Development of architecture for digital I&C system using C4ISR framework

JUNG JaeCheon[1], and QUANG Phamle[2]

1. KEPCO International Nuclear Graduate School, 1456-1 Shinam-ri, Seosang-myeon, Ulju-gun, Ulsan 689-882, (jcjung@kings.ac.kr)
2. Ninh Thuan Nuclear Power Project Management Board, 16/4 road, Phan Ranf-Thap Cham City, Ninh Thuan Province, Vietnam, (lequang0912@gmail.com)

Abstract: The architect framework for the digital I&C system is presented in this work. With rapid changes in digital I&C technology, there is a strong need to provide uniform methods to describe the system functions and their performance in context with the physical configuration and logical behavior. C4ISR framework would provide the process and method for the digital system in that it allows the three different views of operational, systems and services, and technical standards. Therefore, stakeholders can share information that is related to the system interfaces, the actions or activities that those components perform, and rules or constraints for those activities from the initial state of system development. As a result, the lifecycle cost and development time for the digital I&C system can also be optimized. These benefits can be obtained by introducing views and products to reveal the logical, behavioral, and performance characteristics of the architecture. To prove this approach, the plant protection system (PPS) is chosen and the architect framework is developed.

Keyword: PPS; C4ISR; safety critical system; digital I&C systems

1 Introduction

Digital instrumentation and control (I&C) systems in the nuclear power plant (NPP) have been applied to increase the plant safety, reliability, availability, and maintainability while reducing the overall plant risk. They also will give better functionality such as enforced diagnostic function by maximizing the information transferring between the sub-systems. But there are concerns about introducing potential new failure modes that can affect safety [1].

In order to operate and maintain this system properly, better skill and knowledge are needed for an analog system. There are three concerns raised. The first one is the complexity of the system. The inputs and outputs to be processed by a digital plant protection system are 10 times higher than that of an analog based system. The second concern is about the understandability, trouble-shooting capability, and the cost for the system ownership. The third concern comes from system operation and maintenance requirements.

In the aspect of risk, the following factors will also increase the difficulty of managing digital based I&C systems [2]:

- *The utilization profiles of hardware components are determined by software.*
- *Both software and digital hardware have a discontinuous nature.*
- *Various monitoring and recovery mechanisms can be established using microprocessors but the accurate estimation of the effectiveness of these mechanisms is quite difficult.*
- *New initiating events induced by digital systems are possible.*

These environments around the digital I&C technology will benefit from the architect framework that is able to express the technics, systems, and operations holistically.

1.1 Architect for digital I&C system

By applying an architectural framework for NPP design, a designer is able to consider the system as a whole. It also provides for considering, and evaluating interactions between the system and its environment. Those external factors must be taken

Received date: September 9, 2014

into account in order to understand the complex system to be created and developed. A static system is one whose states do not change because it has structural components but no operating or flow components.

On the other hand, a dynamic system exhibits behaviors because it combines structural components with operating and/or flow components. In light with this definition, an NPP I&C system is dynamic due to its characteristics. It has been designed under a well-defined process. When the system is developed, the static components and its functions are more emphasized. It has not been a problem in either the analog based I&C system or non-safety related system. But in the fully digitalized I&C system such as the APR1400 (advance power reactor) plant protection system (PPS), the four (4) basic requirements of architect as: completeness, unambiguity, correctness, and consistency, may not be satisfied under the conventional design structure.

1.2 Architecture framework

"*It is apparent that the success or failure of many defenses, space, and civil systems of the last half century has depended in large part on how they were structured*"[3]. IEEE Std. 610.12 defines architecture as: the structure of components, their relationships, and the principles and guidelines governing their design and evolution over time. [4][5].

With rapid changes in technology, systems structure and operation, those elements cause uncertainties and ambiguities of requirements elicitation when we design the dynamic system.

To deal with such problems, the Department of Defense (DoD) in USA developed an architecture framework for information systems comprising Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR)[6][7].

The purpose of developing this framework is to describe system architectures using multiple views in terms of the operational capability that systems built conformant to the architecture can provide [8]. Moreover, it supplies the acquisition community in its efforts to acquire an interoperable system. It provides common definitions, data, and references, as well as specifying a set of products containing three views of architecture as illustrated on Fig. 1.

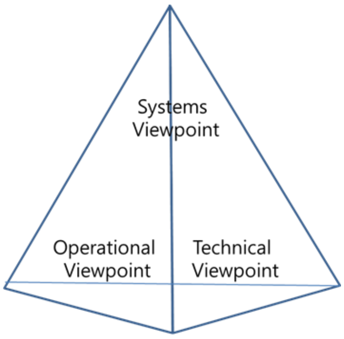

Fig. 1. Triumvirate expressing three viewpoint for the digital I&C system.

1.3 C4ISR implementation into digital I&C system design

A C4ISR framework would provide the process and method for the digital I&C system in that it allows the three different views of operational, systems and services, and technical standards. Therefore, stakeholders can share information related to the system interfaces, the actions or activities those components perform, and rules or constraints for those activities from the initial state of system development [8].

