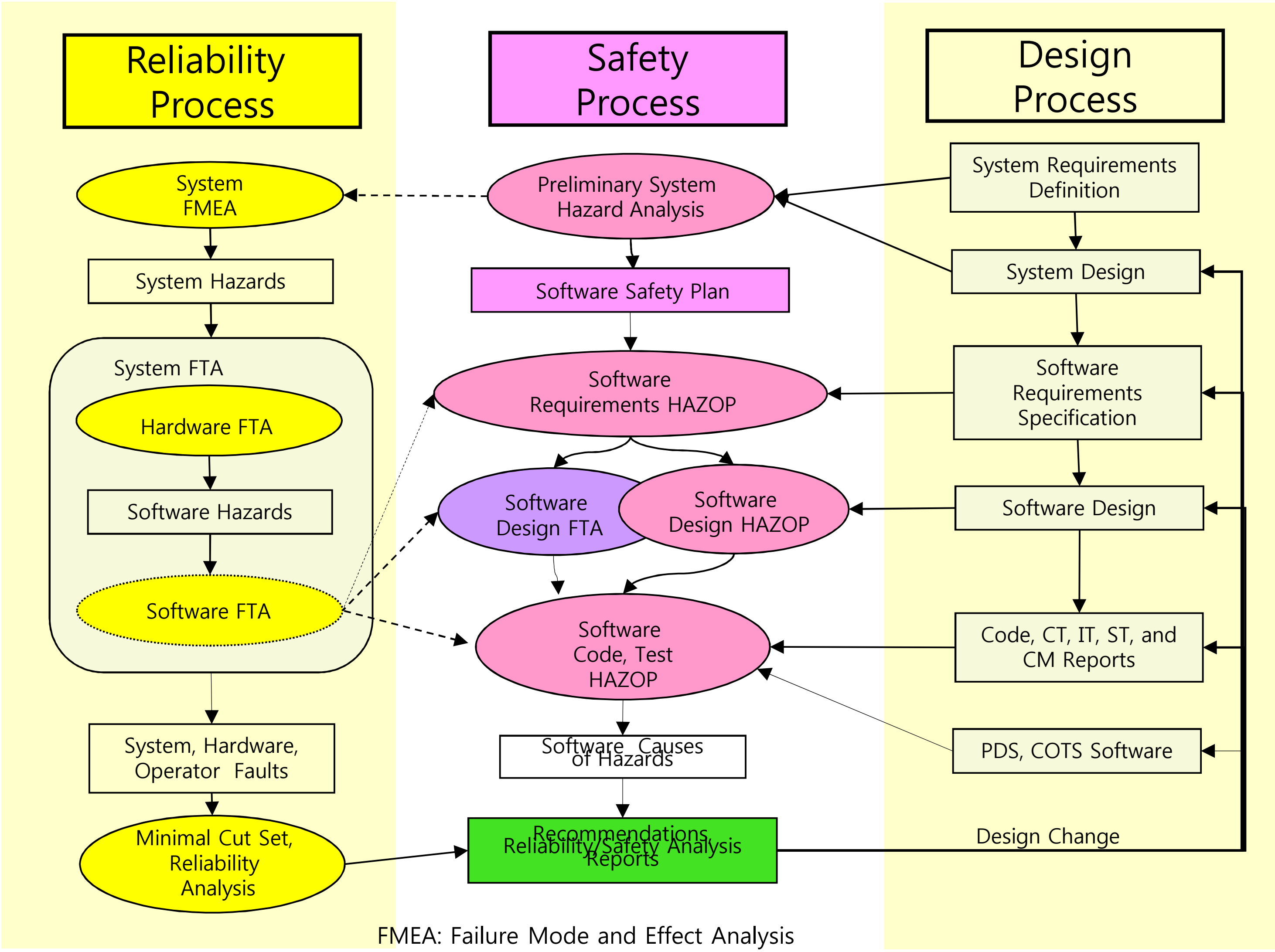
Safety Verification

Level	Means-Ends \ Whole-Part	Environment System Human Hardware Software: Safety Enforcement	Safety Verification	KNICS Methods: PLC	KNICS Methods: RPS
1	Purposes, Safety constraints	WHY	WHY	STPA	STPA
2	Abstract functions	WHY, WHAT	Req. SA, WHY	SW Req. HAZOP	SW Req. HAZOP
3	General functions	WHY, WHAT	HOW, Design SA, WHY	SW Design HAZOP	SW Design FBD FTA
4	Physical processes	WHAT	HOW, Code SA	SW Code HAZOP	SW Code FBD FTA
5	Physical form		HOW	Integration HAZOP	Integration HAZOP

SA: Safety Analysis, FBD: Function Block Diagram

한국원자력연구원 Korea Atomic Energy Research Institute KAERI · KU KONKUK UNIVERSITY

Safety Engineering Processes



FMEA: Failure Mode and Effect Analysis
HAZOP: Hazard and Operability, FTA: Fault Tree Analysis
PDS: Pre-Developed Software, COTS: Commercial-Off-The-Shelf