Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 09, September-2016

Single Point Vulnerability Analysis of CEDMCS in Advanced PWR using a Systems Engineering Approach

Awwal Mohammed Arigi and Yong-kwan Lee
Nuclear Power Plant Engineering Department
KEPCO International Nuclear Graduate School
Ulsan, South Korea

***Abstract*— Single Point Vulnerability (SPV) refers to any component whose failure will lead to power reduction or reactor trip in a nuclear power plant. The instrumentation and control (I&C) systems have been identified as a major cause of reactor trips. The Control Element Drive Mechanism Control System (CEDMCS) is the I&C system selected for this work. The Advanced Power Reactor 1400MWe (APR1400) can deploy either of two different designs of the CEDMCS. Identifying available SPV components in these systems is a key step to mitigating, bridging or eliminating such components. Systems Engineering is an interdisciplinary approach that can enable the realization of successful processes. This work follows the activity or process modelling technique in systems engineering to show a method of identifying the SPV components in two digital rod control systems. The entire process stages of needs analysis, requirement analysis, functional analysis, system design, and process verification is followed. The results show the potential SPVs in both systems and possible management strategies for the identified SPV components are suggested.**

Keywords—Single Point Vulnerability; CEDMCS; APR1400; Systems Engineering

I. INTRODUCTION

Nuclear power plants (NPPs) are regarded as one of the safest and most reliable systems yet you can still find some possibilities of failure. No matter how negligible, the possibility of failure always exists and the Advanced Power Reactor 1400MWe (APR1400) is not an exception. Single Point Vulnerability (SPV) is a component whose failure would directly cause an automatic or manual reactor scram or turbine trip [1]. Although the impact of a scram is much greater than that of a power generation reduction, most power plants consider components that cause power reduction as SPVs. While some power plants do not consider the cause of any reduction in power as SPV, others consider components that cause a reduction in power of as low as 2% as SPV. The U.S. (United States) Nuclear Industry Scram Trend [2] as shown in Fig.1 indicates the total number of manual and automatic scrams per year in the United States of America. This shows that the unwanted reactor trips in Nuclear Power Plants (NPPs) is still prevalent.

This research was supported by the 2016 research fund of the KEPCO International Nuclear Graduate School, Republic of Korea and the International Atomic Energy Agency (IAEA).

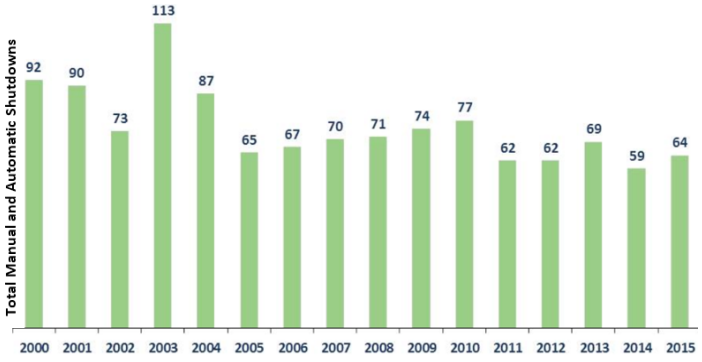

Fig. 1. Trend in US Nuclear Industry Shutdowns.

A proper identification and subsequent management of SPVs should be a priority because they cause plant trip and may also be a reason for reduction in power output. The plant trip will challenge the safety systems, while a reduction or loss of power will ultimately cause revenue loss for the utility.

Systems Engineering (SE) is an interdisciplinary approach and a means to enable the realization of successful systems. It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, and then proceeding with design synthesis and system validation while considering the complete problem [3]. It serves as a guide in the application of scientific principles to practically ensure the efficient and economic operation of complex equipment and systems. The Control Element Drive Mechanism Control System (CEDMCS) also referred to as a Digital Rod Control System (DRCS) is an example of a complex system as can be seen in Fig. 2 with several interfacing systems.

