DISTRIBUTED CONTROL SYSTEM IMPLEMENTATION IN NUCLEAR POWER PLANTS WORLDWIDE: A LITERATURE SURVEY

Nafisah Khan
University of Ontario Institute of Technology
2000 Simcoe Street North
Oshawa, Ontario L1H 7K4 Canada

nafisah.khan@mycampus.uoit.ca

Abstract

Nuclear Power Plant control systems based on conventional control technology face a serious problem of obsolescence. With nuclear power plant life extension and new builds expanding globally, new control techniques are expected to be implemented. The Distributed Control System (DCS) architecture has been attracting more and more attention. Currently, there are a lot of discussions and plans for this replacement in the nuclear industry around the world. Various countries are at different stages in this replacement process. In this paper, the network architecture, risk assessment, reliability analysis and cost of DCS will be explored and discussed.

Introduction

Nuclear power plant control systems are nearing the end of their life. These control systems were designed based on an older control technology. Many other industries have already implemented the modern control technology. However, as anything regarding the nuclear industry, change is slow and requires a lot of work before anything can be changed. Now with nuclear power plant extension plans underway and new builds worldwide, the reliability of these systems are low. The Digital Control Computers (DCCs) will not last the lifetime of the refurbished plant and the new builds require a more advanced modern control technology. The risk and costs associated with this is not feasible. Therefore, this leaves a good opportunity to implement modern control technology to nuclear power plants to increase the reliability and safety of their systems. Various DCS architectures have been proposed throughout the world and many reliability models have been developed to test and analyze the reliability of the DCS.

Distributed Control System Network Architecture

In traditional Instrumentation and Control, the control systems are based on an analog technology where most connections are point-to-point types which is fragile to noise and slow due to a little long analog-to-digital conversion time. Modern digital communication networks are faster and stronger to channel noise.

Nuclear Power Plants:

There have been different structures of DCS architecture proposed around the world for nuclear power plants, however they all carry the same fundamentals. The following description of a DCS architecture for a nuclear power plant [2] was a design proposed by Korean students from Seoul National University.

In a DCS, distributed controllers communicate with each other by networks. The networks are categorized into an information network, a control network, and a fieldbus network according to bandwidth and target level. The information network deals with the exchange of data or command among operator interface stations (OIS) and engineering interface stations (EIS). Input and output (I/O) data that is collected in other parts of field controllers are shared by field controllers in the field network. The control network distributes group controllers as major cells and must guarantee real-time property. The safety system and the non-safety system are made independent by the gateways that communicate in between both. Figure 1 shows the hierarchical architecture of the DCS network.

