Conceptual MMIS for Diversity and Defense in Depth

Yeonsub Jung
KHNP CRI, 70, 1312beon-gil, Yuseong-daero, Yuseong-gu, Daejeon, 34101, Korea
**Corresponding author: ysjung62@khnp.co.kr*

1. Introduction

APR1400 nuclear power plants have been constructed and exported abroad. There are opportunities that APR1400 can be built abroad in the future. APR1400 is being upgraded to APR+ reflecting lesson learned from experience of domestic plants and licensing NRC-DC.

Present MMIS licensing philosophy of NRC is simplified MMIS satisfying diversity and defence in depth (D3). A keynote speaker from NRC at ISOFIC 2017 emphasized simplicity. MMIS with safety and non-safety, with redundant channels makes I&C architecture complicated, and reviewers not to understand resulting in less confidence in design.

A simplified MMIS is valuable for both operators and maintainers to cope with MMIS failures. They have to clearly understand where signals come from and where signals go to.

This paper is to suggest a conceptual MMIS architecture complying with D3. This MMIS is being reviewed to be applied to APR+ MMIS.

2. Simplified MMIS

SSCs(structure, system, and component) in the nuclear power plants have their own roles. Since they are graded differently for both safety and cost, MMIS controlling the SSCs is segmented at leaf nodes to block error propagation, and integrated at root nodes to enhance human performance. Sensors are places in the leaf nodes, and MCR is placed in the root node.

There are lots of regulation documents requiring independence and signal priority, but there are little regulation documents requiring integration. Fortunately I&C-ISG-04 and ISG-05 are about integrated MMIS.

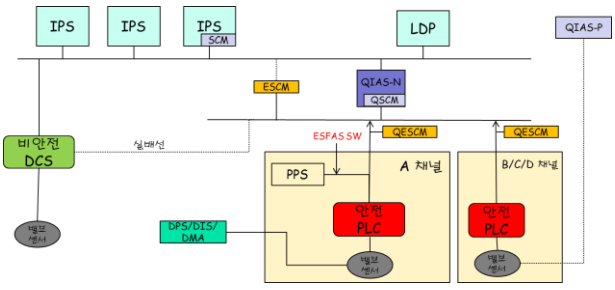

Fig.1 Simplified MMIS

Sensors and valves are typical active components to control flow and energy. They are divided as safety or non-safety. Safety components are controlled by PLC, whereas non-safety components are controlled by DCS. Generally DCS is more powerful and complicate than PLC. DCS is provided with engineering tools to edit input/output, control logic and man machine interface.

Safety components are grouped into 4 channels and controlled by channelized PLC controllers. Even though PPS of one channel is out of order, safety components can be controlled due to redundant 4 channels.

Non-safety components are not grouped as safety components. But components are segmented to get rid of failure propagation. Almost 80 DCS controllers are distributed across plants. Sensor data are transferred to IPS via DCS. IPS is on operator console that shows plant status. There are lots of IPS FPDs where MCR crewmembers are working on. LDP is another display of IPS. LDP is a spatially dedicated and continuous variables(SDCV).

IPS plays role of normal monitoring and control FPD where all plant components can be controlled in one sit-down place. IPS covers both non-safety components and safety components. Therefore safety status shall be integrated in IPS via QIAS-N as Fig.1.

Control modules are divided into Soft Control Module(SCM) and ESCM that are for non-safety and safety components respectively. SCM resides in IPS. When non-safety component is selected, SCM appears and operator can control the component. ESCM, however, is separated from IPS because control signal from non-safety system cannot control safety component. ESCM is placed in safety networks. Component selection signals are sent from IPS to ESCM. After a component is selected, operator controls safety component from ESCM.

PPS is plant protection system to mitigate design base events. PPS generate system level actuation signals as per IEEE 603. Because human beings are difficult to monitor abnormality of plant continuously, PPS is an automatic system to trigger plant shutdown. In case that PPS is not working properly, manual ESFAS switch is provided.

QIAS-N is integrating all safety components from 4 channels for monitoring and control. Even though some selected non-safety devices states are sent to QIAS-N, its main function is collecting all safety components. When IPS fails, QIAS-N is a diverse system of IPS. QIAS-N provides the same mechanism such as Qualified SCM(QSCM) and QESCM that are for non-safety and safety component respectively. QSCM resides in QIAS-N, whereas QESCM is separated from QIAS-N, and channelized. QESCM is different from ESCM in the view that ESCM is not channelized.

Because both PLC and DCS are working on CPU, they can fail due to common cause failure. PLC is actually diverse system of DCS. BTP-7-19 demands another diverse system such as DPS/DMA/DPS from PLC. The diverse system issues both system level actuation signal and component actuation signal. They are connected with different communication network to components directly, so that they are last resort for control.