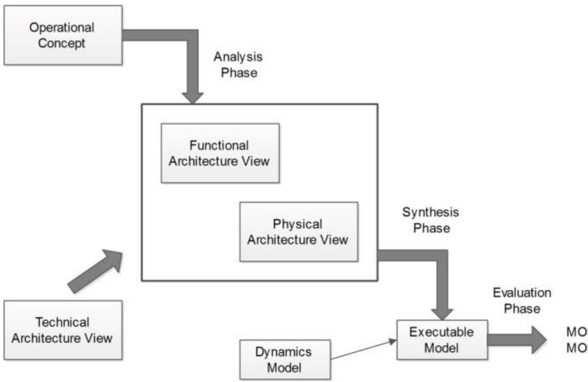

Fig. 2. The three phases of architecture development [7].

Wagenhals and Levis presented the architecture design method based on the traditional structured analysis approach [8]. As presented in Fig. 2, designers have to define activities or processes that need to perform in order to accomplish their mission. It is also necessary to describe system components that will implement the design such as hardware, software, human factors, and facilities which are constituent elements of the C4ISR system.

In the structured analysis approach, architecture is composed of two basic constructs:

- *Functional Architecture*
- *Physical Architecture*

Both definitions should be interpreted broadly to cover a wide range of applications; furthermore, each may require multiple representations of views to describe all aspects.

Following this process, the C4ISR architecture process can be characterized as consisting of three phases which are defined as follows:

- *The Analysis Phase in which the static representations of the Functional and Physical Architecture views are obtained using the operational concept to drive the process and the Technical Architecture view to guide it.*
- *The Synthesis phase in which these static constructs is used, together with descriptions of the dynamic behavior of the architecture, to obtain the executable model of the architecture.*
- *The Evaluation Phase in which measures of performance (MOPs) and measures of evaluation (MOEs) are obtained.*

2 Introducing architect framework into NPP I&C system design

2.1 Define architect view

Figure 3 shows how the C4ISR architect framework is implemented into the NPP I&C system design.

In presentation of the architecture, the integration definition zero (IDEF0) modeling language is adopted as primary technique for defining the system functionality. It is composed of function, input, output, control and mechanism. A function or activity is represented by a box to provide the context. A function in this context is a transformation that turns inputs into outputs [11]. The control guides this transformation while mechanism provides the physical resources to perform the function.

When the I&C operational concept is set, then the architecture views are able to be defined. It needs input, output, control, and mechanism. In this case the operational concept would be an input and the e output from this stage is the view of operation, systems and techniques.

Meanwhile it needs control such as NPP system safety concepts, laws and regulations. It also needs mechanisms including system operation context, and modeling techniques. System modeling language (SysML) would also be a candidate to develop the system context.

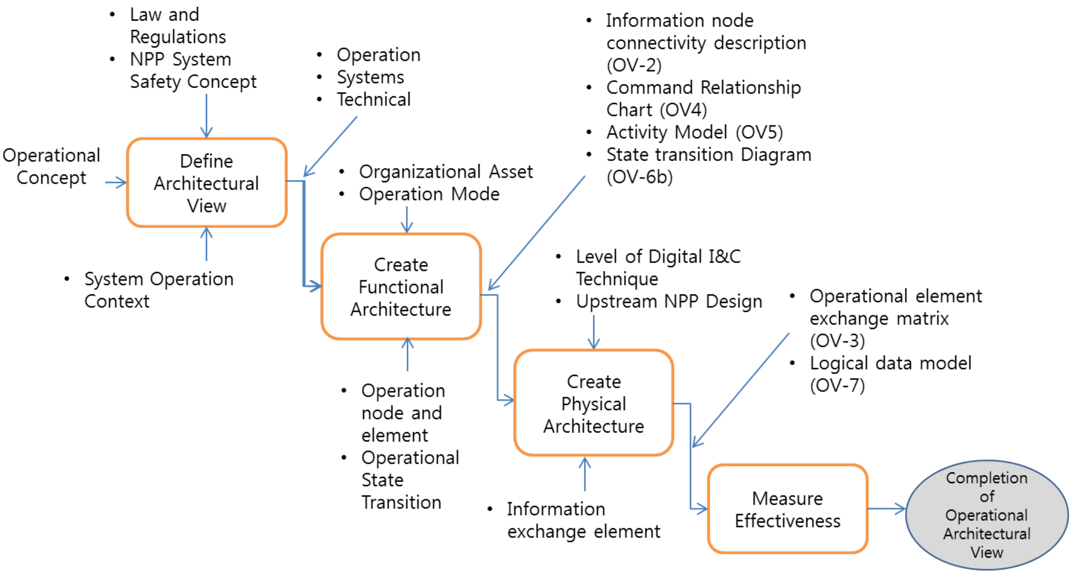
• Law and Regulations
• NPP System Safety Concept
• Operation
• Systems
• Technical
Operational Concept
Define Architectural View
• System Operation Context
• Organizational Asset
• Operation Mode
Create Functional Architecture
• Operation node and element
• Operational State Transition
• Information node connectivity description (OV-2)
• Command Relationship Chart (OV4)
• Activity Model (OV5)
• State transition Diagram (OV-6b)
• Level of Digital I&C Technique
• Upstream NPP Design
Create Physical Architecture
• Information exchange element
• Operational element exchange matrix (OV-3)
• Logical data model (OV-7)
Measure Effectiveness
Completion of Operational Architectural View

Fig. 3. Four (4) stages for NPP I&C design using architect framework (Operational architectural view only).