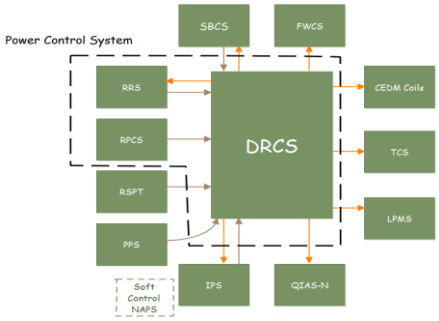

Fig. 2. DRCS interfacing systems [4].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 09, September-2016

The CEDMCS /DRCS is one of the three major parts of the power control system (PCS) in the APR1400 NPP design. Other parts are the reactor regulating system (RRS) and the reactor power cutback System (RPCS). The DRCS controls the holding and motive power associated with the control element drive mechanism (CEDM). The DRCS uses either an automatic control element assembly (CEA) motion demand signal from the RRS or manual motion signals from the DRCS soft control. It converts these signals to direct current (DC) pulses that are transmitted to CEDM coils to cause CEA motion. When the CEA motion is demanded, the coils are energized in sequence to cause either insertion or withdrawal of the CEA or control rod. Nuclear reactivity and therefore the power of the NPP can be controlled by these insertion or withdrawal operations. When the under-voltage relays in the DRCS detect that power in the CEDM has been interrupted, the DRCS provides signals to the Turbine Control System (TCS), Steam Bypass Control System (SBCS), and the Feedwater Control System (FWCS). A reactor trip signal removes the motive power from the DRCS which in turn makes the CEAs to be dropped by gravity. Note that in Fig. 2, LPMS=Loose Parts Monitoring System, RSPT=Reed Switch Position Transmitter, QIAS=Qualified Indication and Alarm System and NAPS= Nuclear Application Systems.

However, one of the major functions of the DRCS is to provide control signals and interlock signals (switch contacts designed to prevent a control system from taking two incompatible actions at once) to the CEDM. These control signals are initiated by the RRS. The DRCS also provides interfacing signals to the Information Processing System (IPS). These control limits and interlocks prevents abnormal power and temperature conditions that may be caused by excessive control rod withdrawal due to control system malfunction or wrong action from the operator.

Systems engineering is used in this work because it is focused on the system as a whole. These include the identification of customer needs, system operational environment, interfacing systems, logistics support requirements, capabilities of operating personnel, and such other factors as must be correctly reflected in system requirements documents and accommodated in the system design. Dealing with risks is one of the essential tasks of systems engineering, requiring a broad knowledge of the total system and its critical elements. In particular, systems engineering is central to the decision of how to achieve the best balance of risks [5]. These risks are evident in the existing SPVs of the CEDMCS.

II. SYSTEMS ENGINEERING APPROACH DEVELOPMENT

The top-level perspective of the entire process design is depicted in Fig.3. It starts with an adequate articulation of the process needs with a needs analysis through to the design and verification stages. The rounded rectangular boxes represent the major stages of the process while the rectangle shaped boxes connected to them are the identified activities at each stage of the process. Arrows indicate the sequence of the process. There is a feedback arrow when a "change request" is demanded at the verification stage.

1.0 Needs Analysis

Fig. 4 illustrates the yearly frequency of reported reactor trip events in Korean NPPs between 2000 and 2016 [6]. The various causes of reactor trips considered were External effects, I&C components, Electrical components, Mechanical components, and Human factors. Sixty-six (25.2%) out of a total of 262 events resulted from instrumentation and control (I&C) systems. This shows that I&C systems are the highest source of reactor trips.