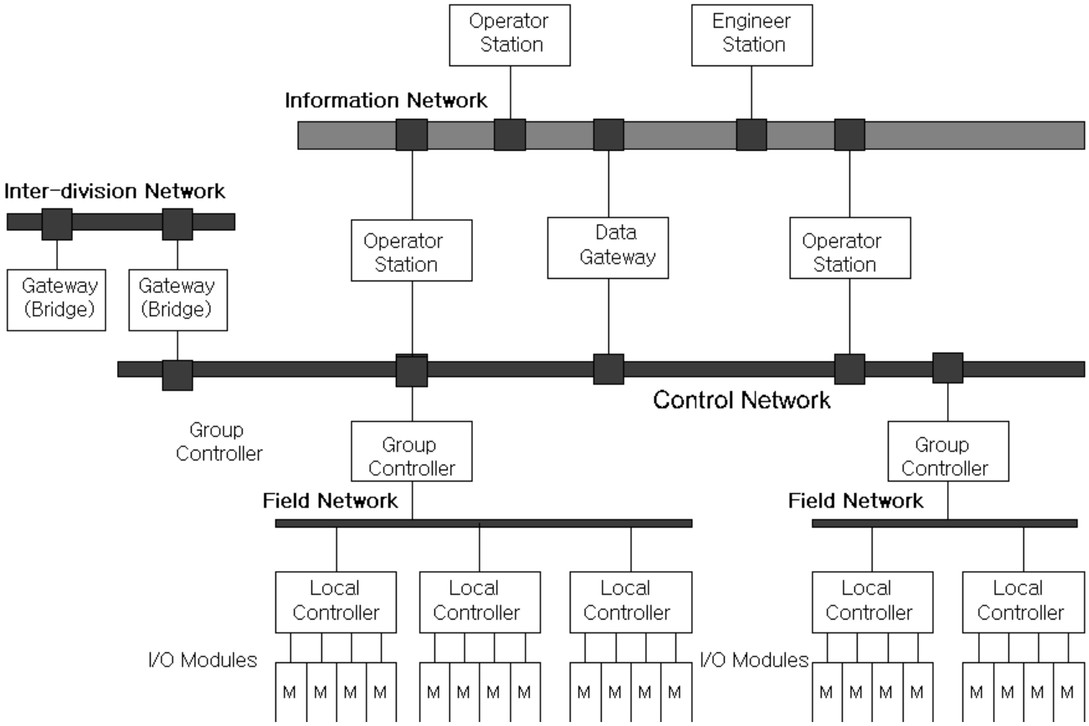

Figure 1: Hierarchical architecture of the DCS network [2]

This is the core communication network in the nuclear power plant. The control network is what connects distributed controllers and enables communication between them. There are network protocols which require real-time property, high-speed, reliability, and maintainability. Popular high-speed networks are IEEE 802.3u Fast Ethernet (or Gigabit Ethernet), Fiber-channel, ATM (Asynchronous Transfer Mode), and FDDI (Fiber Distributed Data Interface).

Communication independence is a must in safety systems of nuclear power generating stations of safety systems. Electrical and communication isolation need are definite for proper independence of the safety computer from the non-safety equipment. This method facilitates a two-way communication between the safety computer and the non-safety computer, considering that the buffering circuit is engaged in the safety computer. To implement the independence of communication in the proposed network, 'data gateway' is defined as a system that supports the communication interface of two different protocols and the function of data buffering. Two data gateways are necessary. It is also essential to remember that the DCS have a strong dependency on this layer of communication that the DCCs did not have.

The field network connects field control module to give the collection of field inputs and outputs to the control network. EIS executes engineer functions and OIS supports monitoring functions. The information network is a load to transfer information between EIS and OIS and between OISs. Since the information network is treated as a non-safety computer network, it does not need redundancy of channels. Its protocol is based on TCP/IP, a general computer network protocol.

Unified Power System:

There have also been general DCS architectures proposed around the world that can be applied to many industries. The following description of a DCS architecture [5] for a unified power system was proposed by some students and industry personnel in Egypt.

DCS is used to control processes in various fields around the world such as unified power systems, factories, airplanes, radar systems and many other industries. This DCS structure consists of many controllers connected together by a fiber optic network. They interact by means of communication protocols in order to understand what each one must do. Data is transmitted from one controller to another to know what action to take. Software is required to design the control algorithm that is needed to utilize the hardware portion. It consists of two components; process control (PC) and a database program. The desired functions are given by using the PC program to run the database program. To carry out this function, there is usually some sort of man intervention implemented by a special operator station. The hardware for the DCS is made up of sub racks that are connected to a controller data bus. The sub racks have specific addresses in which is used to obtain information from the software. The main hardware components are DI (digital input) card, DO (digital output) card, AI (analog input) card, AO (analog output) card which are connected to the controller sub rack. The data manager control is done by an information management system (IMS).

Figure 2 is a control fiber optic network made of three controllers that are connected to the double bus. The IMS is connected to the network. The intervention to the system is the industrial PC mouse and keyboard. The field interfaces with the system via the controller sub rack.