2.2.1 Operational architectural view

The operational architectural view for digital I&C system is shown in Table 1. It indicates the products and related works per the listed applicable view.

The operational view describes the tasks and activities, the operational nodes, and the information flows between nodes that are required to accomplish or support an operation [8][9].

Table 1. Defined operational architectural view

Product Reference	Architecture product	Activity
OV-1	High-level Operational Concept Graphic	Describe high level description of the operation
OV-2	Operational Information Node Connectivity Description	Define organization and asset Identify operational node and element
OV-3	Operational Information Exchange Matrix	List the producing and consuming operational node and activity as well as general information
OV-4	Command Relationships Chart	Describes a key organizational aspect of the operational concept that the architecture supports
OV-5	Activity Model	Create Functional architect Create Physical architect
OV-6a	Operational Rules Model	Review utility requirements Review code and standard
OV-6b	Operational State Transition Description	Analyze operational state transition
OV-6c	Operational Event/Trace Description	Identify operational event Define sequence of events between operational nodes
OV-7	Logical Data Model	Describe the data requirements of the information exchange elements

2.2.1 System architectural view

The systems view translates the required degree of interoperability into a set of system capabilities needed, identifies current systems that are used in support of the operational requirements and facilitates the comparison of current/postulated system implementations with the needed capabilities [8][9]. Table 2 defines system architectural view with the activities to be performed.

The technical view articulates the criteria that govern the implementation of the required system capabilities [9][10] as Table 3.

Table 2. Defined system architectural view

Product Reference	Architecture product	Activity
SV-1	System Interface Description	Define interfacing system
SV-2	Systems Communications Description	Define communication method and interfacing system
SV-4	Systems Functionality Description	Prepare Data Flow Diagram (DFD)
SV-5	Operational Activity to System Function Traceability Matrix	Link between the operational and system architecture views
SV-6	System Information Exchange Matrix	Describe the implementation of the information exchanged between systems and their functions
SV-7	System Performance Parameters Matrix	Provides current and predicted or required future performance characteristics for each system component and element
SV-10a	Systems Rules Model	Describe the dynamic behavior of the architecture System activity sequence and timing descriptions
SV- 10b	Systems State Transition Description	
SV -10c	Systems Event/Trace Description	
SV-11	Physical Data Model	Describe how the information represented in the OV-7 is implemented in the systems architecture view

Table 3. Defined system architectural view

Product Reference	Architecture product	Activity
TV-1	Technical Architecture Profile	Identify technical standards that apply to the architecture and how they need to be implemented
TV-2	Standards Technology Forecast	Identify law and regulation to control the system design Establish safety design concept

As controls, the laws and regulations are applied along with NPP safety concepts such as: defense in depth, diversity, redundancy and fail in safe. In association with this stage, the operational context diagram, information exchange matrix, rules and activity model, and logical data model are prepared for the supporting products.

2.2 Create functional architecture

This stage derives the configured functions of input, output, and transformation. In addition, the controls and mechanisms are also needed to define the digital I&C function correctly. The following sub-sections describe about the control and mechanisms in order to perform the transformative work (functional architect).

2.2.1 Controls

Through the decomposition, the organizations and their assets are able to be defined and they will control the transformative function. The organization represents the external entities which are connected to the system. The asset stands for the system hardware and the governing specification which is required to be performed during the lifecycle.

The operational modes control this stage as well. Not only the normal operational mode from mode 6 (refueling) to mode 1 (power operation), but also the abnormal and accident operation mode are identified and they will control the function.

2.2.2 Mechanism

Operational nodes and operational elements are applied as physical resources that allocate the operational activities to the systems which the operational elements possess.

When the system's operation state is clearly defined it will help to understand the behavior of the designing system.

2.2.3 Outputs

Once the operational nodes and elements are established, the designer is able to create a command relationship chart (OV-4) for the purpose of explaining control, command, and relationships among organizations.

Though the preparation of the activity model (OV-5), the definition of how the system is related to the external systems can be identified. In addition, the decomposition of activities to represent the assets that the operational elements possess is identified.

Also, the information mode connectivity description (OV-2) can be obtained in order to define the function of: system operation, operator action, system status monitoring, system interface and date commutation holistically.

The state transition diagram (STD) is also developed so that the system behavior is described (OV-6b).

2.3 Create physical architecture

The physical architect stage begins with allocation of the operational activities. In addition, the arrangement of system function into the elements will be conducted.

