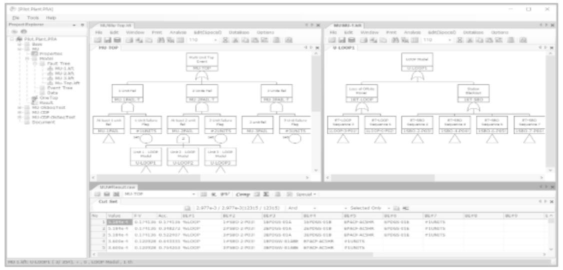


A novel approach for quantitative importance analysis of DI&C systems in NPP

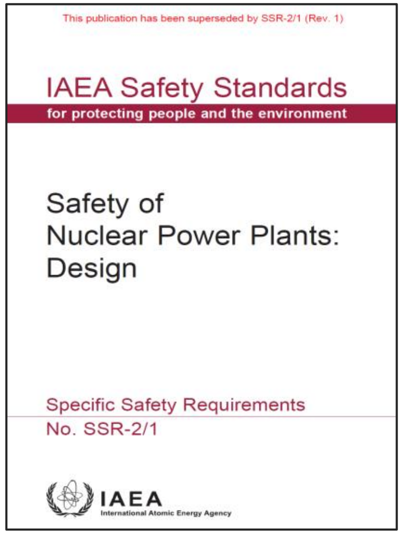
June 27. 2022

KAERI, Risk Assessment Team

Sung-Min Shin, Sang Hun Lee, Seung Ki Shin

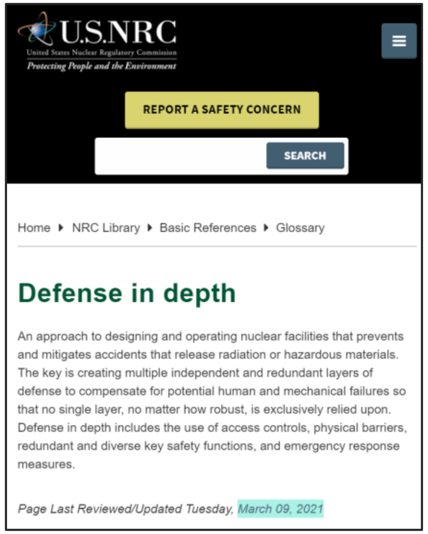
Contents

Introduction | Ideal goal



The defence in depth (DiD) concept is applied to all safety related activities, whether organizational, behavioral or design related, and whether in full power, low power or various shutdown states.

<u>This is to ensure that all safety related activities are subject to independent layers of provisions,</u> so that if a failure were to occur, it would be detected and compensated for or corrected by appropriate measures.



Home ▸ NRC Library ▸ Basic References ▸ Glossary

Defense in depth

An approach to designing and operating nuclear facilities that prevents and mitigates accidents that release radiation or hazardous materials. The key is creating multiple independent and redundant layers of defense to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon. Defense in depth includes the use of access controls, physical barriers, redundant and diverse key safety functions, and emergency response measures.

Page Last Reviewed/Updated Tuesday, March 09, 2021

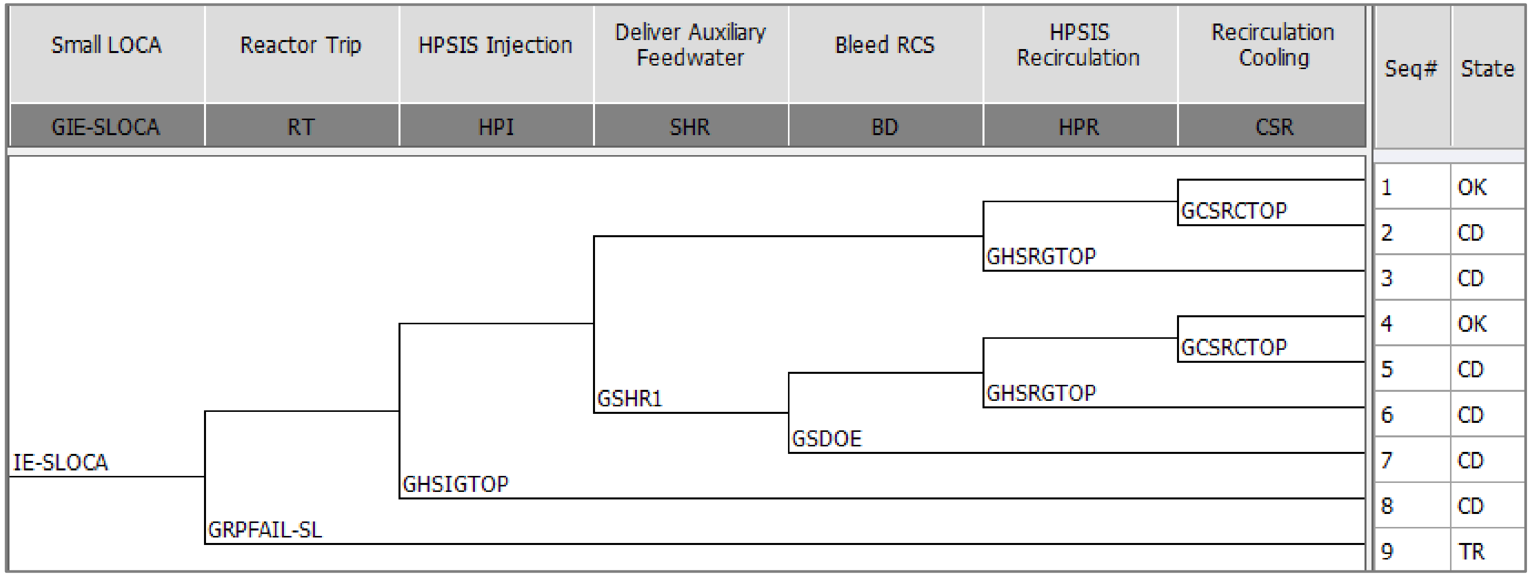
An approach to designing and operating nuclear facilities that prevents and mitigates accidents that release radiation or hazardous materials.

<u>The key is creating multiple independent and redundant layers of defense</u> to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon.

DiD includes the use of access controls, physical barriers, redundant and diverse key safety functions, and emergency response measures.

Introduction | In reality

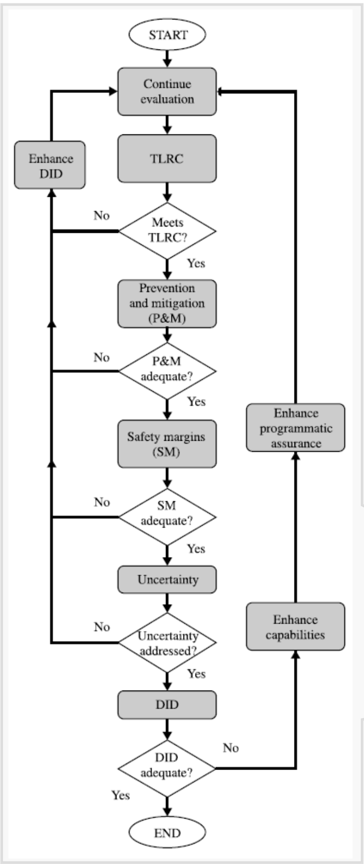
SLOCA ET on OPR-1000



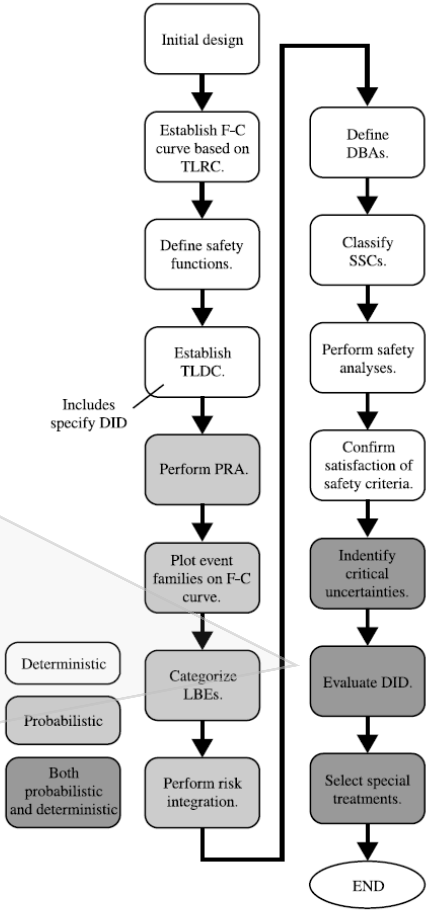
For the I&C systems, in fact, they are not possible to be completely independent of the paths of "instrumentation – decision making – control" required for each mitigation procedure.