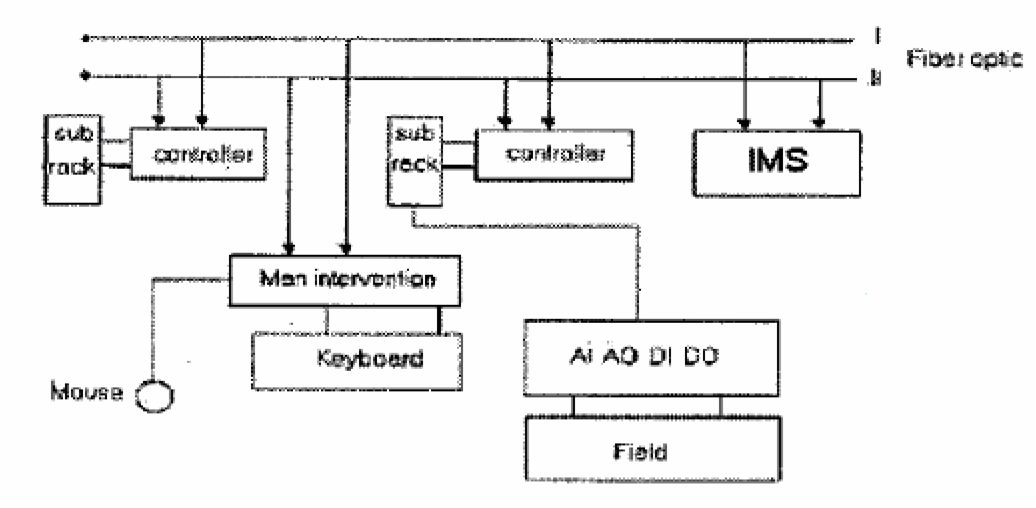

Figure 2: Control Network [5]

Plant Instrumentation and Control Network:

There have been specific networks designed as the control network for nuclear power plants. The following is a description of a new high-speed real-time network named PICNET+ (Plant Instrumentation and Control NETwork) [3] was proposed and implemented by Korean students from Seoul National University as the DCS for the nuclear power plant.

PICNET+ was developed to accommodate large volumes of data quantity, decreasing control period, increasing maintainability and the increasing need for intra-plant communication.

The name of the control network of the DCS is KNX-5. This DCS has a hierarchal structure for independence and to increase the performance. A 3 level architecture is used for KNX-5. The lowest level is the field network which takes charge of the communication between the field control units in the cabinet. The middle layer is the control network, namely PICNET+ that connects the control modules between cabinets. The top layer is the information network which provides monitoring and command services to engineering work station (EWS) and operator interface station (OIS). Data Gate Way (DGW) is when you connect nodes between two different networks. Figure 3 shows the overall architecture of KNX-5.

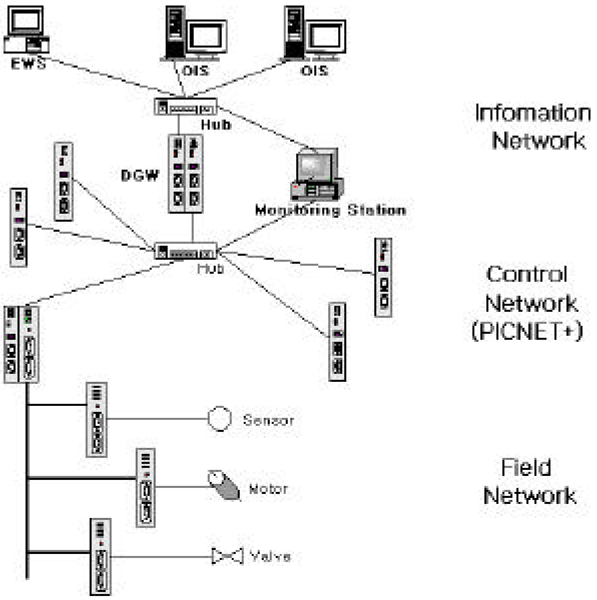

Figure 3: Architecture of KNX-5 [3]

Reliability Analysis

Reliability is a critical requirement in systems. When proposing to replace anything, it is important to look at the reliability of the proposed idea to that of the existing. The current DCCs have been very reliable over the years, only having a dual computer outage once every 10 years. This is mainly due to their physical separation, independency of each other, and little or no communication between them. Therefore, with the modern control technologies that are deemed to be more reliable, it is important to implement, test and analyze a reliability model to ensure it is indeed more reliable.

<u>Plant Instrumentation and Control Network:</u>

PICNET+ [3] whose architecture was introduced in the previous section, was implemented and its design was analyzed for reliability. The main requirements for PICNET+ was reliability, independence, hard real-time property, performance and maintainability.

The physical layer of PICNET+ uses fast Ethernet media and optical fiber is selected at KNX-5 to increase the reliability. Star topology is used as opposed to bus or ring topology because of faults that occur on media or node of communication. Media duplication and system duplication were used to overcome the dependence of the star topology on the switch.