2.3.1 Controls

In this stage, the currently available digital I&C technology is considered. The limitation and constraints from the upstream NPP design will be considered as well. The anticipated limitation and constraint are: limited safety system setting (LSSS) and system response time. Those are given from the upstream system design from safety analysis, fluid design and mechanical design.

2.3.2 Mechanisms

The supplemental mechanisms to be applied are: systems to be interfaced, the communication network that are connected to the defined system, and the states to be transited per operational mode.

2.3.3 Outputs

The information contained in the functional architecture models is also reflected in the operational information exchange matrix (OV-3). Each row of the matrix specifies several characteristics of the operational information elements. These characteristics include the name and several parameters about its content. It also lists the operational elements and the operational activities that it produces and receives.

2.4 Develop MOE (measure of effectiveness)

MOE can be defined a qualitative or quantitative metric of a system's overall performance that indicates the degree to which it achieves its objectives under specified conditions. An MOE always refers to the system as a whole [12]. An MOE would include logical, behavioral, and performance characteristics of the architecture. The logical aspect of architecture can be measured when it represents the main functions. The behavioral measures that characterize the interoperability of the system must be described.

3 Proposed framework for PPS architect

In order to validate the applicability of proposed architect framework, the plant protection system (PPS) is chosen. The PPS provides the reactor trip and engineered safety features actuation during and after the anticipated operational occurrence (AOO) state of the NPP.

The PPS operational mode can be categorized as follows:

- *Operation during Normal or Accident Plant Conditions*
- *Operation during Abnormal Plant Conditions*
- *Surveillance Testing*

The operators are able to bypass, test, or calibrate the system as well as manually trip the reactor through RTSS either in the main control room (MCR) and remote shutdown room (RSR). Furthermore, operating parameters, monitored systems' status is also sent to the data communication network in order to communicate with other systems. The high level operational concept of the PPS is depicted in Fig. 4.

3.1 Create functional architecture

3.1.1 PPS operation modes (control)

For establishing the high-level operational concept, a functional decomposition should be conducted. The hierarchy diagram in Fig. 4 is used to decompose the functions of the system. As a result, three operation modes are identified during normal and accident, abnormal, and surveillance test conditions.

3.1.2 Organizations and their assets (control)

When the operational concept is established, it is the time to derive the organizations and their assets for the system architecture. Table 1 presents the organization that is involved in the PPS design and its physical and governing assets. The technical specifications should be considered since they regulate the system operation and design. Afterward, operational nodes and operational elements are able to be selected from the organizations and assets.

3.1.3 Operational nodes and elements (mechanism)

Table 4 shows the operational nodes and elements for the PPS. It contains information about how the PPS is interfaced with the related systems, components, and equipment along with the entities which interact with the system elements.

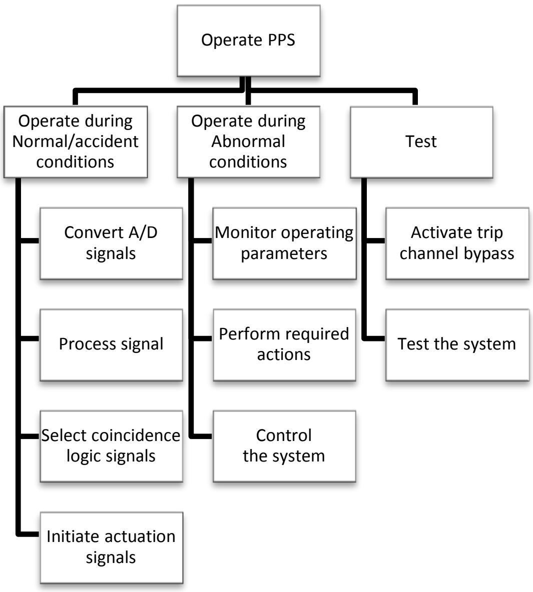
Operate PPS
Operate during Normal/accident conditions
Operate during Abnormal conditions
Test
Convert A/D signals
Process signal
Select coincidence logic signals
Initiate actuation signals
Monitor operating parameters
Perform required actions
Control the system
Activate trip channel bypass
Test the system

Fig. 4. PPS functional decomposition.

Table 4. Operational Nodes and Elements

Organizational Nodes	Elements
Operators	Operators
Man Machine Interface	OM, MTP, MCR-CPM, QIAS-P, RSR-CPM, ITP
Monitoring system	QIAS-P, QIAS-N
Signal process	BP, LCL, RTSS, ESF-CCS
Input	Sensors, Transmitters
Executive component	CEAs, Valves, Pumps

