



System Protection Schemes: Limitations, Risks, and Management

Final Project Report

Power Systems Engineering Research Center

*Empowering Minds to Engineer
the Future Electric Energy System*



System Protection Schemes: Limitations, Risks, and Management

Final Project Report

Project Team

**James McCalley, Project Leader
Olatujoye Oluwaseyi, Venkat Krishnan, Renchang Dai
Iowa State University**

**Chanan Singh, Kai Jiang
Texas A&M University**

PSERC Publication 10-19

December 2010

Information about this Project

For information about this project contact:

James D. McCalley
Professor
Iowa State University
Department of Electrical and Computer Engineering
Ames, Iowa 50011
Phone: 515-294-4844
Fax: 515-294-4263
Email: jdm@iastate.edu

Power Systems Engineering Research Center

The Power Systems Engineering Research Center (PSERC) is a multi-university Center conducting research on challenges facing the electric power industry and educating the next generation of power engineers. More information about PSERC can be found at the Center's website: <http://www.pserc.org>.

For additional information, contact:

Power Systems Engineering Research Center
Arizona State University
577 Engineering Research Center
Tempe, AZ 85287-8606
Phone: 480-965-1643
Fax: 480-965-0745

Notice Concerning Copyright Material

PSERC members are given permission to copy without fee all or part of this publication for internal use if appropriate attribution is given to this document as the source material. This report is available for downloading from the PSERC website.

© 2010 Iowa State University. All rights reserved.

Acknowledgements

This is the final report for the Power Systems Engineering Research Center (PSERC) research project titled “Special Protection Schemes: Limitations, Risks, and Management” (PSERC project S-35). We express our appreciation for the support provided by PSERC’s industrial members and by the National Science Foundation’s Industry/University Cooperative Research Center program.

We very gratefully acknowledge the inputs received from the industry experts, including Ali Chowdhury (CAISO), Jim Gronquist (BPA), Wenyuan Li (BC Hydro), Tony Johnson, and Dede Subakti (MISO), for their insightful comments, which were very helpful in shaping this work.

Executive Summary

Special protection schemes (SPS), known also as remedial action schemes, are designed to detect abnormal system conditions and take predetermined, corrective action (other than the isolation of faulted elements) to preserve system integrity and provide acceptable system performance. Today, in many parts of the world, SPS represents a viable planning alternative to extending transmission system capability. Although SPS deployment usually represents a less costly alternative than building new infrastructure, it carries with it unique operational elements among which are: (1) risks of failure on demand and of inadvertent activation; (2) risk of interacting with other SPS in unintended ways; (3) increased management, maintenance, coordination requirements, and analysis complexity. Additionally, there is a dearth of simulation and assessment tools for performing reliability studies of SPS and enable planners to evaluate the operational complexity that SPS brings into the system along with its various economic and operational advantages.

So the objective of the proposed work is to provide a structured framework for identifying limitations of SPS deployment within a system, and assessing SPS risks and develop proper standards and practices for maintaining SPS reliability over its lifetime.

One of the highlights of the report is the unique assessment framework proposed based on both a *process view* and a *systems view* to identify risks and associated consequences for SPS. The process view based framework will view SPS in terms of a *process* which considers all the building blocks starting with the actuating signals, the equipment and logic used to operate on those signals, communication equipments and so on till the final action. The system view framework will view SPS in terms of its position in and impact on the power *system* in which it exists. This framework proposed is one of the significant contributions of this report, as even though a particular SPS design may appear quite reliable from the process view, it may not be so from system view due to the prospect of failures from interactions among many SPS in the system. So the system view risk assessment framework addresses such critical issues, which otherwise could cause cascading and catastrophic system consequences.

Some of the contributions from this project are:

1. A document with concentrated information pertaining to:

- Background: Summary of relevant literatures on SPS, their operational and maintenance strategies from IEEE transaction papers, CIGRE documents, NERC standards, NERC sub-regions, and individual RTOs, ISOs, and companies.
- Technology or knowledge transfer: An overview of standards and methods from industries such as process control, nuclear and power system, in order to leverage interesting ideas from these mature industries that could be applicable to reliability and maintenance studies related to SPS. Safety instrument systems (SIS) of process control industry lend themselves very well in this regard.

2. SPS failure mode identification: The project provides SPS failure mode taxonomy from both process and system point of view, and proposes approaches to identify and evaluate such SPS failures.
3. Software design for system view risk assessment: Design of a simulation capability to test various SPS logics, with flexibility to vary the SPS logic and intelligence to vary operating conditions and events over a wide range.

Several reliability models and architectures for SPS and PMU-aided SPS have been developed to facilitate system view reliability studies, which would enable capturing impacts of SPS on system level phenomena.

4. Operational complexity metric: The operational and maintenance complexity due to the proliferation of SPS in power system is quantitatively captured by a proposed metric. System planning studies must incorporate such operational complexity metric in their overall formulation to estimate the limit of SPS growth for economical and reliable system operation.

The report identifies the importance of including such metric in power system planning framework, and therefore illustrates a transmission expansion planning study for SPS aided power systems.

In further investigations, the conceptual designs developed in this report will be applied on real time utility systems.

Table of Contents

1	Introduction.....	9
1.1	Types of SPS and typical components	10
1.2	Overview of report.....	14
2	Standards, practices and advancements on SPS	16
2.1	Current industry standards	16
2.1.1	NERC standards and its relationship to other international standards... ..	16
2.2	Existing industry practices.....	19
2.2.1	Design of SPS	19
2.2.2	Documentation for reliability assessments	21
2.2.3	SPS implementation and coordination in industries	23
2.3	Advancements in SPS.....	29
2.3.1	Relationship between SPS and synchrophasor technology	29
2.3.2	Role of SPS in wide area monitoring, protection and control	30
3	Relationship to other industries & applications.....	33
3.1	Process control industry	33
3.1.1	ISA S84.01	33
3.1.2	ISA dTR84.02	34
3.1.3	IEC work.....	34
3.1.4	Methods in Process control industry applicable to SPS.....	35
3.2	Nuclear industry	39
3.2.1	IEC standards.....	40
3.2.2	IAEA standards	44
3.2.3	IEEE standards.....	46
3.2.4	Challenges to the U.S. nuclear standards.....	48
3.2.5	Hints from nuclear industry	48
3.3	System operations for electric power.....	49
3.3.1	Operational security rules from decision trees.....	50
3.3.2	SPS logic design using decision trees.....	51
3.3.3	Illustration.....	53
4	Risk assessment, process view.....	55
4.1	Process view failure modes.....	55
4.2	Process view risk assessment.....	58
4.2.1	Failure mode and effect analysis.....	58
4.2.2	Fault tree analysis	59
4.2.3	Network modeling	59
4.2.4	Markov modeling.....	59
4.3	Formulation of SPS risk expression.....	60
4.3.1	Risk expression with GRS	60
4.3.2	SPS reliability evaluation.....	62
4.3.3	State probabilities.....	64
4.4	Risk assessment of generation rejection scheme	66
4.4.1	Illustration.....	67
4.5	Consideration for future SPS developments	71
4.5.1	Possible SPS architecture.....	72

4.5.2	Illustration of network reduction method	73
4.5.3	Illustration of Markov modeling method to calculate MTTF	77
5	Risk assessment, systems view	82
5.1	Systems view SPS failure- a case study	82
5.1.1	Background of SPS in Nordic grid	82
5.1.2	Event report	83
5.2	Systems view failure modes and their identification process	85
5.2.1	SPS logic design practices	85
5.2.2	SPS logic validation and failure modes	87
5.2.3	Simulation based system view SPS failure mode identification	87
5.3	Systems view risk assessment	91
5.4	Reliability analysis of power systems with impact of SPS operation	92
5.4.1	Modeling SPS operation at the component level	92
5.4.2	Modeling SPS operation at the system level	96
6	Consideration of SPS in planning	102
6.1	Electric system long-term planning with SPS	102
6.1.1	Electric system long-term planning	102
6.1.2	SPS planning related to wind	103
6.1.3	Accounting for SPS in planning	103
6.2	SPS interaction	103
6.2.1	Complexity for high penetration SPS	104
6.2.2	Illustration	105
6.3	Incorporating SPS in generation and transmission expansion planning	108
6.3.1	Case study	108
6.3.2	Transmission expansion options and specifications	110
6.3.3	Transmission expansion tree	110
6.3.4	Operational complexity	115
6.3.5	Production costs	116
6.3.6	Economic factors	116
6.3.7	Study assumptions	117
6.3.8	Optimization model	120
6.3.9	Optimization methods	120
6.3.10	Analytical Hierarchical Process	122
6.4	Optimization and AHP results	124
6.4.1	Penalty factor method	124
6.4.2	Non-linear penalty factor method	124
6.4.3	Ranking non-dominated solutions using AHP	125
7	Summary and conclusions	127
7.1	Summary	127
7.2	Conclusions	128
8	References	129

List of Figures

Figure 1: Buffalo ride area: MW requested vs. transmission capacity	10
Figure 2: General structure of a system protection scheme	11
Figure 3: Process view and system view failure modes	14
Figure 4: IEC 61508 life-cycle model	18
Figure 5: CAISO RAS maintenance program	24
Figure 6: TSA display showing real-time generation shedding arming pattern	24
Figure 7: BCTC central arming RAS system	25
Figure 8: BCTC - EMS/SCADA/protective relay integration	25
Figure 9: California and BPA remedial action schemes controllers	26
Figure 10: Motivation for C-RAS	27
Figure 11: RAS range of functionalities	28
Figure 12: Synchrophasor based vector processor from SEL	29
Figure 13: Smart RAS from SCE	30
Figure 14: Typical PMU	30
Figure 15: Wide-area monitoring and protection design	31
Figure 16: Wide area control system	32
Figure 17: Wide area control system using RAS	32
Figure 18: Economic analysis flowchart	37
Figure 19: Economic analysis of SPS aided transmission upgrade	38
Figure 20: Monte Carlo simulation based power system planning	50
Figure 21: Efficient database generation approach	51
Figure 22: SPS logic design	52
Figure 23: Decision tree: shed load or not?	53
Figure 24: Logic circuit for a GRS	66
Figure 25: Markov model for failure mode 1	68
Figure 26: Markov model for failure mode 2	69
Figure 27: A conceptual all-digital SPS architecture	72
Figure 28: SPS reliability block diagram	73
Figure 29: Reduction of SPS reliability block diagram	75
Figure 30: Simplified SPS reliability block diagram	76
Figure 31: System logical chain of the SPS	78
Figure 32: Algorithm to obtain off-diagonal elements of the matrix R	80
Figure 33: Extraction of submatrix R_{11} from matrix R	81
Figure 34: Nordic SPS case study	83
Figure 35: Confusion matrix- SPS logic testing	87
Figure 36: Simulation study- regular SPS failure mode identification	88
Figure 37: Process view SPS reliability assessment – operating conditions sampling	90
Figure 38: System view SPS risk assessment	91
Figure 39: Modeling component i without SPS operation	92
Figure 40: Modeling component i with desirable SPS operation	93
Figure 41: Modeling component i with desirable and undesirable SPS operation	93
Figure 42: Modeling component i with all SPS operation effects	94
Figure 43: Modeling component j with SPS operation effects	96
Figure 44: Modeling component k not involved in SPS operation	96

Figure 45: Decoupling interactions caused by SPS failing to operate.....	97
Figure 46: Impact of SPS operation on modeling non-contingency system states.....	98
Figure 47: Impact of SPS operation on modeling contingency system states	99
Figure 48: Reliability modeling of power systems without SPS operation	100
Figure 49: Reliability modeling of power systems with impact of SPS operation.....	101
Figure 50: Complexity of SPS	105
Figure 51: Small system for illustrating concepts.....	106
Figure 52: Small system with transmission upgrade	107
Figure 53: 5-bus system.....	109
Figure 54: Transmission tree expansion- numerical optimization.....	111
Figure 55: Transmission tree	112
Figure 56: Simple structure of analytical hierarchical process.....	122
Figure 57: Structure of AHP for power system transmission expansion planning.....	123

List of Tables

Table 1: SPS survey studies.....	9
Table 2: IEC and ISA demand mode SIL in terms of availability.....	17
Table 3: FERC approved penalty matrix	19
Table 4: Traditional vs. synchrophasor based RAS scheme.....	29
Table 5: A sample risk matrix.....	35
Table 6: A prototype illustrating the relationship between SPS and risk matrix.....	36
Table 7: Cost analysis	39
Table 8: Ranking options.....	39
Table 9: Component failure and repair rate	67
Table 10: Probability of each state.....	71
Table 11: Probability of each state of simplified model	71
Table 12: The initial state matrix	78
Table 13: The rearranged state matrix	79
Table 14: Nordic SPS event description	84
Table 15: Branch data for sample system.....	106
Table 16: SPS designs for different wind plant growth stages	107
Table 17: Time periods	108
Table 18: Forecasted load	109
Table 19: Branch data	109
Table 20: Generator data.....	110
Table 21: Generation expansion plans.....	110
Table 22: Possible solutions.....	112
Table 23: Probabilistic load profiles	116
Table 24: Different periods and associated value of load lost.....	118
Table 25: Comparison of economic factors for planning options.....	119
Table 26: Solution for the penalty factor method	124
Table 27: Solution for the non-linear penalty factor method.....	124
Table 28: Non-dominated solutions.....	125
Table 29: Comparison of economic factors and complexity	125
Table 30: Judgment matrix for the criteria	125
Table 31: Judgement matrix for operational complexity.....	126
Table 32: Judgement matrix for reliability	126
Table 33: Judgement matrix for total costs.....	126
Table 34: Final weight and rank for non-dominated solutions	126

1 Introduction

System protection schemes (SPS) (also called remedial action schemes, RAS) are designed to detect abnormal system conditions, typically contingency-related, and initiate pre-planned, corrective action to mitigate the consequence of the abnormal condition and provide acceptable system performance [1]. SPS actions include, among others, changes in load, generation, or system configuration to maintain system stability, acceptable voltages or power flows. SPS is also used as the acronym for *special protection scheme*, with has the same meaning as *system protection scheme*. However, it was recommended in [1] that word *special* be replaced by the word *system*, since it can be argued that all protection is special in some fashion. IEEE uses the System Integrity Protection System (SIPS), RAS is used by (BPA, WECC) others use the term SPS [2].

Today, in many parts of the world, SPS represents a viable planning alternative to extending transmission system capability. Although SPS deployment usually represents a less costly alternative than building new infrastructure, it carries with it unique operational elements among which are: (1) risks of failure on demand and of inadvertent activation; (2) risk of interacting with other SPS in unintended ways; (3) increased management, maintenance, coordination requirements, and analysis complexity. The objectives of the work described in this report are to summarize the state of the art in regards to SPS including closely related technologies in other industries, provide a structured framework for assessing SPS risk, and examine SPS as a viable planning alternative in which we consider how to identify limits of SPS deployment within a system.

These objectives are motivated by the recognition that SPS has proliferated. For example, SCE has 17 RAS on its transmission corridor and has planned to add another 57 [3]. Table 1 presents the results from three survey studies performed over the last 20 years, which indicates significant growth in the use of SPS.

Table 1: SPS survey studies

1989 Survey [4]		1996 Survey [5]		2009 Survey [6]	
Respondents	Schemes	Respondents	Schemes	Respondents	Schemes
18	93	49	111	110	958

According to Vinnakota et. al. [7], “*Due to the increased complexity of network operation in the past 30 years due to several factors such as growth in load, changes in market conditions and increased imports/exports, the network is more stressed in its operation and RAS schemes have grown in numbers.*”

Furthermore, with the heavy growth in renewable resources, especially wind farms that are being connected to the grid prior to the required upgrades, SPS or RAS has become an increasingly critical application that enables quick and economic means of interconnecting them while meeting the required RPS standards [8]. This is supported

by Figure 1 [9] where it is clear that the MW requested in Buffalo ridge area is way ahead of the available transmission capacity, necessitating heavy SPS proliferation for smooth and economical solution strategies. But, this growth in SPS has definitely increased the operational complexity in managing the system with variable wind resources, and poses an interesting challenge to the ISOs.

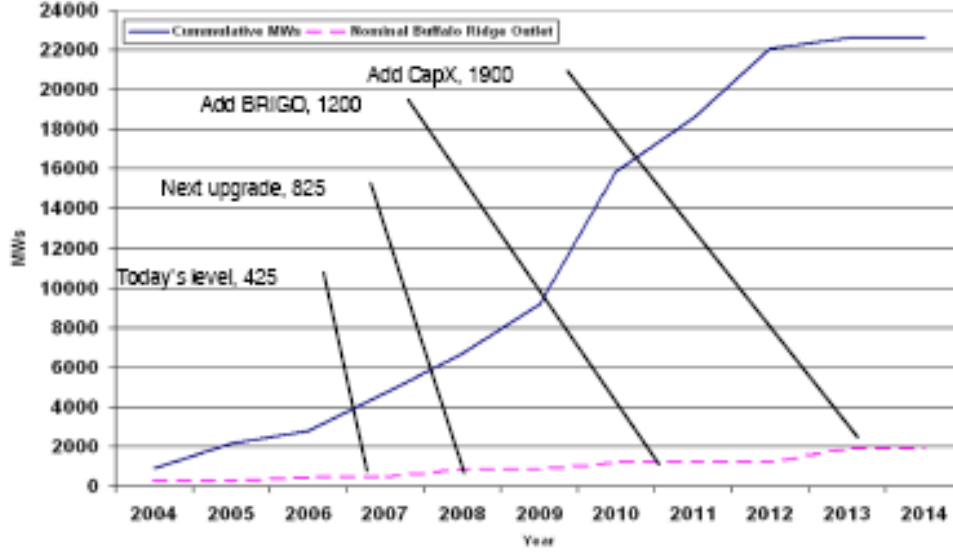


Figure 1: Buffalo ridge area: MW requested vs. transmission capacity

So this work has been motivated by the above cited reasons, with a clear cut focus on the topics such as current standards and industry practices related to SPS operation, their limitations, and future advancements. Special focus has been provided on risk assessment techniques, where the key concept on which our work is based is that SPS-risk may be examined from both a process view and a systems view. Viewing SPS in terms of a process forces consideration of the reliability of each individual component comprising the SPS. Viewing SPS in terms of the overall power system forces consideration of the SPS and the system in which it operates.

In this chapter, we summarize types of SPS and the components comprising them, we expand upon the process-view vs. systems view of SPS, and we will provide an overview of the report.

1.1 Types of SPS and typical components

SPS generally refers to controllers having some or all of the following characteristics [10]:

- SPS can be armed or disarmed depending on the system conditions.
- SPS are “normally dormant” systems; initiating events usually occur less than once a year.
- SPS usually employ discrete, feed-forward control laws.
- The control action taken is predetermined in most cases.

- Typically, some form of communication is involved in the control action.

Figure 2 shows the general structure of an SPS.

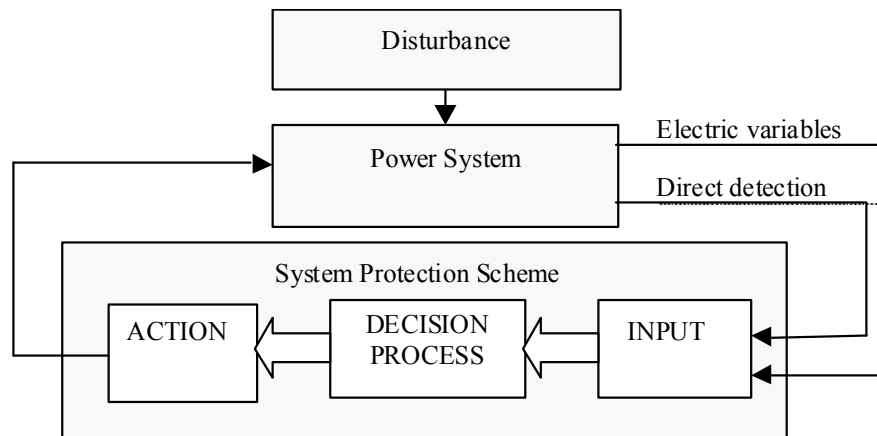


Figure 2: General structure of a system protection scheme

According to their control variables SPS can be classified as response-based or event-based. Response-based SPS are based on measured electric variables (such as voltage, frequency, etc.) and initiate their protective actions when the contingency has caused the measured value to hit the trigger level. The two most common response-based types of SPS are under-frequency load shedding and under-voltage load shedding.

Event-based SPS are designed to operate upon the recognition of a particular combination of events (such as the loss of several lines in a substation). Examples of event-based SPS are below:

- Generation rejection
- Load rejection
- System separation
- Turbine valve control
- Load and generator rejection
- Out-of-step relaying
- Discrete excitation controls
- Dynamic braking
- Generator runback
- VAR compensation
- Combination of schemes

It is useful to give some examples of equipment that are not SPS:

- Transmission devices designed to provide dynamic control of electric system quantities, which typically involve feedback control mechanisms using power electronics to achieve the desired electric system dynamic response, during normal operation conditions, are not considered as SPS but instead as transmission control devices. Examples of such equipment and devices, which are active during normal operational conditions, include: static var compensator, power system stabilizer, active or reactive power flow control or compensation.
- Transmission line auto-reclosing is aimed to improve stability or supply capability of the system, but the auto-reclosing is regarded as being a part of the line protection. Hence transmission line protection with auto-reclosing is regarded as a more advanced form of unit protection for the line than line protection without auto-reclosing. Restoration is not protection.
- Overload protection of equipment is not an SPS.

In general, SPS are distinguished from unit or *equipment protection* in that a protection system is called an SPS when the focus of the protection is on the power system supply capability rather than on specific equipment.

The composition of SPS generally includes measurement inputs, sensors, breakers, communication equipment, logic solvers, and logic solver software [11, 12, 13], as described in what follows:

- **Measurement inputs:** These may include one or more of the following [14]:
 - o Power system voltage and/or currents, synchronized to local measurements in the same substation, or they may be wide-area synchronized.
 - o Power system frequency
 - o Polarity reversal
 - o Control signals including automatic voltage regulator, power system stabilizer, governors, HVDC converters, and reactive power compensators (e.g., HVDC converters and SVC)
 - o Status – circuit breaker positions, tap changer positions, whether generator field current limiter is activated or not.
 - o Last valid state data such as, for example, telemetry data during loss of communication channel
 - o Arming levels and thresholds
- **Sensors:** These are devices that measure the power system condition. Generally, they include relays and breaker/switch status detectors. Relays may be current, voltage, power, frequency, rate of change of each of these, out-of-step, generator power output level, line loading power level, etc. Neither loss of current nor loss of power can be used alone to determine that a line is open, because they both go through zero as power flow reverses direction on the line.

Caution must be taken in determining settings required to distinguish between local faults or system problems by using rate of change of current, voltage, power, or frequency. Out-of-step relays may be used in some cases for detecting pending instabilities. However, these are usually applied only where it is acceptable to wait until the swing is “coming out of” the swing setting of the relay before taking corrective action. Studies must be performed to determine the proper setting to prevent out-of-step tripping on recoverable swings.

- **Breakers:** These are the tripping equipment.
- **Communication equipment:** This is the equipment that communicates the condition of a power system with the help of sensors to the logic solver, and the logic solver output finally to the actuating elements. A robust communication network offers low error-rate, low latency, high availability, high security and is also deterministic. The Southern California Edison (SCE) uses IEC 61850 GOOSE (Generic Object-Oriented Substation Event) communication protocol [15] to perform all the RAS functionalities, beginning from detecting the event at remote location, transmitting the alarm over WAN for about 460 miles, then processing it and deciding suitable control action, and finally implementing the control with the help of RAS IEDs at the remote location. The usage of such a digital communication technology ensures the whole process takes place within 50 milliseconds, which is very fast compared to traditional methods of transmitting control messages.
- **Logic solver:** The logic solver is that portion of an SPS that performs one or more logic functions used to execute the SPS application logic and initiate protective actions. Although it may be electrical or electronic, it is assumed in what follows that it is a programmable electronic (PE) system such as a microprocessor [16], micro-controller, programmable logic controller (PLC), or application-specific integrated circuit (ASIC). If the logic solver is purchased externally, the supplier should provide an integrated design including input module(s), output module(s), maintenance interface device(s), communication(s), and utility software. The logic solver should have a published mean time to failure (MTTF), unsafe failure mode listing, and frequency of unsafe failure mode. It should have a method (internal and/or external) to protect against covert faults (such as a “watchdog” timer). The logic solver should be designed to ensure that the process will not restart automatically when power is restored, unless it is required to do so. Detected failure of the logic solver should not result in an unsafe system condition, if the appropriate, documented, response action is undertaken.
- **Logic solver software:** In developing software necessary for the logic solver, good software development practices should be followed. For example, a software requirements specification and a software design document should be developed. These documents should specify the functionality of the design using functional blocks so that the programmer does not need to make any assumptions about the functionality of each software module. Software

architecture should be clearly identified including specification of the operating system, databases, input/output subsystems, communication subsystems, programming and diagnostic tools, and programming languages used. Coding standards should specify good programming practices (e.g., readability, traceability, checkability, and analyzability), proscribe unsafe language features, and specify procedures for source code documentation. Testing plans should be able to show that each individual software module, each software subsystem, and the entire software system performs their intended functions and does not perform any unintended functions.

- **Power supplies**
- **Monitoring devices**

1.2 Overview of report

The remainder of the report is organized as follows.

Chapter 2 presents the current industry standards for SPS design, maintenance and operation. It also presents the way various prominent industries operate SPSs, and what kind of technology they employ to achieve coordination among various SPSs. Finally it presents some of the latest advancements in the way SPS are being used, with primary focus on centralized SPS and its relationship with Synchronizers.

Chapter 3 sheds focus on the standards and practices of three industries, namely process control, nuclear and electric power industries. The aim is to extract relevant information about processes and methods from these matured industries which may be applicable for reliability studies concerning SPSs.

Chapter 4 and chapter 5 present risk assessment of SPS from two different views, namely ‘process view’ and ‘system view’. The ‘process view’ framework will view SPS in terms of a **process** which considers actuating signals, equipments, logic used to operate on actuating signals, communication channels, and final action. The ‘system view’ framework will view SPS in terms of its position in and impact on the power **system** in which it exists. System related failure modes are typically intended (by design) but undesirable, reflecting faulty logic. Figure 3 presents an overview of these two frameworks, and the kind of failure modes within each.

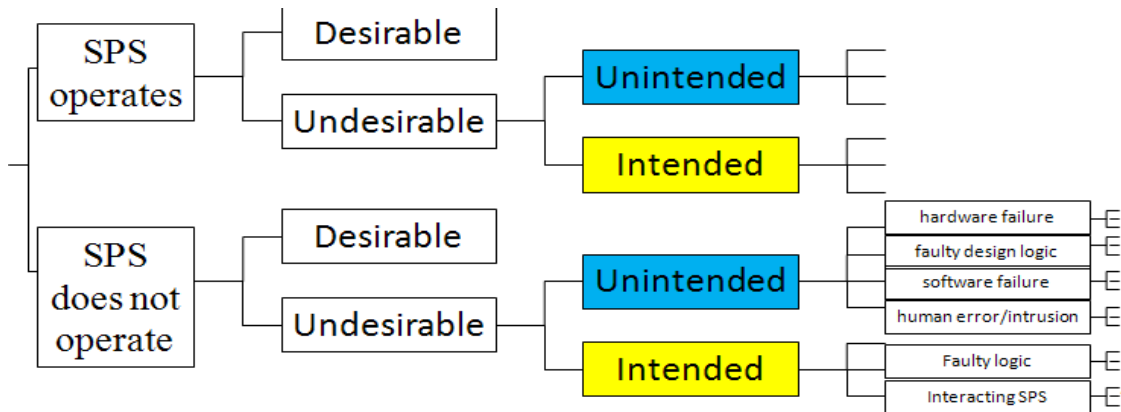


Figure 3: Process view and system view failure modes

Chapter 6 presents two planning studies, namely wind generation expansion study and transmission expansion study. It proposes ways to incorporate SPS in such studies and evaluate the reliability indices of such SPS-aided planning options.

Chapter 7 presents the conclusions.

2 Standards, practices and advancements on SPS

This chapter summarizes current industry standards and practices regarding SPS. Section 2.1 focuses on standards, while Section 2.2 focuses on existing industry practices related to SPS design, documentation, and technologies used for arming and coordinating various SPS operations. Section 2.3 sheds light on some recent advancement in SPS.

2.1 Current industry standards

The North American Electric Reliability Corporation (NERC) maintains the following standards related to SPS, posted at the NERC website [17] under Standards - Protection and Control:

- *PRC-004-WECC-1 Protection System and Remedial Action Scheme Misoperation (WECC)*: This is a Regional Reliability Standard to ensure all transmission and generation Protection System and Remedial Action Scheme (RAS) Misoperations on Transmission Paths and RAS defined in section 4 are analyzed and/or mitigated.
- *PRC-012-0 Special Protection System Review Procedure*: To ensure that all Special Protection Systems (SPS) are properly designed, meet performance requirements, and are coordinated with other protection systems. To ensure that maintenance and testing programs are developed and misoperations are analyzed and corrected.
- *PRC-013-0 Special Protection System Database*: To ensure that all Special Protection Systems (SPSs) are properly designed, meet performance requirements, and are coordinated with other protection systems.
- *PRC-014-0 Special Protection System Assessment*: To ensure that all Special Protection Systems (SPS) are properly designed, meet performance requirements, and are coordinated with other protection systems. To ensure that maintenance and testing programs are developed and misoperations are analyzed and corrected.
- *PRC-015-0 Special Protection System Data and Documentation, PRC-016-0 Special Protection System Misoperations, and PRC-017-0 Special Protection System Maintenance and Testing*: To ensure that all Special Protection Systems (SPS) are properly designed, meet performance requirements, and are coordinated with other protection systems. To ensure that maintenance and testing programs are developed and misoperations are analyzed and corrected.

2.1.1 NERC standards and its relationship to other international standards

This section gives more in-depth summary of current industry standards for special protection schemes and how the standards can be improved by learning from more established international standards such as the *International Society of Automation* (ISA) and the *International Electro-technical Commission* (IEC).

2.1.1.1 PRC-004-WECC-1

According to PRC-004-WECC-1, mis-operations can be classified into two [18]:

1. **Security-based misoperation:** “*Security-based misoperation is a misoperation caused by the incorrect operation of a protection system or RAS. Security is a component of reliability and is the measure of a device’s certainty not to operate falsely.*”
2. **Dependability-based misoperation:** “*Dependability-based misoperation is the absence of a protection system or RAS operation when intended. Dependability is a component of reliability and is the measure of a device’s certainty to operate when required.*”

The ISA and IEC define **Safety Integrity Level (SIL)**. “**Safety Integrity Level (SIL)** is a relative level of risk-reduction provided by a safety function, or it specifies a target level of risk reduction.” SIL may also be enforced for special protection schemes to enhance reliability and availability based on **Probability of Failure on Demand (PFD)**. Table 2 describes SIL from IEC’s and ISA’s view-point [19].

Table 2: IEC and ISA demand mode SIL in terms of availability

IEC SIL	ISA SIL	Availability required	PFD	1/PFD
4	N/A	>99.99%	1E-005 to 1E-004	100,000 to 10,000
3	3	99.90 – 99.99%	1E-004 to 1E-003	10,000 to 1,000
2	2	99.00 - 99.90%	1E-003 to 1E-002	1,000 to 100
1	1	90.00 - 99.00%	1E-002 to 1E-001	100 to 10

2.1.1.2 PRC-012-0, PRC-013-0, PRC-014-0, and PRC-015-0

PRC-012-0, PRC-013-0, PRC-014-0, and PRC-015-0 summarize the review of SPS design, co-ordination with other protection schemes, establishing maintenance programs, and proper and efficient documentations.

The IEC uses the safety life cycle approach as the framework for structuring safety instrumentation system (SIS) requirements [20]. SIS performs specific functions to achieve or maintain a safe state of the process, when unacceptable or dangerous process conditions are detected. They are composed of similar elements as SPS, which includes sensors, logic solvers, actuators and support systems. Therefore a similar process can be developed for SPS as shown in Figure 4.

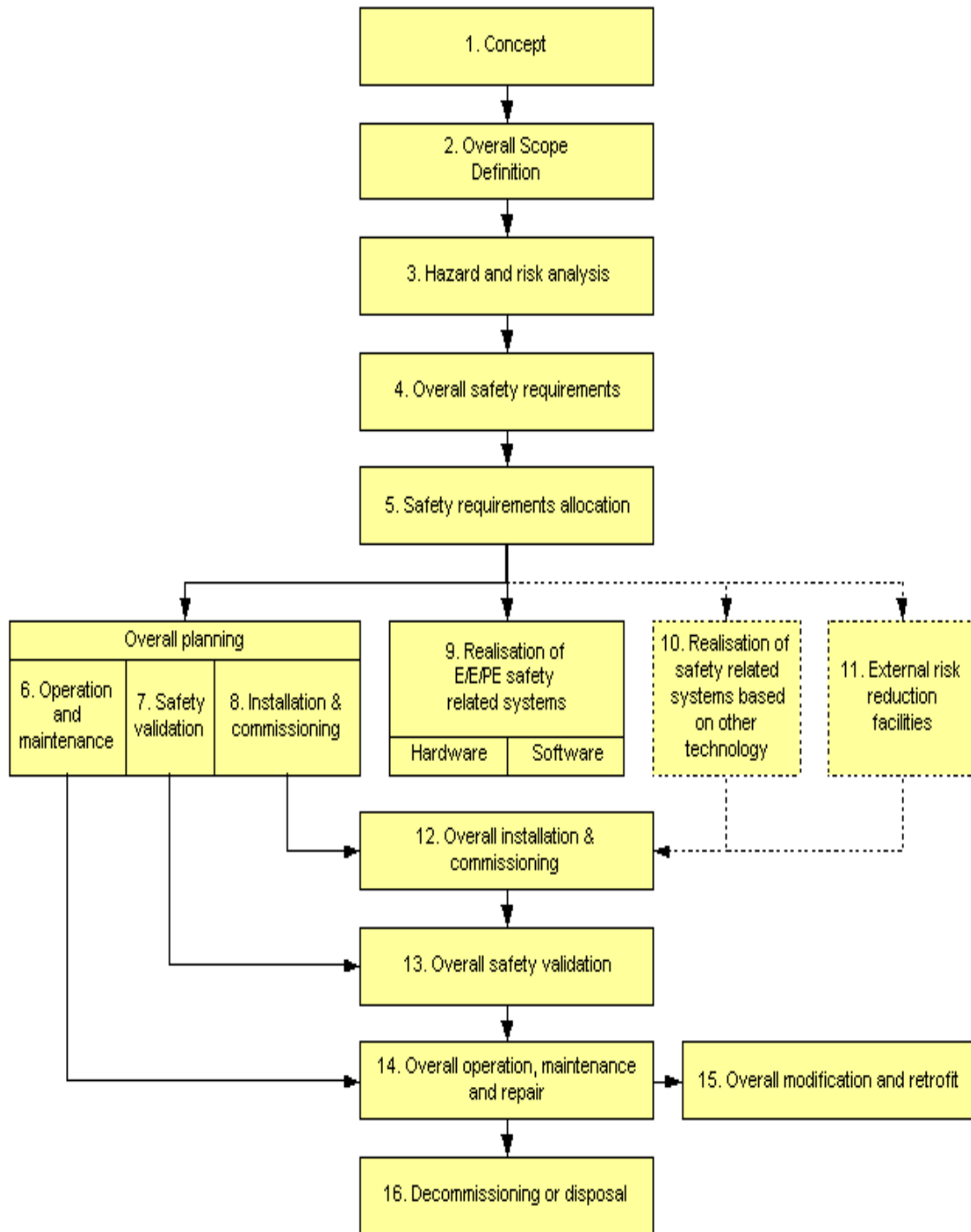


Figure 4: IEC 61508 life-cycle model

2.1.1.3 Penalty Matrix

NERC's sanction guidelines provide a matrix comprising violation risk factors and violation severity levels, the intersection of which establishes "*base penalty amounts*". Table 3 presents the penalty matrix (per day rates) approved by FERC [21].

Table 3: FERC approved penalty matrix

Violation Risk Factor	Violation Security level							
	Lower		Moderate		High		Severe	
	Range Limits		Range Limits		Range Limits		Range Limits	
	Low	High	Low	High	Low	High	Low	High
Lower	\$1,000	\$3,000	\$2,000	\$7,500	\$3,000	\$15,000	\$5,000	\$25,000
Medium	\$2,000	\$30,000	\$4,000	\$100,000	\$6,000	\$200,000	\$10,000	\$335,000
High	\$4,000	\$125,000	\$4,000	\$300,000	\$12,000	\$625,000	\$20,000	\$1,000,000

The levels of risk factors in Table 3 are defined as:

- **Lower** - administrative in nature and, which if violated, is not expected to affect the state of the bulk power system or the ability to monitor, control, or restore the system.
- **Medium** - a requirement that, if violated, could directly affect the electrical state or the capability of the bulk power system or the ability to effectively monitor, control, or restore the system. But it does not result in instability, separation, or cascading failures.
- **High** - a requirement that, if violated, could directly cause or contribute to bulk power system instability, separation, cascading failures, or hinder restoration efforts.

2.2 Existing industry practices

RAS are fast acting automatic control devices, that utilizes protective relays and fast telecommunication networks, to ensure acceptable (reliable and safe) power system performance following critical outages on a power grid. Bonneville Power Administration (BPA) uses SPS to maintain stability, reduce line overloads, maximize transfer capabilities, and provide voltage support [22]. ERCOT employs SPS to maintain system security and reliability in accordance with ERCOT and NERC Reliability Standards, while facilitating the market [23]. BC Hydro heavily employs SPS and RAS to maintain system integrity. It also shares some of these schemes with the interconnected neighbors [24]. Southern California Edison (SCE) mitigates transmission overload problems arising due to contingencies using RAS [25]. According to Alberta Electric System Operator (AESO) [26], “RAS is used primarily on a temporary basis when new market participants are being added to the system in advance of the transmission system’s capability to manage such loads or supplies”. Likewise, many utilities are using SPS especially in the event of increasing penetration of intermittent renewable resources, and plenty of advancements are also being made in such defense system designs to the extent that utilities have started designing PMU based RAS [27].

2.2.1 Design of SPS

Design of SPS is very important due to the fact that SPS help keep the integrity of a power system during extreme disturbance. Therefore SPS must be designed to be highly reliable. One of the most important devices in SPS is the communication system

which enables data exchange between monitoring and controlling devices. Arming is another important functionality in SPS design, wherein arming is usually automatically or manually enabled. Redundancy is a useful technique used in SPS to help improve reliability of SPS. Typically, SPS/RASs are comprised of three parts: monitoring, event detection and mitigation. The quality of SPS is measured in terms of speed and accuracy of operation, and redundancy in design.

The SPS design process comprises of the following five steps, namely [28]:

1. System study

System studies identify limitations under various contingencies. The limitations could be thermal, voltage, or angular instability related system limits. Some of the important aspects of system studies include understanding the requirements and purpose of the application; identifying limits such as overload conditions, under voltage, under frequency and so on; studying SPS requirements based on NERC reliability and regional standards; evaluating many alternate solutions and so on.

2. Solution development

The solution based on system studies must be analyzed and specific recommendations have to be made as a next step. The recommendations are about the stability limits, conditions when SPS is to be armed, the amount of load to be shed when needed, bus voltage limits, various other limits and so on.

3. Design and implementation

At the stage of implementation, typically many practical questions are to be answered such as:

- What technology is needed to meet the functional requirements of the SPS in an economic fashion?
- What kind of communication equipment is needed to meet the SPS standards?
- What is the most reliable way of building redundancy such as voting schemes for the logic solver?

Reference [28] gives a detailed list of such practical issues to be addressed.

4. Commissioning & periodic testing

A comprehensive testing method must be in place for successfully implementing the solution. The errors detected must be rectified and the system specifications must be met. The test plan must include:

- Lab testing: validation in a controlled environment
- Field testing: test against undesirable system conditions likely in reality

The routine of tests are to be performed on a periodic basis and gradually understand the working of SPS better in various conditions.

5. Training & documentation

Failure of SPS due to human intervention, faulty logic design and incorrect settings has been reported to be about 20%, 12% and 10% respectively in past surveys [5]. So proper training of operating and maintenance staff is necessary to ensure reliable operation of SPS and its continuous improvement. A solid documentation about SPS, its functionalities, past experiences, case studies will definitely help in efficiently training the upcoming staff.

2.2.2 Documentation for reliability assessments

Electric system planners are facing unprecedented challenges in managing the risk of using SPS in maximizing the usage of existing and planned transmission grid. The following documenting procedure has been developed by Remedial Action Scheme Reliability Subcommittee of WECC in order to assess the reliability of an SPS [29].