PICNET+ uses the physical layer of a fast Ethernet and token passing RT-MAC (program to control the media access). It is highly reliable due to its duplicated media and system.

The analytical results of PICNET+ showed fault-tolerance, the deterministic characteristic, the high performance, and maintainability.

Fault-Tolerant System:

Some areas in the world have proposed a fault-tolerant type system for the DCS by a means of increasing the reliability. The following is a description of a fault-tolerant architecture for a real-time distributed control system [4] that was proposed by Malaysian students from the Univeristi Sains Malaysia.

A real-time system is a class of application whose accuracy does not depend solely on the logical results of the computation, but also on the time which it takes to produce the results. This DCS is a network where many nodes are interconnected to communicate with each other. Fault-tolerant systems are able to continue to perform in the presence of a failure.

This system is divided into a node stage and a network stage. At each stage, the best solution is established to increase the reliability of the overall system followed by choosing the communication protocol of the system.

At the node stage, the proposed architecture is to get the best fault-tolerant features without considering the cost. The proposed architecture can be seen in Figure 4:

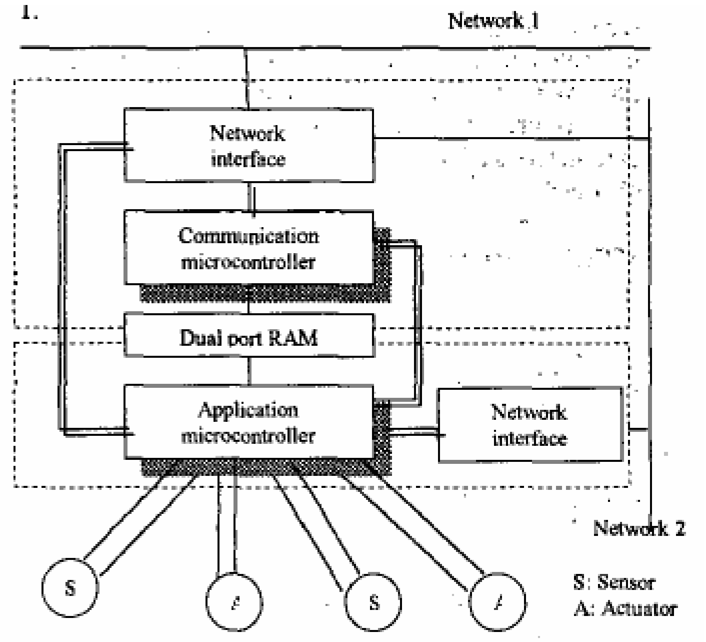

Figure 4: Proposed Architecture at the Node Stage [4]

There are a variety of different methodologies to test reliability. The Markov-chain models were used to evaluate this node. This model is the representation of a single node. Various results were obtained such as reliability, mean time to failure (MTTF), failure rate and mission time (MT), for the 4 architectures obtained by solving different models.

The reliability of each node was calculated using the formula, $R(t) = e^{-\lambda t}$ from the Markov-chain model where R is reliability, t is time and λ is failure rate. Values obtained for reliability were compared with the computed values using SURF-2, a program for dependability evaluation of complex hardware and software systems, for the different architectures. MTTF, failure rate and MT were obtained and compared also using equations, $MTTF = \int_0^\infty R(t)dt$, $\lambda = -\left[\frac{\log R(t)}{\log e}\right]\frac{1}{t}$, and $MT[r] = \frac{-\ln(r)}{\lambda}$.

At the network stage, for the system to be reliable, the network must be reliable since the nodes communicate with each other through the network. RS485 is a balanced serial interface for the transmission of digital data. It can be used for an application with several points that have one master and many slaves. The Controller Area Network (CAN) is a computer network protocol that allows microcontrollers to communicate with each other with a host computer. Both of these were used and compared and were deemed equally suitable for detecting and handling fault.

The CAN protocol was compared with 3 other medium access control protocols like CSMA/CD, master-slave and token passing which can be used by the RS485 network. OMNET++, a discrete event simulation system, was used to compare the 4 protocols under 3 different situations; changes of arrival rate, changes of frame length, and changes of number of nodes.

The best result for the fault-tolerant architecture was having the fault-tolerant nodes interconnected by the CAN bus. Figure 5 shows this architecture.