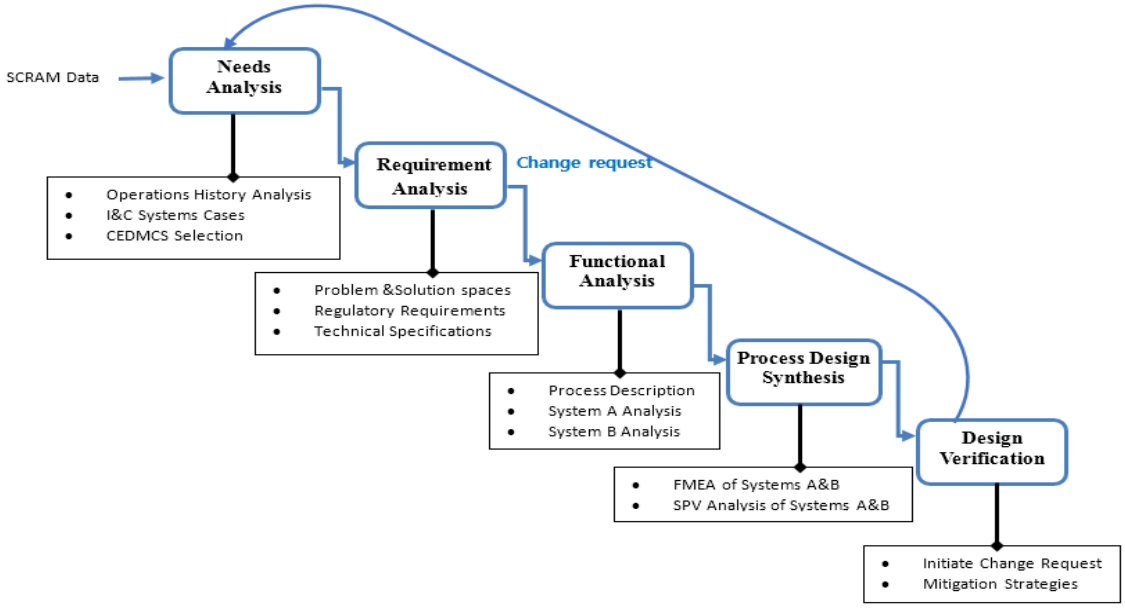

Fig. 3. SPV analysis process stages (where SRAM refers to sudden shutdown of reactor by rapid insertion of control rods)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 09, September-2016

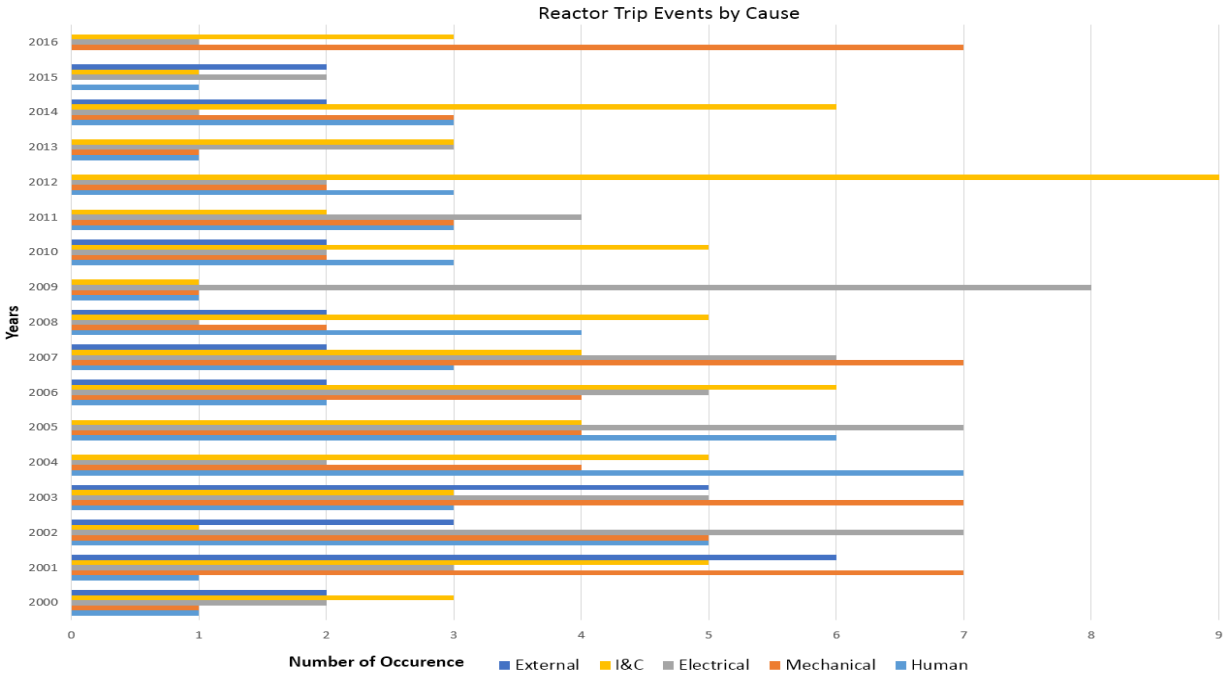

Fig. 4. Yearly reactor trip events in korean NPPs by cause.