➔ We need to evaluate the suitability of redundancy and diversity in the I&C functions for accident mitigation.

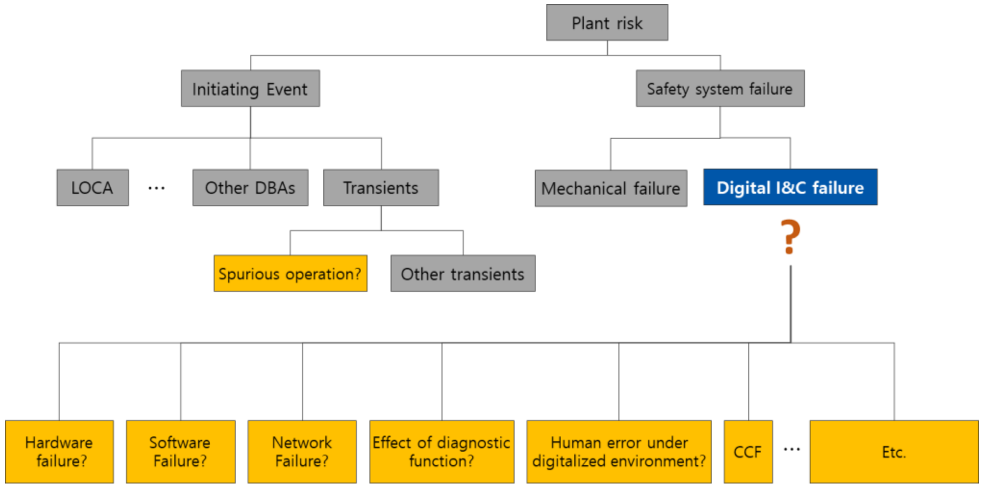
Introduction | In reality



Logic for implementing evaluation of DID



Safety desing process overview[1)2)]



Approximate configuration of DI&C fault tree

Basically, it seems that the evaluation of DID is based on the PSA, but in the case of digital I&C(DI&C), It is difficult to model the correlation of DI&C components according to the FT framework, and it is even more difficult to secure failure information of them.

➔ Can we derive quantitative evaluation results of DI&C systems without failure information or FT framework.

1) Andrea Maioli, David J. Finnicum, Robert H. Lichtenstein, Stephanie Y. Harsche, "Use of PSA in the Development of SMRs", NEA/CSNI/R(2012)2
2) nuclear safety design process for modular helium-cooled reactor plants(ANSI/ANS-53.1-2011)

Introduction | Overview of the approach

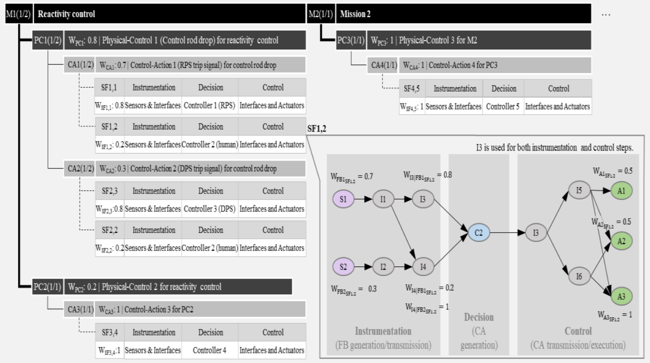
<u>Develop equations</u> to calculate the importance of each component

DI&C systems have complex interactions that are difficult to clearly analyze without a separate model.

- Functional requrirements
- Conceptual design
- Operational strategies

.
.
.

Related Information



<u>Modeling</u> of DI&C system

<u>Assign weights</u> according to the information of system design and operation strategies instead of failure information.

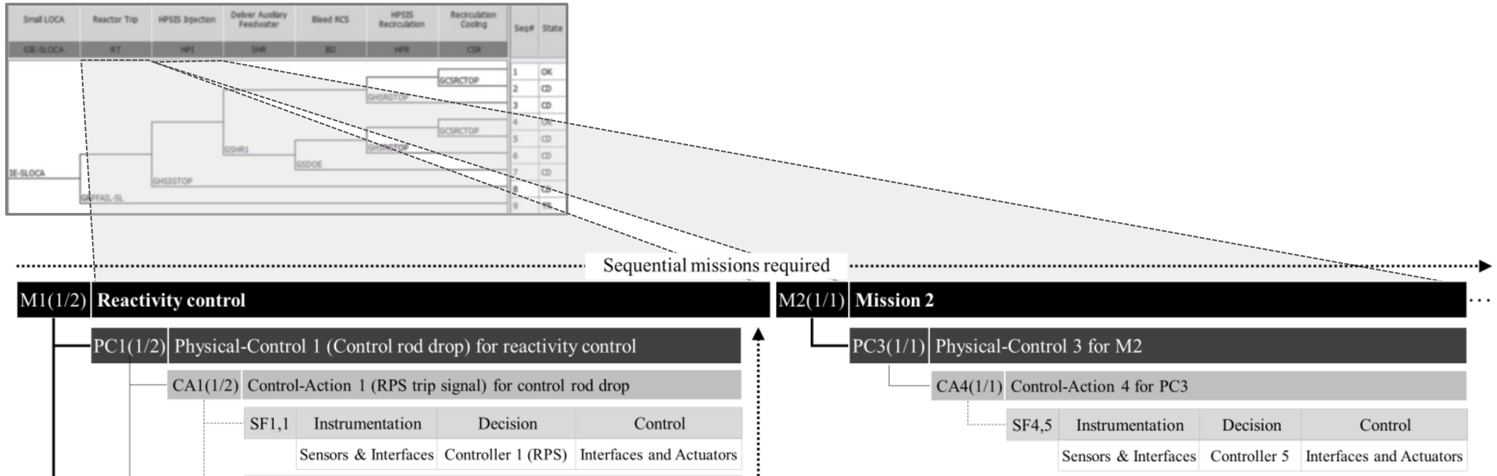
PC	W_{PC1}					0.8	W_{PC2}		0.2	IM_n
CA	W_{CA1}					1	W_{CA2}		1	
SF	$W_{SF1,1}$		0.8	$W_{SF1,2}$		0.2	$W_{SF2,2}$		1	
n	$IM^{INS}_{n\|SF1,1}$	$IM^{DEC}_{n\|SF1,1}$	$IM^{CTL}_{n\|SF1,1}$	$IM^{INS}_{n\|SF1,2}$	$IM^{DEC}_{n\|SF1,2}$	$IM^{CTL}_{n\|SF1,2}$	$IM^{INS}_{n\|SF2,2}$	$IM^{DEC}_{n\|SF2,2}$	$IM^{CTL}_{n\|SF2,2}$	
S1	1			0.7			0.6			0.872
S2				0.3			0.2			0.088
S3							0.2			0.040
C1		1								0.640
C2					1			1		0.360
A1			0.5			0.5				0.400
A2			0.5			0.5				0.400
A3									1	0.200
A4			1			1				0.800
A5									1	0.200
A6			1			1			1	1.000
I1	1									0.640
I2				1			0.8			0.320
I3							0.2			0.040
I4	1									0.640
I5				0.8		1	0.8		1	0.648
I6				0.2			0.8			0.192
I7			1							0.640
I8			0.67			0.67				0.536
I9			1			1			1	1.000