1. RAS scheme purpose and overview- The following information is included:

- a. Name of the RAS
- b. Purpose
- c. Desired in-service date
- d. Ownership
- e. Person responsible for the operation and maintenance
- f. SPS functionality
- g. Single line drawings showing all sites involved, bus arrangement and other protection systems such as breakers
- h. Impact on the WECC power grid

2. RAS design

- a. Design philosophy
- b. Design criteria, including failure of which element or combination of elements causes RAS failure mode
- c. RAS Logic
- d. RAS Logic Hardware
- e. Redundancy
- f. Arming method i.e. manual, automatic, or via SCADA
- g. Define all inputs, including protective relay inputs such as angle, power, current, voltage, frequency, rate of change of frequency power, current and voltage.
- h. List devices used to monitor inputs such as circuit breakers
- i. Coordination with protection and control systems

- j. Telecommunications with the diagram of telecom path, communications system performance, supporting reliability information such as equipment age, history, maintenance, communication architecture, bandwidth of communication system and so on.
- k. Transfer Trip Equipment
- l. Remedial actions initiated

3. Monitoring

- a. RAS monitoring equipment and time resolution
- b. Station alarms
- c. SCADA monitoring
- d. Sequence of Events Recorders
- e. Facilities monitored such as self diagnostics, telecommunications, transfer trip equipment, RAS actions and so on.

4. RAS operating procedures - Procedure for abnormal system conditions like,

- a. Incorrect operation (failure to operate or false operation)
- b. Unavailability of redundant RAS system
- c. Unscheduled or unplanned or uncoordinated loss of RAS
- d. Partial or total loss of input for arming decisions

5. Commissioning, maintenance and testing

- a. SPS commissioning
- b. Overall functional test procedure
- c. Preventative maintenance
- d. Maintenance and test intervals
- e. Maintenance and testing procedures

6. Performance and operational history- Based on system requirements provide assurances on performance and operating time of the SPS. The following information is provided:

- a. How long has the RAS been in operation?
- b. Failure to operate?
- c. Incorrect operation?
- d. Slow operation
- e. Unnecessary operation?

7. **RAS catalog information-** Summary of the salient features of the newly proposed or modified SPS
8. **Revision History-** Information about initial release and approval of the SPS by regulatory bodies

2.2.3 SPS implementation and coordination in industries

SPS is designed to operate in stressed conditions. So properly arming SPS when needed is very important, as failure in such a case could be very catastrophic. Traditionally, RASs are localized, operated by fast algorithms installed at substations or control centers. But with the increasing population of SPS, there have been many disadvantages experienced by localized RASs especially in terms of maintenance and coordination. Therefore, Centralized-RAS, a more technologically driven defense scheme, has been gaining acceptance since it has lot of advantages. This section briefs some of the utilities' practices regarding SPS implementation, arming and coordination under various conditions.

MISO

Midwest independent system operator (MISO) has about 15 RAS. MISO sends the status of RAS to the control room personnel through ICCP (Inter Control Center Protocol) points, who take the decision from real-time information displayed [30]. The RTCA (Real-time Contingency Analysis) tool developed by MISO includes most of the SPS, except a few very complicated ones. The RTCA tool [31] is either scheduled to run at uniform intervals (say, every 5 minutes), or triggered based on a contingency event or by an operator.

CAISO

In CAISO, RAS schemes are written using Data Base Language (DBL), which is prevalently used in EMS related functionalities. The contingency analysis (CA) module calls the RAS DBL code to initiate the simulation of RAS control actions during contingency analysis [32]. Also, CAISO has developed a RAS maintenance program, as shown in Figure 5. The more RAS in an electric grid, maintenance scheduling of RAS and other electric power equipments becomes more and more difficult. Also the electric grid experiences changes all the time, and RAS have to be reviewed whenever there is a change in this system. So a proper documentation must be done in-order to keep track of all the changes in the system.

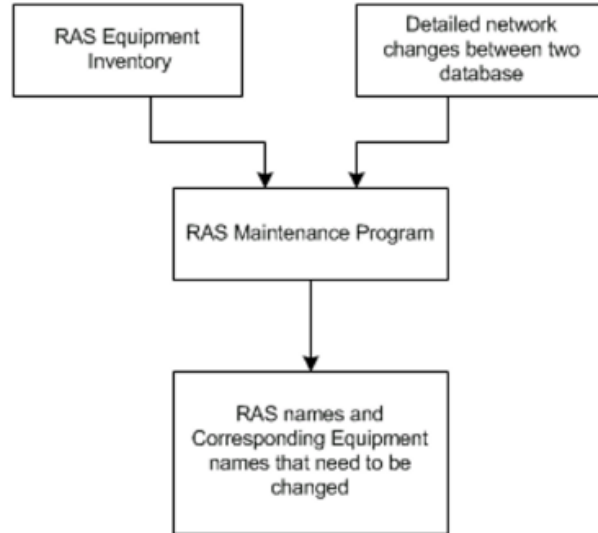


Figure 5: CAISO RAS maintenance program

BC Hydro

In BC Hydro, RAS arming is done centrally at the control center [33, 34]. This has proved to increase system limits as well as reliability. The arming of RAS is automatically performed by TSA (transient stability assessment function) as shown in Figure 6, which is within EMS. The arming is done either immediately after any network configuration change or at systematic intervals of 4 minutes. At regular intervals the system limits are updated automatically. In Figure 7, the patching matrix of each RAS acts as the interface between inputs (multiple contingencies) and the outputs, where outputs are suitable control actions such as generator shedding, line tripping, shunt switching etc. to improve transient, voltage or thermal stability.

GENERATION SHEDDING DISPLAY (1) REAL TIME														
CONTINGENCY	TRANSFER TOTAL	SHED TOTAL	SET	GMS										RMS RMS
				1	2	3	4	5	6	7	8	9	10	
SL1	+ 700.0	300.0	●	■	■	■	■	■	■	■	■	■	■	■
SL2	+ 700.0	300.0	●	■	■	■	■	■	■	■	■	■	■	■
SL3_7	+ 597.0	300.0	●	■	■	■	■	■	■	■	■	■	■	■
SL4	+ 236.6	0.0	●	■	■	■	■	■	■	■	■	■	■	■
SL11	+ 841.0	300.0	●	■	■	■	■	■	■	■	■	■	■	■
SL12	+ 0.0	0.0	●	■	■	■	■	■	■	■	■	■	■	■
SL1_2	+ 1400.0	537.3	●	■	■	■	■	■	■	■	■	■	■	■
SL1_3	+ 1361.3	537.3	●	■	■	■	■	■	■	■	■	■	■	■
SL1_7	+ 1297.0	300.0	●	■	■	■	■	■	■	■	■	■	■	■
SL2_3	+ 1361.3	537.3	●	■	■	■	■	■	■	■	■	■	■	■
SL2_7	+ 1297.0	300.0	●	■	■	■	■	■	■	■	■	■	■	■
SL13_1PH		0.0	●	■	■	■	■	■	■	■	■	■	■	■
SL13	+ 850.0	300.0	●	■	■	■	■	■	■	■	■	■	■	■
SL11_SL12	TRANSFER	300.0	●	■	■	■	■	■	■	■	■	■	■	■
SL11_SL13	+ 1685.6	1582.6	●	■	■	■	■	■	■	■	■	■	■	■
SL12_SL13	SL11/SL2/13	300.0	●	■	■	■	■	■	■	■	■	■	■	■

Figure 6: TSA display showing real-time generation shedding arming pattern

Figure 8 shows the way BC Hydro integrates EMS/SCADA and protective relays in order to effectively handle contingencies [35].

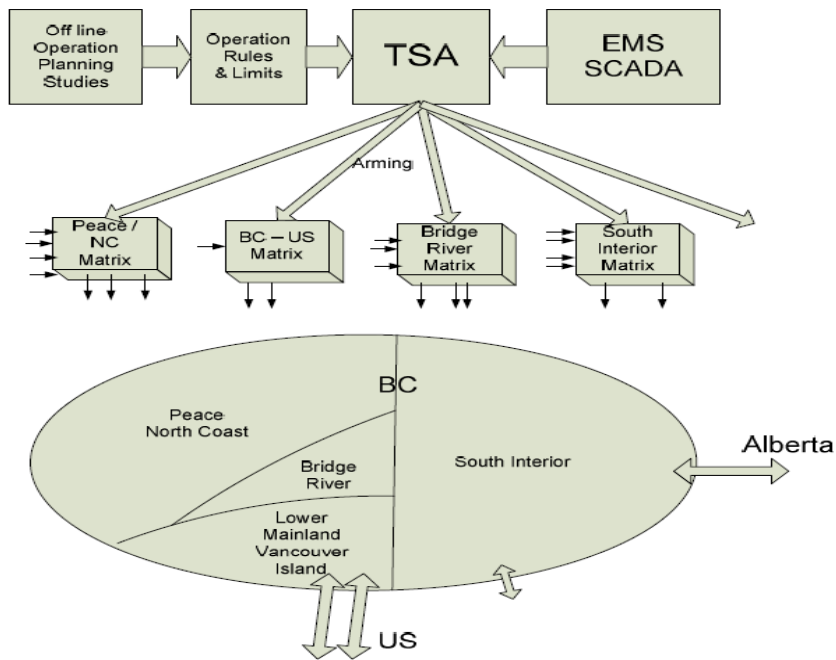


Figure 7: BC Hydro central arming RAS system

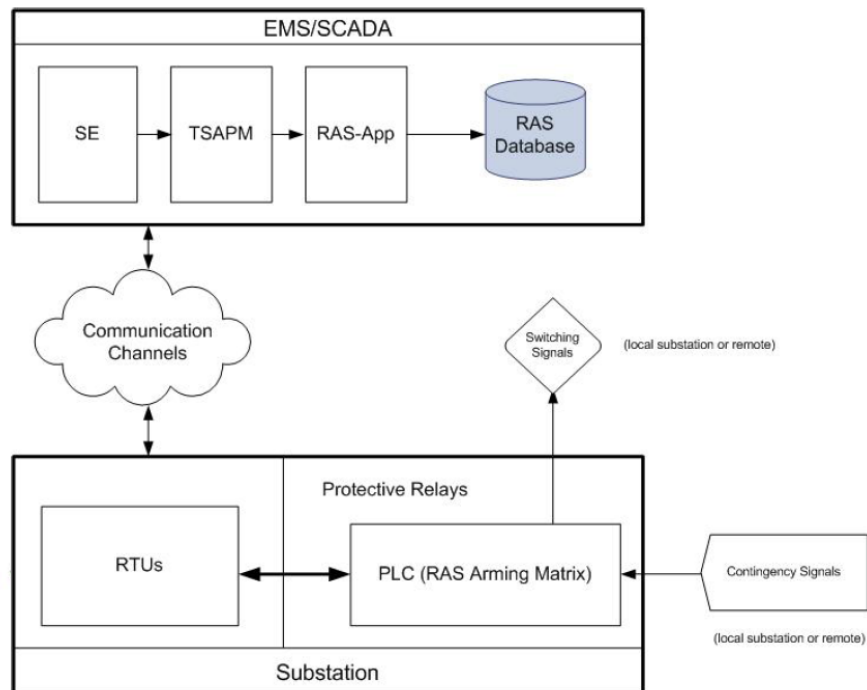


Figure 8: BC Hydro - EMS/SCADA/protective relay integration

RTU: Remote terminal unit; SE: State estimation; TSAPM: Transient stability problem

ERCOT

“To avoid unnecessary SPS operation, the SPS owner may provide a real-time status indication to the owner of any generation resource controlled by the SPS to show when the flow on one or more of the SPS monitored facilities exceeds 90% of the flow necessary to arm the SPS. The cost necessary to provide such status indication shall be allocated as agreed by the SPS owner and the generator owner [36]”

BPA

BPA (Bonneville Power Administration) uses programmable logic controllers for its SPS design. Most RAS in BPA are on their 500KV lines. The way RAS is operated in BPA is that when there is a line loss detection, a transfer trip signal is sent to control centers, from where control signals are sent to power plants and substations [37]. These RAS schemes are designed to be highly redundant using two out of three voting schemes and also information is sent to two control rooms to improve redundancy. In order to avoid frequency problems, there is a limit on generation tripping of 2700MW [38]. BPA also co-ordinates with northern and central California, so that necessary remedial actions can be taken in-order to keep up system integrity in Pacific NW and California. Figure 9 presents the RAS controllers for the coordinated operation of California and BPA RAS [39].

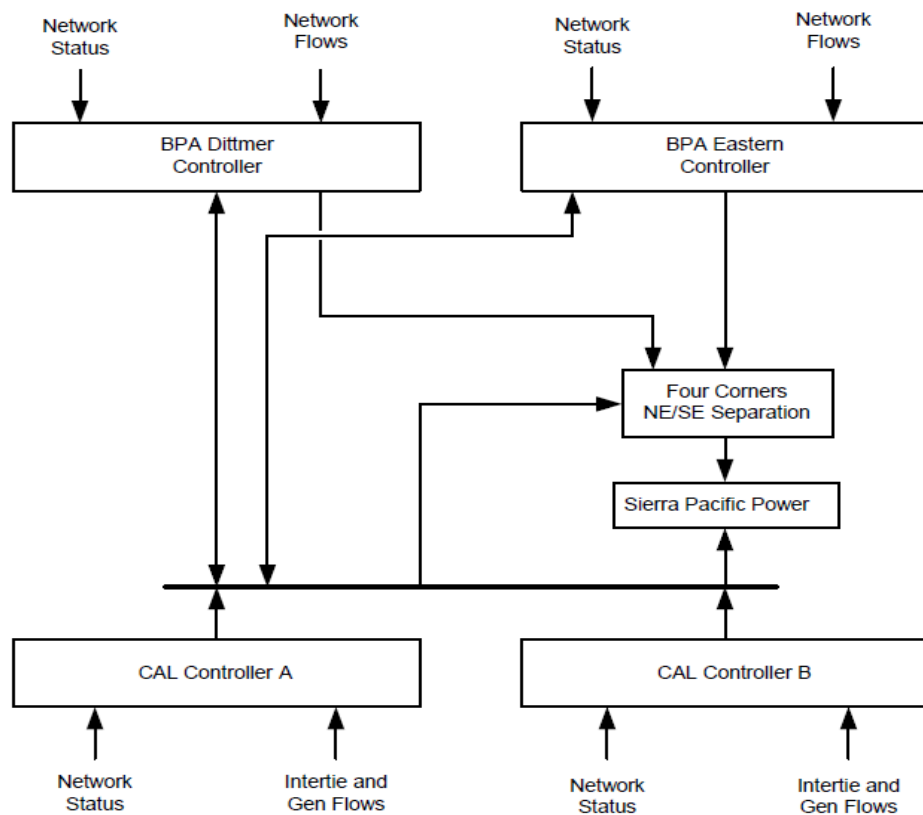


Figure 9: California and BPA remedial action schemes controllers

SCE

Southern California Edison (SCE) faces rapid growth of RAS in its footprint. This is due to aggressive renewable generation expansion and load growth [8]. Consequently, having many isolated RAS leads to coordination problems, maintenance issues with engineers having to traveling long distances for each RAS, and so on. Figure 10 from the work [40] done by P. Arons gives a systematic outline of all the associated problems due to proliferating RAS. So SCE is trying to introduce centralized remedial action scheme (C-RAS), motivated by the fact that having many localized RAS increases operational complexity.

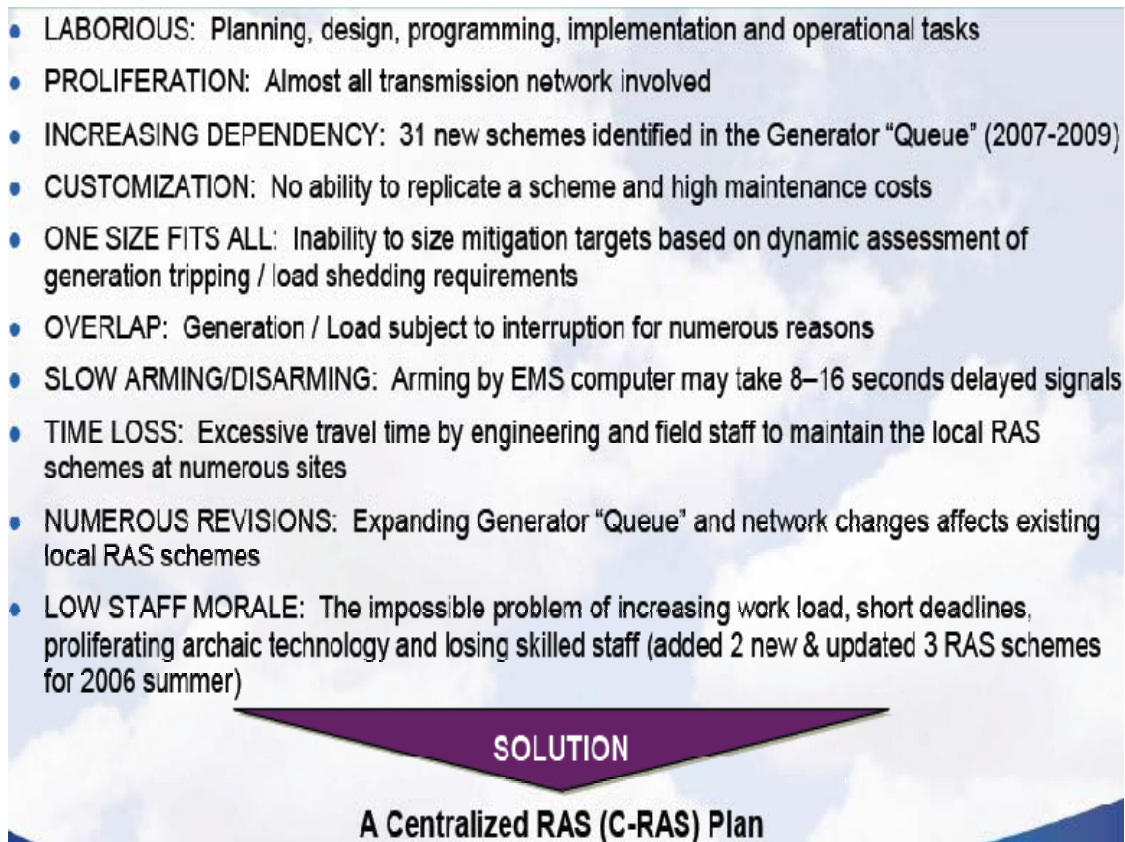


Figure 10: Motivation for C-RAS

Some of the advantages and features of C-RAS developed by SCE are:

1. It will enhance transmission line capacity ratings
2. The various RAS will be to easier to maintain during different seasons and different system operating conditions.
3. It will increase wide-area voltage stability
4. It possesses an additional study tool that can be used for transmission and interconnection planning.

Figure 11 shows the system problems that can be addressed effectively and economically using RAS, wherein RAS implements respective remedial action to alleviate a stressed system which otherwise faces unstable conditions. So with the advent of a Centralized-RAS approach, all the wide-area functionalities such as monitoring, protection, and control could be fit in a single framework.

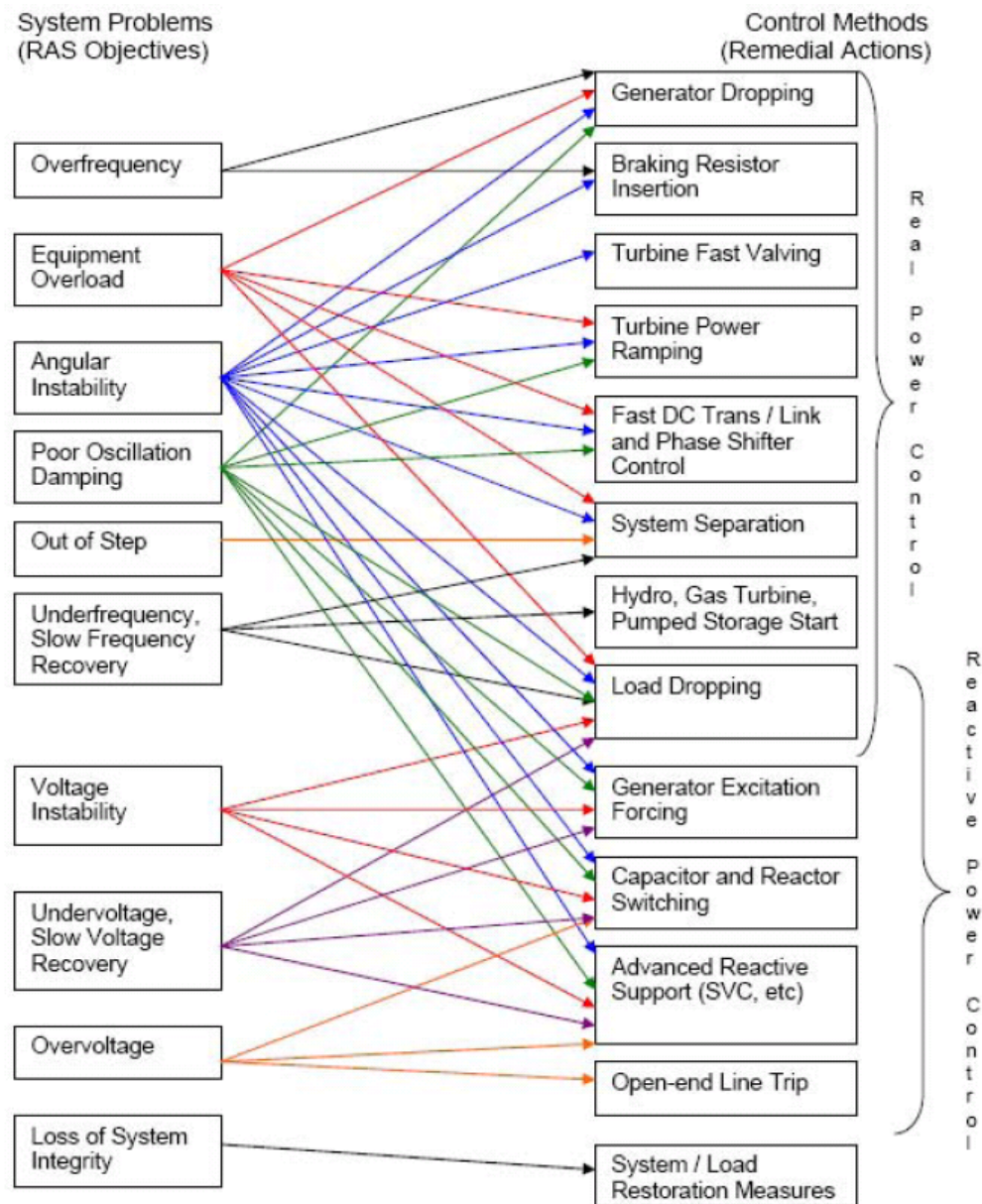


Figure 11: RAS range of functionalities

2.3 Advancements in SPS

2.3.1 Relationship between SPS and synchrophasor technology

Synchrophasor technology provides system status at a much faster rate, compared to SCADA and other traditional state estimators. The publication [41] by Schweitzer Engineering Laboratories (SEL) proposes a synchrophasor based vector processor (SVP) shown in Figure 12, which collects synchronous phasor measurements from the system, processes them and detects any unstable conditions within local as well as large areas.



Figure 12: Synchrophasor based vector processor from SEL

This functionality of SVP when combined with RAS, provides a high improved defense mechanism to enhance power system security. Table 4 [41] presents the advantages of SVP based RAS compared to traditional RAS in terms of increased speed, reduced equipments, and so on.

Table 4: Traditional vs. synchrophasor based RAS scheme

	Traditional RAS	SVP RAS
Logic Processors	7	0
I/O Modules	66	0
SVPs	0	6
Ethernet Switches	0	6
Wiring	730 wires/cables	30 cables
Power	470 W	210 W
Operate Time	5 Cycles	4.25 Cycles
Equipment Price	\$144,000	\$102,000
Installation and Check-out Price	\$21,000	\$8,000
TOTAL	\$165,000	\$110,000

Southern California Edison (SCE) proposed Smart RAS [42], a Centralized RAS technology that uses real power measurements of tie-line between two areas from PMU to actuate suitable remedial action that prevents system out-of-step condition. Figure 13 shows the smart RAS controller with its input and outputs.

The work in [27] presents a PMU based SPS developed and operated by Taipower systems against transient instabilities caused by EHV line contingencies.

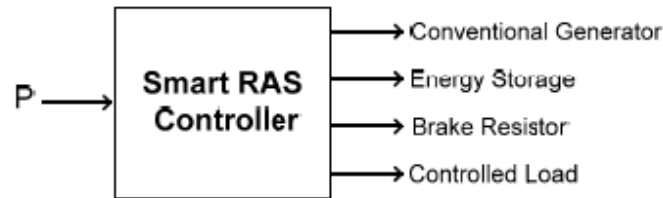


Figure 13: Smart RAS from SCE

2.3.2 Role of SPS in wide area monitoring, protection and control

After the advent of Phasor Measurement Units (PMUs), in 1988 Bonneville Power Administration (BPA) first used it in WECC. Then on inspired by its many advantages to record information useful for crucial system analysis, which were not earlier possible using SCADA or IED data, many utilities have started deploying PMUs. Now in WECC, various companies such as BPA, SCE, WAPA and PG&E take part in data exchange program and benefit each other in having better reliability status of critical transmission corridors [43]. Figure 14 shows a typical data exchange using PMU and PDCs, which provide the ability to monitor system security and limits over a wide-area, and take necessary control actions over a wide-area of the power network.

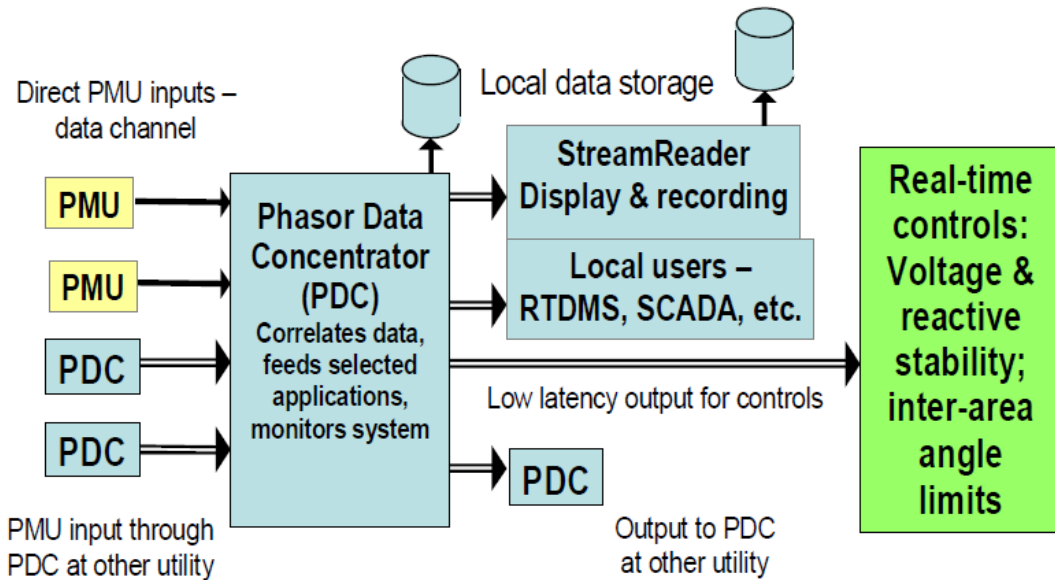


Figure 14: Typical PMU

Wide-area monitoring system (WAMS) based on PMUs is real time monitoring application of electric power grid performing various tasks such as monitoring phase angle, line loading, voltage stability, power oscillations, frequency stability, and event archiving. WAMS has gained a lot of importance in the electric power grid applications since there has been incessant load growth, aggressive renewable generation expansion and, also frequent blackout threat. WAMS are also used in implementing Wide-area protection schemes (WAPS), which are used to stop wide-spread blackout. According to [39], “*WAPS (Wide-area protection systems) schemes are designed to detect abnormal system conditions and take pre-planned, corrective actions intended to minimize the risk of wide-area disruptions and to increase system power transfer capability*”. Figure 15 presents a basic design of WAMS with protection module [44].

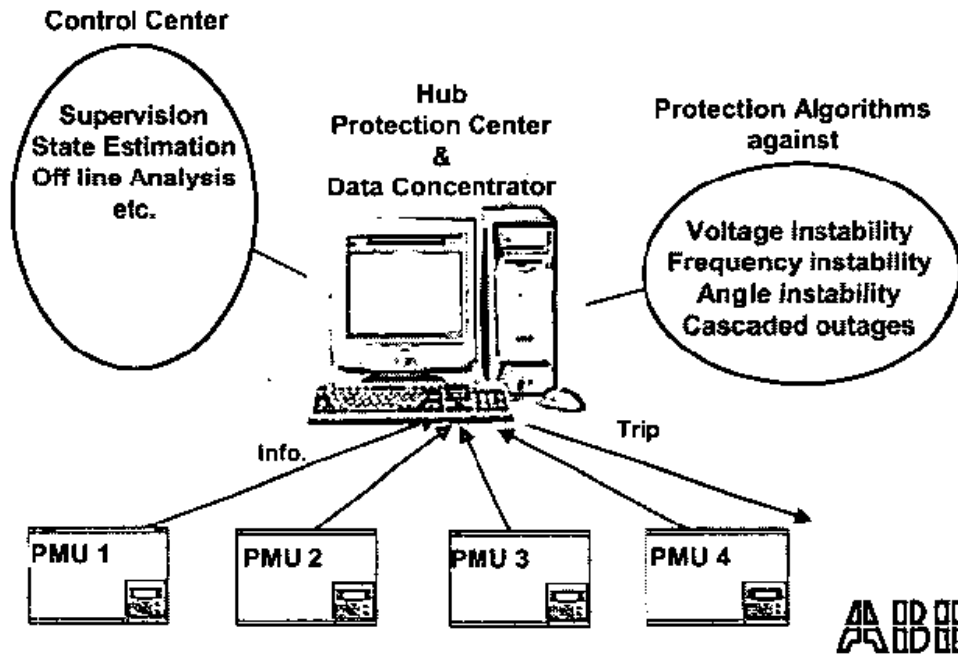


Figure 15: Wide-area monitoring and protection design

Figure 16 shows a response-based Wide-Area Control System (WACS) developed by BPA using PMUs. WACS controller acts a centralized master control that receives system data from PMUs and PDCs, processes them and issues relevant control signals to WAPS controller.

Figure 17 shows the WACS implementation using RAS, where control signal from the centralized master controller is sent to centralized RAS controller that performs the WAPS functionalities. This wide-area system monitoring and control using PMU and RAS respectively proves to be very efficient and faster, and helps in averting any unnecessary RAS actions by proper coordination.

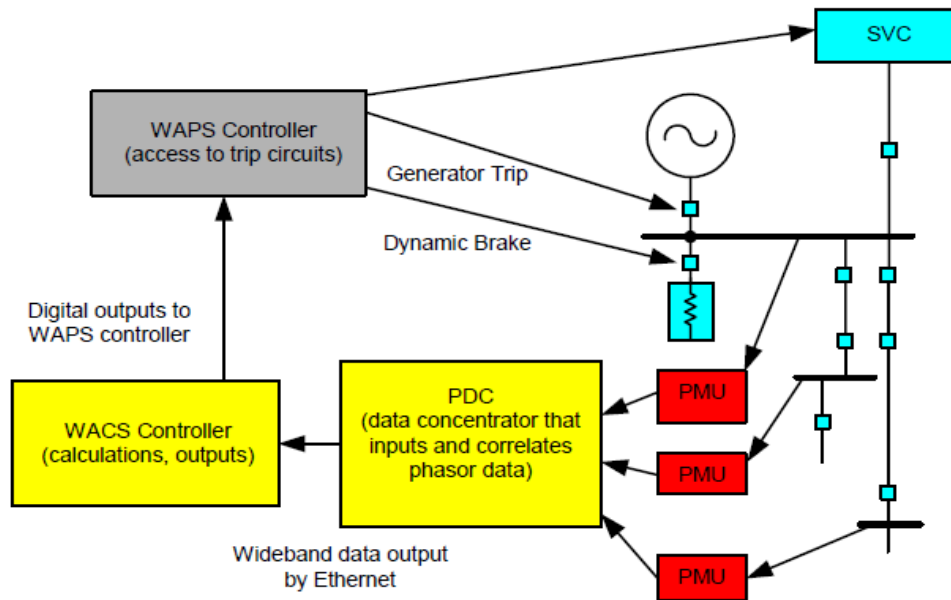


Figure 16: Wide area control system

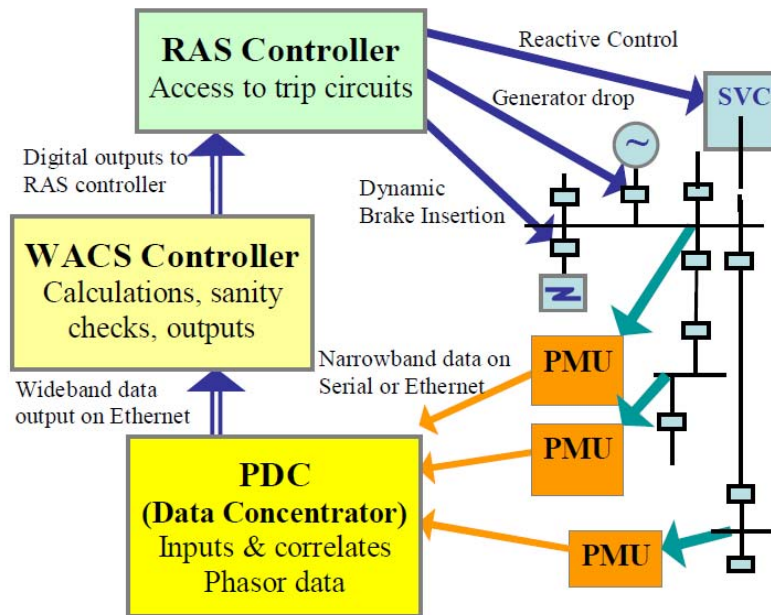


Figure 17: Wide area control system using RAS

3 Relationship to other industries & applications

It is likely that individual companies have documented procedures for performing SPS design, installation, and start-up. However, significant effort fails to identify documentation of these procedures in the literature or in publicly available documentation, available on the internet and elsewhere, with just a few exceptions, including [11, 12, 13, 45, 46]. Yet, most of these are quite general and tend more towards “criteria” rather than “procedures”. Indeed, the IEEE/CIGRE survey conducted by Anderson and Le Reverend [5] found that most often utility criteria for SPS contained at most general requirements for equipment redundancy.

It is found, however, that the other industries have confronted quite similar problems. One of them in particular is the process control industry, summarized in Section 3.1, and the other is the nuclear power industry, summarized in Section 3.2. In addition, we find that, within the electric power industry, the approach to developing operating rules is very similar to the approach for developing SPS logic, as described in Section 3.3.

3.1 Process control industry

This industry is comprised of companies in the petroleum, pharmaceutical, power, chemical, pulp and paper, and textile, and supporting areas. Often, the failure consequence of the various processes implemented can be very high, and so a great deal of attention is paid to standardizing procedures for designing, installing, and maintaining safety instrumented systems (SIS). These are systems that are comprised of sensors, relays, breakers, communication equipment, and logic solvers that take the process to a safe state when predetermined conditions are violated [47]. The SIS equipment and function are quite similar to the equipment and function of SPS in power systems. The process control industry has done an extensive amount of work investigating, modeling, and standardizing of SIS equipment and this work is well documented. The documents in use are: ISA S84.01, ISA dTR84.02, IEC draft 61508 and S84/IEC 61511.

The Instrument Society of America (ISA) is the international society for measurement and control. Members are from many industries with a large number from the petroleum, chemical, and supporting industries. The International Electro technical Commission (IEC) is the world organization that prepares and publishes international standards for all electrical, electronic and related technologies. The membership consists of more than 50 participating countries, including all the world's major trading nations and a growing number of industrializing countries.

3.1.1 ISA S84.01

ISA S84.01 [48] is a standard titled “Application of Safety Instrumented Systems for the Process Industries” that was approved on February, 1996 after many years of development. This standard addresses the application of Safety Instrumented Systems (SIS) for the process industries. ISA S84.01 addresses integrity levels for electrical, electronic, and programmable electronic systems. These systems include electromechanical relays, solid state logic, programmable electronic systems, motor-

driven timers, solid state relays and timers, hard-wired logic, and combinations of the above. A key concept of this document is the definition and use of Safety Integrity Levels (SIL).

The document provides standard criteria for function and integrity specifications, conceptual design, detailed design, installation, commissioning, and prestart-up tests, operation and maintenance procedures, periodic functional testing, management of changes, and decommissioning of such systems. In particular, detailed design requirements are specified for logic solvers and application logic, sensors and motor starters, operator, communication, and maintenance interfaces, power sources, and design of periodic testing capability. It also provides appendices which give SIL assessment methods, design considerations, references, and an illustrative example.

3.1.2 ISA dTR84.02

ISA-dTR84.02 [49] is a supporting document for ISA S84.01 that provides evaluation approaches for safety-instrumented system reliability. The focus of this document is on modeling and calculation, and SIL is the basic performance measure. It describes modeling of system failure elements, failure mode and effect analysis, modeling of electrical, electronic, and programmable electronic systems, safety system selection, common cause failure models, Markov model development and quantification, uncertainty analysis, statistical sensitivity analysis, fault simulation test procedures, and reliability analysis software. The objectives of ISA-dTR84.02 are to:

- 1) provide guidance on SIL analysis
- 2) present methods to implement SISs so that they achieve a specified SIL
- 3) identify failure rates and failure modes of SIS
- 4) address diagnostic, diagnostic coverage, covert faults, test intervals, common cause, systematic failures, and redundancy of SIS
- 5) provide tools for verification of SIL and pre-startup safety review of SIS
- 6) present methods for determining the functional test interval

3.1.3 IEC work

The International Electro technical Commission (IEC) has prepared two documents, IEC 61508 [50] and IEC-61511 [51], that define requirements common to all industries (not just for process control) for electrical, electronic, and programmable electronic systems. It is IEC's intent that, ultimately, there would be additional standards developed to reflect specific requirements for the various industry sectors, including nuclear, pharmaceutical, and aeronautical. Although the power industry is never mentioned explicitly, it seems reasonable to include it as another “sector”. It is therefore likely that anything the power industry wanted to do in the way of standardization or guidelines would be of interest to IEC.

There are three basic ideas on which these ISA and IEC materials depend. One is that the potential harm or danger can be measured by *risk*, which is the combination (usually the product of) the probability of occurrence of the harm and the severity of

the harm. A second basic idea is that the safety instrumented functions, which mitigate or prevent the harm and are therefore much like SPS, can be characterized by their *safety integrity*. This is the probability of a safety instrumented function satisfactorily performing the required functions under all the stated conditions within a stated period of time. In the cited standards, safety integrity is quantified by a *safety integrity level* (SIL). The SIL is a discrete number, 1, 2, 3, or 4, which specifies the requirements of the safety instrumented functions to be allocated to the safety instrumented systems. SIL 4 has the highest level of safety integrity, and SIL 1 has the lowest level. Each SIL has associated target failure measures, according to whether the mode of operation is low demand operation where frequency of demand for operation is not more than once per year or high demand operation where this frequency is greater than once per year. For low demand operation, the average probability of failure to perform the design function on demand should lie in the range: 10^{-4} to 10^{-5} (SIL 4), 10^{-3} to 10^{-4} (SIL 3), 10^{-2} to 10^{-3} (SIL 2), and 10^{-1} to 10^{-2} (SIL 1). For high demand operation, the probability of a dangerous failure per hour should lie in the range: 10^{-8} to 10^{-9} (SIL 4), 10^{-7} to 10^{-8} (SIL 3), 10^{-6} to 10^{-7} (SIL 2), and 10^{-5} to 10^{-6} (SIL 1). The third basic idea embedded in these documents is that risk and SIL are keys in showing how the establishment and maintenance of safety-instrumented system integrity involves many activities over the lifetime of the equipment. This idea is captured via use of the term *safety life cycle*, the necessary activities involved in the implementation of safety instrumented function(s) occurring during a period of time that starts at the concept phase of a project and finishes when all of the safety instrumented functions are no longer available for use.