The data in Fig.4 suggests that over the course of 16 years, the trend in I&C induced reactor trips has barely abated (i.e. year 2000, 33%, year 2005, 19%, year 2010, 37% up to year 2016, 25.2%). When I&C systems fail, they can cause unplanned reactor trips, turbine trips or a violation of technical specifications and by so doing cause unavailability and reduction in plant reliability. The CRDMCS is one of the most important I&C systems in the NPP as it is directly related to the power control system. Almost any failure in the CEDMCS could have similar consequences as previously stated for I&C systems failure. Failures will likely emanate from component parts of a system. Hence the need to properly identify any SPVs in the CEDMCS so that further actions can be taken to mitigate the failure of such components.

The APR1400 is an advanced pressurized water reactor (PWR) type. There are two rod control systems that will each be deployed to this (APR1400) power plant type and therefore they are both analyzed in this paper. They are referred to as System A and System B in this work.

2.0 Requirement Analysis

It is necessary to translate the identified needs into clear requirements. Based on E. Hall's [7] description of the problem and solutions domain, table 1. shows the problem and solution spaces for this work. For the sake of unambiguity, the requirements analysis is approached as the requirements for identification of SPVs. According to reference [1], the SPV program must have a clear direction for identifying what is an SPV. In this work, SPV identification will be qualitative. Only those components that cause reactor trip to be initiated would be considered and only the parts within the CEDMCS would be considered. The following are examples of sources that could be used in the review include: system or component function description; system or component loop, logic, or circuit drawings; Final Safety Analysis Reports and Technical Specifications [1].

TABLE I. PROBLEM AND SOLUTION SPACES

Requirements Layer	Domain	View	Role
Stakeholder Requirements	Problem Domain	Stakeholders View	Determine causes of Reactor Trip in APR1400
System Requirements	Solution Domain	Analyst View	Determine SPVs within the CEDMCS
Architectural Design	Solution Domain	Designers' view	-Develop FMEA of Systems A&B -Derive SPV analysis of Systems A&B

3.0 Functional Analysis

The process functions in this work is shown in Fig. 5, where attention is paid to the particular deliverables of the process designed. The first step is the thorough examination of existing design (system A) and the new design (system B). This is done to understand the workings of the systems. This first step is accomplished with the aid of digital rod control system (DRCS) descriptions, operating manuals, and the Standard Safety Assessment Report (SSAR) of the APR1400. The system B is examined with the aid of System descriptions and publication papers. In the second step a Failure Mode Effect and Analyses (FMEA) was developed for both systems A and B. This is based on the understanding of the unique designs of both systems. In the third step, a qualitative SPV analysis of both systems is derived while considering previous FMEA evaluations of the systems.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 09, September-2016

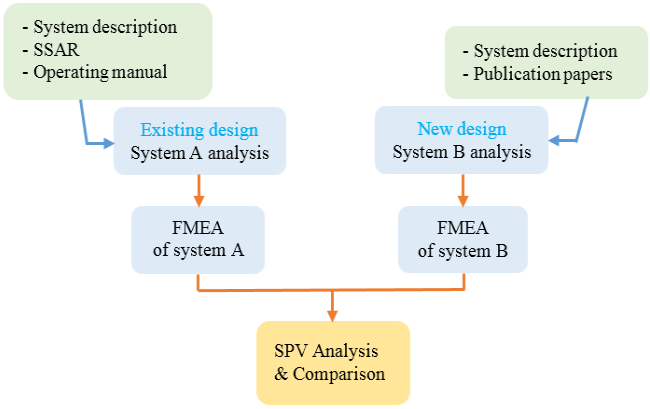

Fig. 5. SPV analysis process functions.