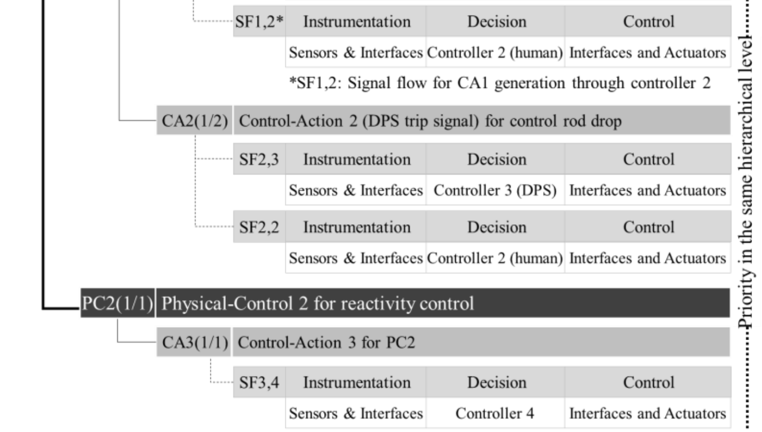
<u>Quantification relative importance</u>
of each component

A component is important if it is used for an important functioning and it is used often.

DI&C system modeling | Macro model for functional redundancy and diversity

- Review the functional redundancy and diversity relevant to the DI&C system at each heading in an ET and re-organize it according to a specific hierarchal form: Mission(M) – Physical control(PC) – Control Action(CA) – Signal Flow(SF)





• • •

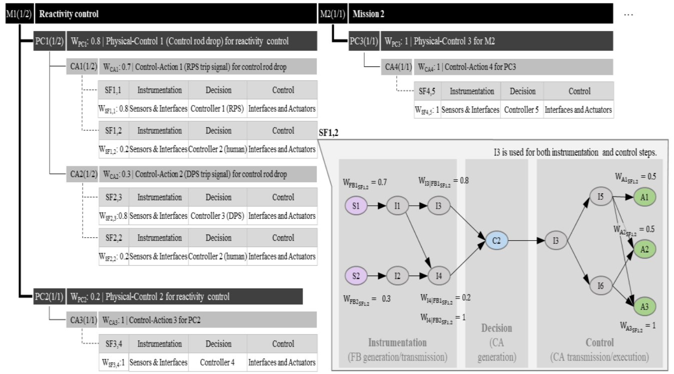
▶ **Hierarchical structure is as follows:**

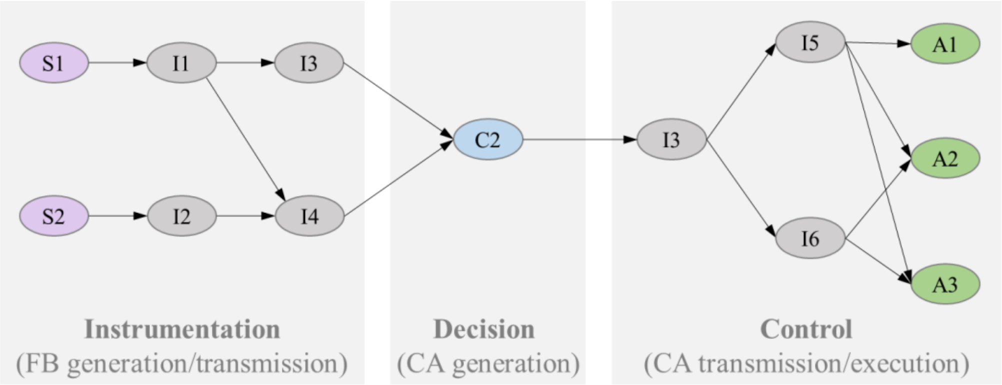
- **Mission (M)**: Role required for I&C system in a specific heading.
- **Physical Control (PC)**: Sub-role to fulfill the upper mission.
- **Control Action (CA)**: The same physical control can be activated by various control actions, which is a kind of safety signal that needs to be generated.
- **Signal Flow (SF)**: The same CA may also be generated by different paths. SF is signal transfer path between related components from measurement to control.

▶ **Clarify the success criteria for the parent hierarchy.**

DI&C system modeling | Micro model for redundancy and diversity in a SF

- Review all the signal transfer paths (instrumentation – decision making – control) in an SF and organize interactions between components used according to a specific form.
  - Three steps in a SF
    - Instrumentation: Generation/transmission of Feedback (FB; sensing signal)
    - Decision: Decision on whether or not to generate a CA
    - Control: Transmission/execution of the CA generated
  - The three steps consists of some of the following four types of components
    - Sensor (S): a component that generates FB
    - Actuator (A): a component that receives a CA and performs corresponding physical actions.
    - Controller (C): a component that determines whether a CA is generated or not, and which CA should be generated
    - Interface (I): a component that transmits FB from a sensor to a controller or a CA from a controller to an actuator





→ It is assumed that each step has a one-way serial signal connection, and that the complete failure of one step leads to the failure of the corresponding SF.

Weight assignment | Functional redundancy and diversity

M1(1/2) | Reactivity control

- PC1(1/2) | W_{PC1}: 0.8 | Physical-Control 1 (Control rod drop) for reactivity control
  - CA1(1/2) | W_{CA1}: 0.7 | Control-Action 1 (RPS trip signal) for control rod drop

SF1,1	Instrumentation	Decision	Control
$W_{SF1,1}$: 0.8	Sensors & Interfaces	Controller 1 (RPS)	Interfaces and Actuators

SF1,2	Instrumentation	Decision	Control
$W_{SF1,2}$: 0.2	Sensors & Interfaces	Controller 2 (human)	Interfaces and Actuators

  - CA2(1/2) | W_{CA2}: 0.3 | Control-Action 2 (DPS trip signal) for control rod drop

SF2,3	Instrumentation	Decision	Control
$W_{SF2,3}$:0.8	Sensors & Interfaces	Controller 3 (DPS)	Interfaces and Actuators

SF2,2	Instrumentation	Decision	Control
$W_{SF2,2}$: 0.2	Sensors & Interfaces	Controller 2 (human)	Interfaces and Actuators

- PC2(1/1) | W_{PC2}: 0.2 | Physical-Control 2 for reactivity control
  - CA3(1/1) | W_{CA3}: 1 | Control-Action 3 for PC2

SF3,4	Instrumentation	Decision	Control
$W_{SF3,4}$:1	Sensors & Interfaces	Controller 4	Interfaces and Actuators

M2(1/1) | Mission 2

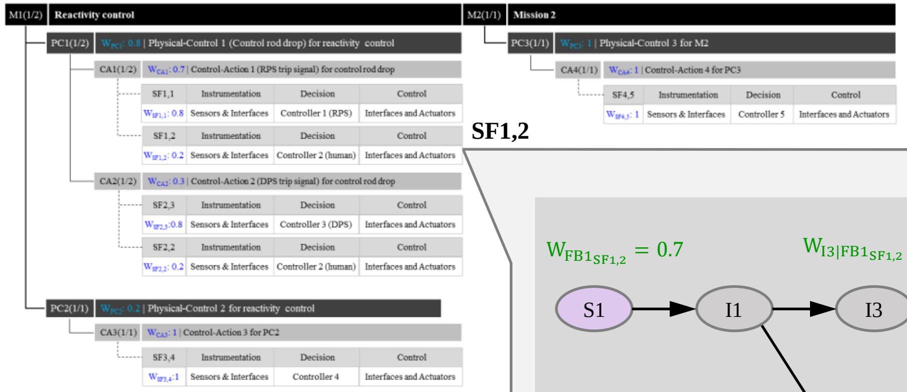
- PC3(1/1) | W_{PC3}: 1 | Physical-Control 3 for M2
  - CA4(1/1) | W_{CA4}: 1 | Control-Action 4 for PC3