3.1.4 Methods in Process control industry applicable to SPS

3.1.4.1 Risk Matrix

One of the most common techniques used among refining, chemical and petrochemical companies is the risk matrix. The Risk Matrix comprises of risk levels based on probability and impact on its two dimensions as shown in Table 5 [52].

$$Risk = frequency \times consequence \quad (3.1)$$

Table 5: A sample risk matrix

Consequence→ Likelihood	Insignificant	Minor	Moderate	Major	Severe
Almost certain	Moderate risk	High risk	High risk	Extreme risk	Extreme risk
Likely	Moderate risk	Moderate risk	High risk	High risk	Extreme risk
Possible	Low risk	Moderate risk	Moderate risk	High risk	Extreme risk
Unlikely	Low risk	Moderate risk	Moderate risk	High risk	High risk
Rare	Low risk	Low risk	Moderate risk	High risk	High risk

The various risk levels are:

- *Extreme risk* - detailed action/plan required
- *High risk* - needs senior management attention
- *Moderate risk* - specify management responsibility
- *Low risk* - manage by routine procedures

The above concept of Risk Matrix can be used to assess SPS related risks. SPS are programmed to engage in forced curtailments when an unwanted event is detected. For instance, the fact that SPS increases operational transfer capability does not mean that we should ignore the fact that frequent curtailments of load cause customer dissatisfaction. Therefore the frequency of forced curtailments and the amount of load interrupted should be regulated in order to minimize risk. Similarly, there are other consequences for a desirable operation of SPS such as generation rejection, penalty due to reduced export, etc. Also the consequences under an undesirable operation of SPS could be equipment damage, system instability, etc. So a risk matrix can be used to evaluate the risk of each of these consequences under different modes of SPS operation. Table 6 shows a proposed matrix which can be used to minimize risk of SPS actions.

Table 6: A prototype illustrating the relationship between SPS and risk matrix

Consequence levels when SPS is armed to trip → Frequency of SPS actions	Insignificant value of consequence	Moderate value of consequence	Minor value of consequence	Significant value of consequence	Major value of consequence
Possibility of repeated events	Significant risk	Significant risk	High risk	High risk	High risk
Possibility of isolated events	Moderate risk	Significant risk	Significant risk	High risk	High risk
Possibility of occurring sometimes	Low risk	Moderate risk	Significant risk	High risk	High risk
Not likely to occur	Low risk	Low risk	Moderate risk	Significant risk	High risk
Rare occurrence	Low risk	Low risk	Moderate risk	Significant risk	Significant risk

3.1.4.2 Economic analysis of a Safety Instrumented System

Economic analysis of SIS is very important because sometimes installation of some SIS may not be a wise idea. Any company that invests in a project wants to know whether the benefit of the projects outweighs the costs. Economic models have been

developed to assess the benefit-cost ratio of installing a SIS [53], as shown in Figure 18.

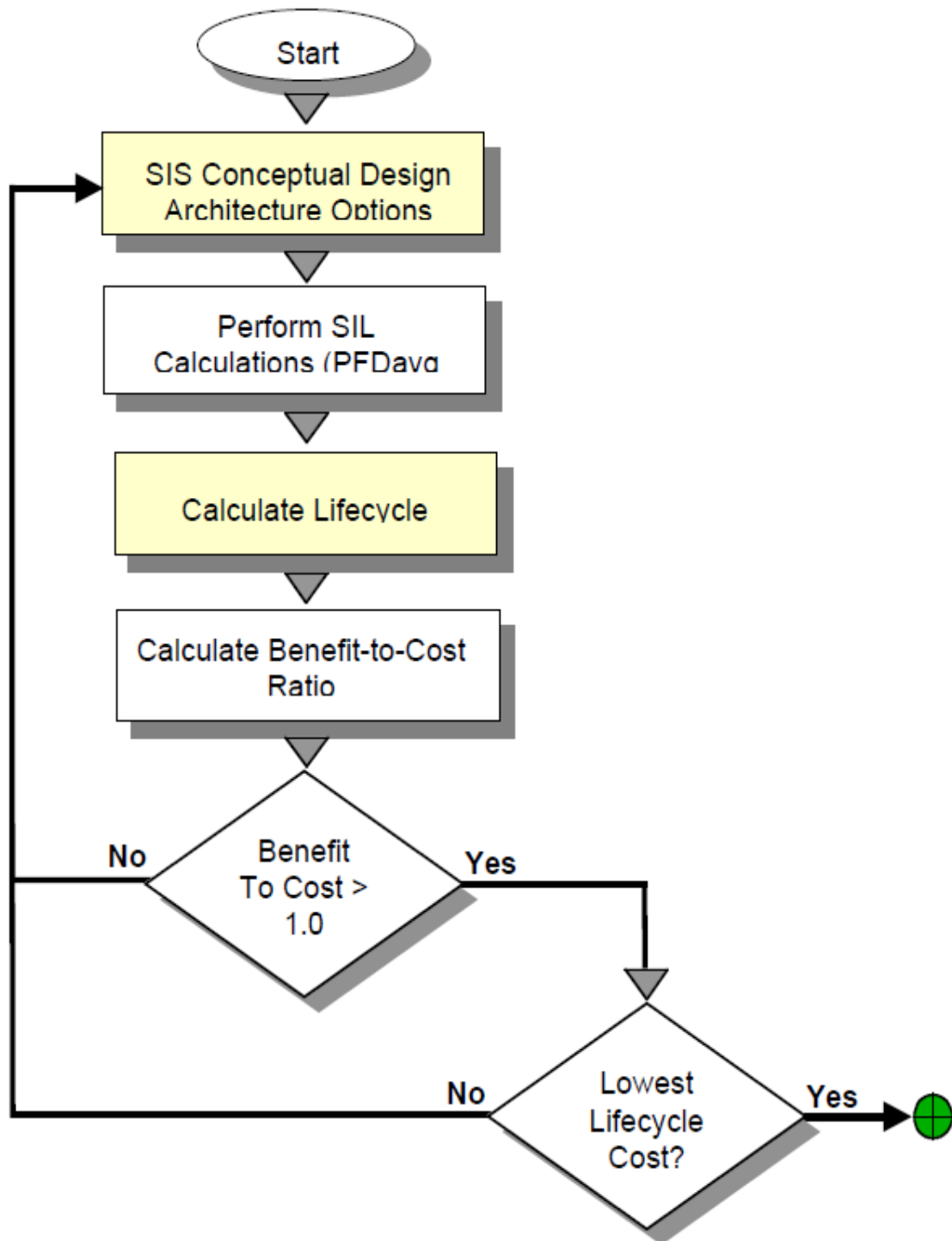


Figure 18: Economic analysis flowchart

The above methodology of economic analysis can be applied to study SPS aided

transmission upgrade. In most cases SPS is a cheaper alternative to transmission upgrade but we should not forget that SPS causes increase in operational costs such as re-dispatch costs, EENS (expected energy not served) costs etc. and maintenance costs. These when accumulated over the years it becomes very large. On the other hand transmission lines are invested over long period of years and all these unnecessary costs can be avoided over the years. A solution combining both SPS and transmission line may strike the right balance. Therefore, it is necessary to do an economic sanity check as shown in Figure 19 to know which transmission expansion plan aided by SPS may be the better option over the long term.

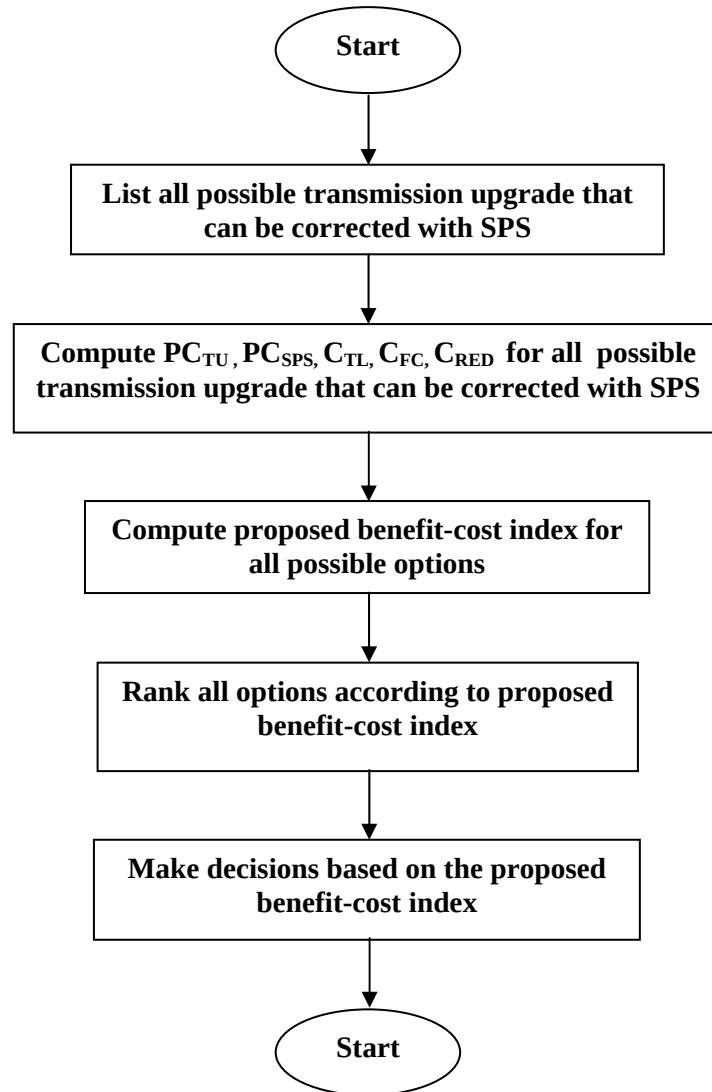


Figure 19: Economic analysis of SPS aided transmission upgrade

A benefit-cost index is proposed and it can help to rank transmission upgrade based on economic benefit.

$$B / C = \frac{(PC_{SPS} - PC_{TU})}{C_{TU} - (C_{SPS} + C_{FC} + C_{SI})} \quad (3.2)$$

where,

B/C = Benefit-cost index

PC_{TU} = Production costs after transmission upgrade

PC_{SPS} = Production costs if SPS is the preferred alternative

C_{TU} = Cost for transmission upgrade

C_{SPS} = Cost for implementing SPS

C_{FC} = Expected cost due to forced curtailments (SPS)

C_{RED} = Expected re-dispatch cost after generation tripping (SPS)

The example shown in Tables 7 and 8 assumes that the study is conducted for a 5-year interval and all monetary values are in present value.

Table 7: Cost analysis

Cost	Option 1	Option 2	Option 3
C_{TL}	\$5,000,000	\$8,000,000	\$3,000,000
C_{SPS}	\$250,000	\$280,000	\$186,000
$(PC_{SPS} - PC_{TU})$	\$1,700,000	\$1,200,000	\$900,000
C_{FC}	\$100,000	\$100,000	\$110,000
C_{SI}	\$120,000	\$180,000	\$90,000

Table 8: Ranking options

Options	Benefit-cost index	Rank
1	0.375	1
2	0.161	3
3	0.332	2

3.2 Nuclear industry

Safety is one of the most important issues in the nuclear power industry. The consequence of safety-related failures in this discipline is always considered vital to both people and the environment. Therefore, it is understandable that there are so many safety-related instrumentation and control (I&C) systems in a nuclear power plant. In addition, many organizations worldwide have developed various standards which give guidance to nuclear I&C systems. These standards play an important role in guiding, shaping, or even regulating the development of safety-related I&C systems in the nuclear power industry.

3.2.1 IEC standards

The International Electro technical Commission (IEC) has been developing its work on functional safety since 1985. As a result, the seven parts of a general industry systems standard IEC 61508 titled “Functional safety of electrical/electronic/programmable electronic safety-related systems” were published during the period of 1998-2000 [54, 55, 56, 57, 58, 59, 60]. In 2005 the part of IEC/TR 61508-0 was published [61]. After that, the revision to this standard has been under progress and the new standard edition is expected to be published soon.

IEC 61508 adopts the overall safety lifecycle as the technical framework for the strategy of achieving functional safety, from initial concept, through hazard analysis and risk assessment, development of the safety requirements, specification, design and implementation, operation and maintenance, and modification, to final decommissioning and/or disposal. The functional safety requirements specification consists of two elements:

- Safety function requirements, and
- Safety integrity requirements.

The safety function requirements are derived from the hazard analysis. It is the safety function that determines what has to be done to achieve or maintain a safe state for the equipment under control [62]. The safety integrity requirements are derived from the risk assessment. It is the safety integrity that determines what degree of certainty is necessary that the safety function will be carried out. In other words, the safety integrity is the referred index of the safety performance.

IEC 61508 specifies four levels of safety performance for a safety function. These are called safety integrity levels (SIL). Safety integrity level 1 (SIL1) is the lowest level of safety integrity and safety integrity level 4 (SIL4) is the highest level. The higher the level of safety integrity, the lower is the intended likelihood of a dangerous failure. It should be noted that when determining the SIL, the mode of operation is an important factor that influences the measures chosen. IEC 61508 classifies the mode of operation into two categories:

- (1) Low demand mode, where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof-test frequency.
- (2) High demand or continuous mode, where the frequency of demands for operation made on a safety-related system is greater than one per year or greater than twice the proof-check frequency.

The target failure measures corresponding to the SIL are specified differently for a safety function operating in different demand modes.

IEC 61508 is both a stand-alone standard and can also be used as the basis for sector and product standards. As for nuclear power industry, IEC 61513 is the sector-application standard published in 2001 with the title “Nuclear power plants-Instrumentation and control for systems important to safety - General requirements for systems” [63]. This standard has adopted a presentation format similar to basic safety

publication IEC 61508 with an overall safety life-cycle and a system life-cycle. The standard also provides an interpretation of the general requirements of IEC 61508, parts 1, 2 and 4, for the nuclear application sector. Compliance with this standard will facilitate consistency with the requirements of IEC 61508 as they have been interpreted for the nuclear industry.

The important parts of IEC 61513 are its normative clauses 5 to 8:

- 1) Clause 5 addresses the total architecture of the I&C systems important to safety:
 - a) Defining requirements for the I&C functions, and associated systems and equipment (I&C FSE) derived from the safety analysis of the NPP, the categorization of I&C functions, and the plant lay-out and operation context.
 - b) Structuring the totality of the I&C architecture, dividing it into a number of systems and assigning the I&C functions to systems. Design criteria are identified, including those to give defense in depth and to minimize potential for common cause failure (CCF).
 - c) Planning the total architecture of I&C systems.
- 2) Clause 6 addresses the requirements for the individual I&C systems important to safety, particularly the requirements for computer-based systems.
- 3) Clauses 7 and 8 address the overall integration, commissioning, operation and maintenance of the I&C systems.

IEC 61513 also includes as its informative part some important annexes:

- 1) Annex A highlights the relations between IAEA and basic safety concepts that are used throughout this standard;
- 2) Annex B provides information on the categorization/classification principles;
- 3) Annex C gives examples of I&C sensitivity to CCF;
- 4) Annex D provides guidance to support comparison of this standard with parts 1, 2 and 4 of IEC 61508. This annex surveys the main requirements of IEC 61508 to verify that the issues relevant to safety are adequately addressed, considers the use of common terms and explains the reason for adopting different or complementary techniques or terms.

In fact, IEC 61513 is the first level standard prepared by subcommittee 45A (SC45A): Instrumentation and control of nuclear facilities, of IEC technical committee 45 (IEC/TC45): Nuclear instrumentation. SC45A core domain is instrumentation and control (I&C) systems important to safety in nuclear energy generation facilities. SC45A standards cover the entire lifecycle of these I&C systems, from conception, through design, manufacture, test, installation, commissioning, operation, maintenance, aging management, modernization and decommissioning. Some other level SC45A standards that are relevant to IEC 61513 are:

- IEC 61226: Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions [64]

This standard classifies nuclear power plants instrumentation and control systems according to their importance for safety. The Standard establishes a method of classification of the information and command functions for nuclear power plants, and the I&C systems and equipment that provide those functions, into categories that designate the importance for safety of the function. The resulting classification then determines relevant design criteria. The design criteria are the measures of quality by which the adequacy of each function in relation to its importance to plant safety is ensured.

- IEC 60709: Nuclear power plants – Instrumentation and control systems important to safety – Separation [65]

For independence is required by IEC 61513, this standard defines the assessments needed and the technical requirements to be met for instrumentation and control (I&C) systems important to safety and their cables, in order to achieve adequate physical separation between redundant sections of a system and between a system and another system. This separation is needed to prevent or minimize the impact on safety that could result from faults and failures which could be propagated or affect several sections of a system or several systems.

- IEC 60987: Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems [66]

This standard is directly referenced by IEC 61513 which addresses the generic issue of hardware design of computerized systems. It is a second-level SC45A standard applicable to computer-system hardware for systems of Class 1 and 2 (as defined by IEC 61513) in nuclear power plants. This standard covers digital systems hardware, including multiprocessor distributed systems and single processor systems. It also covers the assessment and use of pre-developed items, for example, commercial off-the-shelf items (COTS), and the development of new hardware.

- IEC 60880: Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions [67]

This standard is directly referenced by IEC 61513 which deals with the system aspects of high integrity computer-based I&C used in safety systems of nuclear power plants together. It is a second level SC45A document tackling the issue of software aspects for I&C systems performing category A functions, as defined by IEC 61226. This standard provides requirements for the purpose of achieving highly reliable software and addresses each stage of software generation and documentation, including requirements specification, design, implementation, verification, validation and operation. It also gives recommendations on several key issues of using software in nuclear safety

systems, e.g. dealing with software aspects of defence against common cause failures, use of software tools and pre-developed software.

- IEC 62138: Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions [68]

This standard provides requirements and recommendations for the software aspects of computer-based I&C systems of safety classes 2 and 3, as defined by IEC 61513. These I&C systems may be used for category B or C FSEs (Functions, and associated Systems and Equipment), as defined by IEC 61226. Its scope can be compared to the scope of revised IEC 60880, the difference being that IEC 60880 addresses the software aspects of I&C systems of safety class 1.

IEC 60880 and IEC 62138 together cover the domain of the software aspects of computer-based systems used in Nuclear Power Plants to perform functions important to safety, which correspond to IEC 61508, part 3 for the nuclear application sector. Hence, they are consistent with, and complementary to, IEC 61513.

- IEC 62340: Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF) [69]

This standard provides requirements and recommendations for the total architecture of instrumentation and control (I&C) systems. It provides principles and requirements to overcome common cause failure (CCF) by means which ensure independence. The implementation of these requirements leads to various types of defense against initiating CCF events.

- IEC 62342: Nuclear power plants – Instrumentation and control systems important to safety – Management of ageing [70]

This standard provides strategies, technical requirements, and recommendations for the management of ageing of nuclear power plant instrumentation and control systems and associated equipment. It also includes annexes on test methods, procedures, and technologies that may be used to verify proper operation of such equipment and aim to prevent ageing degradation from having any adverse impact on the plant safety, efficiency, or reliability. This standard applies to all types of nuclear power plants and relates primarily to safety.

- IEC 60671: Nuclear power plants – Instrumentation and control systems important to safety – Surveillance testing [71]

This standard lays down principles for testing I&C systems performing functions important to safety, during normal power operation and shutdown, so as to check the functional availability especially with regard to the detection of faults that could prevent the proper operation of the important to safety functions. It covers the possibility of testing at short intervals or continuous

surveillance, as well as periodic testing at longer intervals. It also establishes basic rules for the design and application of the test equipment and its interface with the systems important to safety. Further, the effect of any test equipment failure on the reliability of I&C systems is considered.

3.2.2 IAEA standards

The International Atomic Energy Agency (IAEA) was set up as the world's "Atoms for Peace" organization in 1957 within the United Nations (UN) family. IAEA works with its member states and multiple partners worldwide to promote safe, secure and peaceful nuclear technologies. The IAEA's Statute authorizes IAEA to establish safety standards to protect health and minimize danger to life and property. Many of IAEA's member states have decided to adopt the IAEA's safety standards for use in their national regulations.

In fact, the IEC/Technical Committee 45 (IEC/TC45) standards are closely related to the IAEA's safety standards series. In order to avoid the potential for duplication and even contradiction between IAEA documents and IEC technical standards, a formal agreement of co-operation was reached in 1981 between IAEA and IEC/TC45. The agreement states that IAEA is responsible for the development of safety principles for instrumentation, control and electrical systems in nuclear power plants, while IEC/TC45 is responsible for the design requirements that realize these safety principles [72]. Therefore, the IEC/TC45 standards have been developed to be consistent with the principles and basic safety aspects of the IAEA standards series, while the IAEA documents apply to all IEC/TC45 instrumentation and control standards.

IAEA safety standards series covers nuclear safety, radiation safety, transport safety and waste safety, and also general safety. The three categories within it are Safety Fundamentals, Safety Requirements and Safety Guides. In particular, there are four IAEA documents that are concerned with safety-related instrumentation and control systems:

- IAEA NS-R-1: Safety of Nuclear Power Plants: Design – Safety Requirements [73]

This Safety Requirements can be regarded as the overall guidance for nuclear power industry. It establishes design requirements for safety functions and associated structures, systems and components important to the safe operation of nuclear power plants. It also establishes requirements for a comprehensive safety assessment to identify the potential hazards that may arise in the operation of plants. In relation to the design process, preventive and mitigatory features for severe accidents, the management of safety, design management, plant ageing and wearing out effects, computer based safety systems, external and internal hazards, human factors, feedback of operating experience, and safety assessment and verification are considered.

- IAEA NS-G-1.1: Software for Computer Based Systems Important to Safety in Nuclear Power Plants – Safety Guide [74]

This Safety Guide provides guidance on the collection of evidence and preparation of documentation to be used in the demonstration of safety and reliability of the software for computer based systems important to safety in nuclear power plants for all phases of the system life cycle. It recommends how to meet the requirements established in IAEA NS-R-1.

- IAEA NS-G-1.3: Instrumentation and Control Systems Important to Safety in Nuclear Power Plants – Safety Guide [75]

This Safety Guide recommends how the requirements established in IAEA NS-R-1 should be met for instrumentation and control (I&C) systems important to safety. It provides guidance on the design of I&C systems important to safety in nuclear power plants, including all I&C components, from the sensors allocated to the mechanical systems to the actuated equipment, operator interfaces and auxiliary equipment.

The main content of this Safety Guide is its sections 2 to 7:

- 1) Section 2 discusses the identification of I&C functions and systems within the scope of this Safety Guide, and their further classification into safety and safety related functions and systems.
 - 2) Section 3 describes the determination of the design basis for I&C systems important to safety.
 - 3) Section 4 provides design guidance for I&C systems important to safety. It includes guidance that applies to all I&C systems important to safety as well as guidance that applies only to safety systems. Applicability of the guidance to these two classes is identified and summarized.
 - 4) Section 5 provides additional guidance that is specific to certain I&C systems, namely protection systems, power supplies and digital computer systems. The guidance for these systems comprises the general guidance provided in Section 4 and the specific guidance provided in Section 5.
 - 5) Section 6 expands on the guidance given in Section 4 in the area of human-machine interfaces.
 - 6) Section 7 expands on the guidance given in Section 4 in the area of design processes to ensure quality.
- IAEA NS-G-1.8: Design of Emergency Power Systems for Nuclear Power Plants — Safety Guide [76]

This Safety Guide provides general recommendations and guidance for all types of Emergency Power Systems (EPS) — electrical and non-electrical — and specific guidance on the safety requirements for design and the features of the electrical and non-electrical parts of the emergency power supplies. The recommendations and guidance are focused on the power supplies necessary to power loads important to safety.

3.2.3 IEEE standards

The Institute of Electrical and Electronics Engineers (IEEE) has also been developing nuclear power plant standards through Nuclear Power Engineering Committee (NPEC), one of the Technical Committees of the IEEE Power & Energy Society (PES). NPEC's established policy is to improve, clarify, update and provide application guidance on the standards already produced and when appropriate, to produce new standards.

Although the collections of IEEE and IEC standards have some overlap, but in many cases cover significantly different topics. For example, IEEE standards go to great depth on environmental qualification of many specific types of components, while IEC covers the topic only at the general level. Conversely, certain IEC standards deal with specific instrumentation and control (I&C) functions, a topic area where IEEE standards are largely mute [77]. In fact, IEEE standards look upon the safety-related systems in general, rather than focus on the safety-related I&C systems, which are one but perhaps the most significant part of the former. The following IEEE standards are considered important to affect nuclear safety-related I&C systems:

- IEEE Std 603: IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations [78]

This standard can be regarded as the general principles for nuclear safety systems. It establishes minimum functional and design criteria for the power, instrumentation, and control portions of nuclear power generating station safety systems. The intent of these criteria is to provide a means for promoting appropriate practices for design and evaluation of safety system performance and reliability. However, adhering to these criteria will not necessarily fully establish the adequacy of any safety system's functional performance and reliability; nonetheless, omission of any of these criteria will, in most instances, be an indication of safety system inadequacy.

The important parts of this standard are its clauses 5 to 8:

- 1) Clause 5 provides a large set of safety system criteria, including single-failure criterion, completion of protective action, quality, equipment qualification, system integrity, independence, capability for testing and calibration, information displays, control of access, repair, identification, auxiliary features, multi-unit stations, human factors considerations, reliability, and common-cause failure criteria.
- 2) Clause 6 provides the functional and design requirements on sense and command features, including automatic control, manual control, interaction between the sense and command features and other systems, derivation of system inputs, capability for testing and calibration, operating bypasses, maintenance bypass, and setpoints.
- 3) Clause 7 provides the functional and design requirements on execute features, including automatic control, manual control, completion of protective action, operating bypasses, and maintenance bypass.

- 4) Clause 8 provides the requirements on power source, including electrical power sources, non-electrical power sources, and maintenance bypass.
- IEEE Std 7-4.3.2: IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations [79]

This standard addresses the use of computers as part of safety systems in nuclear power generating stations. It specifies additional computer-specific requirements (incorporating hardware, software, firmware, and interfaces) to supplement the criteria and requirements of IEEE Std 603. This standard should be used in conjunction with IEEE Std 603 to assure the completeness of the safety system design when a computer is to be used as a component of a safety system. This standard recognizes that development processes for computer systems continue to evolve. As such, the information presented should not be viewed as the only possible solution. However, this standard does not provide requirements associated with the operation and maintenance of the computer following installation (i.e., surveillance testing frequency).

- IEEE Std 338: IEEE Standard Criteria for Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems [80]

The standard provides criteria for the performance of periodic testing of nuclear power generating station safety systems. The scope of periodic testing consists of functional tests and checks, calibration verification, and time response measurements, as required, to verify that the safety system performs its defined safety function.

- IEEE Std 336: IEEE Guide for Installation, Inspection, and Testing for Class 1E Power, Instrumentation, and Control Equipment at Nuclear Facilities [81]

This guide provides considerations for the pre-installation, installation, inspection, and testing of Class 1E power, instrumentation, and control equipment and systems of a nuclear facility. It is applicable to initial construction, modification (backfit), and maintenance activities. However, this guide does not apply to periodic testing.

- ANSI/IEEE Std 352: IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems [82]

This Guide is also an American national standard endorsed by the American National Standards Institute (ANSI). It provides the designers and operators of nuclear power plant safety systems and the concerned regulatory groups with the essential methods and procedures of reliability engineering that are applicable to such systems. By applying the principles given, systems may be analyzed, results may be compared with reliability objectives, and the basis for decisions may be suitably documented.

The quantitative principles are applicable to the analysis of the effects of component failures on safety system reliability. The principles are applicable during any phase of the system's lifetime. They have their greatest value during

the design phase. During this phase, reliability engineering can make the greatest contribution toward enhancing safety. These principles may also be applied during the preoperational phase or at any time during the normal lifetime of a system. When the principles are applied during either of these two phases, they will aid in the evaluation of systems, in the preparation or revision of operating or maintenance procedures, and in improving test programs. Although not inherently limited, these principles are intended for application to systems covered in the scope of IEEE Std 603.

- IEEE Std 577: IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Facilities [83]

This standard sets forth minimum acceptable requisites for the performance of reliability analyses for safety-related systems of nuclear facilities when used to address the reliability requirements identified in regulations and other standards. The requirement that a reliability analysis be performed does not originate with this standard. However, when reliability analysis is used to demonstrate compliance with reliability requirements, this standard describes an acceptable response to the requirements.

3.2.4 Challenges to the U.S. nuclear standards

Some other organizations in the United States are also involved in developing standards that significantly affect nuclear applications. These organizations include but not limited to the American National Standards Institute (ANSI), the American Nuclear Society (ANS), the American Society of Mechanical Engineers (ASME), the American Society of Testing and Materials (ASTM), and the Instrumentation, Systems, and Automation Society (ISA), etc. However, the existing standards are more focused on specific types of nuclear components and corresponding safety-related functions, rather than give guidance on the nuclear safety-related I&C systems.

The U.S. Department of Energy (DOE) has undertaken significant investment in nuclear power as a source of non-greenhouse gas emitting energy. DOE's Office of Nuclear Energy sponsored an initiative to identify codes and standards that will be employed in the next generation of nuclear power plants to determine if any gaps exist that could hinder their construction. According to the discussions among the U.S. Nuclear Regulatory Commission (NRC), standards development organizations, and industry, technological advances might provide unique challenges to construction practices and construction quality. New standards may need to be developed to reflect advances in technology, such as standards for digital instrumentation and controls, cyber security, computers used in safety systems, and Probabilistic Risk Assessments (PRA) used for setting surveillance intervals, etc [84].

3.2.5 Hints from nuclear industry

The nuclear safety-related I&C systems are so important that they are indispensable to the safety of nuclear elements and nuclear plants. Although they are different from the SPS in electric power industry, their safety functions to maintain the aimed object in a safe state under predetermined conditions are similar to those of SPS.

Therefore, the contents of the nuclear standards mentioned previously can be useful to the development of SPS. At least, we can have some beneficial hints from the nuclear industry as follows.

- In the design phase, reliability engineering can make the greatest contribution toward enhancing reliability and safety. It is during this phase that the quantitative reliability analysis, i.e. Probabilistic Risk Assessments (PRA) has its greatest value.
- The functional safety requirements specification consists of the safety function requirements and the safety integrity requirements. The former is derived from the hazard analysis. The latter is derived from the risk assessment, which can be evaluated by the safety integrity level (SIL).
- The initial design process has a comprehensive safety assessment to identify the potential hazards that may arise in the operation. In addition, preventive and mitigatory features for severe accidents should also be considered.
- The system should be designed to have the capability against the single failure of its components (N-1 criterion).
- Although redundancy is a widely accepted principle to enhance the system reliability, it is not enough. It is also important to guarantee adequate physical separation between redundant sections of a system and between a system and another system.
- Common cause failures (CCF) should be paid attention to during design of the total system architecture. Various means including independence against initiating CCF events should be considered.
- Digital computer systems have the trend to prevail in the application of instrumentation and control systems. Therefore, reliability of both hardware and software becomes significant to the system reliability.
- Testing at short intervals or continuous surveillance, as well as periodic testing at longer intervals are necessary to check the functional availability especially with regard to the detection of faults that could prevent the proper operation.

3.3 System operations for electric power

Many companies develop so-called operating rules for use in guiding operators in energy control centers during conditions for which contingencies may result in violation of reliability criteria. For example, many companies in the Western US use operating nomograms to do this, where secure operating regions are delineated from insecure operating regions in the space of parameters such as flows, generation levels, and load levels, so that proximity to a security boundary can be easily monitored, and when encountered, the nomogram axes identify the parameters the operator must control in order to move into a more secure operating condition. Next section describes another approach to derive operating rules, which finds its application in relation to SPS.

3.3.1 Operational security rules from decision trees

The French company RTE and others have developed a semi-automated way of obtaining operating rules. Here Monte Carlo simulation of various operating parameters is performed to form many basecases and a database of post-contingency response is extracted, which will be used to derive significant planning and operational information using data mining techniques as shown in Figure 20. Since, decision trees are capable to provide explicit rules to system operators, French transmission operator RTE has been using decision trees to define operational security rules [85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96]. A similar approach has been applied to Entergy [97, 98].

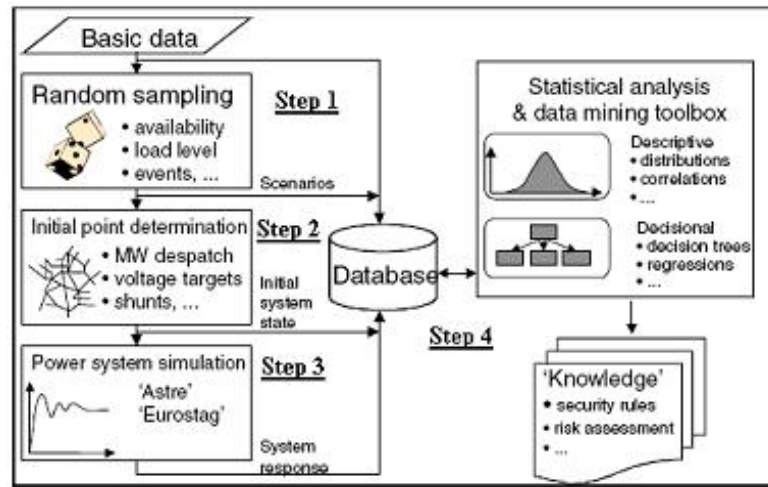


Figure 20: Monte Carlo simulation based power system planning

Typically, the database generation approach using Monte Carlo simulation of operating parameters plays a critical role in obtaining operational security rules with good performance. Studies in the past have used a uniform or random sampling of various parameters such as load level, exchanges at the borders, etc. from their probability distributions to form various basecases. But such an approach has two problems:

(1) Computational requirements: Tedious and time consuming, as there could be a tremendously large number of combinations of variables and topologies.

(2) Error Rates (Classification Accuracy): Some studies expend extra computation after validating the operational rules to increase the unstable (rare) situations in database to improve the accuracy. But, if the sampled unstable situations are unlikely (namely a low probability of occurrence in reality), then it could make the rules very conservative, i.e. either costly to respect or increase false alarms by misclassifying acceptable scenarios as unacceptable.

Researchers at Iowa State University have developed an efficient sampling method to generate likely influential operating conditions that captures high information content for better classification and also reduces computing requirements. The method developed is tested on the Brittany area of RTE's system for a voltage stability

assessment study [99], and decision rules are shown to have improved accuracy. A database has high information content if there are many operating conditions for which the post-contingency performance is close to the threshold or *boundary region*. So, the influential operating conditions are generated directly from the boundary region using Monte Carlo importance sampling by creating a probability re-orientation in the operational parameter (input) state space towards the boundary region, which also preserves the relative likelihood of the sampled conditions.

C. Singh et. al. [100] used a state space pruning method to identify the influential region in the discrete operational parameter space under a single load level. We use stratified sampling to quickly identify the boundary region in the operational parameter state space in stage I, and then apply importance sampling to bias the sampling towards the boundary region in stage II, as shown in Figure 21 depicting the developed efficient sampling approach.

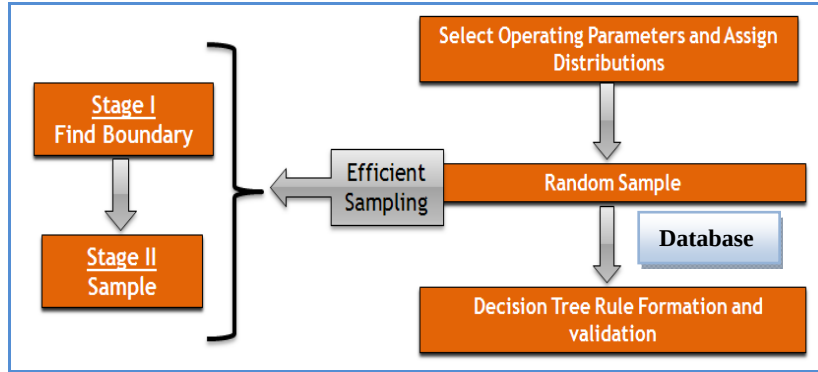


Figure 21: Efficient database generation approach

3.3.2 SPS logic design using decision trees

The approach described in Figure 20 may also be utilized within the SPS logic design step [101, 102, 103], recognizing that the only difference between operating rules and SPS logic are:

1. The SPS logic is *automated*.
2. The SPS logic is *not only limited to critical operating condition detection* with respect to some stability criteria, but also to *automatic preventive/corrective action* to safeguard the system against impending instability or increase the loadability of the system.

A typical SPS logic design procedure is illustrated in Figure 22. A study was performed to demonstrate the SPS logic design using decision trees, with the following study assumptions:

1. SPS location and functionality (i.e., Load Reject, Generator trip, under-voltage load shed (UVLS) etc.) already available
2. Critical contingency for which SPS installed known
3. Study performed to find either or both:

- a. Arming condition for SPS, i.e., IF <condition>... and
- b. Actuating function of SPS. i.e., ... THEN <SPS Action>

As shown in Figure 22, a post-contingency response database is formed with the simulation having the SPS modeled within it, i.e., in the event of any basecase becoming post-contingency unstable, the SPS action is taken to save it. For instance, it may be a single generator trip function or UVLS etc. Then two sets of basecases are obtained:

- a. Stable post-contingency cases with and w/o SPS action
- b. Unstable post-contingency cases with SPS action

The cases that do not become stable even after SPS has been armed, in an effort to save it, are thrown as they do not give any valuable information for SPS logic derivation. The remaining cases are used to form the database for training the decision tree to form the arming logic for SPS.

If the decision to be taken is binary (DT1), i.e., whether to arm SPS or not, then the target (class) attribute contains information on status of SPS for every record in the database. Finally decision tree DT1 would induce operating rules in terms of other system attributes for deciding when to arm.

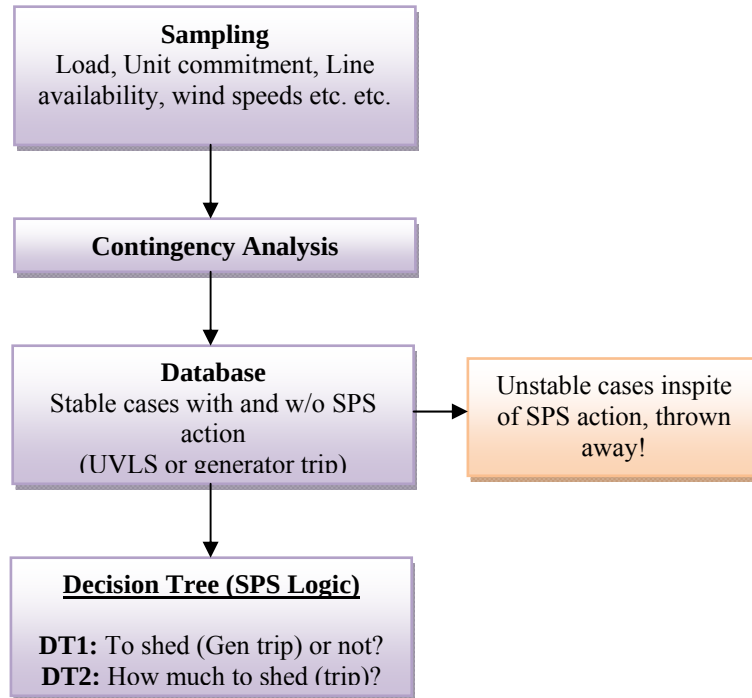


Figure 22: SPS logic design

If the decision to be taken is quantitative (DT2), i.e., how much load to shed or how many generators to trip, then the target attribute could be the discretized version of the actual amount shed load (UVLS) or the numbers of unit trips.

3.3.3 Illustration

This section presents a numerical example of the methodology explained in the previous section to design SPS logic using Monte Carlo simulation of operating conditions and decision tree based inductive learning.

The test system considered is the example case study provided as part of the ASSESS software from French transmission operator RTE-France [104]. The base case consists of 28 nodes and 37 lines forming a 90 kV network, serving 330 MW of total load consumption. It is divided into four zones, namely A, B, C and D. The node names follow a random numbering order from N1 S41 to N27 S41 except for a node, called INTERS41, where there is the HVDC connection. There are 16 hydraulic generators, 11 thermal generators and 5 wind production areas located in 2 zones considered to be windy, zones A and B. Each wind generator area can produce up to 12 MW at 20 kV and is modeled by an asynchronous generator combined with a negative load for static computations. Other generators (hydraulic and thermal) are modeled by synchronous machines.

The study is performed to develop arming logic for a UVLS SPS, which is a response based SPS. The decision to be taken is whether to shed a load or not? The main aim of the study is to analyze the effects of five wind turbines in the test system under various load levels, line and generator unavailabilities. Hence, following are the operating parameters whose effects are captured by probabilistic models in ASSESS:

1. Wind speed in A and B zones
2. Load level
3. Unavailability of some lines and/or generators

For each basecase, an AC optimal power flow is performed using the software TROPIC (integrated with ASSESS), minimizing the production cost under voltage, current, flow constraints in N. The cases that encounter problems with convergence are subjected to load shedding to achieve convergence. The database contains 500 stable basecases, among which 67 involved SPS arming, i.e., load shedding. So a decision tree was induced from the database to derive operational rules for arming the SPS, as shown in Figure 23.

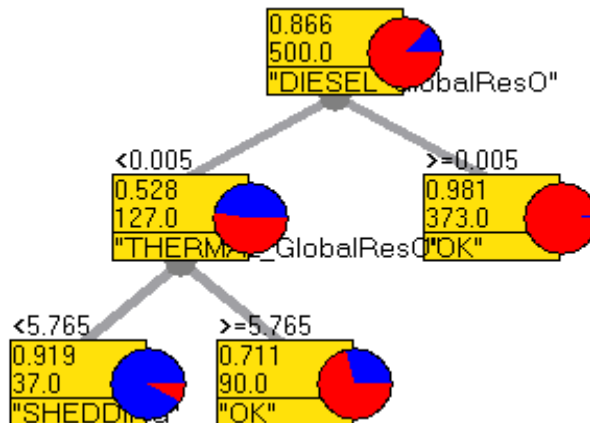


Figure 23: Decision tree: shed load or not?