3.1 System A

This is the existing Control Rod Control System. The major parts of System A are the Power Cabinets (PC), Logic Cabinet (LC), and Remote I/O cabinets (see Fig.6). The control cabinet consists of input modules, power supplies, communication devices and others. It generates the CEDM coil commands to step the rods during startup, shutdown, and power maneuvering operations. It also coordinates all operations within the DRCS including communication with the Nuclear Application System (NAPS) of Information Processing System (IPS) and providing alarm outputs for detectable failures in some DRCS parts.

The power cabinet consists of 13 selecting cabinets and 6 moving cabinets. The selecting cabinets delivers power to the Upper Gripper (UG) and Lower Gripper (LG) coils while the moving cabinets delivers power to the Upper Lift (UL) and Lower lift (LL) coils (see Fig. 7).

The major components of the power cabinet are; power conversion circuit, multiplexing, power regulator, alternative DC hold power, and DC power supplies.

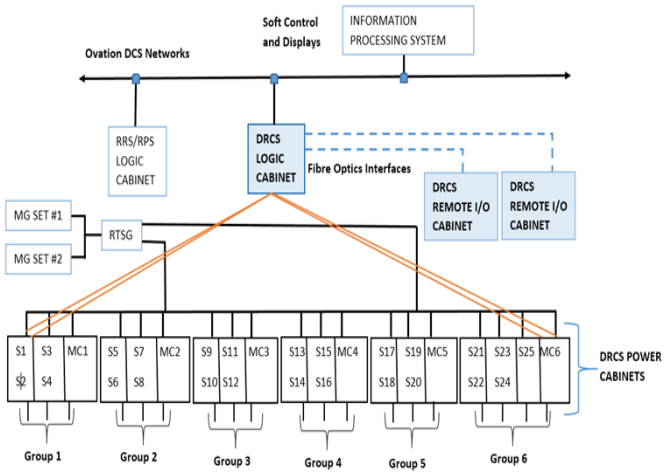

Fig. 6. DRCS configuration of (existing) system A [4].

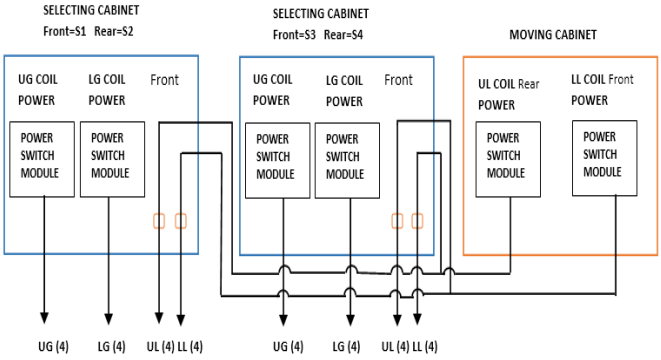

Fig. 7. System A power cabinet configuration [4].

3.2 System B

The new DRCS shown in Fig. 8 consists of two major parts; Control cabinet and Power cabinet. There is only one control cabinet, and a minimum of 3 power cabinets. The number of power cabinets in the APR1400 plant would be eight. The assumption is that at least 93 CEAs are needed in the APR1400 design with 3 CEA groups per Power cabinet (12 CEAs).

The control cabinet receives command signals form the RRS, MCR or other interfacing systems and sends the signals to the appropriate power cabinet. The Main control unit (MCU) and the Local operator Module (LOM) are the major parts of the Control cabinet. The MCU functions to develop the signals received from external interface systems like the RRS, PPS, Reactor operator or etcetera. The power cabinet has the major parts as; the power control unit (PCU) and the power converter module (PCM). The Power cabinet has 3 sets of hardware to control each CEDM group except for the PCM Lift Coil (LC) which is only one per cabinet as shown in Fig. 9.