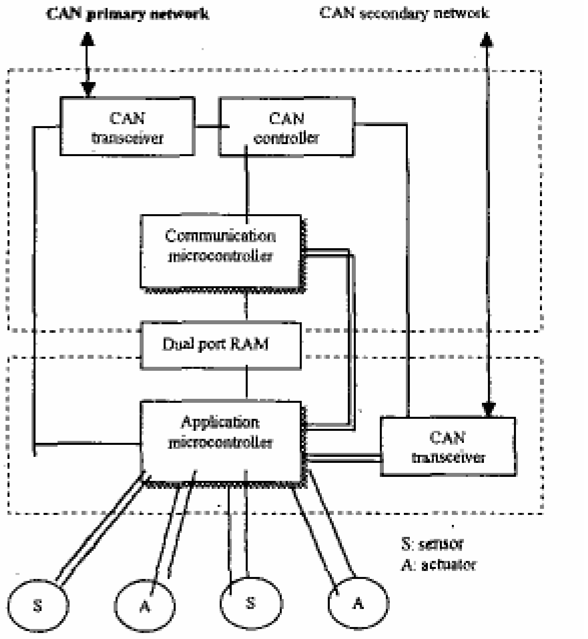

Figure 5: Fault-tolerant node using CAN [4]

The Markov model proved that the fault-tolerant architecture using the CAN network has better fault-tolerant features, therefore being highly reliable.

Risk Assessment and Cost

With this replacement initiative in mind, factors such as risk and cost must be considered. As such, in the design of any system, there is never zero risk however risk is to be minimized as much as possible. The overall cost of developing and maintaining a system is also vital and should be kept as reasonable as possible.

First Energy Nuclear Operating Company (FENOC) Perry Station [1] built in 1974 using the old analog control system still exists today. A recent trip in two of the feedwater control systems was the cause of losing revenue and thousands of dollars. Situations like this happen to be similar in many places around the world. There is a lot of risk involved in these situations and many result in the several expenses. Many plants in the United States and around the world are in need of control modernization which should decrease the risk and cost involved.

Control Technology Generations:

In the first generation, microprocessors made the previously hard-wired control algorithms programmable and also added the capability to run on many microprocessors. This created digital control that did not suffer degradation and was adjustable. In the second and current generation, the digital designs increased processing power and data communication speed. The shift towards using industry standard operating systems (i.e. Microsoft Windows). With these changes, the control design tools and operator interface became easier to use and much more powerful.

The next generation is the third generation. The aims are to increase connectivity more and decrease hardware costs. Communication protocols such as Fieldbus, Profibus, and Plant Ethernet give the ability to control further into the field and decreases the amount of wiring needed. This generation seeks to increases the vertical integration of the control systems along with all of the other plant information systems. This allows the operator to bring up many types of information to be displayed at once (i.e. blueprints, maintenance records, design specifications, electrical diagram etc.) Figure 6 shows the operator tools that DCS incorporates.