QIAS-P is another diverse system according to Reg.1.97. QIAS-P shows critical information after accident. They are connected by hardwire.

This simplified MMIS is a minimum architecture satisfying regulatory guidelines. APR+ is being optimized based on this conceptual architecture. Detail design of this MMIS can have complicate connections but its signal flows are kept.

3. Reliability and Operability

Lots of advance MMIS have been proposed. But there is no standard MMIS in the nuclear power plants. This result in problem that construction period has been extended because of lack of confidence in MMIS. Advance MMIS experts are also rare. When there is trouble in the advance MMIS, they want to go back to analog technology. This behavior is against current MMIS technology. Most other industries are adopting digital technology.

After experiencing digital technology for decade in APR1400, it is time to evaluate reliability of digital I&C technology. Digital technology is based on software that is assumed not free of error even with severe verification and validation effort. When MMIS engineers are captured with this concept, it is difficult to derive reliable MMIS architecture. I&C expert have to evaluate reliability of MMIS quantitatively as Table I

Table I System and functions

Location	System	SRC/DST	Comm.	Safety	Criteria	Failure(%)	Key Design Features
Operator Console	IPS+SCM	P-CCS	DCN	ITA	DI&C-ISG-04, 05	0.1	Integration Minimum Inventory
	ESCM	E-CCS	DCN-Q CCQ	ITS	IEEE603	0.01	Separation Multichannel Control FPD
LDP		P-CCS	DCN	ITA	DI&C-ISG-05	0.1	Spatially Dedicated Continuous Display
Safety Console	PPS	E-CCS	DCN-Q	S	IEEE603	0.01	Autonomous Protection
	ESFAS SW	E-CCS	DCN-Q	S	IEEE603 RG 1.62	0.01	Manual Protection
	QIAS-N	E-CCS P-CCS	DCN-Q HardWire	ITS	DI&C-ISG-04	0.05	Integration for Safety Components Diverse from IPS
	QSCM	P-CCS	HSL	ITS	DI&C-ISG-04	0.05	Control for Non-safety Component
	QESCM	E-CCS	DCN-Q	ITS	IEEE603	0.01	Channelized Control FPD
	DMA/DPS /DIS	CIM	HSL	ITS	BTP-7-19	0.05	Direct control signal to Device
	QIAS-P	Sensor	HardWire	S	Reg1.97 R4 IEEE478	0.001	Direct Monitoring from Device
	CPC OM	CPC	DCN-Q	ITS		0.01	
	TG OM	TG	DCN	ITA		0.1	

DCS controllers are called as P-CCS, whereas PLC controllers are called as E-CCS in nuclear power plant. These two systems are running without failure throughout power operation. They are robust systems executing control logics. Because control logics are written in formal language such as SAMA, its completeness and reliability is assured inherently.

Compared E-CCS or P-CCS, the systems in Table I are written in C. Software in C can have bug that could be removed by strict V&V. Strong V&V method appears these days. However there are still flaws resulting in system crash. Failure column in Table1 is not obtained by strictly calculating failure data, but is obtained by experiencing the systems. While designing simplified conceptual architecture, these reliability data were considered. MMIS designers with different analog background might propose the different architecture. That is why AP1000 and APR1400 have different MMIS architecture.

According to BTP-7-19, DMA/DPS/DIS diversity system is needed. The system displays critical information as well as sends control signals. Because of historical architecture, the system is still divided in 3 systems. It looks like that the three systems can be combined as one system. BTP-7-19 allows that diversity

system be not safety system. Integrated system is more robust than 3 separate systems.

4. Conclusions

MMIS architecture is complicate due to independence requirements in nuclear power plant. At the same time, operator wants MMIS integrated. The integration and independence is achieved by integrated IPS and segmented controller. This paper proposes a simplified and conceptual MMIS architecture without sacrificing regulatory requirements.

REFERENCES

[1] NRC, BTP-7-19, Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer based Instrumentation and Control Systems.
[2] IEEE Std. 7-4.3.2-2003, IEEE Standard Criteria for Digital Computers in Safety Systems in Nuclear Power Generating Stations.
[3] IEEE603, Standard Criteria for Safety System for Nuclear Power Generating Stations, 2009
[4] RG 1.62, Manual Initiation of Protective Actions
[5] Reg1.97, Criteria for accident monitoring instrumentation for nuclear power plants
[6] IEEE497, Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations
[7] DI&C-ISG-04, Highly-Integrated Control Rooms—Communications Issues
[8] DI&C-ISG-05, Highly-Integrated Control Rooms—Human Factors Issues