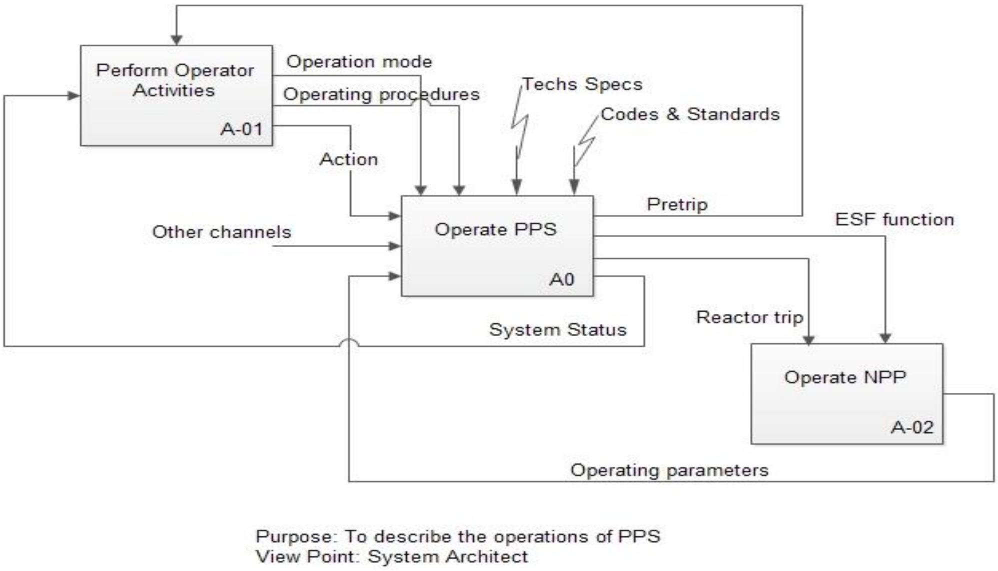

Fig.5. External System Diagram.

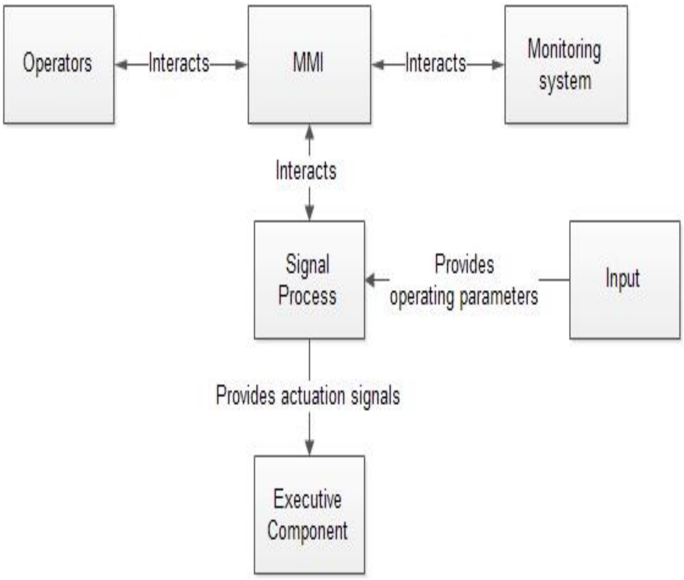

Fig.6. Command relationship chart (OV-4).

3.1.4 Command relationship chart (OV-4)

Once the operational nodes and elements are defined, the designer is able to create a Command Relationship Chart (OV-4) as depicted in Figure 5. It is aimed at explaining control, command, and relationships among organizations.

3.1.5 Activity model (OV-5)

In this stage, the structured analysis is performed using an IDEF0 activity model. This model helps the designer to consider the system as a whole. It also has the capability to be leveled down into subsystems or component depending on the initial purpose.

Firstly, to create the activity model, an external diagram must be built to describe relationships between the systems and its environment by showing interactions and interfaces of the system as shown in Figure 6.

The IDEF0 activity model, then, is easily figured out from the external system diagram by removing the related systems. As stated, from this model, the system can be decomposed into subsystems and components depending on the initial purpose as presented in Fig. 7. The architect is intended to have a deep understanding of PPS, thus, the following levels of decomposition are made for that purpose.

The architect will allocate the operational activities to the system functions that the operational elements possess.

There are two steps are required to allocate the operational activities to the system functions: operational activities to operational element, and operational elements to system functions. Fig. 8 represents the allocated operational functions during normal, and accident conditions.

State transition diagram (STD) shown in Figure 9 indicates the behavioral description of the system operations.