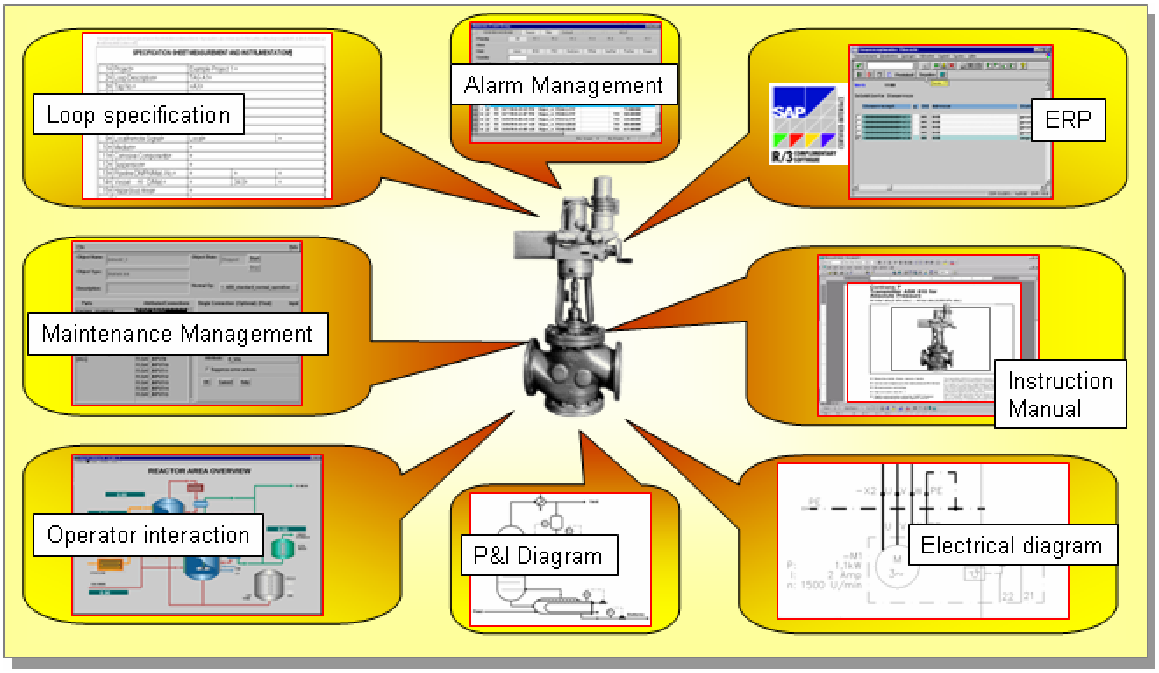

Figure 6: DCS Advanced operator tools [1]

The last item is the introduction of loop self-tuning, neural nets, or Advanced Process Control (APC). This will helpful with control systems that involve multi-variables.

Mitigate Risk and Decrease Costs:

Nuclear power plants are 10-15 years behind second and third generation DCS design. To make up for this large gap, there is a lot of risk involved. Between $500K to $1M of lost generation revenue is estimated for nuclear power plants. This amount of money lost is not justifiable for the possibilities that exist. There have to be ways implemented to mitigate these risks. There is already a given advantage with nuclear power plants over fossil fuel plants. All of the plants already contain good simulators. This simulator can be adapted to the inclusion of simulating for the control system. An appropriate and efficient method must be implemented in order to meet this objective.

For first and some second generation DCS, simulations were always fairly easy to develop. All that was necessary was a simple conversion of the control diagrams from FORTRAN logic statements to be assembled with the rest of the process model source code. Though, with third generation DCS, it has become much too complex to simply use the “Full Emulation” method. Therefore a new approach has been suggested called Virtual Stimulation. This approach ports the underlying controller source code to run on a low-cost computer platform. It has the ability to deliver the basic functions and an added addition and advantage is that it allows multiple controllers to run off a single processor. This would decrease the amount of hardware required and therefore be lower in cost. The way in which the Virtual Stimulation functions is by communicating with the real Operator and Engineering workstations and their designated applications.

There has also been much competition among the DCS suppliers. With more competition, these suppliers are bound to release new software versions on a steady basis. For Virtual Simulation, it is easy to stay in tact with these software releases because of the commonality between the codes. However, for Emulations, there is the need to create processes for each software release. That is another advantage of the Virtual Stimulation.

A comparison between the Emulation approach and Virtual Stimulation approach to model the control system is shown in Figure 7.