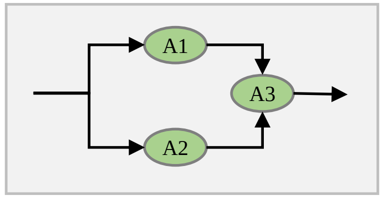
SF4,5	Instrumentation	Decision	Control
$W_{SF4,5}$: 1	Sensors & Interfaces	Controller 5	Interfaces and Actuators

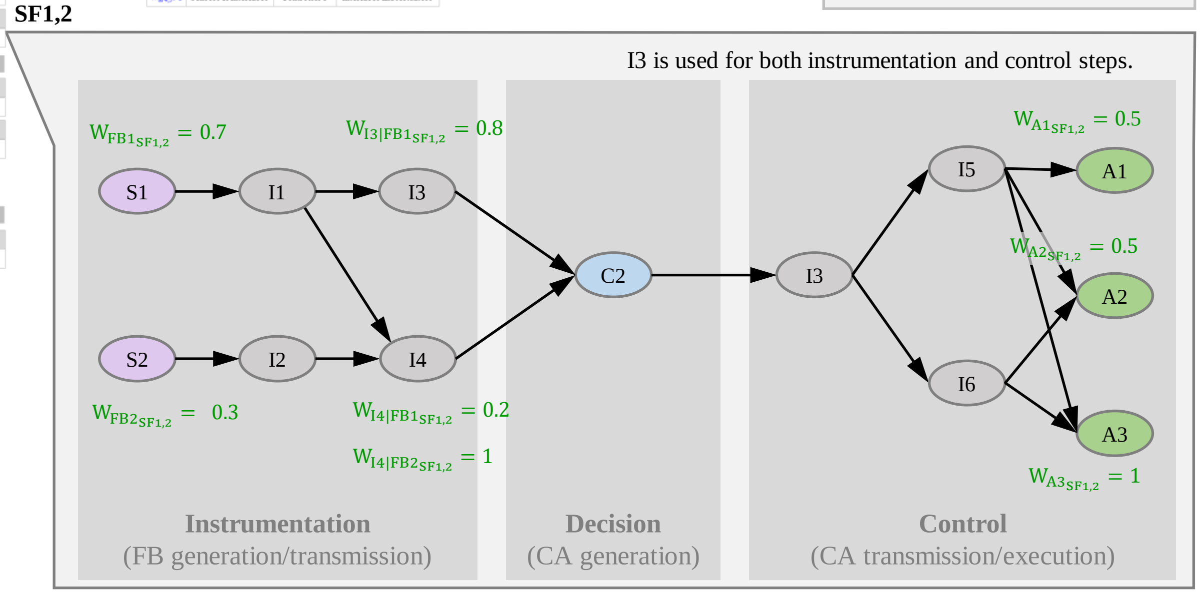
…

- Weights are assigned to the elements in the same functional hierarchy level, from PC to SF.
- According to the relative importance in achieving the needs of the parent hierarchy, the weights are assigned between 0 and 1 to elements at the same hierarchical level.
- Sum of the weights of the elements that cause the failure of the parent hierarchy needs (i.e. minimal cut set: MCS) should be equal to 1.

Weight assignment | SF



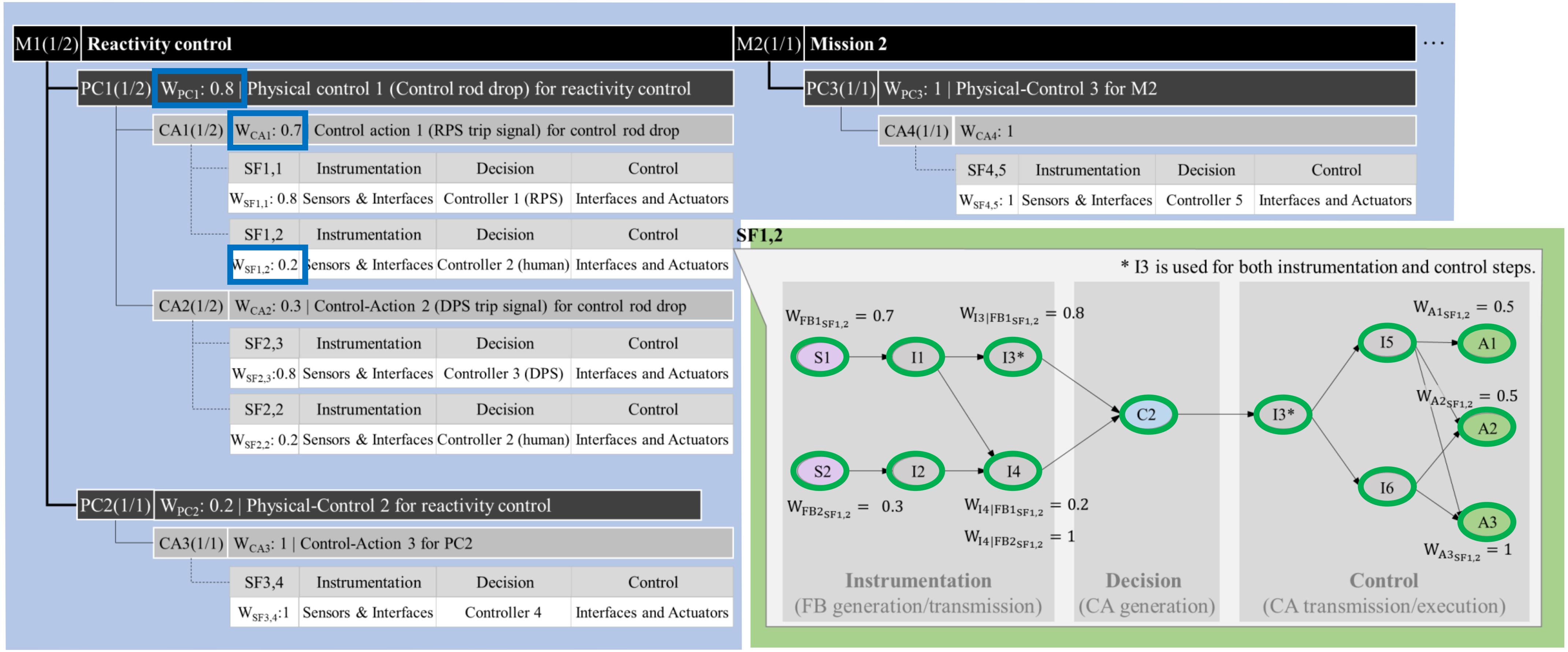




▶ In a single SF, weights are assigned to some components (Sensors, front-end interface, which transfers FBs to the controller, and actuators)in accordance with the following general logic.

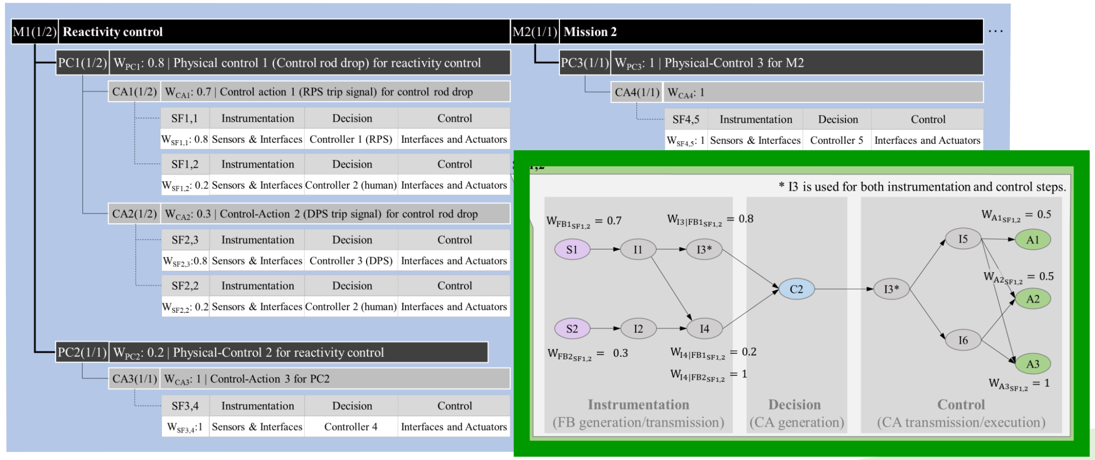
- Some components which transfer a FB significant on decision-making through an effectively recognizable path to the controller are important.
- Minimal set of actuators to complete the control step are important.