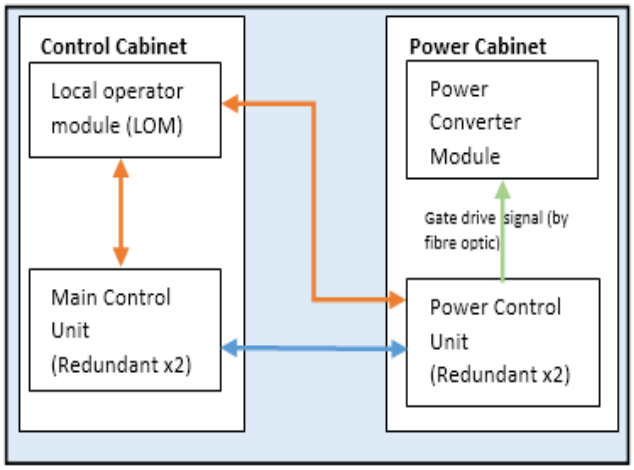

Fig. 8. DRCS configuration of (new) system B [8].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 09, September-2016

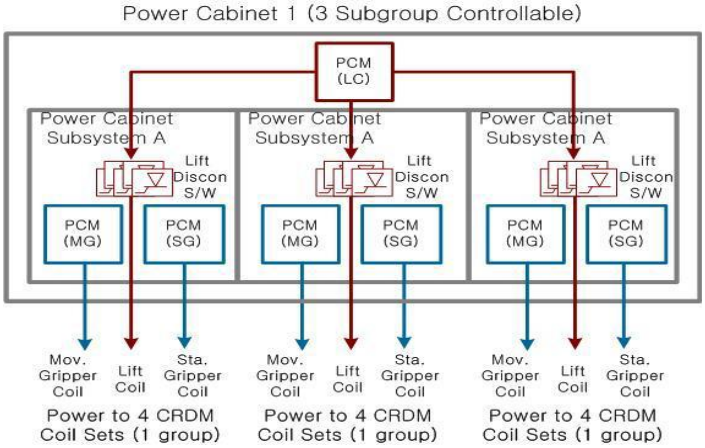

Fig. 9. System B power cabinet configuration [8]

4.0 Process Design Synthesis

This stage involves the system or process developer's analysis. For this work, this is the process outputs of FMEA and SPV analysis. For failure mode and effect analysis, the system or component function description; system or component logic and power circuit drawings; SSAR and Technical specifications; Industry experience on equipment-related scrams; and Vendor recommendations are utilized. A summary of the FMEA result for both systems are shown in the tables II and III.

A qualitative SPV analysis is done at this stage based on the results of the FMEA while paying particular attention to components without redundancy and their operational functions. Only the components strictly within the CEDMCS are considered. Results are shown on tables IV and V. The number (No.) of SPVs for each component type are also indicated.

TABLE II. FMEA FOR SYSTEM A.

Component Name	Failure Mode	Failure Effect
PC- PCC (Power conversion circuit)	Spurious actuation	Lift or Gripper latches of one group close. Control rods drop
PC - Digital Out	Malfunction	Causes turbine trip signal which stops the generator
PC- Current Regulation Card	Fail to operate	No drive signals generated for PCC. Reactor trips due to RPS signal (LO-DNBR/HI-LPD)
PC - Digital Signal buffer Card	Malfunction	No drive signals generated for PCC. Reactor trips due to RPS signal.
PC - Gate firing driver Card	Malfunction	Reactor trips due to control rods drop.
PC -Multiplexing Error Detector	Fail to operate	Related CEA groups are inoperable
PC - Backplane Card	Malfunction	No control signal transmission to PCC. Reactor trips due to control rod drop.
PC - Power supply Card	Fail to operate	Reactor shutdown due to RPS signal
PC - Power Regulator	Malfunction	Reactor shutdown due to RPS signal
PC - Phase control	Malfunction	Coils are energized out of sequence. Reactor trips due to control rods drop.
PC -Fuse	Fuse cut	Causes Reactor shutdown due to RPS signal
PC -Circuit Breaker	Breaker open	Causes Reactor shutdown due to RPS signal
LC -communication card	Failure to transmit or receive data	No manual control of CEAs. The RPS initiates reactor trip
LC -sequence logic of bank & group	Malfunction	Causes Reactor shutdown due to RPS signal
LC -sequence order generator	Malfunction	Causes Reactor shutdown due to RPS signal
LC -data store& diagnostic	Malfunction	No drive signals failure detection.
LC - I/O manager	Malfunction	No drive signals. Rector shutdown due to RPS signal
Master Cycler	Malfunction	Related CEA groups are inoperable
Slave Cycler	Malfunction	Related CEA groups are inoperable

(WHERE DNBR=DEPARTURE FROM NUCLEATE BOILING, LPD=LOCAL POWER DENSITY)

TABLE III. FMEA FOR SYSTEM B.