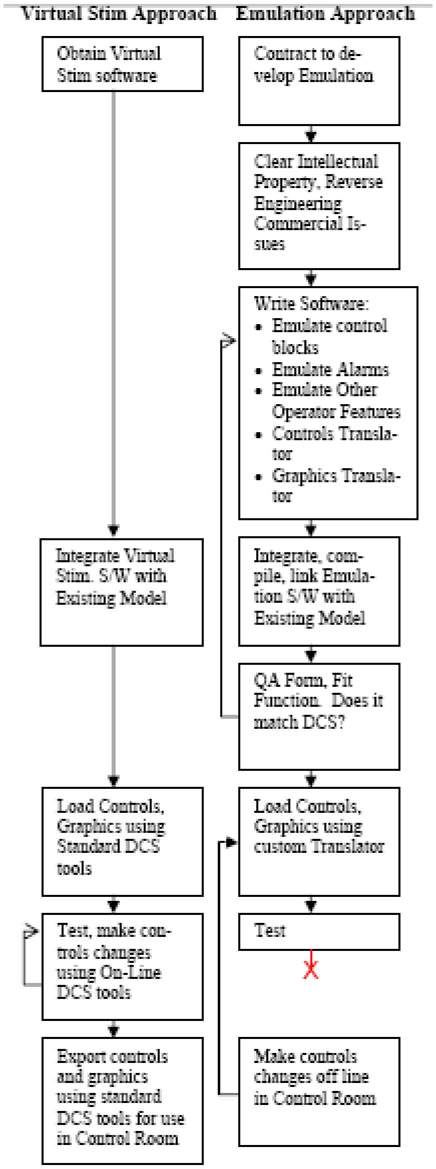
Virtual Stim Approach
Emulation Approach
Obtain Virtual Stim software
Contract to develop Emulation
Clear Intellectual Property, Reverse Engineering Commercial Issues
Write Software:
• Emulate control blocks
• Emulate Alarms
• Emulate Other Operator Features
• Controls Translator
• Graphics Translator
Integrate Virtual Stim. S/W with Existing Model
Integrate, compile, link Emulation S/W with Existing Model
QA Form, Fit Function. Does it match DCS?
Load Controls, Graphics using Standard DCS tools
Load Controls, Graphics using custom Translator
Test, make controls changes using On-Line DCS tools
Test
Export controls and graphics using standard DCS tools for use in Control Room
Make controls changes off line in Control Room

Figure 7: Development workflow diagram for simulation of DCS: Virtual Stimulation vs. Emulation [1]

With the implementation of DCS and the use of this Virtual Stimulation approach, nuclear power plants should be on their way to reducing the cost and risk involved the controls systems area.

Conclusion

The risks and costs involved with keeping older control technology in nuclear power plants are not very feasible anymore. Newer control technologies like the DCS are looked into for mitigating these risks, keeping a low cost, and being very reliable. There have been a fair amount of DCS architecture structures proposed throughout the world. Along with these new designs, their reliability is also undergoing tests and being analyzed. This information was presented.

References

1) G. McKim, M. Yeager, & C. Weirich. DCS Upgrades for Nuclear Power Plants: Saving Money and Reducing Risk through Virtual-Stimulation Control System Checkout. SimSci-Esscor, & FENOC Perry.

2) H. S. Kim, J. M. Lee, T. Park, & W. H. Kwon (2000). Design of Networks in Distributed Digital Control Systems in Nuclear Power Plants. School of Electrical Engineering and ERC-ACI, Seoul National University.

3) T.R. Park, J. M. Lee, J. Y. Choi, S. Y. Shin, H. S. Kim, J. Y. Lee, & W. H. Kwon (2000). Implementation of PICNET+ as the Control Network of the Distributed Control System for the Nuclear Power Plant. School of Electrical Eng. and ERC-ACI, Seoul National University.

4) W. Mariam, W. Muda, & A. Y. M. Shakaff (2002). Designing a Fault-Tolerant Architecture for Real-Time Distributed Control System. School of Electrical and Electronic Engineering, Univeristi Sains Malayia.

5) A. M. Hemeida, M. Z. El-Sadek, & S. A. Younies. Distributed Control System Approach for a Unified Power System. Higher.Institute of Energy, Aswan, Egypt, Assisut University, Assiut, Egypt & Aswan Hydr-Power Station, Aswan, Egypt.

6) J. R. Pimental, & M. Salazar (2002). Dependability of Distributed Control System Fault Tolerant Units. Department of Electrical and Computer Engineering, Kettering University, & Department of Electrical Engineering, Universidad de los Andes.

7) R. Lewis (1997). Design of Distributed Control Systems in the Next Millenium. *Computing & Control Engineering Journal, 148-152.*

8) C. Diedrich, R. Simon, & M. Riedl (2000). Engineering of Distributed Control Systems. Institut fur Automation und Kommunikation Magdeburg e.V. (ifak).

9) E. E. Harmer, G. Mitchel, & A. Hepburn (2003). DCC Replacement Initiative – System Design Process and Standards Framework. *24th Annual Conference of the Canadian Nuclear Society. Atomic Energy of Canada Limited.*

10) G. Bereznai (2005). Nuclear Power Plant Systems and Operation. School of Energy Systems and Nuclear Science, University of Ontario Institute of Technology.