Hence the design logic for SPS arming can be:

"DIESEL_GlobalResD" < 0.005	"OK"
└─ "THERMAL_GlobalResD" < 5.765	"SHEDDING"
└─ "THERMAL_GlobalResD" ≥ 5.765	"OK"
"DIESEL_GlobalResD" ≥ 0.005	"OK"

As mentioned in section 3.3.1, when the operating conditions are sampled near the boundary region of the operating parameter state space (multivariate state space formed by load levels and wind speeds under various combinations of discrete parameters, i.e., line and generator unavailabilities), the resulting operating rules will have better classification accuracy and result in reliable SPS operations.

4 Risk assessment, process view

This chapter will focus on risk assessment from the process point of view. Section 4.1 will describe process-related failure modes, and section 4.2 will summarize methods of process-view risk assessment. Section 4.3 presents formulation of risk expression for a Generation Rejection Scheme (GRS), which was already presented in the publication [105]. Section 4.4 presents an illustration of reliability evaluation of GRS. Section 4.5 presents various advancements in SPS architectures and their reliability models.

4.1 Process view failure modes

We define an “SPS event” to be any one of the following:

- desirable SPS operation,
- undesirable SPS operation, or
- SPS failure to operate when needed.

An SPS operation may be desirable or undesirable, depending on the consequence of the operation relative to the consequence had the SPS not operated. If the consequence of the operation is less severe than the consequence had the SPS not operated, the operation is desirable. This is case, for example, when the action of a generation rejection scheme trips one out of three units following a disturbance when otherwise, all three units would have lost synchronism.

If the consequence of the operation is more severe than the consequence had the SPS not operated, the operation is undesirable. Undesirable operation may either be unintended, due to a hardware, software, or human error, or it can be intended (according to the design), but still undesirable due to a fault in the design logic. A nuisance operation, when an SPS takes unnecessary action when there is no disturbance in the system, is an example of an undesirable, unintended operation. An example of an undesirable, intended operation is when a generator rejection scheme operates and trips a unit following a disturbance for which it was designed to operate, but had the SPS not operated, the plant would have been stable. This situation can occur if the disturbance is single phase to ground fault and the design criteria is based only on three phase faults.

An SPS failure to operate occurs when the SPS fails to respond as designed to conditions for which the SPS is supposed to operate. An SPS may fail to operate as expected for several reasons, among which are:

- hardware failure,
- faulty design logic,
- software failure, or
- human error.

Hardware failure occurs when some physical stress exceeds the capability of one or more installed components. Faulty design logic may occur as a result of inappropriate or incomplete study procedure during the design. Software failure results from errors in vendor written and user

written embedded, application, and utility software. The vendor software typically includes the operating system, I/O routines, diagnostics, application oriented functions and programming languages. User written software failure results from errors in the application program, diagnostics, and user interface routines. Human errors can be classified according to whether they are associated with construction, operation, or maintenance.

Other failure modes that may lead to an undesirable operation or a failure to operate include failure to arm (any failure of a SPS to arm itself for system conditions that are intended to result in the SPS being armed), unnecessary arming (any arming of a SPS that occurs without the occurrence of the intended arming system condition(s)), and failure to reset (any failure of a SPS to reset following a return of normal system conditions if that is the design intent).

When correctly operating, SPS significantly improve system response following a contingency. However, the failure of SPS to accurately detect the defined conditions, or the failure to carry out the required pre-planned remedial action, can lead to serious and costly consequences. The survey by IEEE-CIGRE [5] suggests that the cost of SPS failure can be very high as most of the respondents selected the highest cost category when asked to estimate the cost of an operational failure of SPS.

Review of the U.S. NERC *System Disturbance Reports* from 1986-1995 [10,106] indicates that of the 30 cases that involved the operation of SPS, 21 were reported as successful operation of SPS, while 9 involved operational failures. The reasons for these failure cases include flaw in logic design, software failure, hardware failure, incorrect setting, and inadvertent failure to arm. The following are brief descriptions of these failure cases:

WSCC - Northeast/Southeast Separation Scheme - April 4, 1988:

Scheme: System separation.
Reason: Flaw in design (the scheme was susceptible to misoperation due to short bursts of communications circuit noise).
Consequence: 1902 MW of generation was lost and 253 MW of load was interrupted.
Lessons learned: Faulty design logic.

NPCC - Hydro-Québec - April 18-19, 1988:

Scheme: Load rejection.
Reason: Hardware failure.
Consequence: Systemwide blackout.
Lessons learned: Hardware failure.

NPCC - Hydro-Québec - November 15, 1988:

Scheme: Load rejection.
Reason: Hardware failure.
Consequence: 3950 MW of load was interrupted.
Lessons learned: Hardware failure.

WSCC-British Columbia Hydro/TransAlta Separation - January 7, 1990:

Scheme: Controlled opening of lines.
Reason: Not armed (inadvertently).
Consequence: It caused 230 kV Cranbrook-Nelway circuit to trip on the subsequent swing and resulted in separation (islanding) of the eastern part of the BCHA/TAUC system from the Interconnection.

Lessons learned: Human error.

WSCC-Garrison - Taft 500 kV No.1 and 2 outages - January 8, 1990:

Scheme: Var Compensation (trip two 500 kV bus reactors).
Reason: Flaw in the logic design.
Consequence: It caused the unnecessary dropping of generation at Hauser, Morony, and Ryan (119 MW) as well as the loss of customer load (25 MW) in Helena.

Lessons learned: Faulty design logic.

WSCC-SE Idaho/SW Wyoming Outage - September 12, 1991:

Scheme: Generator rejection.
Reason: Hardware failure (telemetry that automatically arms this scheme was out of calibration).
Consequence: It caused the loss of a second 345 kV line which led to further loss of transmission by overload and out of step conditions.

Lessons learned: Hardware failure.

WSCC-Pacific AC Intertie Separation - November 17, 1991:

Scheme: System separation.
Reason: Software failure in PG&E SPS programmable logic controller caused the delay in initiating remedial actions (also maybe hardware failure).
Consequence: Fail to separate WSCC system into two islands, but did not produce any severe problems (it was expected that there would be load lost and out-of-step conditions).

Lessons learned: Software failure and/or hardware failure.

WSCC-Minnesota - Wisconsin Interface 69 kV conductor burn down - October 13, 1992:

Scheme: Controlled opening of lines.
Reason: Incorrect setting.
Consequence: Two 69 kV lines in the Northern States Power and Dairyland Power Cooperative service burned open causing the lines to fall to ground and trip out.

Lessons learned: Human error.

MAPP & MAIN - Eastern MAPP-Western MAIN Interface Separation -November 6, 1997:

Scheme: Controlled opening of lines.

Reason: Flaw in design (opened the circuit at an ampere level below its setting, possibly due to an unbalanced load.).

Consequence: Resulted in low voltages in the south-western Wisconsin, eastern Iowa and western Illinois (Cordova), heavy loading of parallel, lower voltage transmission systems, and a large phase angle across the open tie at Arpin.

Lessons learned: Faulty design logic.

4.2 Process view risk assessment

There are several existing methods that can be used in SPS reliability evaluation. We summarize four of these methods [107, 108] in what follows. Although these methods are most commonly applied in assessing hardware reliability, we emphasize that their use in SPS reliability assessment must also include assessment of human error [109] and logic integrity [48], as these aspects of SPS reliability are often the weak links in the design.

4.2.1 Failure mode and effect analysis

A Failure Mode and Effect Analysis (FMEA) is a systematic technique that is designed to identify failure modes. It is a “bottom-up” method that starts with a detailed list of all components with the system. An entire system can be analyzed one component at a time. Alternatively, the system can be hierarchically divided into subsystems and modules as required. The basic steps in the process are

- 1) break the system down into subsystems
- 2) list all components
- 3) for each component, list all failure modes
- 4) for each failure mode
 - a. list its effect on the next higher subsystem or system, and its failure rate
 - b. list the severity of the effect
- 5) when the next higher subsystem is the highest system, stop; otherwise, consider the next higher subsystem as a component, and return to 3)

The output of this process is a list including component name, failure mode, failure rate and failure effect.

The FMEA technique is generally poor at identifying combinations of failures that cause critical problems. Since each component is reviewed individually, failures due to combination of components are not addressed. Common cause failures are rarely identified since they require more than one component failure. FMEA can be used as an initial step to identify failure modes for Markov modeling.

4.2.2 Fault tree analysis

Fault tree analysis is a “top-down” approach to the identification of failure modes. It is very complementary to the FMEA in that it requires a deductive approach to finding failure modes. The method is good at finding combinations of failures that may cause problems. The fault tree is developed using fault tree symbols. Fault tree analysis begins with the determination of the top event. The fault tree is constructed by determining the failures that lead to the primary event failures. After the fault tree structure is fully developed, failure rate data, which can be obtained from field experience or from industry published data, is employed to quantify the fault tree.

The basic steps to build the fault tree are

- 1) identify a system or level $L=0$ fault (the top event)
- 2) identify all combinations of “Level $L+1$ ” events that lead to level L failure. The sequences of events are connected by AND, OR, or other logic gates.
- 3) if level $L+1$ constitutes a set of basic or “trigger” events, then stop; otherwise, $L=L+1$ and go to step (2)

4.2.3 Network modeling

Many systems used in industry can be modeled through the use of simple networks. Network modeling (or reliability block diagrams) is used to perform a system integrity analysis through representing the system as a number of functional boxes interconnected to show the effect of each box on the overall system. The resulting networks show components in series, in parallel, or in combination configurations. The key step in the process of reliability modeling is to convert from a physical system into a network model. A good qualitative understanding of system operation during both normal conditions and during failure conditions must exist. A reliability network model is drawn with boxes that represent the modules or the components that comprise the system. Lines are drawn between the boxes to indicate operational dependency. The network model may connect very differently from the physical model. A reliability network may be viewed as showing the “success paths”. If the viewer can find a path from left to right through the reliability network, those components are sufficient to allow the system to operate. Given a network, the rules of probability are used to evaluate success and failure probabilities.

4.2.4 Markov modeling

Markov modeling involves definition of all mutually exclusive success/failure states in a system. These are represented by labeled circles. The system can transition from one state to another whenever a failure or a repair occurs. Transitions between states are shown with arrows and are labeled with appropriate failure or repair probability (often approximated using failure/repair rates). With time modeled in discrete increments (for example, once per hour), calculations can be made showing the probability of being in each state for each time interval. Since some states represent system success, the probabilities of these states are added to obtain either system reliability or system availability as a function of time.

Markov modeling is applicable for systems for which at any given time the subsequent system state only depends on the state at the given time and is not affected by the state at any preceding time. We can assume that an SPS has this characteristic.

Markov modeling is well suited for use in SPS reliability modeling because its flexibility provides that it can account for the variety of features which are common in SPS. Specifically, Markov modeling can incorporate independent and common cause failures, partial and full repairs, maintenance, and diagnostic coverage. Most importantly, it provides that all of these features can be modeled as a function of time. This is in contrast to probability methods which provide steady state results and are accurate only for short repair times and low failure rates.

The necessary data for Markov modeling approach are the failure rate and repair rate for each component of the SPS. There are primarily three sources for them: 1) actual data (field data or test data); 2) published literature (databases, papers, handbooks, technical reports); and 3) experts' opinions.

4.3 Formulation of SPS risk expression

There are many types of SPS in use today. Since the most commonly used SPS type in industry is generator rejection scheme (GRS), we will narrow our focus to the GRS case and develop a reliability evaluation approach for GRS that can also be adapted for other forms of SPS. The typical power plant in which a GRS is installed features high generation capacity and multiple generation units, and the plant depends on two or more transmission lines as its outlets. Without GRS, outage of any one of these lines may cause an out of step condition at the plant. This means that all generators at the plant will accelerate and trip on over-speed. We define any circuit that initiates GRS action during a forced outage condition as a critical circuit. A properly designed GRS, activated by outage of any critical circuit, will trip a limited amount of generation at the plant in order to avoid out of step conditions for the remaining units.

4.3.1 Risk expression with GRS

- F_i : event that there is a fault on circuit i .
- A : fault type random variable. We define one phase to ground, two phase to ground, three phase to ground and phase to phase fault, represented by 1, 2, 3, 4, respectively, as all possible values of A .
- N_c : number of critical circuits.
- E_i : initiating event. The first N_c initiating events correspond to “N-1” outages, i.e., $E_i = \bar{F}_1 \cap \bar{F}_2 \cdots \bar{F}_{i-1} \cap F_i \cap \bar{F}_{i+1} \cdots \bar{F}_N$, $i=1$ to N , and the $N_c + 1$ initiating event is no fault, i.e. $E_{N_c+1} = \bar{F}_1 \cap \bar{F}_2 \cap \cdots \cap \bar{F}_{N_c}$. Initiating event $E_i, i > N_c + 1$ corresponds to simultaneous outage of two or more circuits, but we have not considered multiple outages in this report.
- K : transient instability event.
- X : pre-contingency operating point; it is a vector of critical pre-contingency controllable parameters which significantly influence the post-contingency system performance. As we consider generation level as the only critical pre-contingency parameter.
- T : GPS tripping event.
- $Risk(\cdot)$: risk of an event.

$I_m(\cdot)$: impact of an event.

$Pr(\cdot)$: probability of an event

A GRS is designed to trip some pre-selected generating unit(s) at a plant in order to prevent blackout of the entire plant. This action instantaneously reduces the electrical power input to the transmission system following the occurrence of specified contingencies. Each operation of a GRS is classified into one of the following categories:

- 1) The GRS trips when a contingency occurs $(T \cap E_i)$, $i = 1, 2, \dots, N_c$
- 2) The GRS does not trip when a contingency occurs $(\bar{T} \cap E_i)$, $i = 1, 2, \dots, N_c$
- 3) The GRS trips when there is no contingency $(T \cap E_{N_c+1})$
- 4) The GRS does not trip and there is no contingency $(\bar{T} \cap E_{N_c+1})$

According to these categories, the risk for a system with a GRS comes from three sources:

- 1) If a GRS takes action promptly and correctly as designed, system stability will be maintained, but non-zero impact will occur via a controlled trip of a block of generation capacity.
- 2) If a GRS fails to take corrective measures when armed and initiated, the plant may or may not experience an out of step condition, depending on the pre-fault operating condition, and fault type and location.
- 3) If a GRS takes an unnecessary action when there is no outage for a critical line, then non-zero impact occurs via a controlled trip of a block of generation capacity. This is called a nuisance trip.

We assume most nuisance trips are caused by failure modes inherent to the design. Therefore, variation in operating condition does not significantly influence this risk, and we concentrate on effects on evaluating the risk associated with the first two sources.

The risk of an event $E_i, i = 1, 2, \dots$, which causes either GRS trip T or instability K , is $Risk((K \cup T)/X)$. For simplicity, we drop the dependence on X , leaving the reader to be cognizant of it in what follows. Thus, the risk is

$$\begin{aligned}
 Risk(K \cup T) &= Risk(K) + Risk(T) \\
 &= \sum_{i=1}^{N_c} \Pr(K \cap \bar{T} \cap E_i) I_m(K \cap \bar{T} \cap E_i) + \sum_{i=1}^{N_c} \Pr(T \cap E_i) I_m(T \cap E_i)
 \end{aligned} \tag{4.1}$$

We discuss both the impact and probability terms in the following two subsections.

1. Impact

The impact associated with GRS failure to trip, $\bar{T}$, possibly resulting in instability K , is denoted as $Im(K \cap \bar{T} \cap E_i)$. This term reflects the same impacts of the event "instability" which include energy replacement costs, repair costs, and startup costs.

The impact associated with GRS trip, T , is denoted by $Im(T \cap E_i)$. This impact, although it does not include an instability event, is nonetheless not zero because a unit does in fact trip. This impact also includes energy replacement costs, repair costs, and startup costs. However, whereas instability causes loss of an entire plant, a controlled trip typically includes only 1 unit. Therefore, the impact of a controlled trip is usually much less than the impact of instability.

2. Probability

The probability of the GRS failure to trip, T , resulting in instability K , is denoted as $Pr(K \cap \bar{T} \cap E_i)$. Assuming that E_i may occur in any of 4 different ways, $n=1,2,3,4$, corresponding to the four basic fault types, we may expand the probability term according to

$$\begin{aligned} Pr(K \cap \bar{T} \cap E_i) &= \sum_{n=1}^4 Pr(K \cap \bar{T} \cap E_i \cap (A = n)) \\ &= \sum_{n=1}^4 Pr(\bar{T} \cap E_i \cap (A = n)) Pr(K / (\bar{T} \cap E_i \cap (A = n))) \\ &= \sum_{n=1}^4 Pr(\bar{T} \cap E_i) Pr((A = n) / (\bar{T} \cap E_i)) Pr(K / (\bar{T} \cap E_i \cap (A = n))) \end{aligned} \quad (4.2)$$

The terms $Pr(T \cap E_i)$ in (4.1) and $Pr(\bar{T} \cap E_i)$ in (4.2) are the probabilities of SPS success and failure, respectively, and are addressed in the next section.

4.3.2 SPS reliability evaluation

In this section, we develop an approach for computing $Pr(T \cap E_i)$ and $Pr(\bar{T} \cap E_i)$. This approach integrates three techniques, i.e., the Failure Modes Effects Analysis (FMEA) technique, the Markov modeling technique, and Markov model simplification techniques.

Let $S = \{S_0, S_k, \dots, S_n\}$ represent a state space of the SPS, where S_k is a set of mutually exclusive and exhaustive states. We have

$$\begin{aligned} Pr(E_i \cap T) &= Pr((E_i \cap T) \cap (S_0 \cup S_{1k} \cup \dots \cup S_n)) \\ &= \sum_{k=0}^n Pr(E_i \cap T \cap S_k) \\ &= \sum_{k=0}^n Pr(T | (E_i \cap S_k)) Pr(E_i \cap S_k) \end{aligned} \quad (4.3)$$

Since event E_i is independent of S_k , that is, the occurrence of a fault is independent of the SPS state, then

$$Pr(E_i \cap S_k) = Pr(E_i) Pr(S_k) \quad (4.4)$$

Hence,

$$\Pr(E_i \cap T) = \sum_{k=0}^n \Pr(T | (E_i \cap S_k)) \Pr(E_i) \Pr(S_k) \quad (4.5)$$

and

$$\Pr(E_i \cap \bar{T}) = \sum_{k=0}^n \Pr(\bar{T} | (E_i \cap S_k)) \Pr(E_i) \Pr(S_k) \quad (4.6)$$

Here we concentrate on the procedure for getting $\Pr(S_k)$.

Each SPS state can be in one and only one of the following four categories according to the response of each system state to system input events,

- C_1 --If the input is an active signal, then the SPS trips successfully; if the input is an inactive signal; then the SPS has a nuisance trip.
- C_2 --If the input is an active signal, then the SPS trips successfully; if the input is an inactive signal; then the SPS does not trip, as expected.
- C_3 --If the input is an active signal, then the SPS fails to trip; if the input is an inactive signal; then the SPS has a nuisance trip.
- C_4 --If the input is an active signal, then the SPS fails to trip; if the input is an inactive signal, then the SPS does not trip, as expected.

These four categories comprise another state space of the SPS where the original states S_k ($k=0, 1 \dots n$) have been condensed to C_j ($j=1, 2, 3, 4$). Based on this state space, we have

$$\Pr(E_i \cap T) = \sum_{j=1}^4 \Pr(T | (E_i \cap C_j)) \Pr(E_i) \Pr(C_j) \quad (4.7)$$

and

$$\Pr(E_i \cap \bar{T}) = \sum_{j=1}^4 \Pr(\bar{T} | (E_i \cap C_j)) \Pr(E_i) \Pr(C_j) \quad (4.8)$$

Each basic input event E_i belongs to a group either active (denoted as AC) or inactive (denoted as $\overline{AC}$). The active input is the input that triggers SPS to trip, and the inactive input is the input that does not activate tripping. Given basic input event E_i and C_j , the system output event is completely determined. Therefore, the conditional probability term in (4.5) and (4.6) is 0 or 1 as expressed in (4.9).

$$E_i \subset AC \Rightarrow \begin{cases} \Pr(T | (E_i \cap C_j)) = \begin{cases} 1 & j = 1,2 \\ 0 & j = 3,4 \end{cases} \\ \Pr(\bar{T} | (E_i \cap C_j)) = \begin{cases} 1 & j = 3,4 \\ 0 & j = 1,2 \end{cases} \end{cases} \quad (4.9)$$

and

$$E_i \subset \overline{AC} \Rightarrow \begin{cases} \Pr(T | (E_i \cap C_j)) = \begin{cases} 1 & j = 1,3 \\ 0 & j = 2,4 \end{cases} \\ \Pr(\bar{T} | (E_i \cap C_j)) = \begin{cases} 1 & j = 2,4 \\ 0 & j = 1,3 \end{cases} \end{cases} \quad (4.10)$$

The remaining question is how to calculate the value of $\Pr(C_j)$ ($j=1,2,3,4$); once this is done, then each term on the right hand side of (4.5) and (4.6) can be calculated. Thus the values of $\Pr(T \cap E_i)$, $\Pr(\bar{T} \cap E_i)$ can be obtained.

4.3.3 State probabilities

There are six essential steps in evaluating the probability of each state, $\Pr(C_j)$. We provide a simple description for each step in what follows.

Step 1: Describe the system

There are two sub-steps. The first is to develop a logic block diagram of the understudy SPS. The second is to identify the event to input mapping table, in which we list all possible system input events together with the binary signal input to the SPS. In addition, we classify inputs as “active” or “inactive.” An active event is one that should cause SPS activation; an inactive event is one that should not.

Step 2: Identify the failure modes

We define that a component fails when the component cannot perform its predefined functions. In this step, we use a procedure that is similar to a failure mode and effect analysis (FMEA). We assume that there are two failure modes for each logic gate: output stuck on 1 (mode 1) or output stuck on 0 (mode 2). We do not consider the possibility of having a failure mode such that the output is always the complement of that which it is supposed to be.

Step 3: Define the system states

System states are represented by the combinations of states of all system components. Given that we have defined the modes, e.g.,

0--normal mode

1--failure mode 1

2--failure mode 2

Then we can define the state space of the system as the set of components where each component may be in any of its modes. At this step, it may be possible to merge some states based on physical observation of the system.

Step 4: Classify the states

The Markov model should be simplified as much as possible to retain simplicity. So we classify states into categories, according to some criteria. For GRS, we can classify system states into C_1 , C_2 , C_3 , and C_4 according to the response of each system state to system input events.

Step 5: Reduce the states

We introduce two concepts

- A transition state is a state that has non-zero entry transition probability from other state(s) and non zero exit transition probability to other state(s).
- An absorbing state is a state that has a 1.0 transition probability to itself.

The reduction steps are as follows

- Merge absorbing state belonging to the same category. Entry transition probabilities are added.
- For each absorbing state, eliminate all preceding states that are in the same class C_i as the absorbing state have only one exit transition probability. Add the entry probabilities as the entry probabilities to the absorbing states.
- Merge all transition states in the same class C_j that have identical transition probabilities to common states. Entry probabilities are added. Exit probabilities remain the same.

Step 6: Calculate state probabilities

We assume that the failure of the SPS components has approximately an exponential distribution. Therefore the pdf of component failure is $f(t) = \lambda e^{-\lambda t}$, where λ is the failure rate per unit time interval. Then the probability that the component fails before time t is

$$F(t) = \int_0^t \lambda e^{-\lambda t} dt = 1 - e^{-\lambda t} \quad (4.11)$$

When λt is small, $F(t)$ can be approximated by λt , so

$$F(t) \approx \lambda t \quad (4.12)$$

With this model, we can write a $n+1$ by $n+1$ transition matrix B , where B_{pq} ($p=0, 1, \dots, n$, $q=0, 1, \dots, n$) indicates the probability that the system transfers from state S_p to S_q , and n =the number of states.

Assume the probability list at initial time $t=t_0$ is

$$\text{Pr}^{(0)} = (\text{Pr}(S_0'(t_0)) \quad \text{Pr}(S_k'(t_0)) \quad \dots \quad \text{Pr}(S_n'(t_0))), \quad (4.13)$$

After v time intervals, the probability list is

$$\text{Pr}^{(v)} = \text{Pr}^{(0)} \times B^v = (\text{Pr}(S_0'(t_v)) \quad \text{Pr}(S_k'(t_v)) \quad \dots \quad \text{Pr}(S_n'(t_v))) \times B^v \quad (4.14)$$

The elements in the probability list $\text{Pr}^{(v)} = (\text{Pr}(S_0'(t_v)) \quad \text{Pr}(S_k'(t_v)) \quad \dots \quad \text{Pr}(S_n'(t_v)))$ provide the probability that system is in state S_k' after v time intervals. Then we get

$$\begin{aligned}
\Pr(C_1) &= \sum \Pr(S_k') \quad S_k' \in C_1 \\
\Pr(C_2) &= \sum \Pr(S_k') \quad S_k' \in C_2 \\
\Pr(C_3) &= \sum \Pr(S_k') \quad S_k' \in C_3 \\
\Pr(C_4) &= \sum \Pr(S_k') \quad S_k' \in C_4
\end{aligned} \tag{4.15}$$

This concludes the description of the procedure used to obtain $\Pr(C_j)$. Once obtained, these values are used in (4.5) and (4.6) to compute $\Pr(E_i \cap T)$ and $\Pr(E_i \cap \bar{T})$, respectively.

4.4 Risk assessment of generation rejection scheme

In this section, we will use Markov model to assess SPS reliability and operation risk. We take generator rejection scheme as example to illustrate the approach. Generator rejection scheme is one of the widely used special protection scheme by the industry. According to a survey by industries it the most widely used special protection scheme employed by utilities accounting for about 21.6% of all the special protection schemes used. Therefore proper reliability evaluation of the generation rejection scheme is very important in reliability evaluation of special protection schemes. The generator rejection scheme is designed to improve the transient stability performance of a power system. Figure 24 shows a portion of the IEEE Reliability Test System together with an illustration of the GRS logic. Line 12--13 and line 13--23 are critical lines. The way the generation rejection scheme works is that When the GRS detects a line outage on either of these two lines, it trips promptly only one generator to keep the other two generators in service. The way the GRS logic works is that when there is a fault on a critical line, the breakers on this line open; an «open» signal (high level signal) from any breaker energizes the output of the OR gate. The high level signal from the OR gate output, together with the high level arming signal, sets the AND gate output in high level, which is input to the 2 out of 3 voting scheme. When two or more of the voting scheme input signals are high, the voting scheme output signal is high; otherwise, it is low. The high level signal from the voting scheme will trip the selected generator [105].

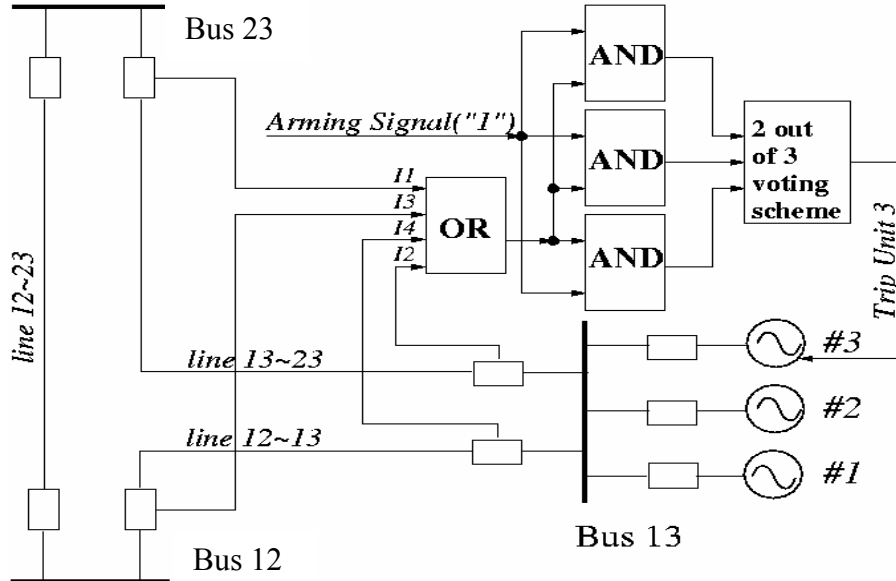


Figure 24: Logic circuit for a GRS

4.4.1 Illustration

Markov modeling is one of the methods used to compute the reliability of safety instrumented systems (SIS). Markov models can be used to compute probability of failure on demand of an SIS and a detailed example is shown in [110]. In this section, this method has been applied for a generation rejection scheme.

Notation

λ_{DD} = Logic gate failure rate for detected failure

λ_{DU} = Logic gate failure rate for undetected failure

μ = Repair rate for detected failure per year

μ_T = Repair rate for undetected failure per year

1. Failure modes

- 1 - OR gate has failed
- 2- Two AND gates have failed

2. Component failure and repair rate

Table 9: Component failure and repair rate

Notation	Rate
λ_{DD}	0.02 (once in 50 years)
λ_{DU}	0.01 (once in 100 years)
μ	1460(6 hours per year)
μ_T	2(6 months time interval test)

3. Markov Model For Failure mode 1

For failure mode 1, there are 3 states as shown in Figure 25.

01: OR gate is working normally

11: OR gate has failed and failure is detected

21: OR gate has failed but the failure is not detected

where, state 21 is most severe

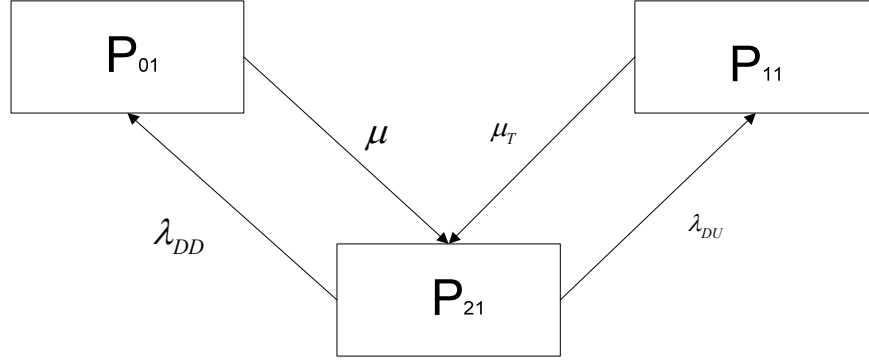


Figure 25: Markov model for failure mode 1

The steady-state equations are:

$$\begin{aligned}
 -(\lambda_{DD} + \lambda_{DU})P_{01} + \mu P_{11} + \mu_T P_{21} &= 0 \\
 -\mu P_{11} + \lambda_{DD} P_{01} &= 0 \\
 -\mu_T P_{21} + \lambda_{DU} P_{01} &= 0 \\
 P_{01} + P_{11} + P_{21} &= 1
 \end{aligned} \tag{4.16}$$

In (4.16), adding last equation to first equation we get,

$$(1 - \lambda_{DD} - \lambda_{DU})P_{01} + (\mu + 1)P_{11} + (\mu_T + 1)P_{21} = 1 \tag{4.17}$$

Then, the probability of each state can be calculated by:

$$\begin{bmatrix} P_{01} \\ P_{11} \\ P_{21} \end{bmatrix} = \begin{bmatrix} 0.97 & 1461 & 3 \\ 0.02 & -1460 & 0 \\ 0.01 & 0 & -2 \end{bmatrix}^{-1} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0.9950 \\ 1.3630 \times 10^{-5} \\ 4.9750 \times 10^{-4} \end{bmatrix} \tag{4.18}$$

As we can see, the probability of the most severe state 21, P_{21} is low. To reduce the probability of the state 21, the redundancy of the OR gate can be employed.

4. Markov Model For Failure mode 2

In the Markov model shown in Figure 26, four states are identified:

- 02: All AND gates are working normally)
- 12: One AND gate has failed and failure is detected
- 22: One AND gate has failed but the failure is not detected
- 32: Sub -system is in the fail state and the condition is detected (2 AND gates has failed)
- 42: Sub -system is in the fail state and the condition is not detected (2 AND gates has failed)

where, the state 42 is most severe.

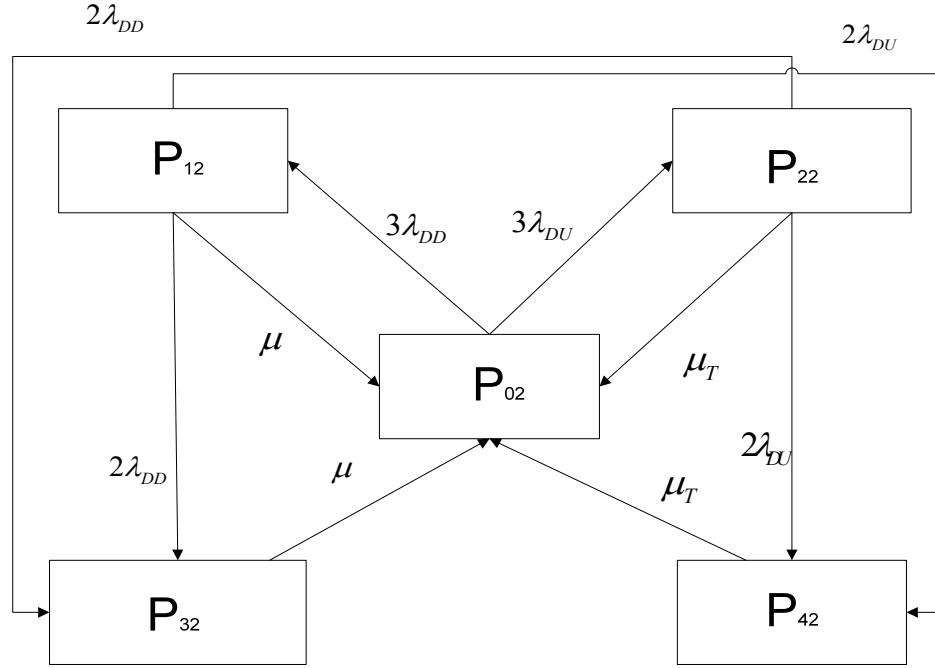


Figure 26: Markov model for failure mode 2

The corresponding steady-state equations are:

$$\begin{aligned}
 &-(3\lambda_{DD} + 3\lambda_{DU})P_{02} + \mu P_{12} + \mu_T P_{22} + \mu P_{32} + \mu_T P_{42} = 0 \\
 &3\lambda_{DD}P_{02} - (2\lambda_{DD} + 2\lambda_{DU} + \mu)P_{12} = 0 \\
 &3\lambda_{DU}P_{02} - (2\lambda_{DD} + 2\lambda_{DU} + \mu_T)P_{22} = 0 \\
 &2\lambda_{DD}P_{12} + 2\lambda_{DD}P_{22} - \mu P_{32} = 0 \\
 &2\lambda_{DU}P_{12} + 2\lambda_{DU}P_{22} - \mu_T P_{42} = 0 \\
 &P_{02} + P_{12} + P_{22} + P_{32} + P_{42} = 1
 \end{aligned} \tag{4.19}$$

In the set of equations of (4.19), adding 4th equation to 1st equation, we get

$$(1 - (3\lambda_{DD} + 3\lambda_{DU}))P_{02} + (\mu + 1)P_{12} + (\mu_T + 1)P_{22} + (\mu + 1)P_{32} + (\mu_T + 1)P_{42} = 1 \tag{4.20}$$

Then, the probabilities of each state can be calculated by:

$$\begin{bmatrix} P_{02} \\ P_{12} \\ P_{22} \\ P_{32} \\ P_{42} \end{bmatrix} = \begin{bmatrix} 0.91 & 1461 & 3 & 1461 & 3 \\ 0.06 & -1460.06 & 0 & 0 & 0 \\ 0.03 & 0 & -2.06 & 0 & 0 \\ 0 & 0.04 & 0.02 & -1460 & 0 \\ 0 & 0.02 & 0.04 & 0 & -3 \end{bmatrix}^{-1} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0.9856 \\ 4.0503 \times 10^{-5} \\ 1.4353 \times 10^{-2} \\ 1.9773 \times 10^{-7} \\ 1.9165 \times 10^{-4} \end{bmatrix} \tag{4.21}$$

As we can see, the probability of the most severe state 42, P_{42} is low because the 2oo3 logic improves the reliability by redundancy design. This result verified that redundancy is an effective way to improve the reliability.

5. Combination of the failure modes

With the increase of number of components, the states increase exponentially that renders system reliability assessment by Markov modeling time consuming. To simplify the computation, the failure modes are combined. In the failure mode 1, we have 3 states and in the failure mode 2, we have 5 states. Altogether we have 15 states as outlined below, with their probabilities given in Table 10.

0102: All gates are working normally

0112: OR gates are working and 1 AND gate has failed and is detected (fail safe)

0122: OR gate is working and 1 AND gate has failed and is undetected (fail safe undetected)

0132: OR gates are working and 2 AND gates have failed and the condition is detected (system fail detected)

0142: OR gate is working and 2 AND gates have failed and the condition is undetected (system fail detected)

1102: OR gate has failed and failure is detected, and all AND gates are working (system fail detected)

1112: OR gate has failed and failure is detected, and 1 AND gate has failed and is detected (system fail detected)

1122: OR gates have failed and failure is detected, and 1 AND gate has failed and is undetected (system fail detected)

1132: OR gates have failed and failure is detected, and 2 AND gates have failed and is detected (system fail detected)

1142: OR gates have failed and failure is detected, and 2 AND gates have failed and is detected (system fail detected)

2102: OR gate has failed and failure is undetected, and all AND gates are working (system fail undetected)

2112: OR gate has failed and failure is undetected, and 1 AND gate has failed and is detected (system fail undetected)

2122: OR gate has failed and failure is undetected, and 1 AND gate has failed and is undetected (system fail undetected)

2132: OR gate has failed and failure is undetected, and 2 AND gates have failed and is detected (system fail undetected)

2142: OR gate has failed and failure is undetected, and 2 AND gates have failed and is detected (system fail undetected)

Table 10: Probability of each state

State	Probability
0102	0.980547605350883
0112	0.000040294820980
0122	0.014279819495401
0132	0.000000392331899
0142	0.000143201143164
1102	1.343215897755340e-005
1112	5.519838491000001e-010
1122	1.956139656925000e-007
1132	5.374409600000000e-012
1142	1.961659495400000e-009
2102	0.004902738026755
2112	2.0146e-007
2122	7.1394e-005
2132	1.9615e-009
2142	7.1595e-007

After the model is simplified by combining the states, the probabilities of each state are shown in the Table 11.

Table 11: Probability of each state of simplified model

States	Probability
All gates are working	0.980547605350883
Fail safe	0.000040294820980
Fail safe undetected	0.014279819495401
Fail detected	1.3228e-004
Fail undetected	0.0050

According to the simplified Table 11, we are going to assume that P (fail undetected) is the probability when the system is unsecure. From the previous results, we can see that the 2oo3 component increases the system reliability of the GRS, and the GRS itself has a high reliability as all the gates are working normally during 98.05% of the time.

Next section presents some future developments in SPS, especially about the process and the architecture getting strengthened by the use of Phasor Measurement Unit (PMU). This in turn promises increase in 'process view' SPS reliability.

4.5 Consideration for future SPS developments

As the era of the so-called "Smart Grid" emerges, the instrumentation, monitoring, control, and protection systems in power industry are facing potentially significant changes due to the penetration of information-age technologies. These technologies include but are not limited to digital signal processing and digital communication, etc. With the development of powerful microprocessors, the trend has been for digital systems to replace the analog ones and the

application of computer relays is such an example. Digital communication plays an important role in the development of digital systems and it is possible to see in the future that bundles of copper wires could be replaced by digital communication equipments such as Ethernet switches and Ethernet media.

In addition, non-conventional instrument transformers have already been available which can directly output digital signals of current and voltage measurements [111]. The synchronized phasor measurement unit (PMU) can provide real-time information of phasors for the same time stamp and will be the foundation of various kinds of wide-area protection and control schemes [112].

It is also notable that a new concept of digital process bus has been raised in IEC 61850 [113]. With the development of intelligent electronic devices (IED), a “one unique” secondary platform based on IEC 61850, called merging unit (MU), has been developed to interface all IED such as protections, meters and control devices, etc [114]. It seems that the power industry is getting ready for more aggressive steps by replacing switchyard hardwired schemes with plug-and-play fiber-based virtual wiring solutions [115].