Importance evaluation



Importance evaluation | in an SF

- Importance of a component (IM) in an SF $\propto$ extent to which a particular component impairs the soundness of each step when that component is unavailable



A SF degraded/failure

- Instrumentation (FB generatio/transmission) degraded/failed
- Decision (CA generation) degraded/failed
- Control CA (transmission/execution) degraded/failed

$$\mathbf{IM^{INS}_{Sn|SF\ i,j}} = W_{FBk_{SF\ i,j}}\ (n = k)$$

$$\mathbf{IM^{DEC}_{Cn|SF\ i,j}} = 1\ (n = j)$$

$$\mathbf{IM^{INS}_{In|SF\ i,j}} = \sum_{k=1}^{\alpha}\left(W_{FBk_{SF\ i,j}} \frac{\sum_{g\in G_{In}|FBk_{SF\ i,j}} W_{g|FBk_{SF\ i,j}}}{\sum_{g\in G_{In}|FBk_{SF\ i,j}} W_{g|FBk_{SF\ i,j}} + \sum_{f\in F_{In}|FBk_{SF\ i,j}} W_{f|FBk_{SF\ i,j}}}\right)$$

where $G_{In}|FBk_{SF\ i,j}$: A group of front-end interfaces transmitting FB k via the interface n in SF i, j

where $F_{In}|FBk_{SF\ i,j}$: A group of front-end interfaces transmitting FB k other than the interface n in SF i, j

$$\mathbf{IM^{CTL}_{In|SF\ i,j}} = \max\{IM_{In|SF\ i,j}(z) : z = 1..\gamma\}$$

where γ is the number of MCS of actuators in SF i,j

$$IM_{In|SF\ i,j}(z) = \frac{\sum_{g\in G_{In}|MCSz_{SF\ i,j}} W_{g_{SF\ i,j}}}{\sum_{g\in G_{In}|MCSz_{SF\ i,j}} W_{g_{SF\ i,j}} + \sum_{f\in F_{In}|MCSz_{SF\ i,j}} W_{f_{SF\ i,j}}}$$

where $G_{In}|MCSz_{SF\ i,j}$: A group of actuators receiving CA i via the interface n in the MCSz in SF i, j

where $F_{In}|MCSz_{SF\ i,j}$: A group of actuators receiving CA i other than the interface n in the MCSz in SF i, j

$$\mathbf{IM^{CTL}_{An|SF\ i,j}} = W_{Ay_{SF\ i,j}}\ (n = y)$$

Importance evaluation | in a mission & entire mitigation procedure

- IM of a component integrated with weights of related SF, CA and PC for a mission

$$IM_{Sn|Mx} = \sum_{y=1}^{a}\sum_{i=1}^{b}\sum_{j=1}^{c} W_{PCy}\left\{W_{CAi}\left(W_{SF_{i,j}} \cdot IM_{Sn|SF\,i,j}^{INS}\right)\right\}$$

$$IM_{Cn|Mx} = \sum_{y=1}^{a}\sum_{i=1}^{b}\sum_{j=1}^{c} W_{PCy}\left\{W_{CAi}\left(W_{SF_{i,j}} \cdot IM_{Cn|SF\,i,j}^{DEC}\right)\right\}$$

$$IM_{An|Mx} = \sum_{y=1}^{a}\sum_{i=1}^{b}\sum_{j=1}^{c} W_{PCy}\left\{W_{CAi}\left(W_{SF_{i,j}} \cdot IM_{An|SF\,i,j}^{CTL}\right)\right\}$$

$$IM_{In|Mx} = \sum_{y=1}^{a}\sum_{i=1}^{b}\sum_{j=1}^{c} W_{PCy}\left[W_{CAi}\left\{W_{SF_{i,j}}\left(IM_{In|SF\,i,j}^{INS} + IM_{In|SF\,i,j}^{CTL}\right)\right\}\right]$$

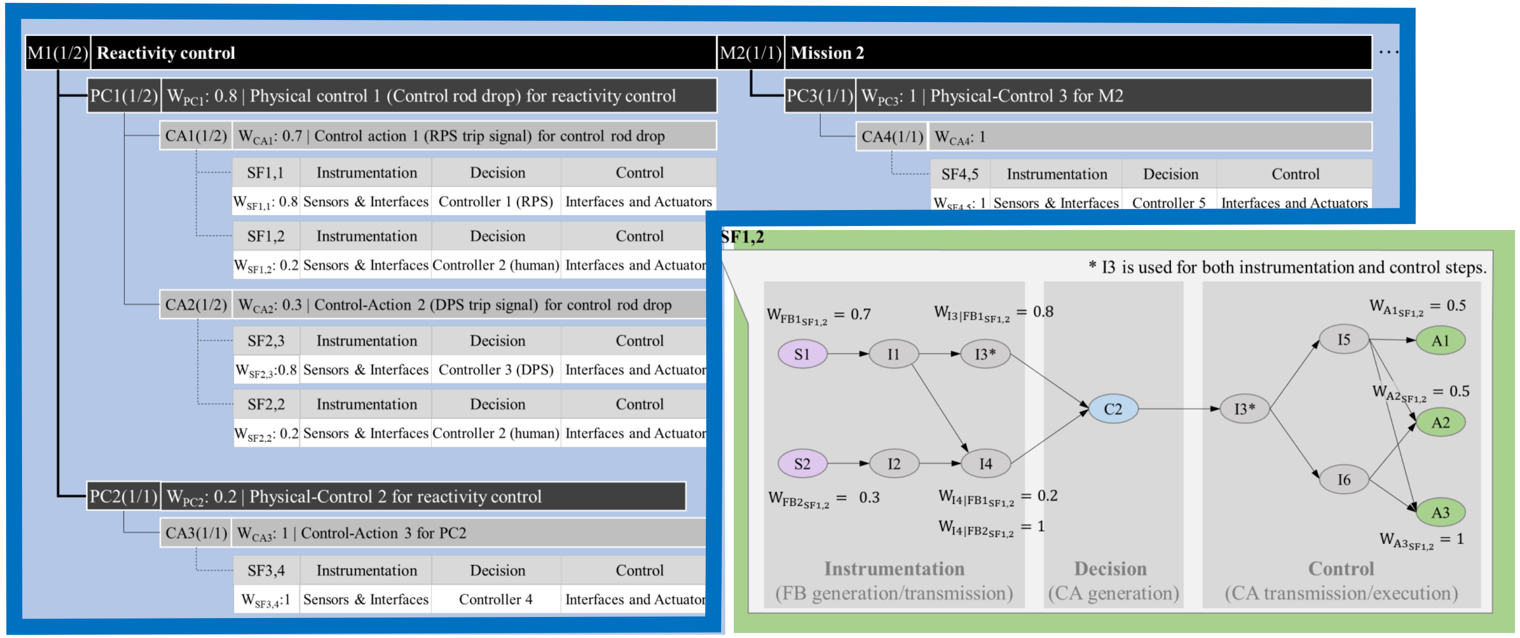
- IM of a component in a mission → integrated over the entire mitigation scenario