Component Name	Failure Mode	Failure Effect
PCM-MGC (movable gripper control)	Spurious actuation	MG latches of one group close. Control rods drop
	Fail to operate	MG latches of one group are inoperable
PCM-SGC (stationary gripper control)	Spurious actuation	SG latches of one group close. Control rods drop.
	Fail to operate	SG latches of one group are inoperable
PCM-LD (Lift disconnect) switch	Fail to ON/OFF	Related group or individual rods are inoperable. Eventual RPS signal is initiated.
PCM-Lift Coil circuit	Spurious actuation	Improper voltage to CEDM coils. Related CEA groups are inoperable
	Fail to operate	Related CEA groups are inoperable
Power Control Unit (PCU)	Fail to operate	No drive signals generated for PCM. Reactor trips due to control rods drop.
Backplane board	Malfunction	No control signal transmission to PCM. Reactor trips due to control rod drop.
LOM communication card	Malfunction	No manual control of CEAs. The RPS initiates reactor trip
MCU-speed pulser	Malfunction	The RPS initiates reactor trip
MCU-sequence logic of bank & group	Malfunction	The RPS initiates reactor trip
MCU- sequence order generator	Malfunction	The RPS initiates reactor trip
MCU-data and diagnostic.	Malfunction	The RPS initiates reactor trip
MCU- I/O manager	Malfunction	No sequence logic signals generated. The reactor condition remains same. Eventual Reactor trip

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 09, September-2016

TABLE IV. SPV COMPONENTS FOR SYSTEM A.

Device Name	No.	Failure Mode	Failure Effect
Digital Out (Under-Voltage Relay)	26	Malfunction	Causes turbine trip signal which stops the generator
Current Regulation Control card	13	Malfunction	No drive signals generated for PCC. Reactor trips due to control rods drop.
DRCS Digital Signal buffer Card	13	Malfunction	Reactor shutdown due to RPS signal
Gate firing driver Card	13	Malfunction	Reactor trips due to control rods drop
Backplane Card	13	Malfunction	Reactor shutdown due to RPS signal
Power supply Card	13	Fails to operate	Reactor shutdown due to RPS signal
Power Cabinet Fuse	13	Fuse cut	Reactor shutdown due to RPS signal
Power Cabinet Circuit Breaker	13	Breaker open	Reactor shutdown due to RPS signal
Total Number of SPVs	117		

TABLE V. SPV COMPONENTS FOR SYSTEM B.

Device Name	No.	Failure Mode	Failure Effect
PCM-MGC	24	Spurious actuation Fail to operate	MG latches of one group close/ inoperable. Control rods drop.
PCM-SGC	24	Spurious actuation Fail to operate	SG latches of one group close/inoperable. Control rods drop.
PCM-LD switch	24	Fail to ON/OFF	Related group or individual rods are inoperable. RPS signal initiated.
PCM-Lift Coil circuit	8	Spurious actuation Fail to operate	Improper voltage to CEDM coils. Related CEA groups are inoperable.
Total Number of SPVs	80		

The PCM (Power Conversion Module) is a prospective SPV part of the CEDMCS in system B, as they have no redundancy. All its major sections including the Lift Coils Module, Stationary Gripper Coil Module, Movable Gripper Coil Modules, and the Lift Disconnect Switches may individually cause reactor scrams. When the Lift Coil PCM fails to operate, three CEDM groups will be non-functional, and thus cause the LO-DNBR or HI-LPD setpoints to be exceeded. This will make the Reactor Protection System Trigger an automatic reactor trip.