The SPS can be regarded as one kind of protection and control systems with special protection purposes. Hence, its development is also likely to be exposed to the potential changes mentioned above from the perspective of its constituent elements. For example, microprocessors can prevail in the future for the choice of SPS logic solvers because their functions become more and more powerful while the costs decrease rapidly. Although the sensor and the actuator are different in functions, their data flow can be integrated in the same platform of merging unit with the help of functional IED. If PMU is utilized as the measurement device, the synchrophasors of voltage and current can be easily obtained and then sent to merging units for data process.

We can see that a possible SPS scheme in the future can be typically composed of digital logic solvers, merging units (including auxiliary IED), PMU, Ethernet switches, and Ethernet communication media. All the signals in them are digitally conveyed through a virtual process bus. Since the all-digital SPS scheme has obviously more electronic components than a conventional hardwired one, it should have some influence on its reliability. Yang Wang et. al. have made considerable contributions towards quantitative reliability evaluation of PMU and WAMS [116, 117, 118], two primary drivers for SPS advancements. The following section presents a way to analyze the possible impacts on SPS considering these developments.

4.5.1 Possible SPS architecture

The all-digital SPS can have a variety of complex structures in the future. However, some architecture of all-digital protection systems has already been proposed [119]. Based on the idea of these configurations, we propose conceptual all-digital SPS architecture possible in the future as shown in Figure 27.

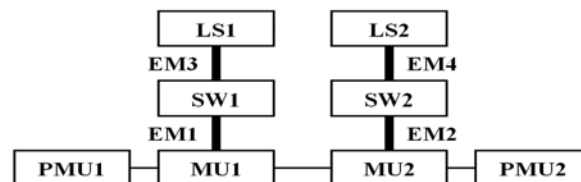


Figure 27: A conceptual all-digital SPS architecture

In this architecture, the SPS consists of two redundant functional sets which are independent of each other. Each set comprises a digital logic solver (LS), an Ethernet switch (SW), Ethernet communication media (EM), merging units (MU), and phasor measurement units (PMU). Specifically, components LS1, EM3, SW1, EM1, MU1, and PMU1 constitute one set of SPS while components LS2, EM4, SW2, EM2, MU2, and PMU2 make up the other set. In addition, the PMU of the two sets, i.e. PMU1 and PMU2 are shared with each other and can act as mutual backup. For simplicity, we assume that one PMU/MU alone can perform the full function needed for one set of SPS, instead of several units actually needed for processing different signals, respectively. We also assume that the Ethernet interface is part of the host device (i.e. LS, SW, MU, etc.) and its reliability is already included in the host device.

The main functional parts of SPS can be designed to be allocated in physically isolated places against mutual interference and fire spreading. Also, every set of SPS can be designed to be supplied by multiple power sources simultaneously, including AC, batteries, and UPS. Hence, we assume its power supplies to be extremely reliable against common cause failure of components due to power supply failures. Therefore, we assume for simplicity that components of the all-digital SPS are independent of each other. In addition, the component state durations are assumed to be exponentially distributed.

As we know, if there is any fault with the component recognized by either self-test routine or manual test procedure, utilities would either fix or replace the problematic component so as to keep the whole protection and control system up. Thus, we will analyze the proposed SPS scheme with a repairable model. Since the estimated repair time for any failed equipment is usually prescribed in power industry and the maintenance staff always conforms to this guideline, we can assume constant repair rates for our repairable model.

Although we only illustrate the reliability analysis of the SPS scheme in Figure 27, we emphasize the methodology to obtain important reliability indices such as state probability of system failures, frequency of system failures, the mean time to failure (MTTF) and the mean time to first failure (MTTFF). Therefore, similar analysis can be conducted for other possible SPS configurations.

4.5.2 Illustration of network reduction method

According to the relationship of the functional components, the reliability block diagram of the SPS architecture in Figure 27 can be drawn as shown in Figure 28. In general, it is not easy to obtain the reliability indices directly for such a complex system. However, we can use the network reduction method to analyze the system.

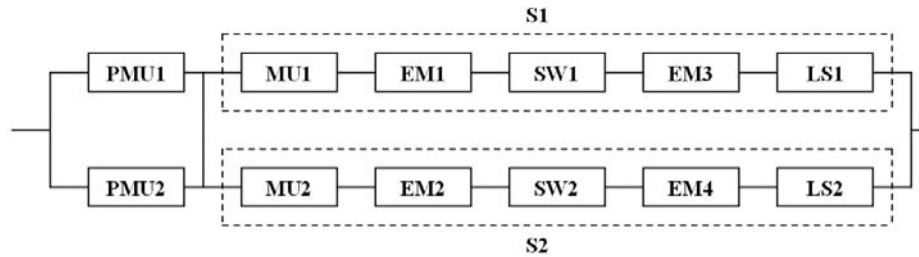


Figure 28: SPS reliability block diagram

As we can see in Figure 28, components MU1, EM1, SW1, EM3, and LS1 comprise the subsystem S1 of a series structure. If we regard S1 as a composite component using the concept of equivalent transition rates [120], this composite component will have the same values of failure and repair rates, state probabilities of success and failure, and frequencies to success and failure with the original subsystem, respectively. Similarly, we can use another composite component to represent the series subsystem S2 formed by components MU2, EM2, SW2, EM4, and LS2. Then the reliability block diagram is reduced to a simpler one as shown in Figure 29.

Here we represent the failure and repair rates of a general component i by λ_i and μ_i , respectively. In addition, we use $p_{i,s}, p_{i,f}$ and $f_{i,s}, f_{i,f}$ for component i to represent the state probabilities of its success and failure, and the frequencies to its state of success and failure, respectively. Then the equivalent reliability parameters for subsystems S1 and S2 can be calculated as following.

The state probabilities of success are

$$p_{S1,s} = p_{MU1,s} p_{EM1,s} p_{SW1,s} p_{EM3,s} p_{LS1,s} = \prod_{i \in S1} \frac{\mu_i}{\lambda_i + \mu_i}, \quad S1 = \{MU1, EM1, SW1, EM3, LS1\} \quad (4.22)$$

$$p_{S2,s} = p_{MU2,s} p_{EM2,s} p_{SW2,s} p_{EM4,s} p_{LS2,s} = \prod_{i \in S2} \frac{\mu_i}{\lambda_i + \mu_i}, \quad S2 = \{MU2, EM2, SW2, EM4, LS2\} \quad (4.23)$$

The state probabilities of failure are

$$p_{S1,f} = 1 - p_{S1,s} = 1 - \prod_{i \in S1} \frac{\mu_i}{\lambda_i + \mu_i}, \quad S1 = \{MU1, EM1, SW1, EM3, LS1\} \quad (4.24)$$

$$p_{S2,f} = 1 - p_{S2,s} = 1 - \prod_{i \in S2} \frac{\mu_i}{\lambda_i + \mu_i}, \quad S2 = \{MU2, EM2, SW2, EM4, LS2\} \quad (4.25)$$

The equivalent failure rates are

$$\lambda_{S1} = \sum_{i \in S1} \lambda_i, \quad S1 = \{MU1, EM1, SW1, EM3, LS1\} \quad (4.26)$$

$$\lambda_{S2} = \sum_{i \in S2} \lambda_i, \quad S2 = \{MU2, EM2, SW2, EM4, LS2\} \quad (4.27)$$

The frequencies to state of success and failure are

$$f_{S1,s} = f_{S1,f} = p_{S1,s} \lambda_{S1} = \left(\prod_{i \in S1} \frac{\mu_i}{\lambda_i + \mu_i} \right) \left(\sum_{i \in S1} \lambda_i \right), \quad S1 = \{MU1, EM1, SW1, EM3, LS1\} \quad (4.28)$$

$$f_{S2,s} = f_{S2,f} = p_{S2,s} \lambda_{S2} = \left(\prod_{i \in S2} \frac{\mu_i}{\lambda_i + \mu_i} \right) \left(\sum_{i \in S2} \lambda_i \right), \quad S2 = \{MU2, EM2, SW2, EM4, LS2\} \quad (4.29)$$

The equivalent repair rates are

$$\mu_{S1} = \frac{f_{S1,s}}{p_{S1,f}} = \left(\prod_{i \in S1} \frac{\mu_i}{\lambda_i + \mu_i} \right) \left(\sum_{i \in S1} \lambda_i \right) / \left(1 - \prod_{i \in S1} \frac{\mu_i}{\lambda_i + \mu_i} \right), \quad S1 = \{MU1, EM1, SW1, EM3, LS1\} \quad (4.30)$$

$$\mu_{S2} = \frac{f_{S2,s}}{p_{S2,f}} = \left(\prod_{i \in S2} \frac{\mu_i}{\lambda_i + \mu_i} \right) \left(\sum_{i \in S2} \lambda_i \right) / \left(1 - \prod_{i \in S2} \frac{\mu_i}{\lambda_i + \mu_i} \right), \quad S2 = \{MU2, EM2, SW2, EM4, LS2\} \quad (4.31)$$

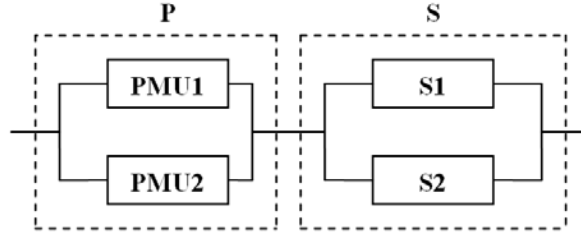


Figure 29: Reduction of SPS reliability block diagram

Now let us see the reduced SPS reliability block diagram of Figure 29. There are two parallel structures in this diagram, i.e. components PMU1 and PMU2 comprise one parallel subsystem P while the composite components S1 and S2 form the other parallel subsystem S. Again, if we regard these two subsystems as two composite components in a higher level, we can further simplify the SPS reliability block diagram to a much concise one as shown in Figure 30. By the concept of equivalent transition rates, the new higher-level composite components will have the same values of transition rates, state probabilities, and corresponding frequencies with the original subsystems P and S, respectively. The equivalent reliability parameters for higher-level subsystems P and S can be calculated as follows.

The state probabilities of failure are

$$p_{P,f} = p_{PMU1,f} p_{PMU2,f} = \prod_{i \in P} \frac{\lambda_i}{\lambda_i + \mu_i}, \quad P = \{PMU1, PMU2\} \quad (4.32)$$

$$p_{S,f} = p_{S1,f} p_{S2,f} = \prod_{i \in S} \frac{\lambda_i}{\lambda_i + \mu_i}, \quad S = \{S1, S2\} \quad (4.33)$$

The state probabilities of success are

$$p_{P,s} = 1 - p_{P,f} = 1 - \prod_{i \in P} \frac{\lambda_i}{\lambda_i + \mu_i}, \quad P = \{PMU1, PMU2\} \quad (4.34)$$

$$p_{S,s} = 1 - p_{S,f} = 1 - \prod_{i \in S} \frac{\lambda_i}{\lambda_i + \mu_i}, \quad S2 = \{S1, S2\} \quad (4.35)$$

The equivalent repair rates are

$$\mu_P = \sum_{i \in P} \mu_i, \quad P = \{PMU1, PMU2\} \quad (4.36)$$

$$\mu_S = \sum_{i \in S} \mu_i, \quad S = \{S1, S2\} \quad (4.37)$$

The frequencies to state of failure and success are

$$f_{P,f} = f_{P,s} = p_{P,f} \mu_P = \left(\prod_{i \in P} \frac{\lambda_i}{\lambda_i + \mu_i} \right) \left(\sum_{i \in P} \mu_i \right), \quad P = \{PMU1, PMU2\} \quad (4.38)$$

$$f_{S,f} = f_{S,s} = p_{S,f} \mu_S = \left(\prod_{i \in S} \frac{\lambda_i}{\lambda_i + \mu_i} \right) \left(\sum_{i \in S} \mu_i \right), \quad S = \{S1, S2\} \quad (4.39)$$

The equivalent failure rates are

$$\lambda_P = \frac{f_{P,f}}{p_{P,s}} = \left(\prod_{i \in P} \frac{\lambda_i}{\lambda_i + \mu_i} \right) \left(\sum_{i \in P} \mu_i \right) / \left(1 - \prod_{i \in P} \frac{\lambda_i}{\lambda_i + \mu_i} \right), \quad P = \{PMU1, PMU2\} \quad (4.40)$$

$$\lambda_S = \frac{f_{S,f}}{p_{S,s}} = \left(\prod_{i \in S} \frac{\lambda_i}{\lambda_i + \mu_i} \right) \left(\sum_{i \in S} \mu_i \right) / \left(1 - \prod_{i \in S} \frac{\lambda_i}{\lambda_i + \mu_i} \right), \quad S = \{S1, S2\} \quad (4.41)$$

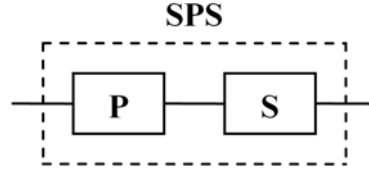


Figure 30: Simplified SPS reliability block diagram

The simplified SPS reliability block diagram of Figure 30 consists of only two composite components in series. Thus, it is now easy to get the reliability indices of the whole system of SPS using the parameters of composite components derived previously.

The system reliability of SPS (i.e. state probability of SPS success) is

$$p_{SPS,s} = p_{P,s} p_{S,s} = \frac{\mu_P \mu_S}{(\lambda_P + \mu_P)(\lambda_S + \mu_S)} \quad (4.42)$$

The system unavailability of SPS (i.e. state probability of SPS failure) is

$$p_{SPS,f} = 1 - p_{SPS,s} = \frac{\lambda_P \lambda_S + \lambda_P \mu_S + \lambda_S \mu_P}{(\lambda_P + \mu_P)(\lambda_S + \mu_S)} \quad (4.43)$$

The system failure rate of SPS is

$$\lambda_{SPS} = \lambda_P + \lambda_S \quad (4.44)$$

The frequency of SPS system failure is

$$f_{SPS,f} = p_{SPS,s} \lambda_{SPS} = \frac{\mu_P \mu_S (\lambda_P + \lambda_S)}{(\lambda_P + \mu_P)(\lambda_S + \mu_S)} \quad (4.45)$$

The mean cycle time of SPS is

$$T_{SPS} = \frac{1}{f_{SPS,f}} = \frac{(\lambda_P + \mu_P)(\lambda_S + \mu_S)}{\mu_P \mu_S (\lambda_P + \lambda_S)} \quad (4.46)$$

The mean down time (MDT) of SPS is

$$MDT_{SPS} = \frac{p_{SPS,f}}{f_{SPS,f}} = \frac{\lambda_P \lambda_S + \lambda_P \mu_S + \lambda_S \mu_P}{\mu_P \mu_S (\lambda_P + \lambda_S)} \quad (4.47)$$

The mean time to failure (MTTF), i.e. the mean up time (MUT) of SPS is

$$MTTF_{SPS} = MUT_{SPS} = T_{SPS} - MDT_{SPS} = \frac{1}{\lambda_{SPS}} = \frac{1}{\lambda_p + \lambda_s} \quad (4.48)$$

4.5.3 Illustration of Markov modeling method to calculate MTTF

The mean time to first failure (MTTFF) is also an important reliability index. It represents the mean value of time from the moment the system starts operating until it fails for the first time. MTTFF is actually the concept of the first passage time applied to the reliability engineering field. However, it cannot be obtained from the previous network reduction method. In fact, the calculation of MTTFF is more complex than that of MTTF. Based on the model of continuous parameter Markov chains, we can derive the ultimate formula for calculating MTTFF using the transition rate matrix of the system as follows [121].

$$MTTFF = p_+(0)(-R_{11})^{-1}U_k \quad (4.49)$$

Here, R_{11} is the sub-matrix of the full system transition rate matrix $R = \begin{bmatrix} R_{11} & R_{12} \\ R_{21} & R_{22} \end{bmatrix}$ and represents the set of transition rates from system success to system success. $p_+(0)$ is the probability row vector of system success states for the initial state (all components up), while U_k is the unit column vector of dimension k which is equal to the number of states of system success.

In practice it is not simple to utilize this formula for computing the MTTFF of the SPS. We do not know how many success states this SPS would have just by looking at the system structure. We only know that the total number of states of this SPS is $2^{12} = 4096$ since the system consists of 12 components. In addition, it seems that we also cannot give the details of vectors $p_+(0)$ and U_k unless we know the number of states of system success, or the dimension of the matrix R_{11} . But the details of R_{11} are even more difficult to know. So, we must use a systematic strategy to obtain the MTTFF value of our SPS. The key issue is that we can get R_{11} after we obtain the full system transition rate matrix R which is $2^{12} \times 2^{12}$ in its size. The strategy to achieve this is illustrated in the following steps.

Step I: Initializing the state matrix

In order to analyze the system states, we initially form a state matrix which can represent the status of the system and all of its components. In this state matrix, each row represents a distinct state of the system and each column represents a component state. For a system consisting of n components, the size of this state matrix would be $2^n \times n$. For our SPS to be analyzed, this state matrix size is $2^{12} \times 12$. Now every element of this matrix represents the status of a component in a specific system state. If we use the values 0 and 1 indicating the success and failure states of a component, respectively, the complete system states can be represented by this state matrix consisting of exhaustive combinations of 0's and 1's. We can arrange an initial state matrix as shown in Table 12.

Table 12: The initial state matrix

Components	PMU1	MU1	EM1	SW1	EM3	LS1	PMU2	MU2	EM2	SW2	EM4	LS2
State 0001	0	0	0	0	0	0	0	0	0	0	0	0
State 0002	0	0	0	0	0	0	0	0	0	0	0	1
State 0003	0	0	0	0	0	0	0	0	0	0	1	0
State 0004	0	0	0	0	0	0	0	0	0	0	1	1
State 0005	0	0	0	0	0	0	0	0	0	1	0	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
State 4092	1	1	1	1	1	1	1	1	1	0	1	1
State 4093	1	1	1	1	1	1	1	1	1	1	0	0
State 4094	1	1	1	1	1	1	1	1	1	1	0	1
State 4095	1	1	1	1	1	1	1	1	1	1	1	0
State 4096	1	1	1	1	1	1	1	1	1	1	1	1

Step II: Identifying system states of success and failure

Since we can draw the reliability block diagram as shown in Figure 28, it is natural to think that we can use the minimal cut set method to distinguish system states of success and failure. The method could be carried out in three steps: Firstly, we find all the minimal cut sets of the system. Secondly, we use minimal cut sets to find all the system states of failure. Finally, the rest of the states represent system success. However, this method is not smart and convenient for our SPS architecture to be analyzed. For one reason, it is not easy to find out all the minimal cut sets if the number of components of the system is relatively large. For another reason, there will be some overlapping system states of failure based on different minimal cut sets. Unless we can identify all the overlapping states, this method is likely to yield a wrong number of system states of failure.

Here we propose a better way to distinguish states of success and failure for our SPS. Although this method is also based on the concept of cut set, the main difference is that we do not need to search all the minimal cut sets of the system. Since the reliability block diagram of this SPS can be decomposed into combinations of simpler series and parallel structures, we can get the logical chain of the system as shown in Figure 31.

$$\text{SPS fails} \Leftrightarrow \left\{ \begin{array}{l} \text{(P) fails} \Leftrightarrow \left\{ \begin{array}{l} \text{(PMU1) fails} \\ \text{AND} \\ \text{(PMU2) fails} \end{array} \right. \\ \text{OR} \\ \text{(S) fails} \Leftrightarrow \left\{ \begin{array}{l} \text{(S1) fails} \Leftrightarrow \text{(MU1) OR (EM1) OR (SW1) OR (EM3) OR (LS1) fails} \\ \text{AND} \\ \text{(S2) fails} \Leftrightarrow \text{(MU2) OR (EM2) OR (SW2) OR (EM4) OR (LS2) fails} \end{array} \right. \end{array} \right.$$

Figure 31: System logical chain of the SPS

In the previous Step I of initializing the state matrix, we have already used the values 0 and 1 indicating the success and failure states of a component, respectively. Now in the logical chain of Figure 31, let us replace each component by its state value (0 or 1) and treat the relationship conditions "AND" and "OR" as the corresponding logical operation symbols. Thus, the logical chain of Figure 31 is translated into a Boolean calculation. And the final result of the Boolean calculation is just the indication of the system state, i.e. the value 0 of "SPS fails" indicates the

system success and the value 1 of "SPS fails" as system failure. If we scan each row of the initial state matrix already setup in Step I and do the Boolean calculation, all the system states can be distinguished as success or failure without omission or overlapping.

For our SPS architecture to be analyzed, the number of states of system success and failure are counted to be 189 and 3907, respectively. After all the system states are identified, we can reorder the initial state matrix in a better form as shown in Table 13. All the system states of success are moved to the first 189 rows of the state matrix and all the system states of failure are gathered in the latter part of 3907 rows. This rearrangement will be better for use in the following steps.

Table 13: The rearranged state matrix

	Components	PMU1	MU1	EM1	SW1	EM3	LS1	PMU2	MU2	EM2	SW2	EM4	LS2
Success	State 0001	0	0	0	0	0	0	0	0	0	0	0	0
	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
	State 0189	1	1	1	1	1	1	0	0	0	0	0	0
Failure	State 0190	0	0	0	0	0	1	0	0	0	0	0	1
	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
	State 4096	1	1	1	1	1	1	1	1	1	1	1	1

Step III: Forming the full system transition rate matrix R

Since we have identified all the states of system success and failure and rearranged the state matrix, it is now possible to obtain the full system transition rate matrix R . However, the diagonal and off-diagonal elements of the transition rate matrix R are very different. They represent single-step transition rates from a given state to itself and to another state, respectively. As a strategy, we need to get the off-diagonal elements of the transition rate matrix R first and then obtain the diagonal elements from the off-diagonal ones.

It is recognized that there are two types of relationships between any two system states [122]. Suppose we choose two arbitrary system states i and j . If we need at least two components to change their status for a transition between system states i and j , the interstate relationship is not a single-step transition and thus the corresponding transition rates do not exist, i.e. the elements (i, j) and (j, i) of the matrix R are both zeroes. If, however, there is only one component, say component k , that changes its status between system states i and j , then the interstate relationship is indeed a single-step transition and the corresponding transition rates do exist. Further in this case, if component k is working in system state i and fails in system state j , then the transition rate from state i to j is the failure rate of component k , i.e. the element (i, j) of the matrix R is λ_k . Accordingly, the transition rate from state j to i is the repair rate of component k , i.e. the element (j, i) of the matrix R is μ_k . After we scrutinize all the interstate relationships of any two distinct system states, we can get all the off-diagonal elements of the transition rate matrix R . Figure 32 is a brief flow chart of this algorithm.

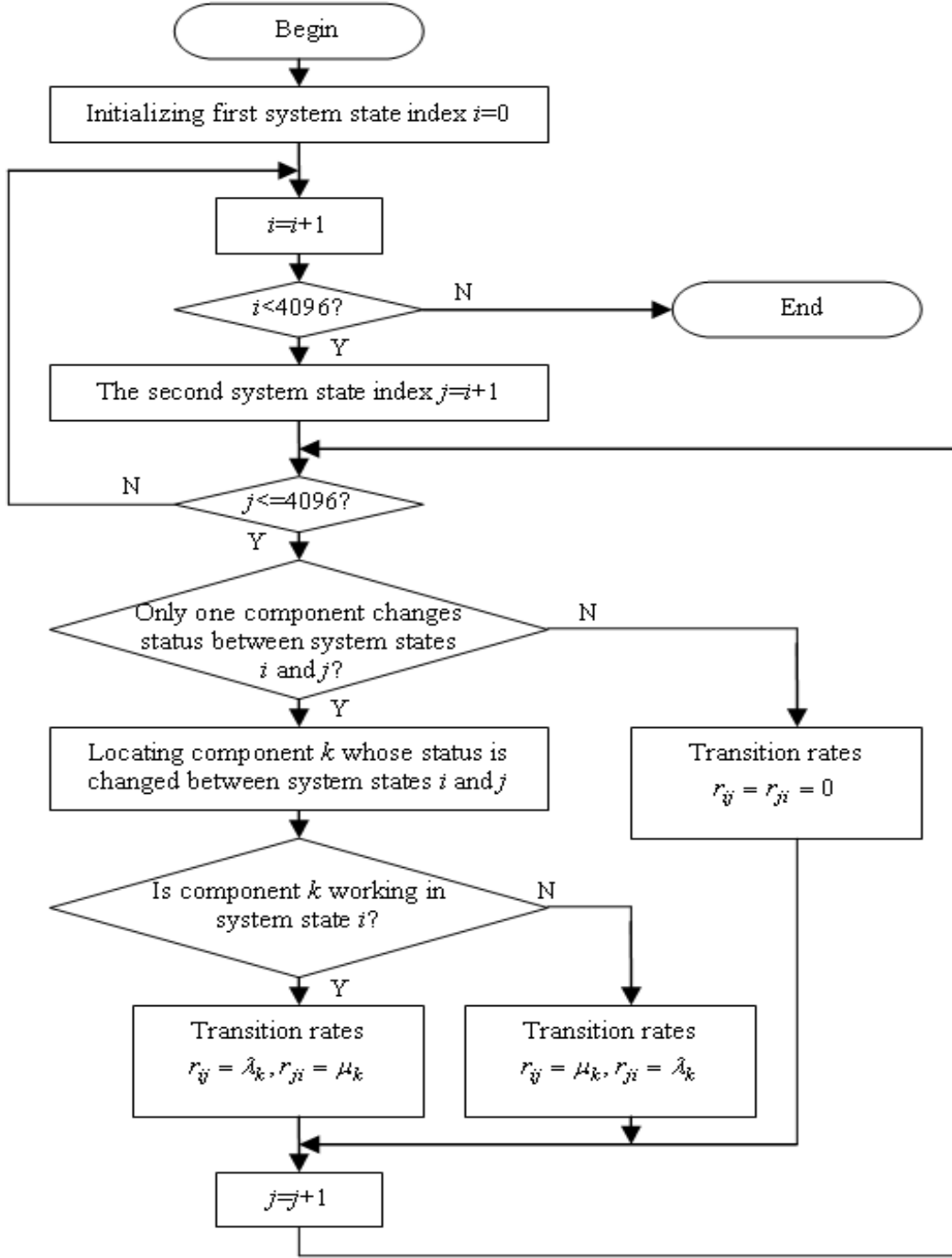


Figure 32: Algorithm to obtain off-diagonal elements of the matrix R

Now it is easy to calculate the diagonal elements of the full transition rate matrix R because the diagonal element of any row has a definite relationship with the off-diagonal elements of the same row, i.e.

$$r_{ii} + \sum_{j \neq i} r_{ij} = 0 \quad (4.50)$$

wherein r_{ii} and r_{ij} represent diagonal and off-diagonal elements, respectively. The subscripts i and j represent the row and column indices of the matrix R , respectively.

Therefore, the diagonal elements can be obtained by the formula as below.

$$r_{ii} = -\sum_{j \neq i} r_{ij} \quad (4.51)$$

Hence, the full system transition rate matrix R is known after we obtain all of its elements.

Step IV: Extracting the submatrix R_{11} from the full system transition rate matrix R

If we form the full system transition rate matrix R based on the rearranged state matrix as shown in Table 13 of Step II, we can see that it is quite easy to obtain its submatrix R_{11} , i.e. the set of transition rates between states of system success. Because all the system states of success are located in the first 189 rows of the rearranged state matrix, R_{11} is just the upper left square submatrix (size of 189×189) of the matrix R (size of 4096×4096) obtained in Step III. In a word, we can extract R_{11} directly from R as shown in Figure 33.

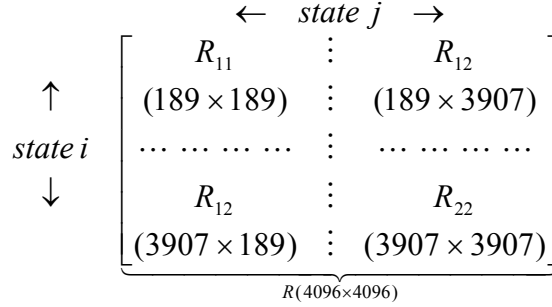


Figure 33: Extraction of submatrix R_{11} from matrix R

Step V: Computing the MTTF of the system

Since the submatrix R_{11} is obtained, we can give the details of vectors $p_+(0)$ and U_k as follows.

The probability row vector of system success states for the initial state (all components up) is

$$p_+(0) = (1 \quad \underbrace{0 \quad 0 \quad \dots \quad 0}_{188 \text{ 0's}}) \quad (4.52)$$

The unit column vector of dimension k which is equal to the number of states of system success is

$$U_k = (\underbrace{1 \quad 1 \quad \dots \quad 1}_{189 \text{ 1's}})^T \quad (4.53)$$

As the final step of the strategy, we are now able to compute the MTTF of our SPS using the following formula.

$$MTTFF_{SPS} = p_+(0)(-R_{11})^{-1}U_k \quad (4.54)$$

5 Risk assessment, systems view

In the previous chapter, SPS risk assessment from a ‘process view’ was thoroughly discussed. It basically involved studying the influence of each and every component in the SPS, and ascertaining the risk associated with them using traditional methods such as fault-tree, failure mode and effect analysis, Markov modeling etc. A particular SPS design may appear quite reliable from the process view, i.e., from sensor to actuation. However, there remain questions such as:

1. Are there system operating conditions (topology, loading, flows, dispatch, voltage levels etc.) that may generate a failure mode for the SPS, e.g., an undesirable operation or a failure to operate?
2. Are there two or more SPS that may interact to produce a failure mode?

Most companies answer these questions using engineering experience and judgment, coupled with tedious trial and error testing involving manual computer simulations. However, it would be beneficial to have a decision-support tool that has an automated simulation capability having flexibility to vary the SPS logic, and having intelligence to vary operating conditions and events over a wide range so that various SPS logic may be tested against various operating conditions and events. Monte Carlo simulation techniques have been used prevalently in many fields over the years to model and study complex factors influencing a phenomenon. So in this chapter the focus is on developing a Monte Carlo simulation based procedure for ‘systems view’ SPS risk assessment.

Section 5.1 presents a report of an interesting case study of a typical system view SPS failure happening in NRDIC grid. Section 5.2 focuses on identifying ways that SPS can fail from a systems view, and proposes methods to identify such failures. Section 5.3 briefly proposes a Monte Carlo simulation based ‘system view’ SPS risk assessment. Section 5.4 presents various reliability models of power system, considering the impact of SPS on the network.

5.1 Systems view SPS failure- a case study

The following section presents a report on mis-operation of special protection schemes in the Nordic grid on December 1st 2005 [123]. This case study demonstrates the possibility of interactions between SPS leading to cascading effect on SPSs in the network, which is undesirable.

5.1.1 Background of SPS in Nordic grid

In Norway two SPS have been implemented to deal with problems concerning high generation in the northwest region. These SPS relieve the burden in important transmission corridors by shedding generation, and thus maintain system integrity. The SPS are actuated by monitoring critical bottleneck from the focus area with respect to a predefined limit. A brief description of both the SPS’s functionalities are given below:

(i) SPS “Nordland”

The shaded area in Figure 34 shows the northern Scandinavia region, which is rich in generation with a very low demand. It contains about 6000 MW hydroelectric power, which is about 15% of the installed capacity in the Nordel grid. In the event of any critical transmission

corridor contingency (i.e., either 420 kV through Northern Sweden or 300 kV through Middle Norway), the rest of the transmission lines must be protected against overload. So the SPS Nordland's functionality is to:

- (1) Generation Shedding: up to 1200 MW
- (2) Net Split: if there is surplus generation in the northernmost part of Norway, it is disconnected from the main Nordel grid.

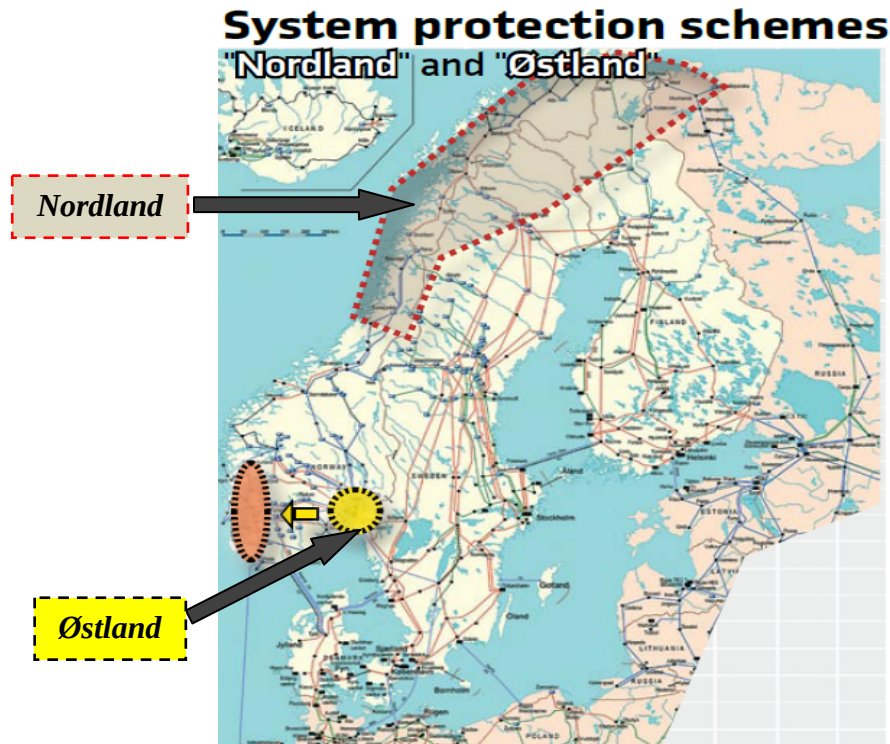


Figure 34: Nordic SPS case study

(ii) SPS “Østland”

The eastern part around Oslo, shown by the yellow-shaded region in Figure 34, is the main load center in Norway. The SPS “Østland” is actuated on outage or overload of central lines in the Oslo area, thereby shedding up to 1200MW of generation on the west coast of Norway, shown by ellipsis in Figure 34. So in cases where there are high power transfers from west to east, i.e., either into the Oslo area or from Norway to Sweden, this SPS will protect the remaining lines in the Oslo area from overloading.

5.1.2 Event report

This section provides the description of events related to SPS mis-operation, their sequence and the consequences. At 3:02 pm (CET) on December 1st 2005, the breaker failure protection disconnected a 420kV busbar at Porjus power plant, due to an occurrence of fault on the 420kV breaker at the power plant. Consequently, important transmission corridors out of northern Scandinavia got overloaded, which as per design should have triggered the SPS at Nordland instantaneously. But this SPS operation failed, leading to Nordel grid going out of limits and ensuing a series of cascading events. The operation of the grid outside design limits led to

undesirable triggering of the second SPS at Østland, which was supposed to trip about 1150 MW of generation from the Nordic grid. Fortunately this SPS also failed, and an imminent system breakdown was evaded. Table 14 summarizes the sequence of events, following the first SPS mis-operation at Nordland.

Table 14: Nordic SPS event description

Events	Time elapse	Description of events	Mis-operation?
1	0 s	- High hydroelectric production in the northwest Nordel region - Breaker fault while switching out 420kV reactor at <i>Porjus power station</i>, Northern Sweden - Fault cleared by tripping a line out of Northern Scandinavia through Sweden, which overloaded remaining lines (2300MW out of Scandinavia)	
2		Triggered Nordland SPS, which tripped 600 MW generation as designed but failed to instantaneously trip 1030 MW generation in Nordel grid	Yes
3	0.8 s	1700 MW of surplus generation went south and caused overloads, which finally lead to tripping of a 220kV line in Sweden (0.8s) and 2-300kV lines in Middle Norway (0.85s)	
4	2.2 s	Nordland activated <i>Grid split</i> and tripped about 487 MW generation in both the split islands (Middle & North Norway) to counter rapid frequency rise	No , but Undesirable cascading
5	3.3 s	Nordland Generator tripping function of step 2 above finally worked, tripping 300 MW generation in North Norway that lead to 128MW shedding by automatic UFLS	Yes , delayed response
6		Due to grid split, under frequency condition prevailed in main Nordel grid leading to west coast generation pickup, causing high west-to-east MW transfer in Southern Norway	
7		Due to heavy west-east transfer, SPS Østland got triggered	No , but Undesirable cascading
8		Østland failed to actuate 1150 MW generation trip in west coast of Norway	Yes , due to human error
9	15 mins	Middle Norway was joined back to main Nordel grid	
10	24 mins	North Norway was joined back to main Nordel grid	

From Table 14, event 2 (Nordland SPS mis-operation) has been the initiating SPS failure which has caused the rest of the consequences in a cascading manner, starting with the event 4 when Nordland implemented the Grid split due to surplus generation. The reason for Nordland mis-operation was found to be due to changes made in SCADA and communication systems that slowed the response time of the SPS Nordland. Thereby, event 5 in Table 14 is the delayed response of Nordland SPS, which is unnecessary at that instant. All these created a scenario that demanded SPS Østland's triggering as intended by design (event 7), though under current

stressed circumstances its successful activation would have worsened the situation. ***This is a typical example of potential failures in power system due to interactions between SPS.*** So had the event 8 in Table 14, i.e., SPS Østland tripping 1150 MW generation, taken place, there might have been one of the two post-event consequences:

- Best scenario: Under-frequency load shedding of 2400 MW
- Worst Scenario: Nordel grid breakdown

Fortunately it failed to operate, due to a technician forgetting to reclose switches following a routine maintenance test of the SPS! On the whole, this sequence of disturbances due to SPS failures incurred a total loss of 250MW load, and the two SPS were deemed unfit for operation until they are rectified. The costs involved with this event for Nordic was about 4.2 million Norwegian kroner.

Therefore, this event shows how critical it is to categorize and investigate SPS failure modes from a system view-point also. Depending upon the system in which SPSs are functioning and the associated operating scenarios, many SPS related failures may arise that may lead to catastrophic system collapses. Hence identification of such failure modes and the associated power system scenarios, will aid us to perform ‘system view’ SPS risk assessment and SPS logic re-design.

5.2 Systems view failure modes and their identification process

SPS operations can be classified into desirable, undesirable or failure to operate as explained in section 4.1. The ‘systems view’ failure mode identification method will focus on identifying the possibility of SPS undesirable operations and failure to operate happening due to fault in logic design (i.e., intended failures). The study also focuses on identifying scenarios that may induce interactions among SPS, giving rise to undesirable cascading SPS operations even if they were originally intended according to logic design. This type of failures due to interaction could be a valid case for concern especially in today’s SPS-rich power networks, where SPS are touted as effective and economic means of strengthening transmission networks, increasing power transfer capability and deferring investment decisions. Some examples of such undesirable interactions could be:

- A desirable (or undesirable) operation of SPS followed by inadvertent operation of another SPS under certain operating conditions producing undesirable consequences, or
- Operation of two separate SPS under rare events such as loss of two elements that initiate those two SPS, or
- A failure of one SPS leading to intended but undesirable triggering of another SPS, as was the case with Nordic grid event.

In the following sub-sections, we shed some light on current industrial practices in designing operational logic for SPS, and we propose ways of identifying ‘system view’ failure modes due to limitations in SPS logic design.

5.2.1 SPS logic design practices

The operating rules for SPS and other similar protection systems are conventionally derived based on deterministic techniques that consider only the worst-case scenario, combined with

expert's judgment. But due to the probabilistic nature of power system that comprise a wide range of network topologies, operating conditions and possible events; such deterministic techniques do not give forth optimal level of settings for generator rejection schemes or remote load shedding schemes or any other SPS [102]. Many recent studies have utilized a risk-based analysis to ensure reasonable coverage of operational scenarios and events, and design robust rules for SPS operations. Van Cutsem et. al. [124] use such simulation methods to build a set of training scenarios to find the minimal load shedding settings for the protection device. They find the optimal triggering rule for the load shedding controllers using combinatorial optimization, in terms of average voltage over several buses in a study area and reactive reserve of critical generators. This kind of load shedding scheme has been programmed in French transmission operator RTE's ASSESS software [125], which is being used by them for their planning studies. The works in [126] and [127] perform many contingency simulations under various operating conditions to design generation trip and load shedding defense plans against transient, small signal and voltage stability problems in longitudinal Taiwan power system. Here the monitoring locations for SPS arming is decided based on operational experience and the thresholds are found out from simulation studies. The work in [128] performs simulation of several outage scenarios such as critical generators and tie lines, for different values of anticipated system overloads and study the loci of frequency-frequency rate plot to decide on the settings of under frequency load shedding SPS for preserving the integrity of the system in the event of islanding. In spite of so many systematic methods to design SPS logic, it is still a challenging task to come up with appropriate settings under wide range of system events and achieve coordination between other SPS in the system.

BC Hydro [33] designed and implemented a centralized automatic RAS arming scheme that ensures system's integrity under critical events based on the measurements from EMS. This provides opportunity to achieve coordination among various RAS actions. The pre-outage security limits and operating rules for the various RAS schemes such as generator rejection are derived from Monte Carlo simulation based operational planning studies performed offline. Any system growth, topological/network change, generator change or any major equipment change triggers RAS logic redesign process.