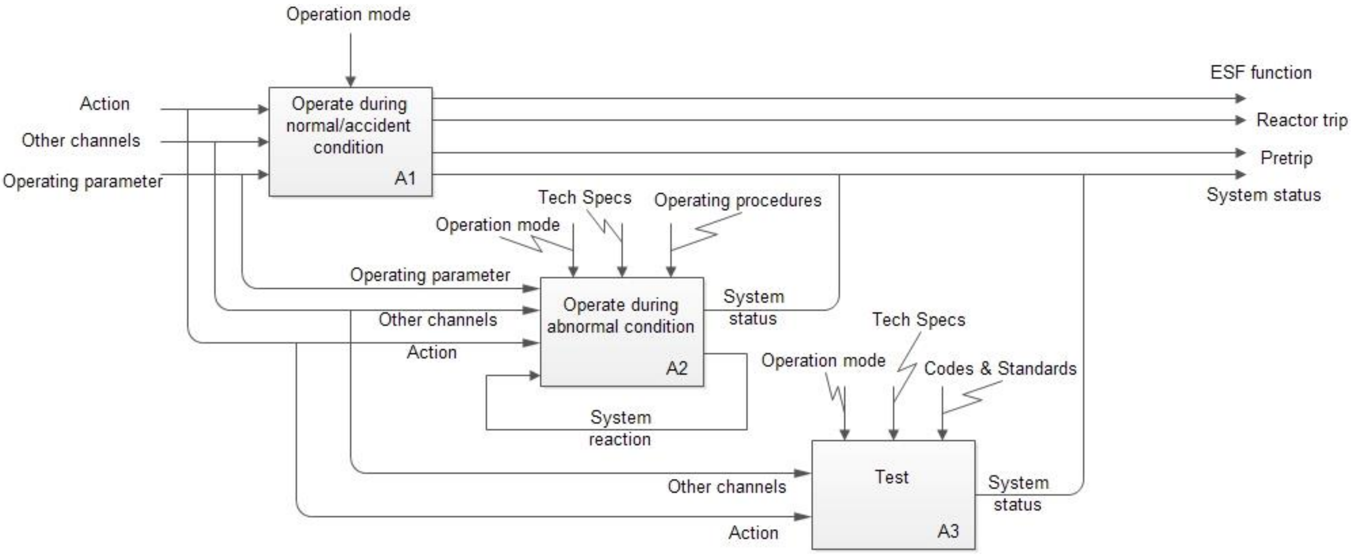

Fig.7. First level of decomposition.

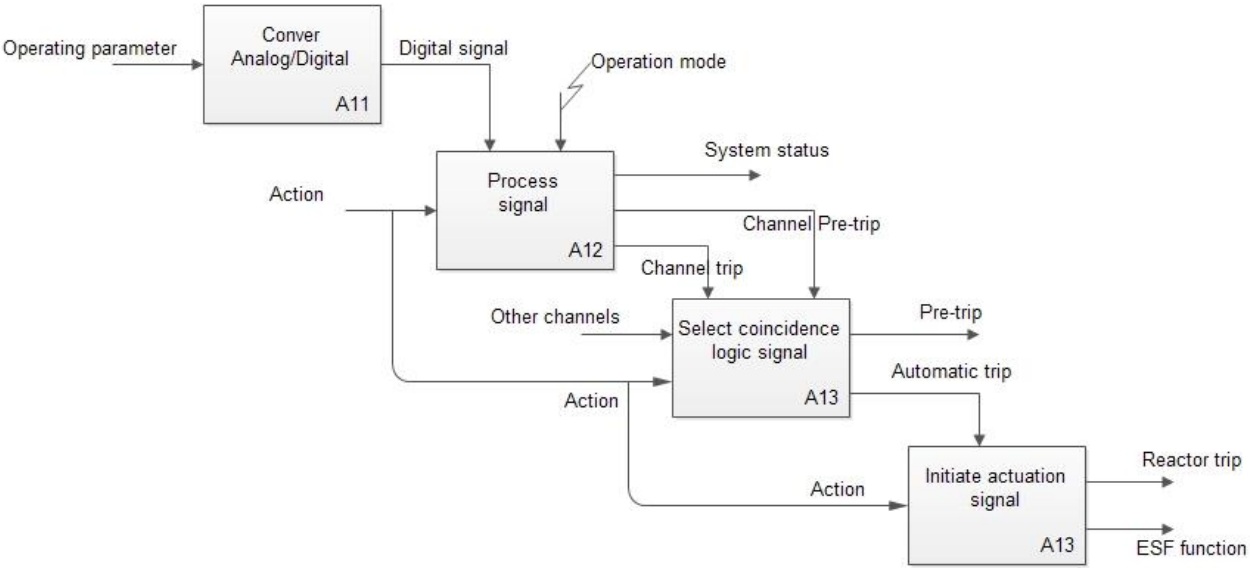

Fig.8. Operate during normal/accident conditions.