5.0 Process Verification

Verification encompasses the tasks, actions, and activities performed to evaluate the progress and effectiveness of the evolving system solutions (people, products, and process) and to measure compliance with requirements [3]. The primary purpose of verification is to determine that this process and products are compliant with the earlier assigned requirements. When it is found that the process is defective or fails to meet its initial requirements, a change request may be issued. However we have applied the process to effectively determine the SPV components in the CEDMCS as shown in tables IV and V.

5.1 Management of SPV

The preventive maintenance basis database developed by the Electric Power research Institute (EPRI) can be an effective tool in the successful management of SPVs. This is because the database is being continuously updated to provide component failure modes, mitigation of such failure modes, and sometimes may also include the effectiveness of those mitigation strategies.

The best method for eliminating these SPV components shown in this work would be by changing trip logic or adding parallel circuits. However, considering the recent deployment of these CEDMCS systems, management (mitigation) of these components will be appropriate for now. A strong mitigation strategy includes actions for prevention, detection, and correction but a mitigation strategy can be effective only for modes of failures that can be prevented or have degradation modes that can be detected [1].

Mitigation strategies for the CEDMCS may include maintenance mitigation and supply chain mitigation. In maintenance mitigation, a preventive maintenance (PM) program should be established to address the identified failure modes. This program should be within the scope and frequency of already approved PM template of the NPP. CEDMCS is classified as a non-safety system and therefore the current procurement policies may not be stringent enough. Supply chain mitigation can be implemented for the identified SPVs by improving the quality of procurement process, post-manufacturing testing, and testing before and after installation.

III. CONCLUSION

This paper has shown the application of systems engineering process to achieve SPV analysis. By implementing an SE approach in the CEDMCS design, we could get a broad perspective of the process at the early stages. The process and activities to be performed were identified at the budding stage enabling, the schedule and investment to be optimized.

System A design has employed a fail-safe concept to its design with less redundancies while System B design provides redundancy and design change although this comes at a high price for the Utility. System B design has improved reliability but not necessarily eliminating the SPV items. The total number of SPVs is found to have reduced from 117 components in system A to 80 components in system B. Naturally, the cost of a new redundant system will be more. However, future work may examine the economic effect of the new system considering the operating experiences of power plants on the CEDMCS (i.e. SCRAM rates and power outage cost).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 09, September-2016

A limiting factor for this work is that none of the APR1400 NPPs have gone into commercial operation as at the time of writing this paper. Therefore SCRAM analysis for other operating NPPs in Korea have been used in the needs analysis stage of this work.

Further work on this subject may also attempt to produce a risk ranking of the potential SPVs. This will help utilities in determining the kind of maintenance strategy that should be applied to individual SPVs components.

REFERENCES

[1] Single Point Vulnerability (SPV) Process Guide. EPRI, Palo Alto, CA: 2015.3002005419. pp.2.2 - 3.10.

[2] Trend in US Nuclear Industry Shutdowns [Internet]. [Cited 2016 Aug 29] Available from: http://www.nei.org/Knowledge-Center/Nuclear-Statistics/US-Nuclear-Power-Plants/US-Nuclear-Industry-Scram-Trend.

[3] INCOSE, "Systems Engineering Handbook", version 3.2.2., INCOSE-TP 2003-002-03.2.2., October 2011. pp. 129-365

[4] NPP Systems Textbook – Control and Protection Systems, Rev.2, KHNP-HRDI, BNP-FU-COM-SYS-TB-DRCS. pp.9-16.

[5] Alexander Kossiakoff, William N. Sweet, Samuel J. Seymour, and Steven M. Biemer, "Systems Engineering Principles and Practice", 2nd Ed. Wiley & Sons, Inc. 2011. pp.7.

[6] KINS-OPIS, Nuclear event evaluation database: recent nuclear events [Internet]. [Cited 2016 Aug 29] Available from: http://opis.kins.re.kr/opis

[7] Elizabeth Hull, Ken Jackson, and Jeremy Dick, "Requirements Engineering", Springer, 2011 pp.20-21.

[8] Chae-Ho Nam, Jung-Han Nam, Sim-Kyun Yook, and Chang-Ho Cho, "Design and Implementation of Advanced Digital CRCS for Pressurised Water Reactors", (European Nuclear Conference) ENC 11-14 Dec, 2005.