The process of deriving operating rules has been made more effective with the introduction of data mining techniques such as decision trees, association rule mining etc. They seem to provide good information about most critical system attributes, which are otherwise not possible from conventional analytical techniques or manual interpretation by experts. Further due to such automatic learning technique's ability to process huge database and extract knowledge easily, database of larger sizes with diverse set of situations and events can be used to identify the most relevant attribute and their appropriate settings for SPS [102, 103,]. Hsiao et. al. [129] proposed a risk based contingency selection method for SPS applications. Here the risk of a contingency is computed as the product of its probability and severity under various loading conditions and inter-zone transfers, where severity is quantified in terms of amount of load shedding and generation tripping.

In spite of all these efforts, 'system view' type of failures may still occur due to inherent limitations in logic design procedures or incomplete/inappropriate study procedures such as limited types of faults considered in design phase etc. This is because it is practically impossible to capture all the influencing factors and interesting events, and come up with efficient operating rules for SPS logic that can accurately detect and operate under various operating conditions.

5.2.2 SPS logic validation and failure modes

Generally operating rule can be validated against an *independent test database* containing post-contingency simulation results and SPS arming status for a wide range of operating conditions and events. The testing results of the operating rule against the test database can be expressed in the form of a confusion matrix, as shown in Figure 35.

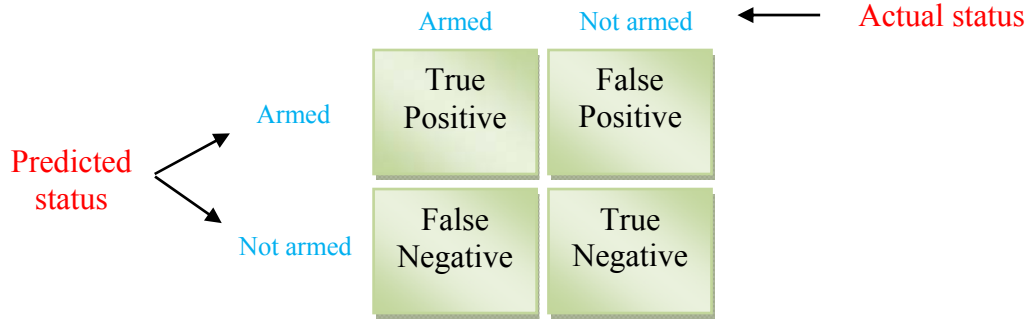


Figure 35: Confusion matrix- SPS logic testing

The percentage of instances/scenarios that are tested false positive and false negative give the expected failure rates of SPS. The false positives denote intended inadvertent operation such as over tripping of generation rejection scheme etc., and the false negatives denote failure to operate. Among these, the false negatives are expensive failures as in a stressed conditions failure of SPS operation would have maximum damage to components, system and the economy than inadvertent operation. Consequently, we can further analyze these situations that produce false negative failures for improving the SPS logic. Furthermore, even though this study gives false positive failure percentage (i.e., inadvertent operation of SPS), it doesn't give any information on whether the consequence of inadvertent operation of SPS is desirable or undesirable from economic or reliability point of view. Therefore, this further requires a complete simulation study, which is explained in the next section.

Apart from these two types of regular SPS failures, there is possibility of another type of failure from a system point of view, which is due to interactions among SPS, as mentioned earlier using Nordic grid event. Identifying such failure modes require time domain simulation of many interesting system conditions with as many system dynamics modeled, especially of all the SPSs in the system, and other important equipments & protective devices.

The next subsection focuses on designing a simulation methodology to identify ways that SPS can fail from a systems view, i.e., undesirable intended SPS operation or failure to operate, and failures due to SPS interactions.

5.2.3 Simulation based system view SPS failure mode identification

5.2.3.1 Regular SPS failure mode identification

The typical failure modes due to undesirable operation and failure to operate of a single SPS is referred here as regular failure modes. Figure 36 depicts the risk based simulation methodology to identify such failures using a comparative study between two sets of simulation, one with SPS and another without the particular SPS. This can be done for every single SPS in the system to detect its regular failure modes.

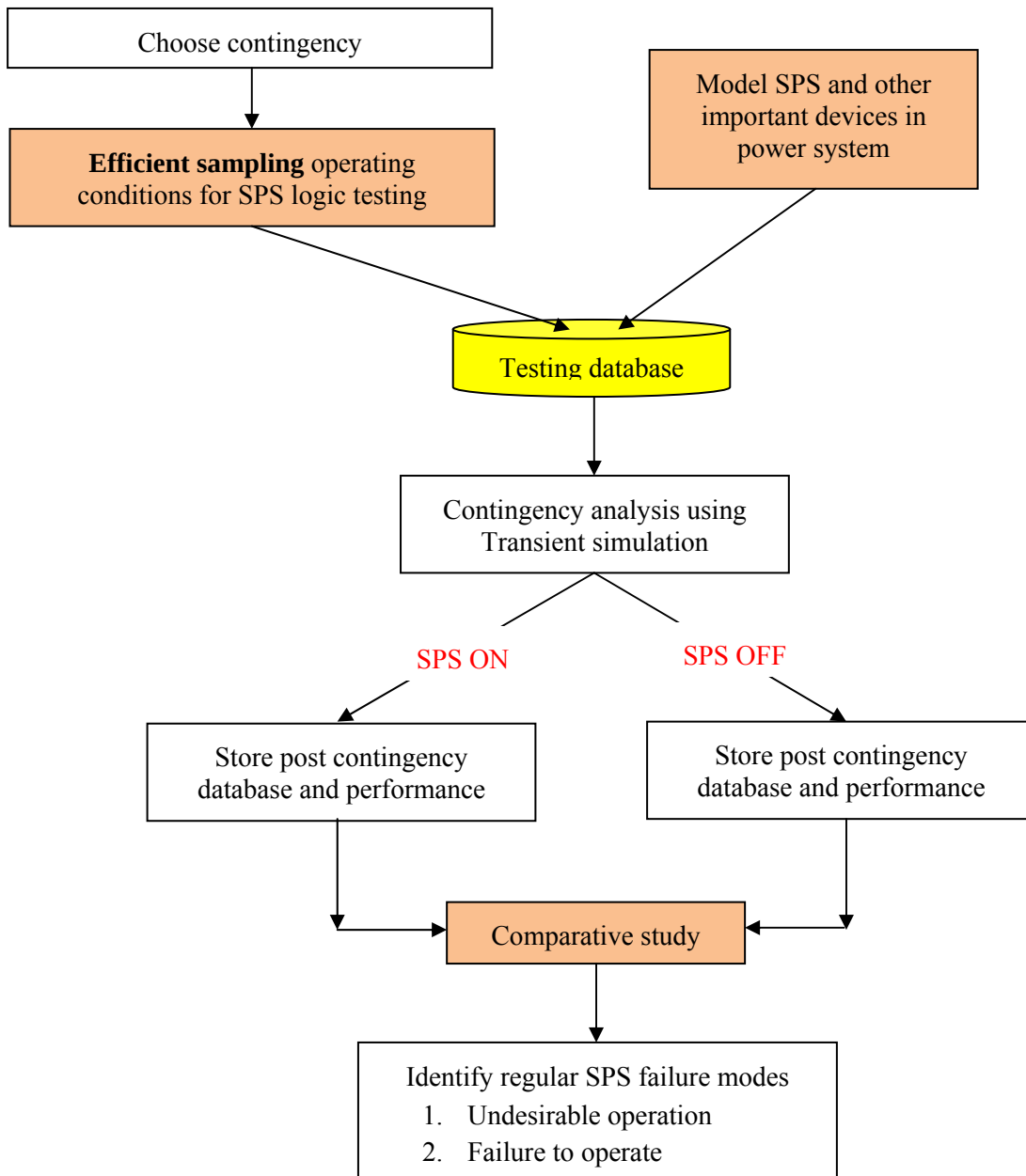


Figure 36: Simulation study- regular SPS failure mode identification

(1) Efficient Sampling of operating conditions: First the corresponding contingency for which the SPS is planned is chosen. Then efficient sampling of operating conditions based on importance sampling method, as explained in chapter 3, is performed. This is because the traditional Monte Carlo sampling generates operating conditions according to the probability distribution of the operational parameter state space. But in the case of SPS, since they are especially designed to operate in stressed operating conditions, operating conditions close to stability threshold should be given more importance in the sampling. So importance sampling is utilized to bias the sampling and generate operating conditions from the stability boundary region of the operational parameter state space.

Furthermore, the proposed sampling strategy based on importance sampling also reduces the computational burden in validating SPS logic by focusing only on important situations. Some conditions from the far tail of the parameter distribution (lower probability) may also be sampled, as the likelihood of SPS mis-operation and their consequences are high for these situations.

This proposed efficient sampling procedure can be realized starting with identifying the key operating parameters that would have influence on the operation of the particular SPS under consideration. The stability boundary region is then found in that parameter state space, and finally important operating conditions from that region are sampled according to their relative likelihood. Depending upon the nature of the operating parameter probability distribution, i.e., if parametric, correlated etc., suitable parametric [130] or non-parametric methods (Copulas [131], Latin Hypercube Sampling [132]) are used to generate realistic operating conditions.

- (2) Simulation and Comparative study:** Then two sets of transient contingency simulation are performed on these sampled scenarios, one with the SPS functionality modeled and other without SPS. Then comparative studies are done to see the effectiveness of the SPS and obtain factual information on the kind of regular failures happening, i.e., the false positives and false negatives.

The software available for such simulations at Iowa state university are Siemens' PTI PSS/E and Eurostag® embedded to ASSESS. PSS/E has the capability to model SPS using the tripping functionality in multiple-contingency analysis module. Generation trip, load shedding, branch tripping based on bus voltage, line loading and generator output are some variety of special protections that can be designed in PSS/E. The risk based analysis in PSS/E has to be automated using scripting language such as Python or IPLAN or using batch files. Eurostag can also be used to model SPS such as UVLS, UFLS, overload branch tripping and other such automata. The advantage in working with Eurostag is the ability to interface Eurostag with ASSESS software, which facilitates automation of such risk based statistical simulation studies and post-processing of the simulation results.

5.2.3.2 Interaction based SPS failure mode identification

The failures resulting from interaction can also be detected using comparative study by modeling all the system SPSs in the simulation, as depicted by Figure 37. The generation of operating conditions is similar to what was explained before, i.e., sample from the stability boundary region of a contingency for which the particular SPS is installed. Since the interest is for capturing interactions, we could sample operating conditions from the union of pairwise intersections of stability boundary regions of all the SPS in the study. To reduce the complexity of the study (i.e., the number of combinations of possible SPS interactions), firstly the SPS can be grouped. The grouping of SPS may be done with respect to some of the following criteria:

1. Contingency locations corresponding to various SPS,
2. SPS locations,
3. Intersection among SPS solution strategies (ex. common generators tripped?)
4. Intersection among stability boundaries

5. Probability of any two contingencies happening in a cascading manner
6. Sensitivity of one SPS's action on another's actuating criteria

Figure 37 depicts the process of sampling operating conditions in an efficient manner for process failure mode identification, where SPS A and SPS B are considered to be grouped together. The sampling state space is considered to be made of two operating parameters (1 & 2).

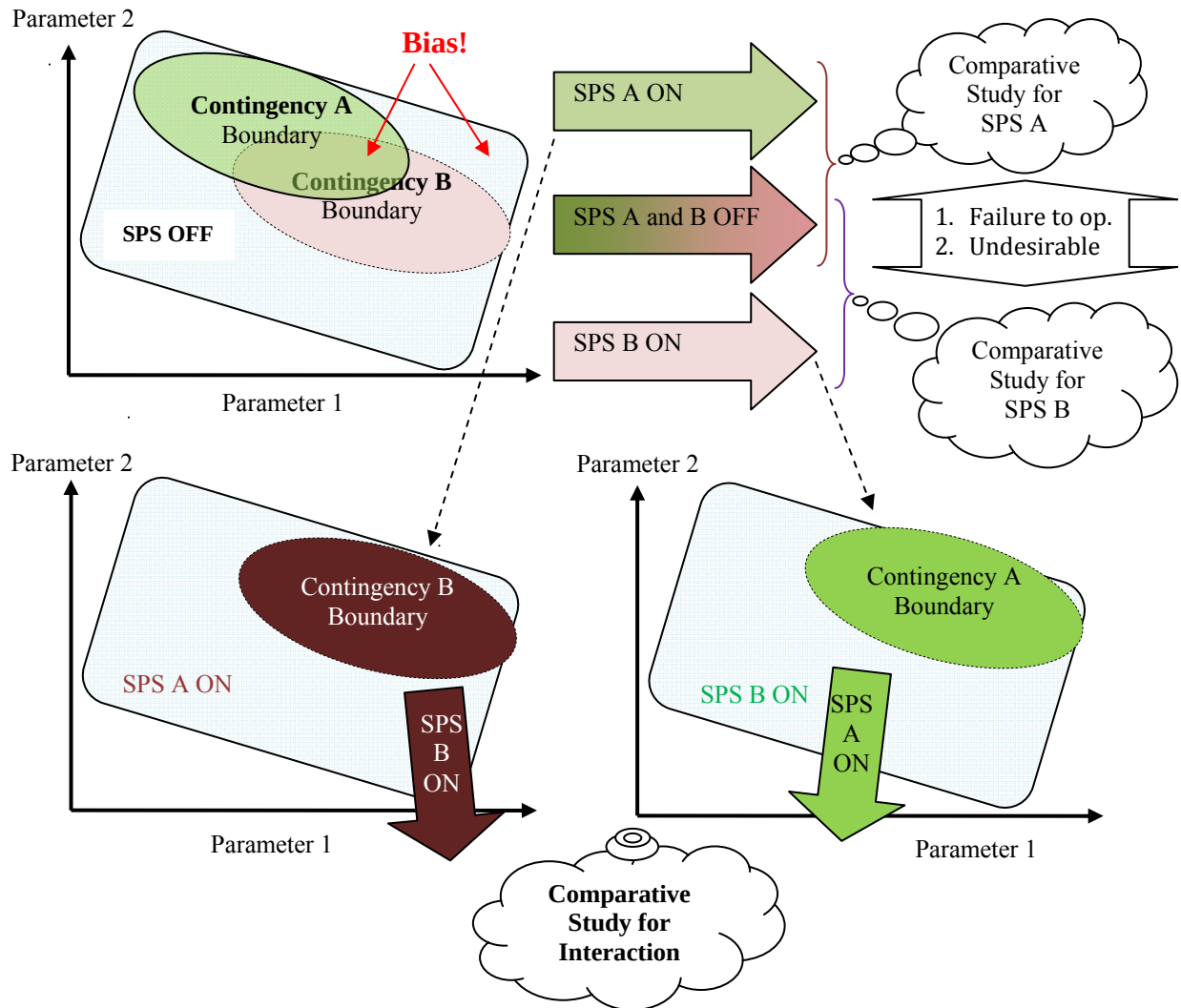


Figure 37: Process view SPS reliability assessment – operating conditions sampling

Figure 37 shows that in the case of identifying regular failure modes related to SPS A operation, the operating conditions sampling process is biased towards the stability boundary region of contingency A when both SPS are in OFF state. Similarly, in the case of identifying regular failure modes related to SPS B operation, the sampling process is biased towards the stability boundary region of contingency B with both SPS in OFF state. When it comes to identifying interactions between SPS A and SPS B, two sets of operating conditions are sampled. One set is to test the SPS B operation on operating conditions that are biased towards the stability boundary region of contingency B, where the state space is made of post-contingency A operating conditions subject to SPS A operation. The other set is to test the SPS A operation on

operating conditions that are biased towards the stability boundary region of contingency A, where the state space is made of post-contingency B operating conditions subject to SPS B operation. Then the two sets of simulation results are analyzed to identify any failure or undesirable scenarios due to interactions among the two SPS. This can be extended to identifying interactions among several SPSs. While this will surely require extra computational requirements, the process of efficient sampling that biases the sampling procedure only to the important conditions will reduce the burden of computation. Furthermore, linear sensitivity measures may be used to further decrease the computational requirements to a greater degree.

5.3 Systems view risk assessment

The effects of various ‘system view’ failures (identified in previous section) on the system reliability can be estimated using a risk index, which is the product of probability of the failure and its severity. The severity value of a particular failure mode in terms of performance measure is computed from Monte Carlo simulation study (similar to failure identification study) as shown in Figure 38. Various initiating SPS failures are embed in the simulation, and the system-level SPS failures and their severities are computed. The severities can be quantified in terms of reliability indices such as expected cost of electricity (EC), tripped generator cost (TGC), expected energy not served (EENS) due to SPS forced curtailments and so on.

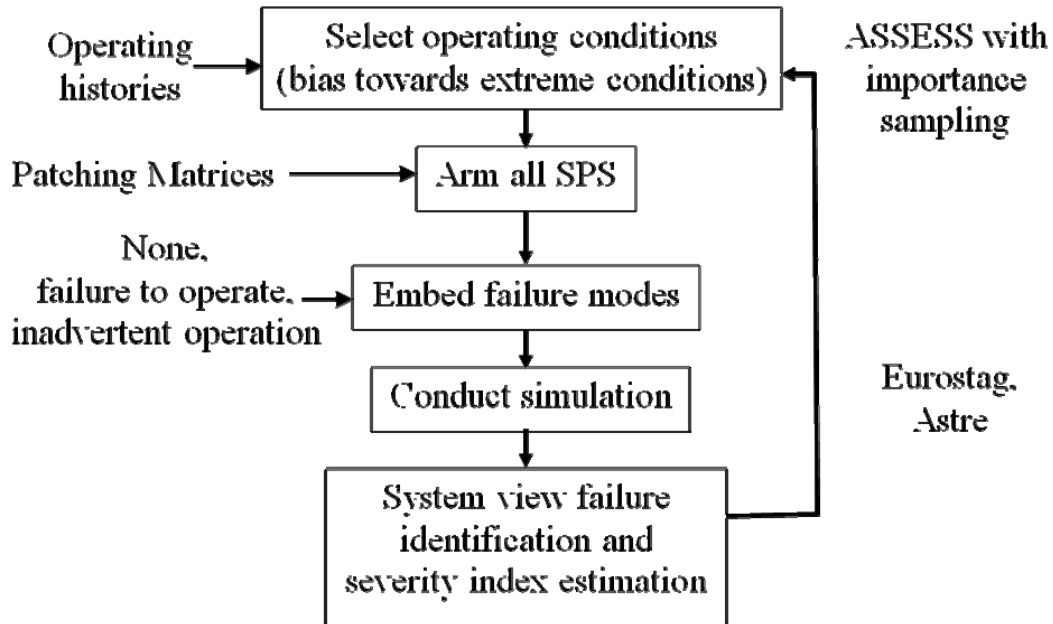


Figure 38: System view SPS risk assessment

If a particular failure mode imposes big risk, then the appropriate SPS logic can be re-defined by using decision tree based method as explained in section 3.3, wherein the operating conditions that lead to this failure mode in the simulation study are included in the database for training the decision tree for rule re-design. Consequently, any tightening of SPS logic and its consequent effect on solution strategy, say for example, the rule is re-designed to contain some expensive generator trip strategy, will enable evaluating the additional expense necessary to maintain a system with a large number of SPS.

5.4 Reliability analysis of power systems with impact of SPS operation

It is obvious that SPS operation would have an impact on the power system reliability as SPS can operate inadvertently or simply fail to operate when needed. However, it is not simple to evaluate the power system reliability including the impact of SPS operation. One reason is that there are various types of SPS such as generation rejection, load rejection, system separation, etc. and these different SPS have varying design and operational action. Another reason is that SPS failures can cause such complicated interactions between current-carrying components that both component and system states experience intricate changes.

Thus, we first need to unify the effects of different SPS operations in order to make reliability analysis of power systems feasible. In steady state point of view, effects of all SPS operations can be classified ultimately into two categories: 1) tripping current-carrying components; 2) changing bus power injection where load is regarded as a negative injection. If we further divide the power injection at each bus into two parts, unchanging part and changing part due to SPS operation, we can think of these two parts as two imaginary generators connected to the bus independently. Therefore, all SPS operations can be uniformly represented by the tripping effect for steady state reliability analysis.

All SPS operations including SPS failures along with their ultimate tripping effects can be summarized into three cases as following. Firstly, for a desirable SPS operation, some components of the power system trip as designed. These components are called intended components hereafter. Secondly, for an undesirable SPS operation, i.e. the SPS operating inadvertently, the intended components are also tripped down but undesirably. Thirdly, for the case if the SPS fails to operate, the intended components do not trip initially. However, the failure of SPS operation can only result in more severe and wider impacts on the power system than if SPS operates as designed. As the ultimate tripping effect after possible transient stability process, we can assume that more components of the power system including intended components will trip eventually.

5.4.1 Modeling SPS operation at the component level

It is important to consider the reliability modeling of current-carrying components including the impact of SPS operation. Including SPS operation at system level may be difficult or even impossible if we do not incorporate this effect into the component modeling.

5.4.1.1 Modeling intended components

Suppose component i is an intended component of a SPS design. We realize that even if not involved in the SPS design, component i can trip due to possible faults on it. Considering repair of the component, we use a two-state Markov model to represent this effect as shown in Figure 39. The up and down states of the component are illustrated by i and $\bar{i}$, respectively. The parameters λ_i and μ_i in the figure are failure and repair rates of the component, respectively.



Figure 39: Modeling component i without SPS operation

When involved in SPS operation, we assume that there is no simultaneous fault on component i when it is called upon for a SPS operation. Hence, for a SPS operation component i is tripped to a state distinct from state $\bar{i}$.

For a desirable SPS operation, we use $\hat{i}$ to represent the down state of component i after the SPS operation. When the power system is returned to a normal operation condition later, component i can be restored to its up state again. Thus, we add another two-state process representing the desirable SPS operation effect to the previous one and the Markov model of component i becomes the one as shown in Figure 40. The parameters $\hat{\lambda}_i$ and $\hat{\mu}_i$ in the figure are failure and repair rates of the component for desirable SPS operation, respectively.

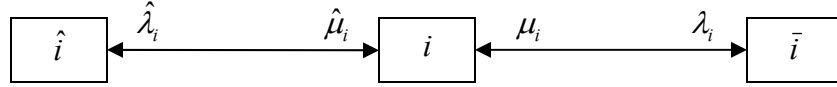


Figure 40: Modeling component i with desirable SPS operation

For an undesirable SPS operation, we use i' to represent the down state of component i after the SPS operation. However, since the SPS operation is inadvertent and the power system is actually in a normal operation condition, component i will be corrected back to its up state again after some checking processes later. Therefore, we need a third two-state process representing the undesirable SPS operation effect integrated into the previous modeling. The Markov model of component i will evolve to the one as shown in Figure 41. The parameters λ'_i and μ'_i in the figure are failure and repair rates of the component for undesirable SPS operation, respectively.

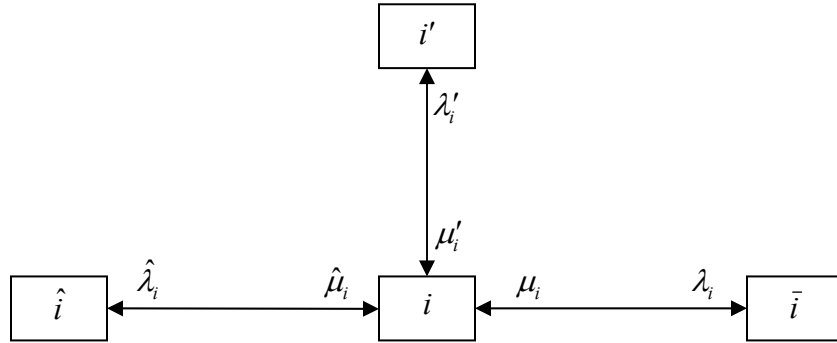


Figure 41: Modeling component i with desirable and undesirable SPS operation

As for the case when the SPS fails to operate, we have assumed that component i will be ultimately tripped from the steady state viewpoint. Here we use $\tilde{i}$ to represent this down state of component i . However, because the power system has suffered more severe impacts and more components have been tripped, we consider the system restoration in two steps. In the first step, the extra components tripped due to SPS failing to operate other than intended components are switched back to their up states. The second step is the same as if SPS did operate as designed, i.e. the power system returns to a normal operation condition and intended components are restored to their up states again.

Now the operation effect of SPS failing to operate can be illustrated by the Markov process loop connecting states i , $\tilde{i}$, and $\hat{i}$ as shown in Figure 42. In this figure, the parameter $\tilde{\lambda}_i$ is the failure rate of component i towards its eventual down state $\tilde{i}$ caused by SPS failing to operate. The parameter $\tilde{\mu}_i$ is the switching rate of the first restorative step after the ultimate tripping effect of SPS failing to operate. The parameter $\hat{\mu}_i$ is the switching rate of the second restorative step, which is the same as the repair rate of component i for its desirable SPS operation as defined in Figure 40 and Figure 41. In fact, Figure 42 is based on and further developed from Figure 41.

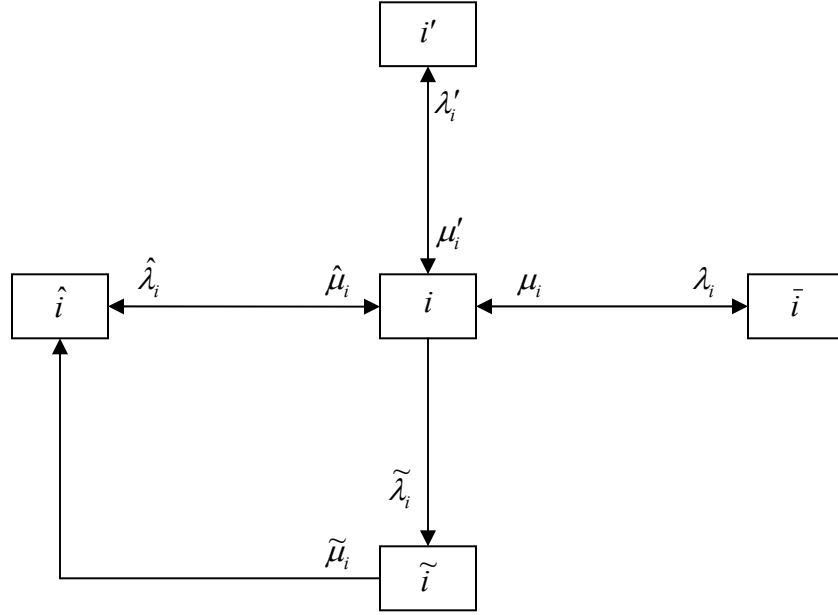


Figure 42: Modeling component i with all SPS operation effects

The Figure 42 depicts the overall reliability model for the intended component i including all SPS operation effects. In summary, component i has five states: the up state i , the down state $\bar{i}$ due to faults on component i , the down state $\hat{i}$ due to desirable SPS operations, the down state i' due to undesirable SPS operations, and the down states $\tilde{i}$ due to SPS failing to operate, respectively. If we use P_i , $\bar{P}_i$, $\hat{P}_i$, P'_i , and $\tilde{P}_i$ to represent the probabilities of states i , $\bar{i}$, $\hat{i}$, i' , and $\tilde{i}$, respectively, we can figure out these probabilities using the frequency balance approach as following.

For state i , we have

$$\bar{P}_i \mu_i + \hat{P}_i \hat{\mu}_i + P'_i \mu'_i = P_i (\lambda_i + \hat{\lambda}_i + \lambda'_i + \tilde{\lambda}_i) \quad (5.1)$$

For state $\bar{i}$, we have

$$P_i \lambda_i = \bar{P}_i \mu_i \quad (5.2)$$

For state $\hat{i}$, we have

$$P_i \hat{\lambda}_i + \tilde{P}_i \tilde{\mu}_i = \hat{P}_i \hat{\mu}_i \quad (5.3)$$

For state i' , we have

$$P_i \lambda'_i = P'_i \mu'_i \quad (5.4)$$

For state $\tilde{i}$, we have

$$P_i \tilde{\lambda}_i = \tilde{P}_i \tilde{\mu}_i \quad (5.5)$$

We also have

$$P_i + \bar{P}_i + \hat{P}_i + P'_i + \tilde{P}_i = 1 \quad (5.6)$$

Using any four of the five equations (5.1)-(5.5) together with equation (5.6), we can solve and obtain the state probabilities as below.

$$P_i = 1/K_i \quad (5.7)$$

$$\bar{P}_i = \lambda_i / (K_i \mu_i) \quad (5.8)$$

$$\hat{P}_i = (\hat{\lambda}_i + \tilde{\lambda}_i) / (K_i \hat{\mu}_i) \quad (5.9)$$

$$P'_i = \lambda'_i / (K_i \mu'_i) \quad (5.10)$$

$$\tilde{P}_i = \tilde{\lambda}_i / (K_i \tilde{\mu}_i) \quad (5.11)$$

wherein

$$K_i = 1 + \frac{\lambda_i}{\mu_i} + \frac{\hat{\lambda}_i + \tilde{\lambda}_i}{\hat{\mu}_i} + \frac{\lambda'_i}{\mu'_i} + \frac{\tilde{\lambda}_i}{\tilde{\mu}_i} \quad (5.12)$$

5.4.1.2 Modeling extra components tripped due to SPS failing to operate other than intended components

In the case of SPS failing to operate, the power system suffers more severe impacts and some components other than intended components will be ultimately tripped from the steady state viewpoint. Here we suppose component j represents the extra component. Since we have assumed the system restoration in two steps, component j is switched back directly to its up state in the first step. Thus, the process can be represented by a two-state Markov model, which is illustrated in Figure 43.

Figure 43 shows the overall reliability situation for the extra component j including SPS operation effects. Component j has three states: the up state j , the down state $\bar{j}$ due to faults on component j , and the down states $\tilde{j}$ due to SPS failing to operate, respectively. In this figure, the parameter $\tilde{\lambda}_j$ is the failure rate of component j towards its eventual down state $\tilde{j}$ caused by SPS failing to operate. The parameter $\tilde{\mu}_j$ is the switching rate of the first restorative step after the ultimate tripping effect of SPS failing to operate. The parameters λ_j and μ_j in the figure are failure and repair rates of the component due to faults on itself, respectively.

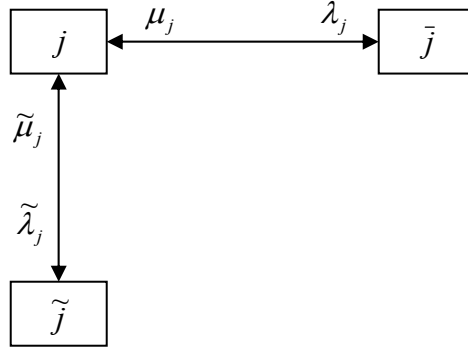


Figure 43: Modeling component j with SPS operation effects

If we use P_j , $\bar{P}_j$, and $\tilde{P}_j$ to represent the probabilities of states j , $\bar{j}$ and $\tilde{j}$, respectively, it is also easy to calculate these probabilities using the frequency balance approach. The results are obtained as follows.

$$P_j = 1/K_j \quad (5.13)$$

$$\bar{P}_j = \lambda_j / (K_j \mu_j) \quad (5.14)$$

$$\tilde{P}_j = \tilde{\lambda}_j / (K_j \tilde{\mu}_j) \quad (5.15)$$

wherein

$$K_j = 1 + \frac{\lambda_j}{\mu_j} + \frac{\tilde{\lambda}_j}{\tilde{\mu}_j} \quad (5.16)$$

5.4.1.3 Modeling components not involved in SPS operation

All other components not analyzed above are those not involved in SPS operation. Suppose component k is such a component. It is obvious that component k is only influenced by its own faults. Thus, we can model it the same way as if SPS does not exist, which is shown in Figure 44.

In Figure 44, the up and down states of component k are illustrated by k and $\hat{k}$, respectively. The parameters λ_k and μ_k in the figure are failure and repair rates of the component, respectively.

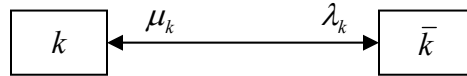


Figure 44: Modeling component k not involved in SPS operation

5.4.2 Modeling SPS operation at the system level

After we have incorporated SPS operation effects into the component modeling, it becomes feasible to analyze reliability at the power system level including SPS operation. However, the interactions between current-carrying components caused by SPS operations may raise the

complexity and discourage modeling at the system level. Hence, we need to decouple these component interactions first. We still use i , j , and k to represent the intended components, the extra components, and the components not involved in SPS operation, respectively.

5.4.2.1 Decoupling component interactions by SPS operation

We assume that the faults on a component are independent of those on other components. Thus, the failure mode of a component due to faults on itself has influence only on it without interaction with other components. It is also obvious that in case of desirable SPS operation or undesirable SPS operation, only intended components are tripped without interaction with other components. Hence, the component interactions exist only in the case of SPS failing to operate when called upon.

We have analyzed and modeled the extra components tripped due to SPS failing to operate other than intended components in the previous section. However, this tripping effect is actually not independent. It is always accompanied by the ultimate tripping effect of the intended components from the steady state viewpoint. Considering these two types of components together, we can see that their ultimate tripping effect is actually a kind of common cause failure. For clear illustration, we extract out the related parts in Figure 42 of component i and in Figure 43 of component j , and then put them together with little modification as shown in Figure 45. The common cause failure process can be explained as following.

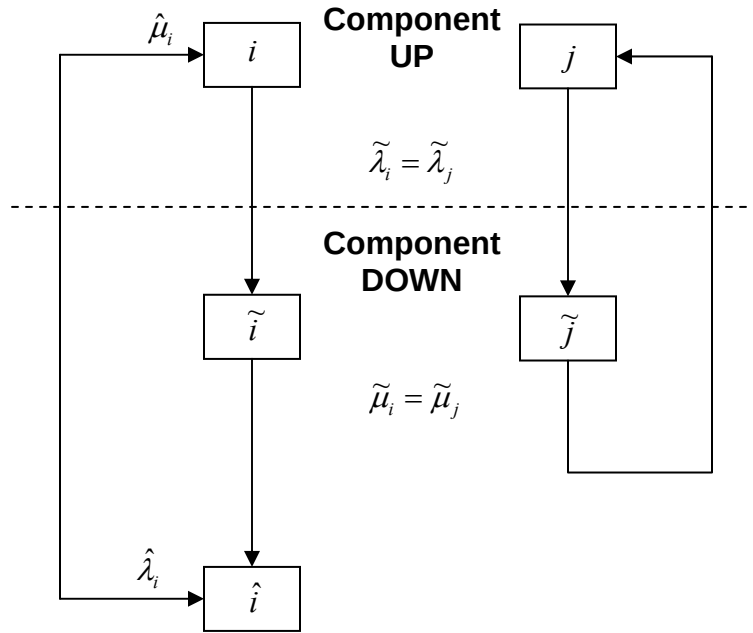


Figure 45: Decoupling interactions caused by SPS failing to operate

In the first transition of this process, component i transfers from the up state i to the down state $\tilde{i}$ with the failure rate $\tilde{\lambda}_i$, while component j transfers from the up state j to the down state $\tilde{j}$ with the failure rate $\tilde{\lambda}_j$, which equals to $\tilde{\lambda}_i$ in value due to common cause failure of the two components. The second transition of this process is actually the first restorative step after

SPS failing to operate as mentioned previously. Component i transfers from state $\tilde{i}$ to another down state $\hat{i}$ with the switching rate $\tilde{\mu}_i$, while component j returns from state $\tilde{j}$ to its up state j with the repair rate $\tilde{\mu}_j$, which is the same as $\tilde{\mu}_i$ due to the switching operation. The third and last transition of the process is actually the second restorative step after SPS failing to operate. Component i transfers from state $\hat{i}$ to its up state i with the switching rate $\hat{\mu}_i$, which is the same as the repair rate of component i for its desirable SPS operation. Therefore, if we are only concerned with transitions between up and down states of component j , this kind of common cause failure makes the extra component j experience a two-state process with its transition rates derived directly from the intended component i .

5.4.2.2 Impact of SPS operation on modeling non-contingency system states

SPS operations do have influence on modeling system states. However, for system states in which the intended components are already down due to their own faults, SPS cannot be put into operation. Hence, there will be no change for modeling these states as if without SPS. The system state $(\dots \bar{i} \dots j \dots k \dots)$ in Figure 46 is such a case, which represents the intended component i already being down due to faults on itself, the extra component j being up, and component k not involved in SPS operation also being up.

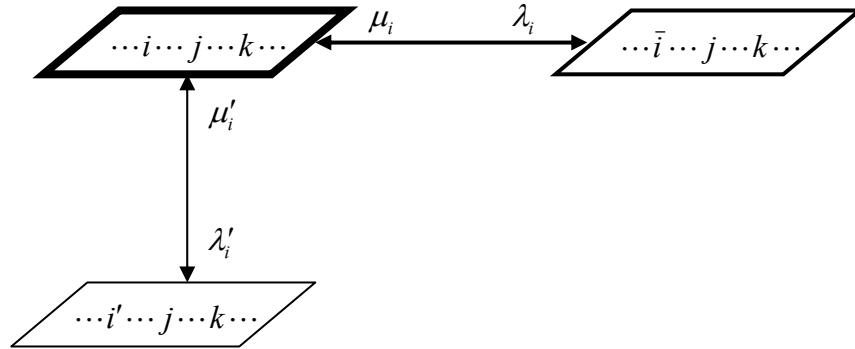


Figure 46: Impact of SPS operation on modeling non-contingency system states

If the intended components are in their up states, SPS can be alarmed and put into operation. Nevertheless, the impact of SPS operation on modeling system states is still dependent upon whether the states are in contingency or not.

For non-contingency system states, SPS is not designed to operate. The case of desirable SPS operation will not occur and so does the case of SPS failing to operate. But SPS could operate mistakenly, i.e. undesirable SPS operation could exist. Figure 46 is the illustration of the impact of SPS operation on modeling non-contingency system states. In this figure, the system state $(\dots i \dots j \dots k \dots)$ is such a non-contingency state that components i , j , and k are all in up states. We already know that undesirable SPS operations only influence intended components without interaction with other components. Thus, a new system state $(\dots i' \dots j \dots k \dots)$ with connection to this non-contingency state is added, in which i' represents the intended component i being tripped down due to undesirable SPS operation.

5.4.2.3 Impact of SPS operation on modeling contingency system states

For contingency system states, SPS is designed to operate. Hence, inadvertent SPS operation, i.e. undesirable SPS operation will not occur. So, there are two types of SPS operation effects relating to this situation, i.e. desirable SPS operation and the case of SPS failing to operate. Figure 47 is the illustration of the impact of SPS operation on modeling contingency system states. In this figure, the system state $(\dots i \dots j \dots \bar{k} \dots)$ is a contingency state with components i and j being up but component k being down.

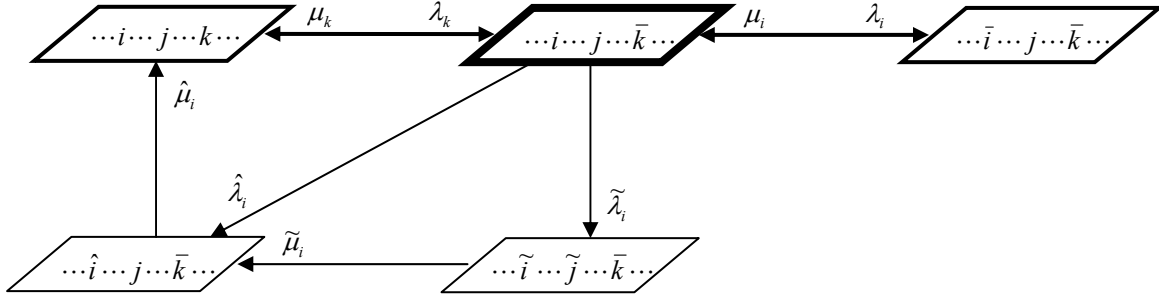


Figure 47: Impact of SPS operation on modeling contingency system states

Although desirable SPS operations only influence intended components without interaction with other components, it is always practical to restore the power system to a normal or non-contingency state rather than the original contingency state after desirable SPS operations. Therefore, after the system transfers from the contingency state $(\dots i \dots j \dots \bar{k} \dots)$ to a new state $(\dots \hat{i} \dots j \dots \bar{k} \dots)$ representing the desirable SPS operation, it will not go back to state $(\dots i \dots j \dots \bar{k} \dots)$ again as component i being restored to its up state. Instead, we assume the system will be restored to a non-contingency system state which is in the nearest connection but has more components up than the original contingency state $(\dots i \dots j \dots \bar{k} \dots)$. Suppose the state $(\dots i \dots j \dots k \dots)$ is one of such non-contingency system states. The three system states $(\dots i \dots j \dots \bar{k} \dots)$, $(\dots \hat{i} \dots j \dots \bar{k} \dots)$, and $(\dots i \dots j \dots k \dots)$ form a Markov loop as shown in Figure 47.