$$IM_{Sn} = \sum_{X=1}^{T} IM_{Sn|Mx}$$

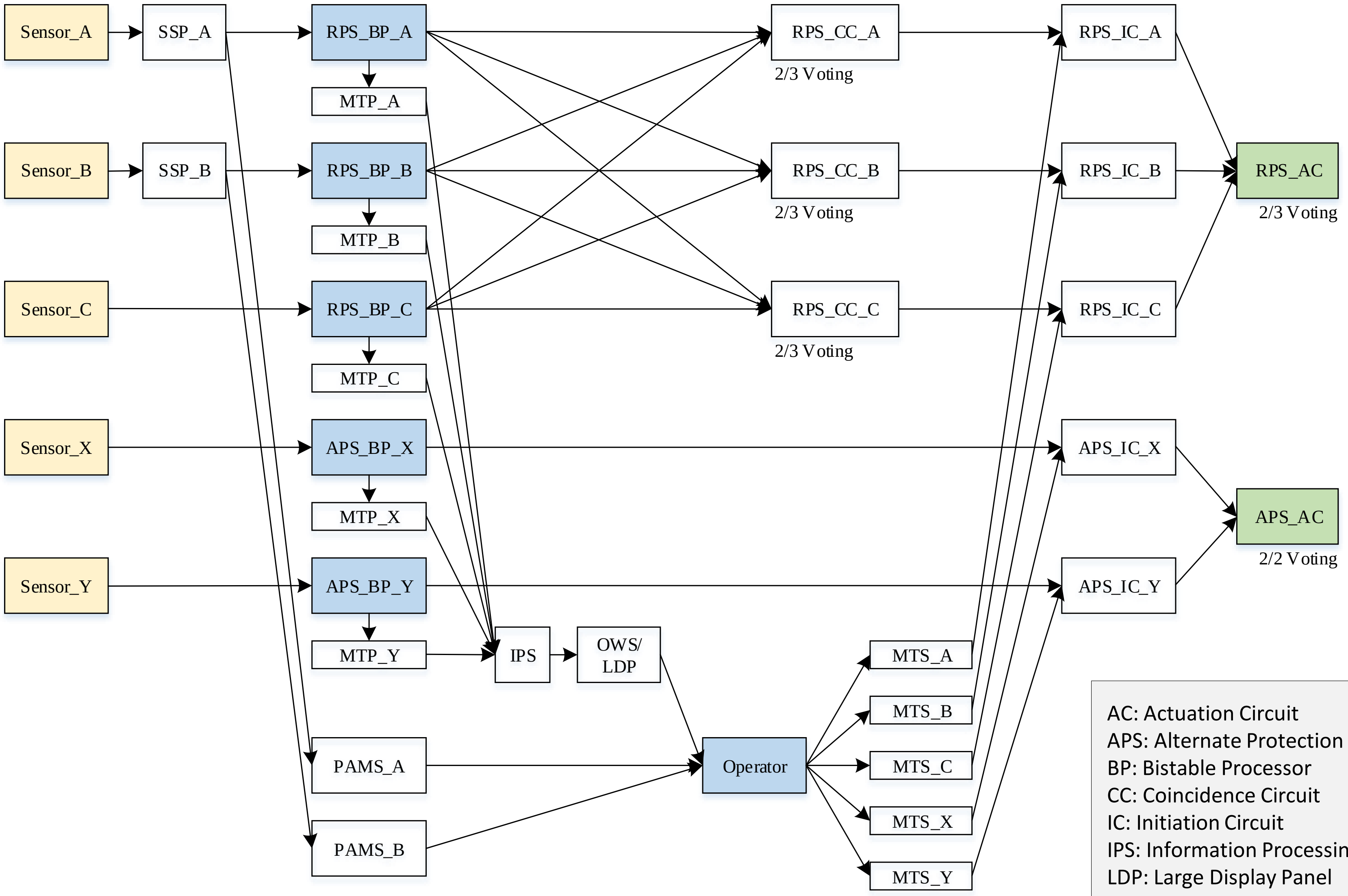
$$IM_{Cn} = \sum_{X=1}^{T} IM_{Cn|Mx}$$

$$IM_{An} = \sum_{X=1}^{T} IM_{An|Mx}$$

$$IM_{In} = \sum_{X=1}^{T} IM_{In|Mx}$$



Case study | Protection I&C systems for a 5MW open-pool type research reactor



AC: Actuation Circuit
APS: Alternate Protection System
BP: Bistable Processor
CC: Coincidence Circuit
IC: Initiation Circuit
IPS: Information Processing System
LDP: Large Display Panel
MTP: Maintenance and Test Panel
MTS: Manual Trip Switch
OWS: Operator Workstation
PAMS: Post Accident Monitoring System
RPS: Reactor Protection System
SSP: Signal Splitter Panel

* To simplify the system, components connected in series to each other without branching were combined as one component.

Case study | Protection I&C systems for a 5MW open-pool type research reactor

M1(1/1) **Reactivity control**

PC1(1/2) W_{PC1}: 1 | Physical control 1 (Control rod drop) for reactivity control

CA1(1/2) W_{CA1}: 0.7 | Control action 1 (RPS trip signal) for control rod drop

Weight of RPS auto-trip: 0.8 (2/3)

SF1,1*	INS	DEC	CTL
$W_{SF1,1}$: 0.58	S1, I1	C1 (PRS A)	I5, I6, I7, I9, I10, I11, A1

SF1,2*	INS	DEC	CTL
$W_{SF1,2}$: 0.58	S2, I2	C2 (PRS B)	I5, I6, I7, I9, I10, I11, A1

SF1,3*	INS	DEC	CTL
$W_{SF1,3}$: 0.58	S3	C3 (PRS C)	I5, I6, I7, I9, I10, I11, A1

* SF1,1, SF1,2, and SF1,3 are three channels of RPS auto-trip, respectively. In order to perform PC1 through A1, CA1 must be generated and transmitted to A1 in at least two of the three channels.

SF1,6	Instrumentation	DEC	Control
$W_{SF1,6}$: 0.2	S1, S2, S3, S4, S5 I1, I2, I3, I4, C1, C2, C3, C4, C5, I8	C6 (human)	I9, I10,I11, A1

CA2(1/2) W_{CA2}: 0.3 | Control action 2 (APS trip signal) for control rod drop

Weight of APS auto-trip: 0.8 (2/2)

SF2,4**	INS	DEC	CTL
$W_{SF2,4}$: 1	S4	C4 (APS X)	I12, A2

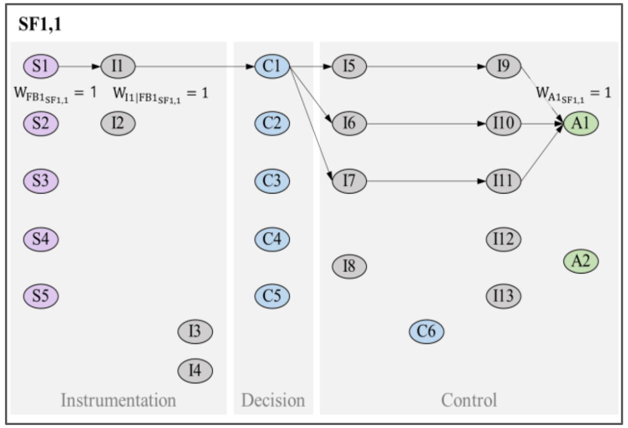
SF2,5**	INS	DEC	CTL
$W_{SF2,5}$: 1	S5	C5 (APS Y)	I13, A2

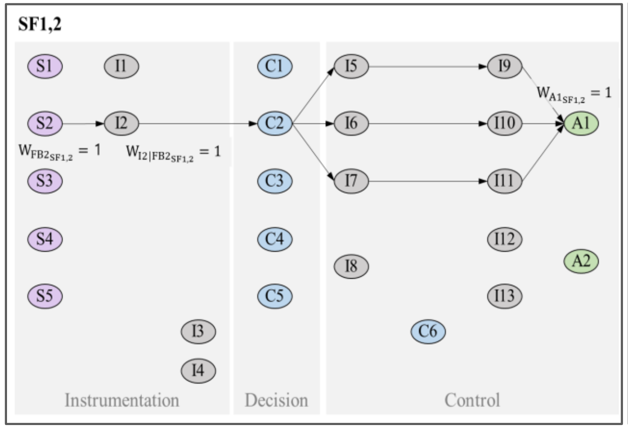
** SF2,4 and SF2,5 are two channels of APS auto-trip, respectively. In order to perform PC1 through A2, CA2 must be generated and transmitted to A2 in both channels.