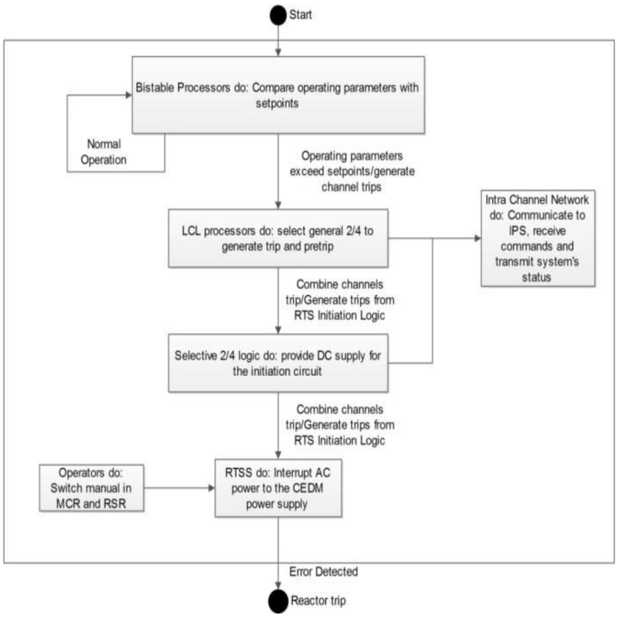
Start
Bistable Processors do: Compare operating parameters with setpoints
Normal Operation
Operating parameters exceed setpoints/generate channel trips
Intra Channel Network do: Communicate to IPS, receive commands and transmit system's status
LCL processors do: select general 2/4 to generate trip and pretrip
Combine channels trip/Generate trips from RTS Initiation Logic
Selective 2/4 logic do: provide DC supply for the initiation circuit
Combine channels trip/Generate trips from RTS Initiation Logic
Operators do: Switch manual in MCR and RSR
RTSS do: Interrupt AC power to the CEDM power supply
Error Detected
Reactor trip

Fig. 9. State Transition Diagram (OV-6b).

3.2 Create physical architecture

The last activity in this stage is to create two forms of the initial physical architecture. Firstly, the operational nodes are used to construct the operational node connectivity description. Needlines are linked between nodes to show the transferred information as depicted in Fig. 10.

The initial physical architecture shows system's nodes and elements. Moreover, the communication links are also defined.

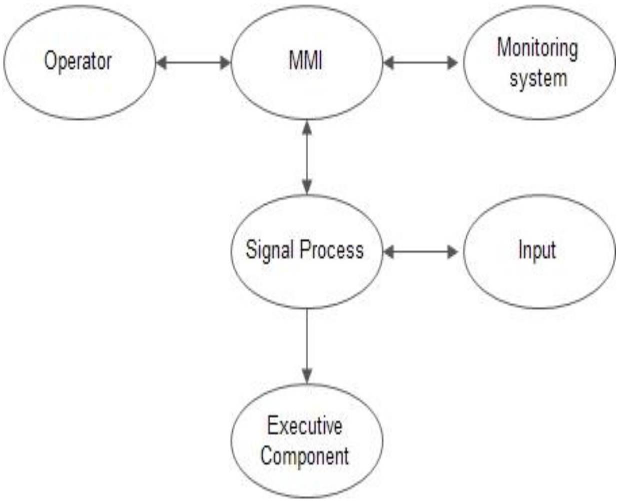

Fig.10. Operational nodes and needlines.

3.2.1 Operational information node connectivity description (OV-2).

The first step in this stage is to define the operational information node connectivity description (OV-2) shown in Figure 11. This diagram which is an essential architect product from this operational view consists of operation nodes or elements that show necessary connectivity and the flow of operational information elements between the nodes. Each node is annotated with the activities it performs and each need line is annotated with the operational information element that flows from one operational node to another [8].

Table 5. Operational information exchange matrix (OV-3)

Information Description		**Information Source**		**Information Destination**	
Operational information element	Data type	Operational element	Activity	Operational element	Activity
Operating selection	Digital	Operator	Bypass system Manual trip	OM	Transmit commands via ITP
		Tester	Test/Calibrate	MTP	Transmit commands via ITP
Commands	Digital	MMI	Transmit commands	Signal Process	Operate logic combinations
Operating parameters	Analog/Digital	Inputs	Provide operating parameters	BP	Compare to setpoints
Trip/pretrip	Digital	BP	Provide trip/pretrip	LCL	Operate logic combination
System information	Data	Signal Process	Communicate to intra channel network	MMI	Update system status
System status	Data	MMI	Update system status	Operator	Monitor the system
Initiation Logic signal	Digital	LCL	Operate logic combination	Switches	Active switches states
Activate	Analog	Switches	Active breakers	Breakers	Interrupt power supply