For the case of SPS failing to operate, we previously analyzed the existing common cause failures and decoupled the interactions between current-carrying components. Based on the information, we know that the system will transfer from the contingency state $(\dots i \dots j \dots \bar{k} \dots)$ to a new state $(\dots \tilde{i} \dots \tilde{j} \dots \bar{k} \dots)$ representing the ultimate tripping effect of SPS failing to operate from the steady state viewpoint as shown in Figure 47. Then as the first restorative step, the system will transfer to the state $(\dots \hat{i} \dots j \dots \bar{k} \dots)$ representing the desirable SPS operation. The second restorative step is all the same as the restorative process of the desirable SPS operation, i.e. the system is restored to the non-contingency state $(\dots i \dots j \dots k \dots)$. The four system states $(\dots i \dots j \dots \bar{k} \dots)$, $(\dots \tilde{i} \dots \tilde{j} \dots \bar{k} \dots)$, $(\dots \hat{i} \dots j \dots \bar{k} \dots)$, and $(\dots i \dots j \dots k \dots)$ also form a Markov loop as shown in Figure 47.

5.4.2.4 Reliability modeling of power systems with impact of SPS operation

We have assumed the failure mode of a component due to faults on itself is independent. Therefore, the reliability modeling of power systems without SPS operation is a one-layer Markov chain as illustrated in Figure 48. In this figure, each block represents a system state and all system states are independent of each other. In addition, all transitions between any two states are single-step transitions.

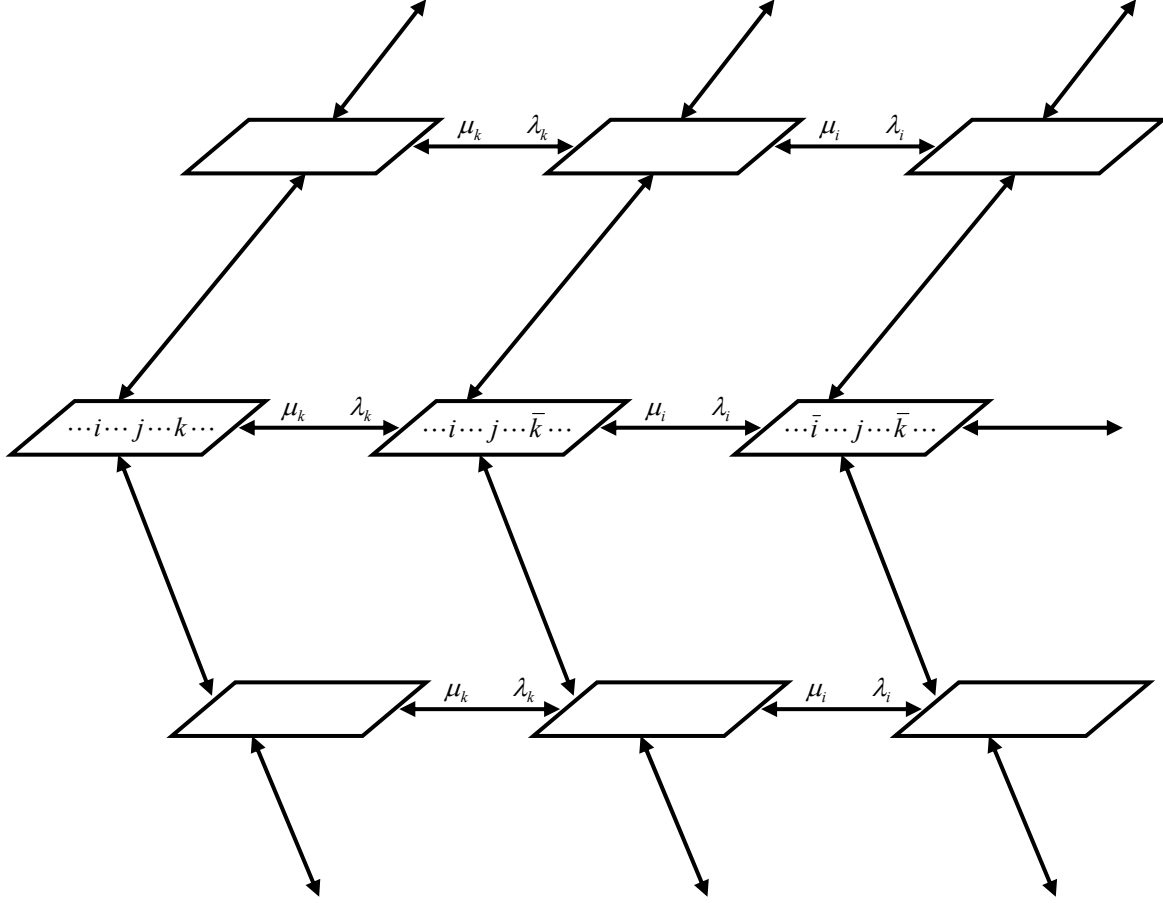


Figure 48: Reliability modeling of power systems without SPS operation

However, if the impact of SPS operation needs to be considered, the reliability modeling of power systems will become a two-layer Markov chain as shown in Figure 49. The first layer is all the same as that in Figure 48. We name it the primary layer, which consists of the independent system states with single-step transitions. The second layer is a dependent one added to the primary layer to reflect the impact of SPS operation. As we have explained in previous content, different system states correspond to different SPS operation effects.

For a system state in which the intended components are already down due to their own faults, SPS cannot be put into operation. Hence, there will be no dependent second-layer state attached to this system state, e.g. $(\dots \bar{i} \dots j \dots \bar{k} \dots)$.

For a non-contingency system state with the intended components up, the tripping effect of undesirable SPS operation exists. Thus, there will be a dangling second-layer state attached to this system state, e.g. $(\dots i \dots j \dots k \dots)$.

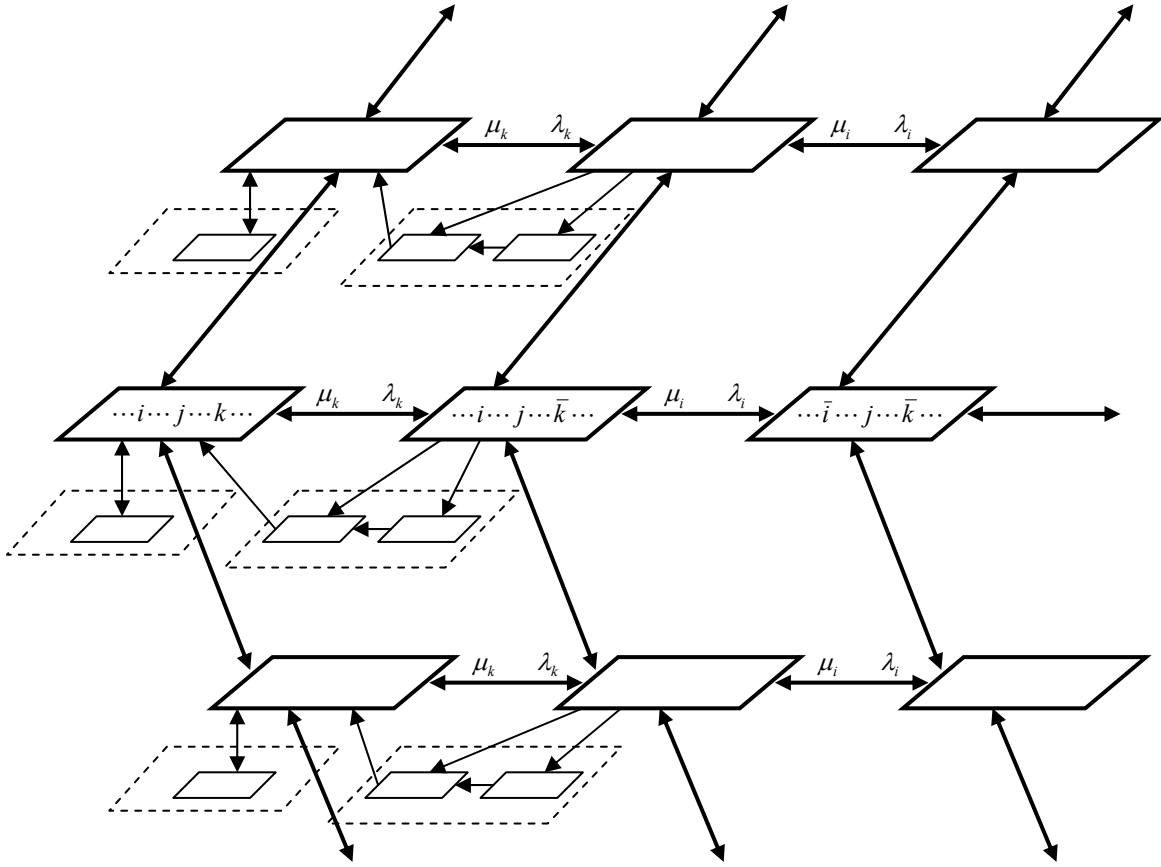


Figure 49: Reliability modeling of power systems with impact of SPS operation

For a contingency system state with the intended components up, there exist two types of SPS operation effects, i.e. desirable SPS operation and that of SPS failing to operate. Therefore, there will be a group of two second-layer states attached to this system state, e.g. $(\dots i \dots j \dots \bar{k} \dots)$. In addition, this second-layer group also attaches to a non-contingency system state, e.g. $(\dots i \dots j \dots k \dots)$, which is in the nearest connection with but has more components being up than the original contingency state, i.e. $(\dots i \dots j \dots \bar{k} \dots)$.

The methodology of power system reliability modeling with impact of SPS operation can be summarized as following.

- 1) Set up the primary layer Markov chain.
- 2) Classify system states of the primary layer.
- 3) Attach the second-layer states to non-contingency states of the primary layer.
- 4) Attach the second-layer states to contingency states of the primary layer.
- 5) Use analytical method or Monte Carlo Simulation for reliability calculation.

6 Consideration of SPS in planning

This chapter considers SPS within the context of long-term planning. With the background of fast growing wind energy in power system, SPS applications motivated by wind energy becomes increasingly interesting in long-term planning. This topic is discussed in section 6.1.

High penetration of SPS increases the complexity of system planning and operation. The complexity increases the possibility of undesirable and unintended interactions among SPS, potentially degrading to system reliability. In this chapter, section 6.2 conceptually discusses the increase in operational complexity with higher levels of SPS penetration.

It is typical that reliability problems encountered within planning studies may be corrected either by building new transmission or by installing an SPS. SPS are almost always much less expensive ways to correct reliability problems, since they generally require only relays, communication equipment, computing and associated actuation logic, and tripping devices. Section 6.3 presents a framework to address the problem of SPS-aided transmission expansion planning in power system, and section 6.4 discusses the results.

6.1 Electric system long-term planning with SPS

6.1.1 Electric system long-term planning

The electric system planning process is the systematic assembly and analysis of information about electric energy supply, transport, and demand, and the presentation of this information to decision-makers who must choose an appropriate course of action. The composite power system expansion planning usually is developed by reliability justification or economic justification. Traditional system expansion planning is reliability based.

Reliability evaluation has been segregated into hierarchical levels HL-I (generation only), HL-II (generation and transmission), and HL-III (generation, transmission, and distribution), where the last is normally addressed by assuming the generation and transmission sides are perfectly reliable. The generation and transmission adequacy of composite system at hierarchical level HL-II is generally evaluated with the loss of load probability (LOLP) and the loss of load expectation (LOLE) [133].

In generation and transmission adequacy assessment, power system uncertainties, including load uncertainty, generation outage and transmission system contingency are modeled to calculate the reliability indices. Practically, there are two ways to perform the reliability evaluation: enumeration and Monte-Carlo simulation. Monte Carlo simulation, in theory, can include effects of all possible events on system. The required number of samples is independent of the size of the system to maintain a given accuracy level. Monte Carlo simulation is more flexible when complex operating conditions are incorporated for large-scale system. Reference [134] gives a thorough description of reliability evaluation for generation and transmission planning procedures.

Wind energy is growing fast and becoming a major portion of energy portfolio in many states. The federal government committed to supply 20% or more of the nation's electric energy needs from wind energy resources by 2030 [135]. Identifying what type and location of transmission is required to effectively integrate wind power is an important planning issue. It is a long term decision which involves decision criteria in terms of security, economy and

environment. Generation and transmission expansion for wind power integration rely on adding generation and transmission capacity to support transmission and reserve margin requirements when confronted with increasing wind power. To perform the planning procedure for wind power integration, the wind power uncertainty is typically characterized by a probability distribution. Then by using Monte-Carlo simulation, the reliability indices are calculated and generation and transmission capacity requirements can be chosen.

6.1.2 SPS planning related to wind

In the US, generation is growing 4 times faster than transmission, and the transmission capacity growth rate has been $\sim 1/3$ of peak load. Transmission upgrades are considered to be expensive and is constrained by time, land and environment. In Texas, which has about 25% of U.S. wind power, significant growth in 2008 pushed generation past transmission capacity by 65% by the end of that year [136]. In the near future, utilities will need devices such as SPS to trip non-priority generation since if transmission does not grow at the required pace. Thus, SPS, mainly in the form of wind generation rejection, is used to facilitate meeting reliability requirements while interconnecting wind power to the grid.

6.1.3 Accounting for SPS in planning

Special protection scheme, different from conventional local protection relay to isolate the faulted elements, is a wide area protection scheme. SPS uses wide area measurements to observe system behaviors [137], and takes wide area countermeasures to avoid unstable and unusual stresses on power systems. SPS actions include, among others, changes in load, generation, or system configuration to maintain system stability, acceptable voltages or power flows. Most of SPS are implemented by feed forward control. With feed forward control, the effect of disturbances or contingencies must be predicted accurately, and there must not be any unmeasured disturbances. Otherwise, the unmeasured disturbances will result in unintended action by SPS. Once a control signal has been sent by feed forward control in SPS, it cannot be further adjusted; any corrective adjustment must be by way of a new control signal. The reliability of SPS on precise control thus highly depends on the original control logic design.

The benefit of SPS is that it is a relatively inexpensive way to expand secure operation conditions. The cost of SPS is that its implementation results in exposure to additional failure modes. In generation and transmission expansion planning, potential unintended events corresponding to these additional failure modes can be predicted, assessed, and considered within a planning decision framework.

6.2 SPS interaction

The topic of SPS interaction and the proposed ways to identify such fault modes and their reliability indices using Monte Carlo simulation were presented in chapter 5. In this section, further insights into it in the light of planning is presented, especially weighing the issues related to high SPS penetration with respect to high cost transmission upgrade solution. The undesirable interactions among SPS degrade the reliability of system operation. Two major sources trigger undesirable and unintended interactions among SPS. One is failure of SPS. Another is faulty design logic of SPS.

Typically, SPS involves input (measurements), decision making system and action. Each component has failure rate though usually the failure rate is very low. The component failure of

SPS may result in interactions with other SPS. For example, a mis-operation of a generation rejection scheme which mis-trips a generation unit may result in a under frequency load shedding. Thus, a reliable SPS requires an appropriate level of redundancy. To enhance the reliability of SPS itself, the following NERC standards apply to SPS design [17]:

- SPS shall be designed so that cascading transmission outages or system instability do not occur for failure of a single component of an SPS, which would result in failure of the SPS to operate when required.
- Mis-operation, incorrect operation, or unintended operation of an SPS when considered by itself and not in combination with any other system contingency shall meet the system performance requirements as defined under NERC Planning Standards on Transmission Systems.
- All SPS installations shall be coordinated with other system protection and control schemes.
- All SPS operations shall be analyzed for correctness and documented.

Fault in SPS design logic is another source for undesirable interaction. Taking generation rejection scheme as an example, when the system is stressed with heavy loading, after a generation rejection scheme takes action to depress a stress of overload, the generation reschedule changes the power flow may result in overload on another transmission line and trip another generator by SPS, and result in cascading trip of generators if the SPS are not designed properly. It is difficult to design a backup scheme to avoid the incorrect logic for high penetration SPS. In contrary, transmission network upgrade can release the stress of operation thoroughly.

In Chapter 4, the reliability model of SPS was presented. To analyze the impacts of SPS interaction to system reliability, the SPS reliability model should be modeled in the simulation. By Monte Carlo simulation, the impacts can be calculated and associated with reliability indices.

6.2.1 Complexity for high penetration SPS

The interactions among SPS discussed above increase the complexity of power system planning, particularly for high penetration of SPS. Comparing with transmission planning, SPS planning is relatively new in power industry. Analysis on complexity of high penetration SPS is meaningful for power system planning.

According to Cambridge Advanced Learner's Dictionary, the definition of the word complexity is “when something has many parts and may be difficult to understand or find an answer to.” In the definitions of complexity in science and technology, it often used to describe a system with numerous elements which have intricate relationships among them. Warren Weaver categorized complexity as disorganized complexity and organized complexity [138] which influenced contemporary thinking about complexity. For the interactions under high penetration of SPS, it is a problem in which the number of elements is large, and the behavior of interactions triggered by the chain of unpredictable events associated with a contingency is difficult to manage or perhaps totally unknown which is characteristic of disorganized complexity.

Conceptually, the relation between the number of SPS and system operational risk is shown in Figure 50.

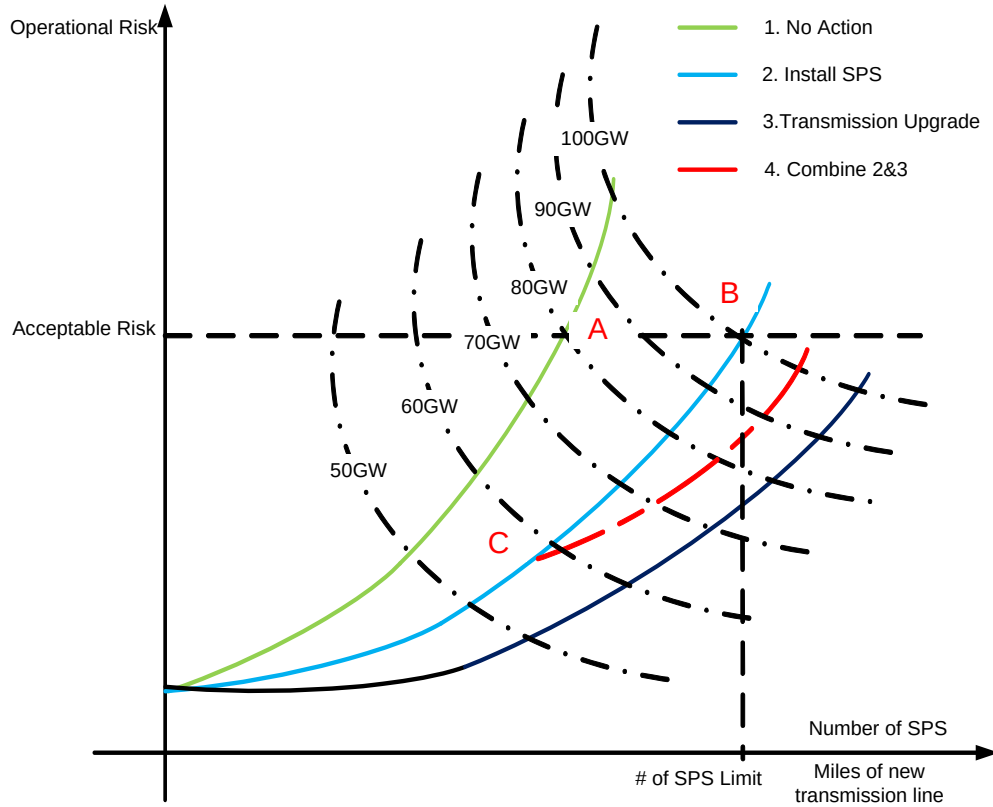


Figure 50: Complexity of SPS

Illustrated in Figure 50, when the system load increases, for example, from 50GW to 100GW gradually shown by the dotted line, the system becomes increasingly stressed. Without any action, as shown by the green line, the operational risk is increasing and becomes unacceptable when the load demand is increased beyond 80GW as shown at point A in Figure 50. With SPS, the operational risk can be reduced. But as the number of SPS increases, the operational risk associated with the undesirable interactions among SPS increases. Without transmission upgrade, utilizing more SPS reaches the limit of acceptable operational risk at a load of 100 GW, as shown at point B. On the other hand, use of transmission network upgrades enable operation within the acceptable risk limit for loading levels well beyond 100 GW, as shown by the dark blue line in the figure. But use of transmission upgrades only is an expensive approach. A practical way is to combine the two approaches, SPS installation and transmission network upgrade, to achieve secure operation of the system. In Section 6.2.2 below, a small system case study is used to illustrate the limit of SPS, the number of events increasing exponentially and more lost load occurring with the increasing number of SPS.

6.2.2 Illustration

Small system for overload-motivated wind plant rejection

Assume three 100 MW wind plants are built in sequence A, B, and C, as shown in Figure 51. Branch data for the system on a 100 MVA base are given in Table 15.

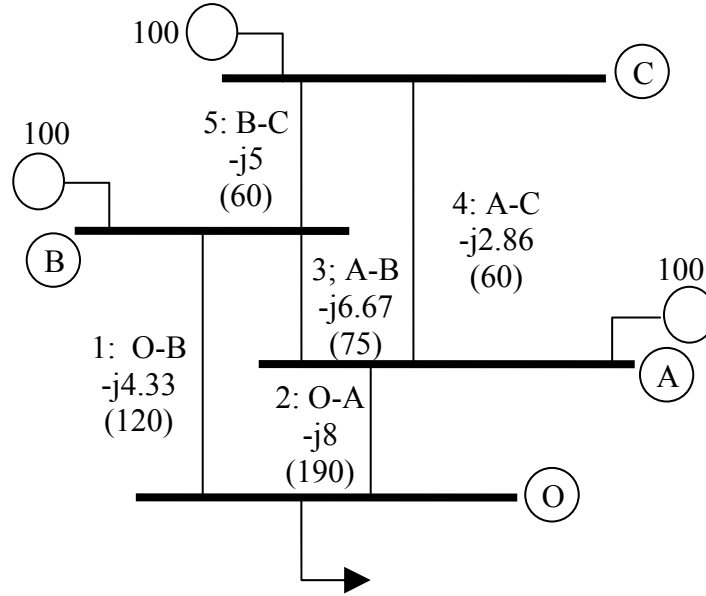


Figure 51: Small system for illustrating concepts

Table 15: Branch data for sample system

Line	Reactance	Susceptance
O-A	0.125	8
O-B	0.231	4.33
A-C	0.35	2.86
B-C	0.2	5
A-B	0.15	6.67

Matlab code was written to perform DC power flow analysis on this system, assuming Bus O as the reference bus. Assessment was done for various combinations of wind plants on-line, line outages, and wind plants tripped based on SPS. Results are summarized in Table 16. We can notice from the simple illustration that the chances of interactions among SPS increases under certain contingencies. Such Monte Carlo simulation based on the approach presented in chapter 5 can be done for many loading conditions for a system with many SPS, to identify the undesirable consequences and plan to mitigate them.

All post-contingency overload problems may also be corrected without SPS by building one transmission line with impedance 0.111 and capacity 182 MW from node C to node O, as shown in Figure 52.

Table 16: SPS designs for different wind plant growth stages

Wind plants operating	Actuating line outages	Gen trip	Post-contingency line flows (percent of normal rating)					Events resulting in lost load					
								Lost load, SPS works	Lost load, SPS fails	Inadvertent SPS operations following first trip			
										Event		Event	
			1: O-B	2: O-A	3: A-B	4: A-C	5: B-C			What trips	Lost load	What trips	Lost load
A	none	none	.22	.39	-.28	-.09	0.09	NA	NA	NA	NA	NA	NA
A	O-B	none	-	.53	0	0	0	NA	NA	NA	NA	NA	NA
A	O-A	none	-					NA	NA	NA	NA	NA	NA
A,B	none	none	.65	.64	.23	.08	-.08	NA	NA	NA	NA	NA	NA
A,B	O-B	none	-	1.05	1.05	.36	-.36	NA	NA	NA	NA	NA	NA
A,B	O-B	B	-	.53	0	0	0	100	200	A	100	NA	NA
A,B	O-A	none	-		0	0	0	NA	NA	NA	NA	NA	NA
A,B	O-A	A										NA	NA
A,B,C	none	none	1.0	.95	.46	.76	.90	NA	NA	NA	NA	NA	NA
A,B,C	O-B	none	-	1.58	1.71	1.19	.48	NA	NA	NA	NA	NA	NA
A,B,C	O-B	B,C	-		0.53	0	0	200	300	A	100	NA	NA
A,B,C	O-A	none	2.5	-	-1.4	.12	1.55	NA	NA	NA	NA	NA	NA
A,B,C	O-A	A,C	.83	-	0	0	0	200	300	B	100	NA	NA
A,B,C	A-C	none	1.27	.96	1.10	-	1.67	NA	NA	NA	NA	NA	NA
A,B,C	A-C	C	.75	.69	.41	-	0	100	300	A	100	B	100
A,B,C	B-C	none	1.39	1.31	.65	1.67	-	NA	NA	NA	NA	NA	NA
A,B,C	B-C	B,C	.33	.46	-.16	0	-	200	300	A	100	NA	NA

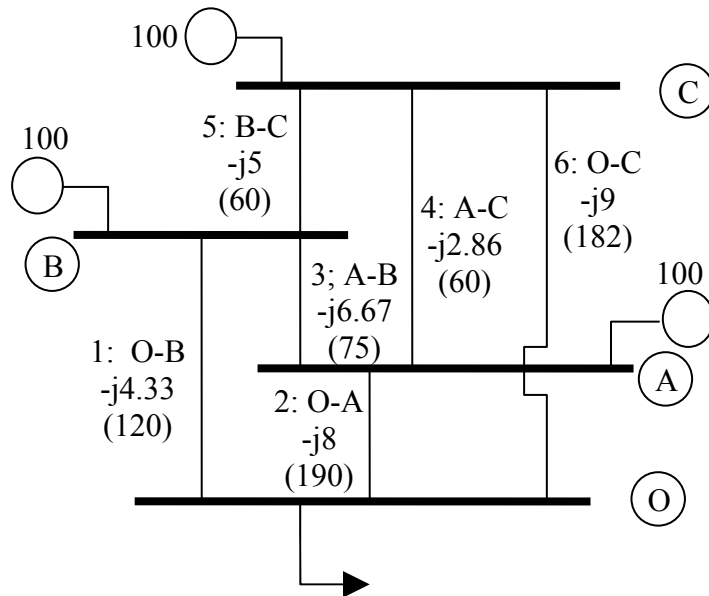


Figure 52: Small system with transmission upgrade

Although construction of the line would be expensive, there is significant benefit in two main ways:

- **Reduced level of complexity:** The overall system is simpler to operate and maintain. Without SPS,
 - there is no need to perform periodic maintenance, including self-checks for operability, to ensure integrity of sensing, communication, and actuation;
 - there is no need to monitor arming of schemes;
 - there is no anxiety felt by individuals responsible for ensuring the integrity of the SPS and of the power system being operate
- **More reliable system:** Without SPS,
 - there is no possibility of lost load due to an inadvertent trip during normal conditions;
 - there is no tripping for the actuating line outages (this refers to the lost load when SPS works in Table 16)
 - there is no possibility of lost load due to SPS failure
 - there is no possibility of lost load due to inadvertent SPS operations following a first-trip

6.3 Incorporating SPS in generation and transmission expansion planning

The electric grid has been undergoing rapid growth in load. Also more and more generation especially renewable sources are being connected to the grid. However, limited transmission poses a problem to this growth, which if not taken care of will lead to the electric grid not being able to meet demand and accommodate cheaper generating resources. SPS are economically cheaper than transmission expansion and could help alleviate the problem of ever increasing load and aggressive renewable generation installation.

6.3.1 Case study

The system used is a 5 bus system with 4 generators as shown in Figure 53. This system is used to illustrate and solve a 15 year planning problem that incorporates SPS and transmission expansion plans into achieving demand and generation expansion plans from 2015-2029. The goal is to minimize production costs and investments costs while also minimizing operational complexity that comes with increasing number of SPS. The loads at Bus 2, Bus 3, and Bus 4 are assumed to be growing at 3%, 4%, and 3.5% respectively as shown in Table 18. Table 19 presents the test system branch data. Table 20 shows the generator cost data, and Table 21 presents the generation expansion plans through the various planning period.

Table 17: Time periods

Periods	Time Periods
1	2015 - 2019
2	2020 - 2024
3	2025 - 2029

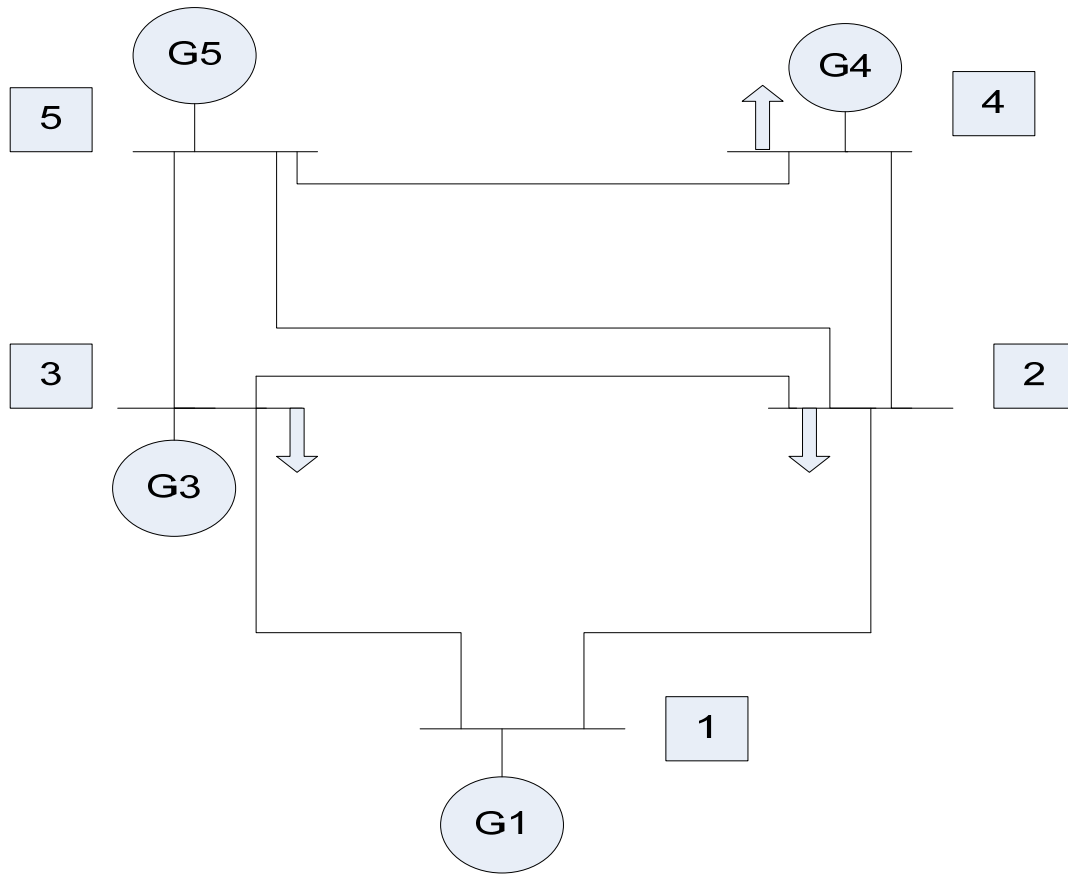


Figure 53: 5-bus system

Table 18: Forecasted load

Bus\Year	2010	2015	2020	2025
Bus 2	500	579.65	671.95	779
Bus 3	400	486.68	592.08	720.36
Bus 4	350	415.70	493.71	586.36

Table 19: Branch data

Line	Reactance	Capacity
1-2	0.2	90MW
1-3	0.25	90MW
2-3	0.1	800MW
2-5	0.1	800MW
3-4	0.1	800MW
3-5	0.1	800MW
4-5	0.1	800MW

Generator cost curves are assumed to be in a quadratic form,

$$z = a + bP + cP^2 \quad (6.1)$$

Table 20: Generator data

Generator	c co-efficient	b co-efficient	Capacity at 2015
G1	0.09	20	80MW
G3	0.25	20	800MW
G4	0.20	40	800MW
G5	0.01	40	800MW

Table 21: Generation expansion plans

Generator (G1)	Year	Expansion plans
G1	2015	80MW to 200MW
G1	2020	200MW to 300MW
G1	2025	300MW to 400MW

6.3.2 Transmission expansion options and specifications

❖ Options

- Build line from bus 1 to bus 2
- Build line from bus 1 to bus 3
- Build double lines from bus 1 to bus 2, and bus 1 and bus 3

❖ Specifications

- Line capacity should vary between 50MW to 200MW
- SPS cannot be used on a new line

❖ Operational constraints

- Only one generating unit should be tripped at a given time
- Not more than two lines can be tripped at the same time

6.3.3 Transmission expansion tree

Transmission expansion tree is a tree that shows possible actions (i.e., transmission only or SPS-aided transmission expansion options) that can be taken at different periods to accommodate more generation expansion plans and load growth, as shown in Figures 54 and 55. We found 27 possible solutions that include transmissions only solution as well as many SPS-aided transmission expansion options, as shown in Table 22 that is continued over 3 pages. In Table 22, for instance build 1-23 means building third line from bus 1 to bus 2, where the original line is names as 1-21.

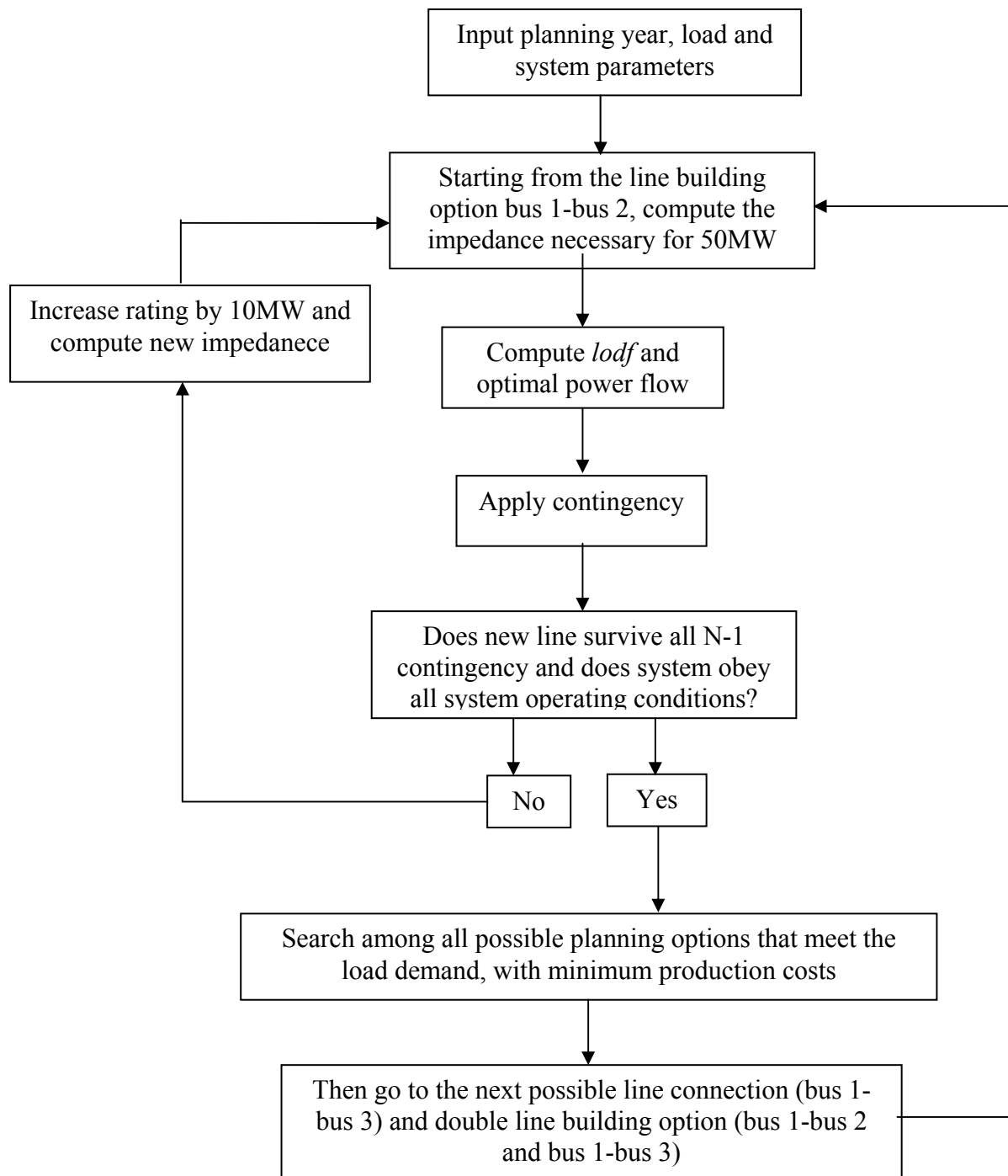


Figure 54: Transmission tree expansion- numerical optimization

IN 2015 THE FOLLOWING OPTIONS ARE AVAILABLE

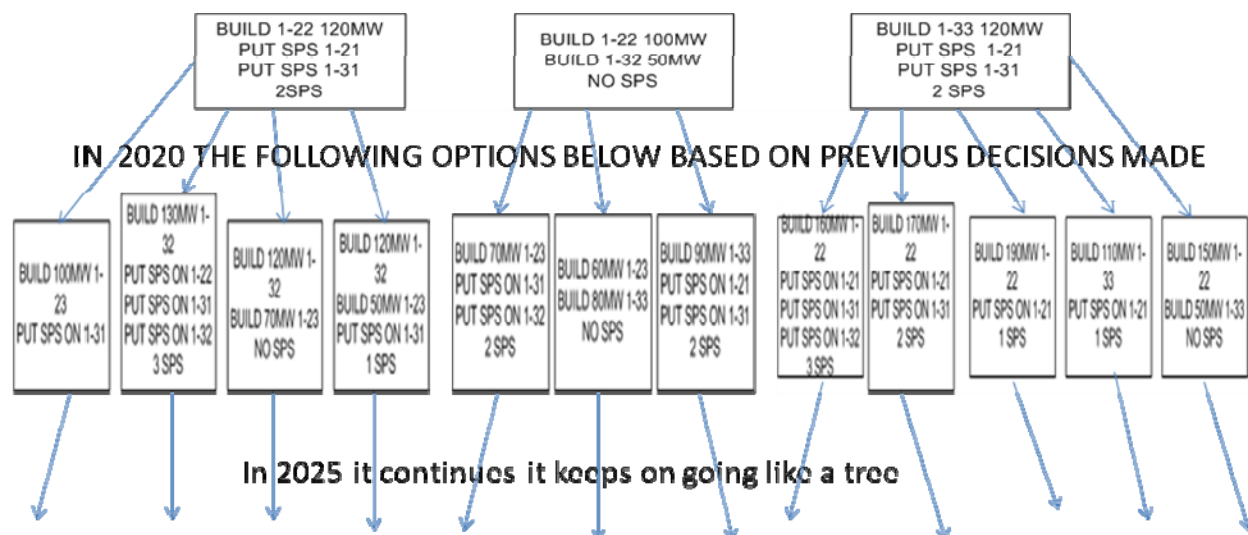


Figure 55: Transmission tree

Table 22: Possible solutions

Year	2015	2020	2025
X1	Build 1-22 100MW X=0.18 Build 1-32 50MW X= 0.45; NO SPS	Build 1-23 60MW X = 0.30 Build 80MW 1-33 X= 0.2813; NO SPS	Build 1-24 50MW X=0.36 Build 1-34 90MW X= 0.25; NO SPS
X2	Build 1-22 100MW X =0.18 Build 1-32 50MW X= 0.45 NO SPS	Build 1-23 70MW X=0.2571 Put SPS on 1-31 Put SPS on 1-32 2 SPS	Build 1-24 90MW X= 0.36 Put SPS on 1-31 Put SPS on 1-32 2 SPS
X3	Build 1-22 100MW X =0.18 Build 1-32 50MW X= 0.45 NO SPS	Build 90MW 1-33 X= 0.25 Put SPS on 1-21 Put SPS on 1-22 2 SPS	Build 90MW 1-23 X=0.20 Build 80MW 1-34 X= 0.2813 NO SPS
X4	Build 1-22 120MW X=0.15 Put SPS on 1-21 Put SPS on 1-31 2 SPS	Build 100 MW 1-23 X=0.1636 Put SPS on 1-31 1 SPS	Build 100 MW 1-24 X=0.1636 Put SPS on 1-31 1 SPS
X5	Build 1-22 120MW X=0.15 Put SPS on 1-21 Put SPS on 1-31 2 SPS	Build 100 MW 1-23 X=0.1636 Put SPS on 1-31 1 SPS	Build 150MW 1-24 X=0.12 Build 200MW 1-32 X=0.1125 NO SPS
X6	Build 1-22 120MW X=0.15 Put SPS on 1-21 Put SPS on 1-31 2 SPS	Build 130MW 1-32 X=0.1731 Put SPS on 1-21 Put SPS on 1-22 Put SPS on 1-31 3 SPS	Build 90MW 1-23 X=0.20 Put SPS on 1-31 Put SPS on 1-32 2 SPS