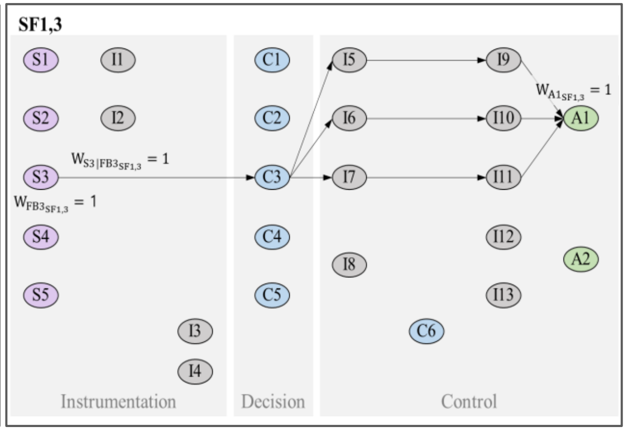
SF2,6	INS	DEC	CTL
$W_{SF2,6}$: 0.2	S1, S2, S3, S4, S5 I1, I2, I3, I4, C1, C2, C3, C4, C5, I8	C6 (human)	I12, I13, A2

Case study | Protection I&C systems for a 5MW open-pool type research reactor

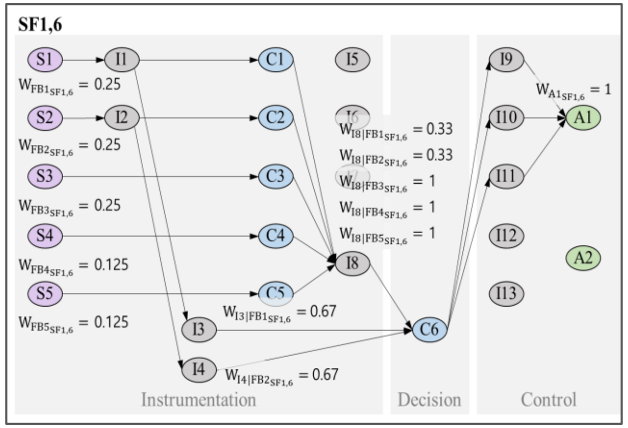
RPS auto trip



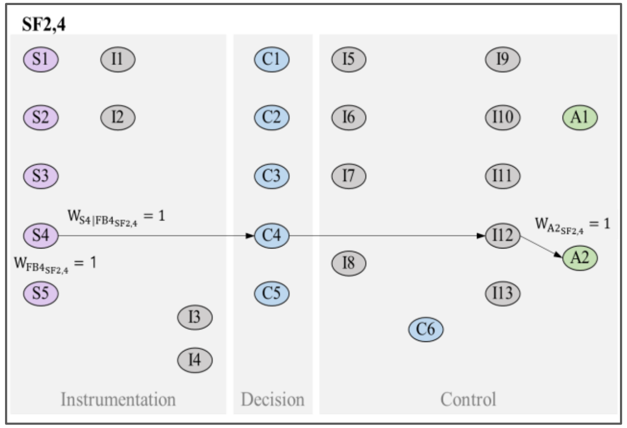


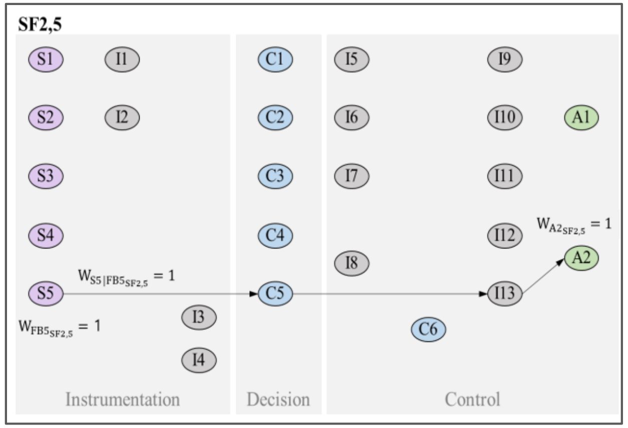


RPS manual trip

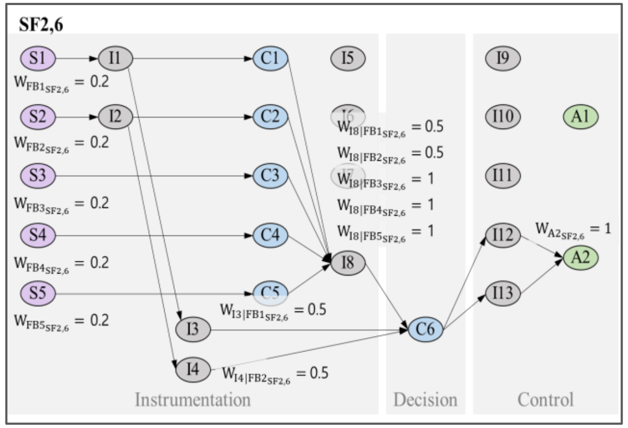


APS auto trip

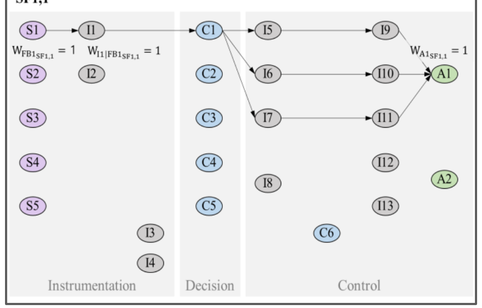


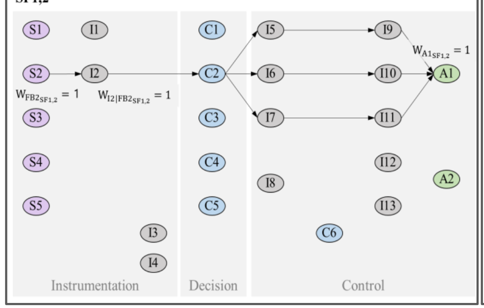


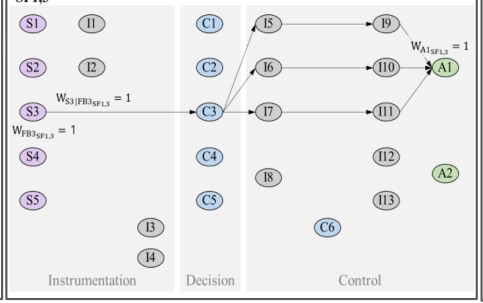
APS manual trip

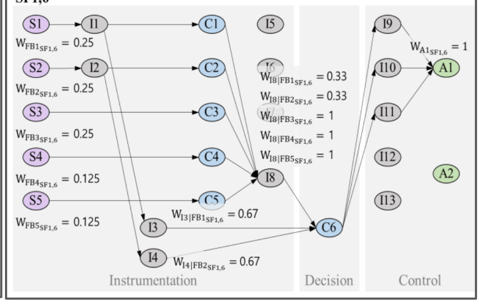


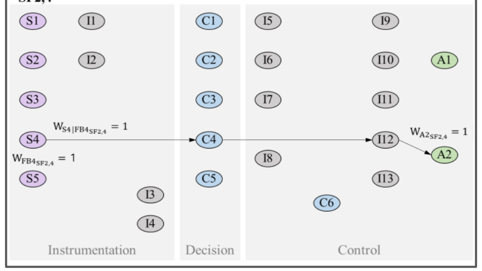
Case study | Protection I&C systems for a 5MW open-pool type research reactor