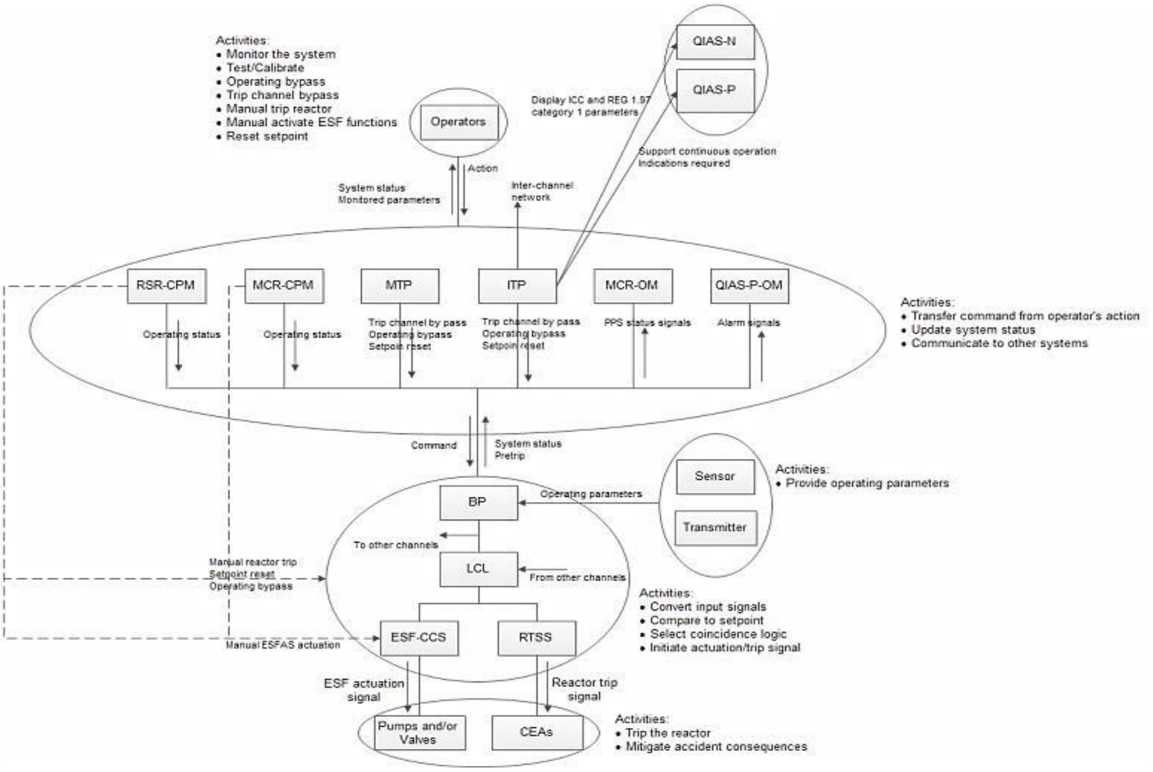

Fig.11. Operational node connectivity description (OV-2).

3.2.2 Operational element exchange matrix (OV-3)

OV-3 is the operational information exchange matrix. It contains, in tabular form, information about each operational Information element that is contained in the operational node connectivity description as shown in Table 5. For each element it lists the producing and consuming operational node and activity as well as general information including a description, size, composition, frequency of occurrence, timeliness requirements, throughput, security level, and interoperability requirements [8].

Each row of the matrix specifies several characteristics of one of the operational information elements.

4 Conclusions

As stated, this work is intended to describe the framework for a digital I&C system using the C4ISR architecture. Throughout this work, the understanding of digital I&C system is expected to be increased. In addition, the function, performance, and information interoperability can be expressed by the unified framework.

Although this work is only focuses on the analysis phase of the PPS, by using C4ISR framework the benefits of expressing logical, behavioral and performance characteristics of the architecture can be checked. Moreover, it provides uniform methods to describe PPS systems and their performance in context with mission and functional effectiveness. It also can share information related to the system interfaces, the actions or activities the components perform, and the rules or constraints for those activities from the initial state of system development. The proposed framework for representing PPS architecture is validated where the views of operation, system, and technical are effectively represented. In addition, the measures of effectiveness in the element of architect as: functional, performance, and interoperability are chosen and evaluated through qualitative assessment.

The results show C4ISR is able to depict those views and measures effectively. The defined stages to implement PPS system using this framework are: define architectural view, perform functional and physical architecture, create system activity model for making an executable model.

References

[1] GARRETT C. J. and APOSTOLAKIS G. E., Automated hazard analysis of digital control systems, Reliability Engineering & System Safety, Vol. 77, Issue 1, 2002.

[2] KANG H. G. and SUNG T. Y., An analysis of safety-critical digital systems for risk-informed design, Vol. 78, Issue 3, 2002.

[3] IEEE Std. 610.12-1990 IEEE Standard Glossary of Software Engineering Terminology

[4] KOSIAKOFF A., SWEET W. N., SEYMOUR S.J., and BIEMER S. M.: Systems Engineering Principles and Practice, Wiley, 2011.

[5] EBERHARDT Rechtin: The art of systems architecting, IEEE Spectrum, Vol. 29, Issue 10, 1992.

[6] DoD Architecture Framework Version 1.0, Volume I: Definitions and Guidelines, 30 August 2003.

[7] DoD Architecture Framework Version 1.0, Volume II: Product Descriptions, 30 August 2003.

[8] LEVIS A. H. and LEE W. Wagenhals: C4ISR Architectures:I. Developing a Process for C4ISR Architecture Design, Systems Engineering, Vol. 3, No. 4, 2000.

[9] LEE W. Wagenhals, INSUB Shin, DAESIK Kim, and ALEXANDER H. Levis: C4ISR Architectures II. A Structured Analysis Approach for Architecture Design, Systems Engineering, Vol. 3, No. 4, 2000.

[10] MICHAEL P. BIENVENU, SHIN Insub, and ALEXANDER H. Levis: C4ISR Architectures III. An Object-Oriented Approach for Architecture Design, Systems Engineering, Vol. 3, No. 4, 2000.

[11] DENNIS M. BUEDE: The Engineering Design of Systems, Wiley, 2009.