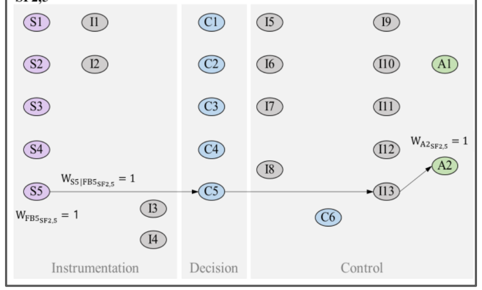
SF1,1


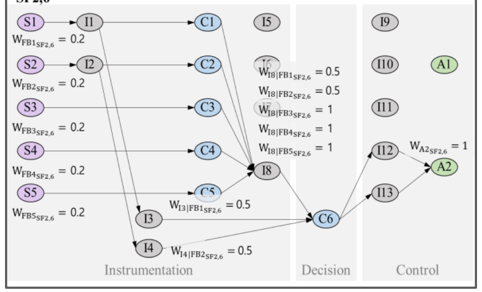
SF1,2


SF1,3


SF1,6


SF2,4


SF2,5


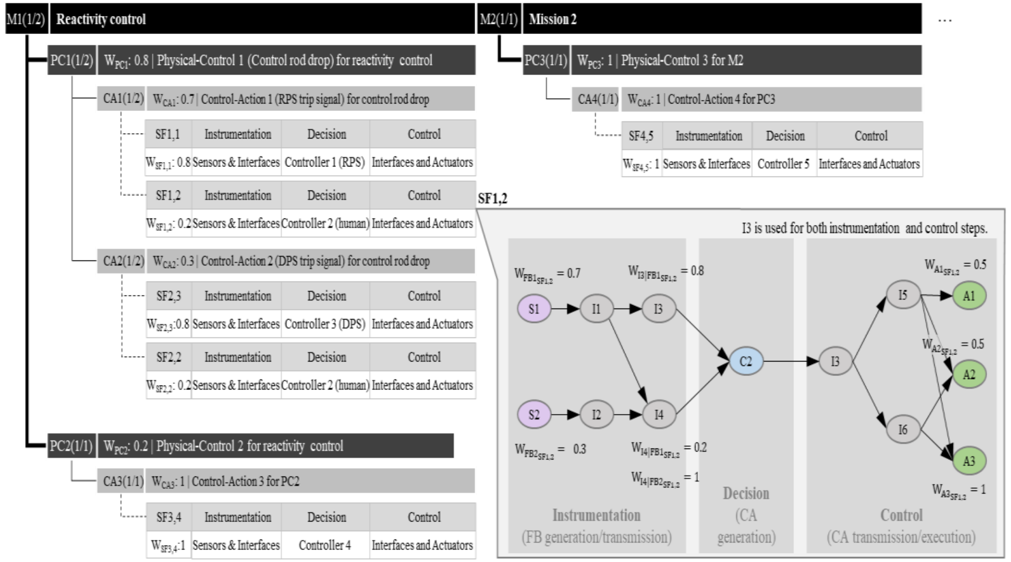
SF2,6


PC	W_{PC1}																				1.000	IM_n	
CA	W_{CA1}											0.700	W_{CA2}								0.300		
SF	Weight of RPS auto-trip (2/3)								0.800	$W_{SF1,6}$		0.200	Weight of APS auto-trip (2/2)					0.800	$W_{SF2,6}$		0.200		
	$W_{SF1,1}$		0.577	$W_{SF1,2}$		0.577	$W_{SF1,3}$		0.577				$W_{SF2,4}$		1.000	$W_{SF2,5}$		1.000					
n	$IM^{INS}_{n\|SF1,1}$	$IM^{DEC}_{n\|SF1,1}$	$IM^{CTL}_{n\|SF1,1}$	$IM^{INS}_{n\|SF1,2}$	$IM^{DEC}_{n\|SF1,2}$	$IM^{CTL}_{n\|SF1,2}$	$IM^{INS}_{n\|SF1,3}$	$IM^{DEC}_{n\|SF1,3}$	$IM^{CTL}_{n\|SF1,3}$	$IM^{INS}_{n\|SF1,6}$	$IM^{DEC}_{n\|SF1,6}$	$IM^{CTL}_{n\|SF1,6}$	$IM^{INS}_{n\|SF2,4}$	$IM^{DEC}_{n\|SF2,4}$	$IM^{CTL}_{n\|SF2,4}$	$IM^{INS}_{n\|SF2,5}$	$IM^{DEC}_{n\|SF2,5}$	$IM^{CTL}_{n\|SF2,5}$	$IM^{INS}_{n\|SF2,6}$	$IM^{DEC}_{n\|SF2,6}$	$IM^{CTL}_{n\|SF2,6}$		
S1	1.000									0.250									0.200			0.370	S1
S2				1.000						0.250									0.200			0.370	S2
S3							1.000			0.250									0.200			0.370	S3
S4										0.125			1.000						0.200			0.270	S4
S5										0.125						1.000			0.200			0.270	S5
C1		1.000								0.083									0.100			0.341	C1
C2					1.000					0.083									0.100			0.341	C2
C3								1.000		0.250									0.200			0.370	C3
C4										0.125				1.000					0.200			0.270	C4
C5										0.125							1.000		0.200			0.270	C5
C6											1.000									1.000		0.200	C6
A1			1.000			1.000			1.000			1.000										1.110	A1
A2															1.000			1.000			1.000	0.540	A2
I1	1.000									0.250									0.200			0.370	I1
I2				1.000						0.250									0.200			0.370	I2
I3										0.168									0.100			0.030	I3
I4										0.168									0.100			0.030	I4
I5			0.330			0.330			0.330													0.320	I5
I6			0.330			0.330			0.330													0.320	I6
I7			0.330			0.330			0.330													0.320	I7
I8										0.665									0.800			0.141	I8
I9			0.330			0.330			0.330			0.330										0.366	I9
I10			0.330			0.330			0.330			0.330										0.366	I10
I11			0.330			0.330			0.330			0.330										0.366	I11
I12															1.000						0.500	0.270	I12
I13																		1.000			0.500	0.270	I13

- The actuators are the most important components. Especially, A1 is the remarkably important component as it is used in the high-weighted CA (RPS auto-trip).
- S1, S2, S3, C3, I1, and I2 are important, for the same reason as that of A1. Regarding the controllers, C3 has a little higher importance than C1 and C2 because FB1 and FB2 can be transmitted to the human operator via I3 and I4 even if C1 and C2 fail, while FB3 cannot be transmitted to the human operator at all when C3 fails.
- In terms of the interfaces, I9, I10, and I11 are slightly more important than I5, I6, and I7 because the former are additionally used to transmit the RPS manual-trip signal in SF1,6 as well as in the transmission of the RPS auto-trip signal.
- Otherwise, most components excluding the actuators (A1 and A2) and some interfaces (I3, I4, and I8) are distributed evenly between 0.200 and 0.370 importance, regardless of their type. In this regard, it can be said that the I&C system for reactivity control is well-balanced.

Concluding remarks (1/2)

- **The new approach to evaluate the quantitative importance of components in I&C systems has been proposed**
  - The method organizes the signal flow configuration within the I&C system according to the hierarchy of mission, physical control, control action, and the correlation between the elements consisting each hierarchy.
  - The method separates each signal flow into 3 steps (instrumentation, decision, and control) and quantifies the impact of a particular component on each step based on the assigned weight.
  - The pre-importance of each component calculated for each SF is then derived as final importance in conjunction with the weights assigned to physical control, control action, and SF.



- **The method can provide quantified analysis results even failure data of components cannot be obtained.**

Concluding remarks (2/2)

- **It is necessary to consider the following prerequisites and precautions in utilizing this method**
    - It is assumed that signals (FBs or CAs) do not deteriorate or changed in the process of transmission.
    - It is assumed that one CA is created by only one controller.
    - The results of analysis vary depending on the assigned weights.
    - The boundary and balance between components should be properly considered and defined.
- **Based on the analysis results, the safety of the control system might be achieved**
    - by modifying the system design to do not concentrate the importance on a few components, or
    - by forcing the implementation of high reliability for certain components with high importance.
- **In order to ensure the validity of the method, a method that objectively and systematically assigning weights must be supported.** (*Regarding this subject, the authors plan to conduct a follow-up study)

Thank you for your attention

smshin@kaeri.re.kr