Year	2015	2020	2025
X7	Build 1-22 120MW X=0.15 Put SPS on 1-21 Put SPS on 1-31 2 SPS	Build 130MW 1-32 X=0.1731 Put SPS on 1-21 Put SPS on 1-22 Put SPS on 1-31 3 SPS	Build 140MW 1-33 X=0.1607 Put SPS on 1-21 Put SPS on 1-22 Put SPS on 1-31 Put SPS on 1-32 4 SPS
X8	Build 1-22 120MW X=0.15 Put SPS on 1-21 Put SPS on 1-31 2 SPS	Build 130MW 1-32 X=0.1731 Put SPS on 1-21 Put SPS on 1-22 Put SPS on 1-31 3 SPS	Build 80MW 1-23 X=0.225 Build 90MW 1-33 X=0.25 NO SPS
X9	Build 1-22 120MW X=0.15 Put SPS on 1-21 Put SPS on 1-31 2 SPS	Build 120MW 1-32 X=0.1875 Build 70MW 1-23 X=0.2571 NO SPS	Build 50MW 1-24 X=0.36 Put SPS on 1-31 Put SPS on 1-32 2 SPS
X10	Build 1-22 120MW X=0.15 Put SPS on 1-21 Put SPS on 1-31 2 SPS	Build 120MW 1-32 X=0.1875 Build 70MW 1-23 X=0.2571 NO SPS	BUILD 100MW 1-33 X=0.225 NO SPS
X11	Build 1-22 120MW X=0.15 Put SPS on 1-21 Put SPS on 1-31 2 SPS	Build 120MW 1-32 X=0.1875 Build 70MW 1-23 X=0.2571 NO SPS	BUILD 100MW 1-33 X=0.225 BUILD 50MW 1-24 X=0.36 NO SPS
X12	Build 1-22 120MW X=0.15 Put SPS on 1-21 Put SPS on 1-31 2 SPS	Build 120MW 1-32 X=0.1875 Build 50MW 1-23 X=0.36 1 SPS	Build 70MW 1-24 X=0.2571 Put SPS on 1-31 Put SPS on 1-32 2 SPS
X13	Build 1-22 120MW X=0.15 Put SPS on 1-21 Put SPS on 1-31 2 SPS	Build 120MW 1-32 X=0.1875 Build 50MW 1-23 X=0.36 1 SPS	BUILD 100MW 1-33 X=0.225 BUILD 50MW 1-24 X=0.36 NO SPS
X14	Build 1-32 120MW X=0.15 Put SPS on 1-21 Put SPS on 1-31 2 SPS	Build 160MW 1-22 X=0.1125 Put SPS on 1-21 Put SPS on 1-31 Put SPS on 1-32 3 SPS	Build 90MW 1-23 X=0.2 Put SPS on 1-31 Put SPS on 1-32 2 SPS
X15	Build 1-32 120MW X=0.15 Put SPS on 1-21 Put SPS on 1-31 2 SPS	Build 160MW 1-22 X=0.1125 Put SPS on 1-21 Put SPS on 1-31 Put SPS on 1-32 3 SPS	Build 120MW 1-33 X=0.1875 Put SPS on 1-21 Put SPS on 1-22 2 SPS

Year	2015	2020	2025
X16	Build 1-32 120MW X=0.15 Put SPS on 1-21 Put SPS on 1-31 2 SPS	Build 160MW 1-22 X=0.1125 Put SPS on 1-21 Put SPS on 1-31 Put SPS on 1-32 3 SPS	Build 100MW 1-33 X=0.225 Build 50MW 1-23 X=0.36 NO SPS
X17	Build 1-32 120MW X=0.15 Put SPS on 1-21 Put SPS on 1-31 2 SPS	Build 170MW 1-22 X=0.1059 Put SPS on 1-21 Put SPS on 1-31 2 SPS	Build 90MW 1-23 X=0.2 Put SPS on 1-31 Put SPS on 1-32 2 SPS
X18	Build 1-32 120MW X=0.15 Put SPS on 1-21 Put SPS on 1-31 2 SPS	Build 170MW 1-22 X=0.1059 Put SPS on 1-21 Put SPS on 1-31 2 SPS	Build 120MW 1-33 X=0.15 Put SPS on 1-21 Put SPS on 1-22 2 SPS
X19	Build 1-32 120MW X=0.15 Put SPS on 1-21 Put SPS on 1-31 2 SPS	Build 170MW 1-22 X=0.1059 Put SPS on 1-21 Put SPS on 1-31 2 SPS	Build 100MW1-33 X=0.225 Build 50MW 1-23 X=0.36 NO SPS
X20	Build 1-32 120MW X=0.15 Put SPS on 1-21 Put SPS on 1-31 2 SPS	Build 190MW 1-22 X=0.0947 Put SPS on 1-21 1 SPS	Build 90MW 1-23 X=0.2 Put SPS on 1-31 Put SPS on 1-32 2 SPS
X21	Build 1-32 120MW X=0.15 Put SPS on 1-21 Put SPS on 1-31 2 SPS	Build 190MW 1-22 X=0.0947 Put SPS on 1-21 1 SPS	Build 120MW 1-33 X=0.15 Put SPS on 1-21 1 SPS
X22	Build 1-32 120MW X=0.15 Put SPS on 1-21 Put SPS on 1-31 2 SPS	Build 190MW 1-22 X=0.0947 Put SPS on 1-21 1 SPS	Build 100MW1-33 X=0.225 Build 50MW 1-23 X=0.36 NO SPS
X23	Build 1-32 120MW X=0.15 Put SPS on 1-21 Put SPS on 1-31 2 SPS	Build 110MW 1-33 X=0.2045 Put SPS on 1-21 1 SPS	Build 190MW 1-22 X=0.0947 Put SPS on 1-21 1 SPS
X24	Build 1-32 120MW X=0.15 Put SPS on 1-21 Put SPS on 1-31 2 SPS	Build 110MW 1-33 X=0.2045 Put SPS on 1-21 1 SPS	Build 120MW 1-34 X=0.1875 Put SPS on 1-21 1 SPS
X25	Build 1-32 120MW X=0.15 Put SPS on 1-21 Put SPS on 1-31 2 SPS	Build 110MW 1-33 X=0.2045 Put SPS on 1-21 1 SPS	Build 50MW 1-34 X=0.45 Build 180MW 1-22 X=0.1 No SPS

Year	2015	2020	2025
X26	Build 1-32 120MW X=0.15 Put SPS on 1-21 Put SPS on 1-31 2 SPS	Build 150MW 1-22 X=0.12 Build 50MW 1-33 X=0.45 NO SPS	Build 70MW 1-34 X= 0.3214 Put SPS on 1-21 Put SPS on 1-22
X27	Build 1-32 120MW X=0.15 Put SPS on 1-21 Put SPS on 1-31 2 SPS	Build 150MW 1-22 X=0.12 Build 50MW 1-33 X=0.45 NO SPS	Build 1-23 50MW X=0.36 Build 1-34 50MW X=0.45 NO SPS

6.3.4 Operational complexity

SPS are economically cheaper but their increase can actually increase operational complexity of the electric grid. In regards to power system maintenance, SPS increases operation complexity because with the increased transmission system utilization that comes with the application of SPS, planned transmission outages may become more difficult to schedule. In the area of protection co-ordination, coordinating multiple SPS with other protection systems causes co-ordination complexity. With regards to mis-operation, mis-operation of one SPS could bring about serious cascading consequences. Therefore, it is necessary to come up with a metric that can measure how much complexity we bring into the system by using SPS, and use that metric as one of the decision criteria at the planning stage.

An operational complexity metric proposed in this report is the total number of states of SPS failure modes that will be encountered in reliability studies. The states will increase as the number of SPS in the system increases, which will indicate the possibility of increasing operational complexity. For instance, one SPS has at least 3 states:

1. No failure mode
2. Will fail to operate
3. Will inadvertently operate

Likewise,

- 2 SPS will have 8 states
- 3 SPS will have 27 states
- 4 SPS will have 64 states
- 20 SPS will have 8000 states
- 50 SPS will have 125000 states

For example, in option X16 of Table 22,

- For 2015 - Build 120MW 1-32 and put SPS on 1-21 and 1-31 (2 SPS)
- For 2020 - Build 160MW 1-22 and put SPS on 1-21, 1-31, 1-32 (3 SPS)
- For 2025- Build 100MW 1-33 and 50MW 1-23 (no SPS)

Based on our definition, we have a total complexity of $2^3 + 3^3 + 0^3 = 35$ states.

6.3.5 Production costs

Production cost refers to the operational costs accompanied with producing electric energy. The optimized production cost for a planning option is computed as,

$$\text{Min} \sum_j \sum_i \text{ProC}_{ij} * P_i * 8760 \quad (6.2)$$

where,

ProC_{ij} is the production cost for i^{th} loading scenario of j^{th} year,

P_i is the probability of i^{th} loading scenario of j^{th} year.

The optimization is subject to generator capacity constraint, transmission capacity constraint, power balance, and network flow constraints. The system loading scenarios used for computing production cost of various planning options are represented in terms of percentage of peak load. The probabilities of load profile shown in Table 23 were estimated from MISO load duration curve [139].

Table 23: Probabilistic load profiles

Loading scenarios	Probability
40%	0.0297
45%	0.0191
50%	0.0894
55%	0.1084
60%	0.1998
65%	0.2317
70%	0.145
75%	0.097
80%	0.0365
85%	0.0228
90%	0.0114
95%	0.008
100%	0.0034

6.3.6 Economic factors

6.3.6.1 EENS costs

EENS is the expected energy not served due to forced curtailment actions by SPS. The cost of a particular occurrence is computed by multiplying the associated EENS and a coefficient called the value of lost load (VOLL).

$$\text{EENS} = \sum_{j \in LC} L_{kj} \times D_j \times f_i \quad (6.3)$$

where,

L_{kj} is load curtailed at bus k due to contingency j ,
 D_j is duration (hours) of load curtailment due contingency j , and
 f_j is frequency of occurrence of outage j .

$$EENS_{cost} = \sum_k EENS_i * VOLL_j \quad (6.4)$$

where,

k is number of years,

$EENS_{cost}$ is Expected Energy not served due to forced curtailments of SPS actions,

$EENS_i$ is Expected Energy not served due to forced curtailments of SPS actions i^{th} option, and

$VOLL_j$ is value of load lost at period j .

6.3.6.2 System interruption costs

This is the difference between post-contingency production costs and pre-contingency production costs due to SPS action of tripping a cheaper generator and employing a more expensive generator.

$$SysIntcost_{ij} = \sum_{\forall j} \sum_{\forall k} (PostCProd_{ij} - PreCProd_{ij}) * DTG * (1.05)^k \quad (6.5)$$

where,

k is 0, 1, 2, 3, 4 (number of years in time period)

j is (2015, 2020, 2025)

$SysIntcost_{ij}$ = System interruption cost associated with i^{th} option at period j .

$PreCProd_{ij}$ = Pre-contingency production cost associated with i^{th} option at period j

$PostCProd_{ij}$ = Post-contingency production cost associated with i^{th} option at period j

DTG = Down time of tripped generator

6.3.6.3 Investment costs

There is cost associated with the investment in SPS and transmission expansion projects, with their inflation rate assumed to be about 5%.

6.3.6.4 Congestion rent

Congestion rent is the difference between the price of electricity at the point of delivery and at the point of generation. Congestion rent is also called the re-dispatch cost because it is the extra cost expended for dispatching more expensive generators that would be needed if the transmission system had enough capacity and did not constrain power transfer.

6.3.7 Study assumptions

- The **cost of transmission upgrade** is assumed to be \$600,000/MW. It is also assumed that the cost of materials for building transmission lines has an inflation rate of 2%.

- The **cost of SPS** is assumed to be \$1,000,000. It is also assumed to have an inflation rate of 2%. All the costs are expressed in present value.
- The **congestion rent** is the difference between constrained and unconstrained production costs. The production costs are computed for different loading scenarios for 15 years which includes three 5-year planning intervals.
- Similarly, **EENS cost** is computed for 15 year planning period. For options with SPS, EENS is computed from the forced curtailments. In this study, the probability of each contingency that enables SPS to operate is assumed to be 0.1. The forced load curtailment is assumed to be the generator output of G1, due to load-generation balance. The duration for lost load is assumed to be 3hrs. The VOLL (Value of load lost) for the 3 planning intervals are given in Table 24.

Table 24: Different periods and associated value of load lost

Period	VOLL
1	\$300/MWh
2	\$500/MWh
3	\$800/MWh

Table 25 presents a comparison of different economic factors for various possible planning options comprising of transmission only and SPS aided transmission expansion options.

Table 25: Comparison of economic factors for planning options

Options	Transmission costs	SPS costs	Congestion rent	Interruption Costs	EENS (MWh)	EENS Costs	Complexity	Budget	Total costs
X1	\$285,140,400	\$0	\$0	\$0	0	\$0	0	\$285,140,400	\$285,140,400
X2	\$202,198,200	\$2,208,200	\$1,804,138	\$3,274,100	7800	\$4,809,000	16	\$204,406,400	\$214,293,638
X3	\$273,959,400	\$2,208,200	\$0	\$666,050	1800	\$90,000	8	\$276,167,600	\$276,923,650
X4	\$211,386,000	\$2,000,000	\$14,347,000	\$3,543,100	7800	\$5,160,000	14	\$213,386,000	\$236,436,100
X5	\$394,236,000	\$2,000,000	\$0	\$1,590,900	4050	\$1,845,000	11	\$396,236,000	\$399,671,900
X6	\$223,945,800	\$4,323,100	\$0	\$2,947,100	7050	\$4,785,000	41	\$228,268,900	\$236,001,000
X7	\$260,515,800	\$4,323,100	\$0	\$1,353,100	3450	\$1,905,000	99	\$264,838,900	\$268,097,000
X8	\$282,457,800	\$3,104,100	\$0	\$821,710	2250	\$945,000	35	\$285,561,900	\$287,328,610
X9	\$234,437,400	\$4,438,000	\$0	\$1,839,000	4500	\$3,150,000	16	\$238,875,400	\$243,864,400
X10	\$271,007,400	\$2,000,000	\$0	\$244,900	900	\$54,000	8	\$273,007,400	\$273,306,300
X11	\$307,577,400	\$2,000,000	\$0	\$244,900	900	\$270,000	8	\$309,577,400	\$310,092,300
X12	\$235,816,200	\$3,219,000	\$0	\$2,031,200	4950	\$3,375,000	19	\$239,035,200	\$244,441,400
X13	\$294,328,200	\$2,000,000	\$0	\$437,170	1350	\$495,000	11	\$296,328,200	\$297,260,370
X14	\$243,819,600	\$3,104,100	\$0	\$2,415,800	5850	\$3,825,000	43	\$246,923,700	\$253,164,500
X15	\$265,761,600	\$4,323,100	\$0	\$1,353,100	3450	\$1,905,000	43	\$270,084,700	\$273,342,800
X16	\$287,703,600	\$3,104,100	\$0	\$821,710	2250	\$945,000	35	\$290,807,700	\$292,574,410
X17	\$250,444,200	\$3,219,000	\$0	\$2,223,500	5400	\$3,600,000	24	\$253,663,200	\$259,486,700
X18	\$272,386,200	\$3,219,000	\$0	\$1,160,800	3000	\$1,680,000	24	\$275,605,200	\$278,446,000
X19	\$294,328,200	\$2,000,000	\$0	\$629,440	1800	\$720,000	16	\$296,328,200	\$297,677,640
X20	\$263,693,400	\$4,323,100	\$0	\$2,031,200	4960	\$3,375,000	19	\$268,257,100	\$273,663,300
X21	\$285,635,400	\$2,000,000	\$0	\$702,840	1950	\$975,000	14	\$287,635,400	\$289,313,240
X22	\$307,577,400	\$2,000,000	\$0	\$437,170	1350	\$495,000	11	\$309,577,400	\$310,509,570
X23	\$283,836,600	\$2,000,000	\$0	\$1,279,700	3300	\$1,650,000	14	\$285,836,600	\$288,766,300
X24	\$232,638,600	\$2,000,000	\$52,911	\$2,342,400	5700	\$3,570,000	14	\$234,638,600	\$240,603,911
X25	\$313,092,600	\$3,219,000	\$0	\$1,014,000	2700	\$1,170,000	11	\$316,311,600	\$318,495,600
X26	\$255,690,000	\$4,323,100	\$0	\$776,250	2700	\$1,230,000	16	\$260,013,100	\$262,019,350
X27	\$277,632,000	\$2,000,000	\$0	\$244,900	900	\$270,000	8	\$279,632,000	\$280,146,900

6.3.8 Optimization model

Multi-objective optimization (or programming), also known as multi-criteria or multi-attribute optimization, is the process of simultaneously optimizing two or more conflicting objectives subject to certain constraints.

$$\begin{aligned}
& \text{Min } X_i \sum \text{INVT}_{ij} + X_i \sum \text{INVSPS}_{ij} + X_i \sum \text{EENS}_{FCij} + X_i \sum \text{ConRent}_{ij} + X_i \sum \text{SysInt cost}_{ij} \\
& \text{Min } X_i \sum \text{OPC}_{ij} \\
& \text{for all } i, j \\
& \text{subject to} \\
& \text{Budget} \\
& \text{EENS} \\
& X_i \text{ Binary}
\end{aligned} \tag{6.6}$$

where,

$X_i = i^{\text{th}}$ possible planning option,

INVT_{ij} = Transmission investment cost associated with i^{th} option at period j ,

INVSPS_{ij} = SPS investment costs associated with i^{th} option at period j ,

EENS_{FCij} = EENS costs due to forced curtailments associated with i^{th} option at period j ,

ConRent_{ij} = Congestion rent associated with i^{th} option at period j ,

OPC_{ij} = Operational complexity associated with i^{th} option at period j .

The conflicting part here is the cost vs. operational complexity, as even though SPS is cheaper option, its increase in the system will increase the operational complexity as discussed before. In this formulation, it is to be noted that the influence of transmission investment decision on the operational complexity metric has not been modeled. In reality, a transmission investment decision will certainly have its effect on operational complexity, which could even be a negative effect, i.e., of reducing the maintenance requirements, and making system operation and maintenance a lot easier. So it is very important to model it in this problem. But in this case, we have made an assumption that any transmission investment decision, irrespective of its high investment cost, will not contribute to increase in the system operational complexity. So the second objective of this problem always supports transmission investment decisions.

6.3.9 Optimization methods

6.3.9.1 Penalty factor method

This approach is based on weighting the objectives, similar to the approached in [140]. The bi-level optimization problem can be converted into a single objective optimization by introducing a cost-complexity penalty factor as follows,

$$p = \frac{C_d - C^*}{D_c - D^*} \tag{6.7}$$

where,

C^* is the optimal value of complexity objective function of the optimal solution,
 D^* is the optimal value of cost objective function of the optimal solution,
 C_d is the cost value of the optimal solution for complexity objective function, and
 D_c is the complexity value of the optimal solution for cost objective function.

The problem now becomes

$$\begin{aligned}
 \text{Min } \theta_T &= w * f_1(x) + (1 - w) * p * f_2(x) \\
 \text{subject to} \\
 \text{Budget} \\
 \text{EENS} \\
 X_i &\text{ Binary}
 \end{aligned} \tag{6.8}$$

where,

$f_1(x)$ is the cost function,

$f_2(x)$ is the operational complexity metric,

p is the cost-complexity penalty function, and

w is the weighting factor such that $0 \leq w \leq 1$.

When $w = 0$, the optimization is minimizing complexity, and when $w = 1$ it is minimizing cost.

6.3.9.2 Non-linear penalty factor method

This technique is analogous to the weighted method but different weights are assigned to objective values of different options, making the cost-complexity penalty factor independent and non-linear. The nonlinear relationship between complexities of various planning options is assumed be an exponential ratio.

$$w_i = \left(\frac{C_i}{C_d} \right)^k \left(\frac{C_d - C^*}{D_c - D^*} \right) \tag{6.9}$$

where, C_i is the complexity value for the i^{th} option.

The problem now becomes

$$\begin{aligned}
 \text{Min } \theta_T &= f_1(x) + w_i * f_2(x) \\
 \text{subject to} \\
 \text{Budget} \\
 \text{EENS} \\
 X_i, &\text{ Binary}
 \end{aligned} \tag{6.10}$$

where,

w_i is a co-efficient computed for each option.

6.3.10 Analytical Hierarchical Process

Analytical Hierarchical Process (AHP) was developed by Thomas Saaty, and is being prevalently used for decision making in various fields. AHP is a structured method for ranking a list of objectives. AHP doesn't prescribe a "correct" decision, but helps in finding the best alternative according to the user's needs and problem comprehension.

The following are the steps for implementing the AHP algorithm [141]

Step 1: A structural model of the hierarchy as shown in Figure 56 is set up.

Step 2: A judgment matrix is formed.

Depending upon the user's knowledge on the relative importance of every pair of criteria, each element in the judgment (or comparison) matrix is attributed a value. The measurement scale used by AHP consists of the following elements, $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, and their reciprocal. In the pair-wise comparison matrix, the number in the i th row and j th column gives the relative importance of the criterion C_i as compared to criterion C_j . For instance,

- $a_{ij} = 1$ indicates the criteria are equal in importance
- $a_{ij} = 3$ indicates C_i is weakly more important than C_j
- $a_{ij} = 5$ indicates C_i is strongly more important than C_j
- $a_{ij} = 7$ indicates C_i is very strongly more important than C_j
- $a_{ij} = 9$ indicates C_i is absolutely more important than C_j

The values 2, 4, 6 and 8 can also be used as intermediate values. These values form the upper triangle of the comparison matrix. The lower triangle is filled with reciprocal of the value in the upper triangle, indicating the relative importance of the criteria in a reciprocal manner. The diagonal elements are always 1.

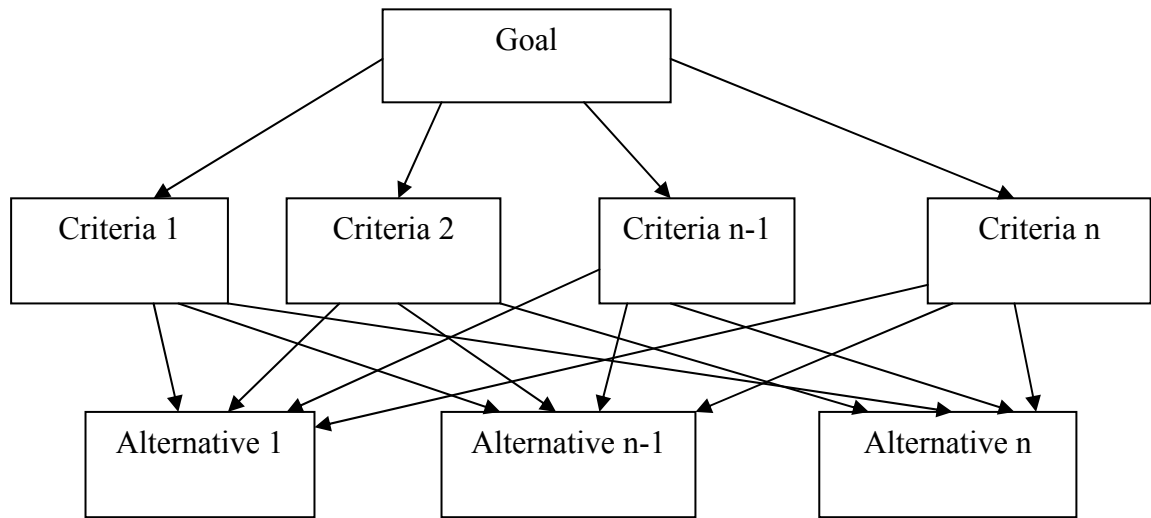


Figure 56: Simple structure of analytical hierarchical process

Step 3: The maximal eigenvalue of the judgment matrix and its corresponding eigenvector is computed. This provides the value of the weighting coefficients of all criteria.

Step 4: Hierarchical rank and consistency of results are checked.

The element's values in the eigenvector gives the relative importance of all the criteria. So the hierarchical ranking is performed according to these values of eigenvector elements. The hierarchy ranking's consistency index is checked using the below formula,

$$CI = \frac{(\lambda_{\max} - n)}{(n-1)} \quad (6.11)$$

where,

$\lambda_{\max}$ - the maximal eigenvalue of judgment matrix, and

n - the dimension of the judgment matrix.

Generally, a value less than 0.1 is a very acceptable consistency index.

Application of AHP to SPS aided transmission planning

Most electric power planning decisions are usually based on reliability and economic factors. When incorporating SPS into transmission and generation expansion, it is necessary to take into account the operational complexity that SPS adds to the electric power grid operations. Because without SPS, planned outages will be easier to schedule and maintenance becomes easier. Analytical hierarchical process (AHP) is used to evaluate the non-dominated solutions based on the conflicting objectives of total costs and proposed operational complexity index. Three criteria, i.e., the total cost, reliability (EENS - forced curtailments due to SPS) and operational complexity are used in this problem to rank the alternatives. Figure 57 presents the structure of the hierarchy for power system SPS aided transmission expansion planning. Since AHP is a preference based ranking, the power system planner has the facility to weigh the various criteria based on the utility's needs and their understanding of the problem.

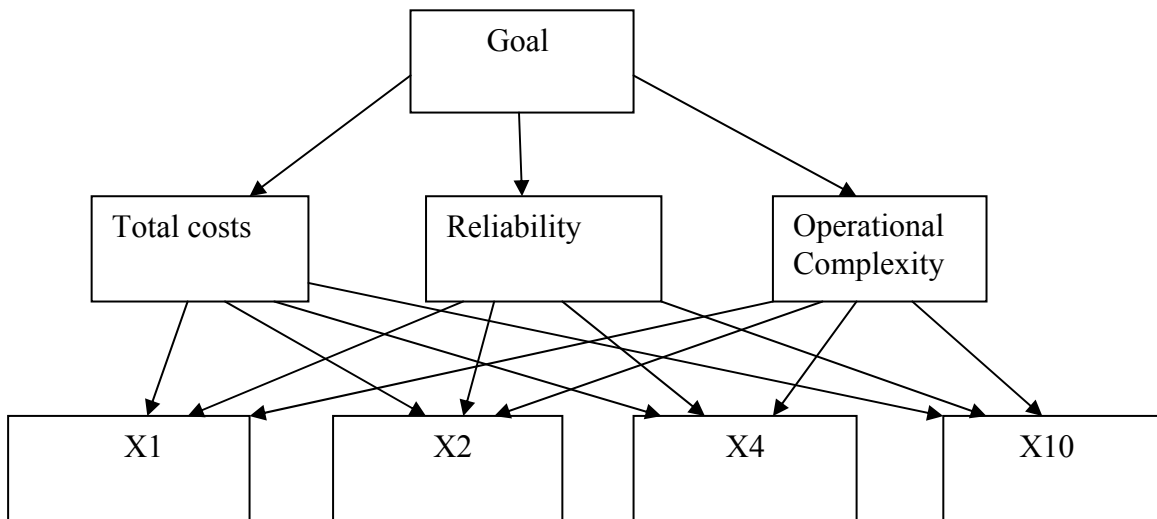


Figure 57: Structure of AHP for power system transmission expansion planning

6.4 Optimization and AHP results

The optimization methods are solved and the corresponding results are presented in the next section. The budget constraint is set to be \$285,140,400.

6.4.1 Penalty factor method

The computed cost-complexity penalty factor is:

$$p = \frac{285,140,400 - 214,293,638}{16 - 0} = 4,427,922.63\$ / complexity$$

The solutions as we change the weights are presented in Table 26.

Table 26: Solution for the penalty factor method

Weight	Optimal solution
0	X1
0.1	X1
0.2	X1
0.3	X1
0.4	X1
0.5	X2
0.6	X2
0.7	X2
0.8	X2
0.9	X2
1	X2

6.4.2 Non-linear penalty factor method

The solutions as we assign different exponential powers (k) for the non-linear method are presented in Table 27.

Table 27: Solution for the non-linear penalty factor method

k	Optimal solution
0	X2
1	X2
1.5	X2
2	X10
2.5	X10
3	Infeasible
3.5	X4
4	X4

Therefore, X1, X2, X4 and X10 are the four non-dominated Pareto optimal solutions. Table 22 and Table 25 presented earlier contain the description of each of these solution options, and their corresponding economic factors and complexity measure. Table 28 and Table 29 present the extracted contents of Tables 22 and 25 for the four non-dominated solutions.

Table 28: Non-dominated solutions

Options	2015	2020	2025
X1	Build 1-22, 100MW, X =0.18 Build 1-32, 50MW, X= 0.45 NO SPS	Build 1-23, 60MW, X = 0.30 Build 1-33, 80MW, X= 0.2813 NO SPS	Build 1-24, 50MW, X=0.36 Build 1-34, 90MW, X= 0.25 NO SPS
X10	Build 1-22, 120MW, X=0.15 Put SPS on 1-21 Put SPS on 1-31 2 SPS	Build 1-32, 120MW, X=0.1875 Build 1-23, 70MW, X=0.2571 NO SPS	Build 1-33, 100MW, X= 0.225 NO SPS
X4	Build 1-22, 120MW, X=0.15 Put SPS on 1-21 Put SPS on 1-31 2 SPS	Build 1-23, 100MW, X=0.1636 Put SPS on 1-31 1SPS	Build 1-24, 100MW, X=0.1636 Put SPS on 1-31 1SPS
X2	Build 1-22, 100MW, X=0.18 Build 1-32, 50MW, X= 0.45 NO SPS	Build 1-23, 70MW, X = 0.2571 Put SPS on 1-31 Put SPS on 1-32 2 SPS	Build 1-24, 90MW, X=0.36 Put SPS on 1-31 Put SPS on 1-32 2 SPS

Table 29: Comparison of economic factors and complexity

	Transmission costs	SPS costs	Cong. Rent	Interr. cost	EENS (MWh)	EENS Cost	Comp lexity	Budget	Total costs
X1	\$285,140,400	\$0	\$0	\$0	0	\$0	0	\$285,140,400	\$285,140,400
X10	\$271,007,400	\$2,000,000	\$0	\$244,900	900	\$54,000	8	\$273,007,400	\$273,306,300
X4	\$211,386,000	\$2,000,000	\$14,347,000	\$3,543,100	7800	\$5,160,000	14	\$213,386,000	\$236,436,100
X2	\$202,198,200	\$2,208,200	\$1,804,138	\$3,274,100	7800	\$4,809,000	16	\$204,406,400	\$214,293,638

6.4.3 Ranking non-dominated solutions using AHP

Table 30 presents the judgment matrix that shows the relative importance of various criteria in selecting the best planning option. Tables 31, 32 and 33 present the judgment matrices that show the relative importance of every planning option with respect to the various decision criteria. The consistency index of every judgment matrix is also computed, which are found to be less than 0.1 in all the cases.

Table 30: Judgment matrix for the criteria

	Total costs	Reliability	Operational complexity	Avg score
Total costs	1	4	4	0.666
Reliability	1/4	1	1	0.1667
Operational complexity	1/4	1	1	0.1667

Consistency index= 0

Table 31: Judgement matrix for operational complexity

	X1	X2	X4	X10	Avg score
X1	1	9	8	4	0.639
X2	1/9	1	1/2	1/4	0.0545
X4	1/8	2	1	1/4	0.0822
X10	1/4	4	4	1	0.2241

Consistency index=0.0341

Table 32: Judgement matrix for reliability

	X1	X2	X4	X10	Avg score
X1	1	8	8	2	0.5303
X2	1/8	1	1	1/7	0.0581
X4	1/8	1	1	1/7	0.0581
X10	1/2	7	7	1	0.3535

Consistency index=0.0133

Table 33: Judgement matrix for total costs

	X1	X2	X4	X10	Avg score
X1	1	1/7	1/5	1/2	0.0596
X2	7	1	4	6	0.5908
X4	5	1/4	1	4	0.2562
X10	2	1/6	1/4	1	0.0933

Consistency index=0.0549

Table 34 provides the final ranking of the non-dominated planning options using AHP, which is obtained by weighing various options according to the relative importance attributed by the user for various decision criteria, namely the total cost, reliability (EENS) and operational complexity. For the given relative importance, planning option X2 is ranked high.

Table 34: Final weight and rank for non-dominated solutions

	Total costs (0.666)	Reliability (0.167)	Operational complexity (0.167)	Weight	Rank
X1	0.0596	0.5303	0.639	0.2346	2
X2	0.5908	0.0581	0.0545	0.4122	1
X4	0.2562	0.0581	0.0822	0.1940	3
X10	0.0933	0.3535	0.2241	0.1584	4

7 Summary and conclusions

7.1 Summary

Special Protection Schemes (SPS) have been proved to be a quick and economic way of ensuring power system reliability, especially in the wake of drastically increasing renewable generation resources and an invariably stagnant transmission up-gradation policy. SPS postpones transmission upgrades while maximizing the usage of transmission capacity by enabling system operation closer to stability limits, and at times even beyond. Therefore this technology very much bolsters the current market's paradigm of optimizing the network resources, especially transmission usage, while supplying uninterrupted and economic power.

While the usage of SPS is encouraging, it has many downsides, especially in the eve of its tremendous proliferation in the system due to the increase of intermittent generation facilities. Many utilities have started to implement SPS for tripping wind farms to unburden the system during transmission overloads. So this increase in SPS has raised several reliability issues, one of which is the serious and undesirable consequences of inadvertent interactions among SPS. But there is a dearth of simulation and assessment tools that could capture such phenomenon during reliability studies and enable planners to come up with reliable planning option at the system planning stage.

This report has shed a considerable focus on these and other related range of topics, such as:

1. Introduction to SPS and its components
2. Current industry standards, practices and advancements in SPS – A survey of various technologies used by a cross section of industries to achieve SPS centralization and coordination have been presented.
3. Standards and methods of related industries such as process control, nuclear and power system planning – The attempt is to leverage interesting ideas from these mature industries that could be applicable to reliability and maintenance studies related to SPS.
4. Risk assessment of SPS based on two frameworks – process view and system view. Process view framework is the traditional way of computing risk associated with a system taking into account its various individual components and processes that serve as the building block of the entire system. System view framework is a new idea proposed in this report where the nature of the system and the operating conditions faced in reality are considered in the process of estimating risk associated with SPS's operation.
5. A design of Monte Carlo simulation based reliability assessment and SPS failure mode identification has been presented.
6. The report identifies the importance of including SPS in the power system planning framework, and so it illustrates system planning studies for SPS aided power systems. Two illustrations have been presented:
 - a. Accommodating more wind generation using SPS
 - b. Incorporating SPS in generation and transmission expansion planning

7.2 Conclusions

1. Special Protection Schemes (SPS), also known as Remedial Actions Schemes (RAS) have been a major technological advancement that aids in economical usage of transmission resources and smooth interconnection of renewable generation.
2. SPS has proven to be greatly economical and easy to implement compared to transmission lines, and many utilities are favoring SPS to meet their generation and transmission expansion goals.
3. Maintenance standards and documentation have been developed by industries deploying SPS to ensure meeting NERC reliability standards. One of the prominent features of all standards has been the emphasis in embedding redundancy into SPS architectures, to ensure SPS operations are immune to failures and uncertainties.
4. The advent of synchrophasors (PMUs) has given a major boost to SPS's operational performance and has increased the range of SPS applications. SPS along with PMUs and PDCs (Phasor Data Concentrators) have been instrumental in advancing the Wide Area Monitoring, Protection and Control Systems (WAMPACS).
5. Power industry has seen a drastic proliferation in SPS, which is proving to offset the advantage these individual SPS brings in by causing coordination and maintenance issues. This has served as great motivation for industries to move from a localized-RAS to Centralized-RAS technology with the help of EMS and PMUs.
6. As the dependence on SPS is growing, there is a greater need to build our knowledge base and expertise in understanding SPS better and maintaining them. Interestingly, this can be accomplished by extracting relevant standards and practices from existing industries. Safety instrument systems (SIS) of process control industry in one such example. The process of building operational rule for power system operators using Monte Carlo and machine learning techniques is another example that could contribute in SPS logic derivation and evaluation.
7. In modern SPS-rich systems, inadvertent interactions among SPS may prove to be catastrophic. Therefore the report emphasizes the need to perform studies that identify SPS failures and quantify risk associated with SPS from 'system' point of view. The report also proposes a study design based on operational planning framework using Monte Carlo simulation to identify 'system view' SPS failures, estimate their reliability/risk indices and re-design SPS logic. The proposed system study and decision support tool harnesses the advancement in computing power.
8. Several reliability models and architectures for SPS and PMU-aided SPS have been proposed in this report to facilitate system level reliability studies that account SPS.
9. The report has introduced the concept of *operational complexity* due to the proliferation in SPS and has provided a quantitative definition. System planning studies must incorporate such *operational complexity* metric in their overall formulation to estimate the limit of SPS growth for economical and reliable system operation, and also find the best SPS-aided transmission expansion plan.

8 References

- [1] "System Protection Schemes in Power Networks," *International Conference on Large High Voltage Electric Systems (CIGRE)*, January, 2001.
- [2] *Workshop on SPECIAL PROTECTION SYSTEMS for Transmission operations and Emergencies*, Almaty, Kazakhstan, available online: http://www.usea.org/programs/EUPP/SPS_Workshop_Almaty_KZ_2-18to20-2009/SPS_Handbook_English.pdf
- [3] Dana Callell and Shashi Pandey (SEC), "Centralized Remedial Action Scheme (C-RAS) using Emerging Telecommunication (IEC61850), Protection Technologies, and OSIsoft Controller software," Colorado Transmission Planning Meeting, 2008 Available online: http://www.westconnect.com/filestorage/C-RAS%20Presentation%20for%20CRT%20Mtg_9-17-08.pdf
- [4] W. Winter and B. LeReverend, "Operational performance of bulk electricity system control aids," *Electra*, N. 123, March 1989
- [5] P. M. Anderson and B. LeReverend,, "Industry experience with special protection schemes, discussion," *IEEE Trans. Power Syst.*, vol. 11, pp. 1167–1179, Aug. 1996.
- [6] V. Madani, M. Begovic, et al., "Global Industry Experiences with System Integrity Protection Schemes," IEEE PSRC Working Group C4, Oct., 2009
- [7] R. Vinnakota, M. Yao, D. Atanackovic, BCTC, "Modeling issues of system protection schemes in energy management systems," IEEE Electrical Power & Energy Conf., 2008
- [8] J. Wen, P. Arons, W. Liu, "The role of remedial action schemes in renewable generation integrations," IEEE, 2010
- [9] D. Manjure, M. McMullen, D. Subakti, D. Tewari, "Managing Wind Energy: From Interconnection planning to real time operations, an integrated approach to ensure energy and transmission capacity," PES Meeting, 2009
- [10] J. McCalley and W. Fu, *Reliability of Special Protection Systems*, IEEE Trans. on Power Systems, Vol. 14, No. 4, pp.1400-1406, November, 1999.
- [11] Western Systems Coordinating Council, *Guide for Remedial Action Schemes*, April, 1991.
- [12] Northeast Power Coordinating Council, *Special Protection System Guideline*, February, 1992.
- [13] Northeast Power Coordinating Council, *Bulk Power System Protection Criteria*, August, 1995.
- [14] V. Madani and W. Higinbotham, "Advantages in Modern Communications as applied to remedial action schemes and control centers," IREP Symposium – Bulk Power System Dynamics and Control – VII, August 19-24, Charleston, SC, USA.
- [15] David Dolezilek (SEL), "Case Study Examples of Interoperable Ethernet Communications Within Distribution, Transmission, and Wide-Area Control Systems," *IEEE International Conference on Communications Workshops (ICC)*, May 2010
- [16] P. C. K. Lau, M. Grover, and W. Tanaka, *Reliability Assessment of Special Protection Systems*, CIGRE paper AA-11, presented at the CIGRE Symposium on Electric Power System Reliability, Montreal, September, 1991
- [17] NERC reliability standards, *Protection and control*, website <http://www.nerc.com/page.php?cid=2%7C20>
- [18] WECC Standard PRC-004-WECC-1 – Protection System and Remedial Action Scheme Misoperation available online: <http://www.nerc.com/files/PRC-004-WECC-1.pdf>
- [19] *Safety Instrumented Functions (SIF) - Safety Integrity Level (SIL) Evaluation Techniques*, The Instrumentation Systems and Automation Society 2002, Available online:

http://www.isa.org/Content/Microsites195/SP5_2_Binary_Control_Logic_Diagrams_for_Process_Operations/Home193/Committee_Archives126/TR_8402p1.pdf

[20] Peter B. Ladkin, “*The Concepts of IEC 61508: An Overview and Analysis*,” Available online: <http://www.rvs.uni-bielefeld.de/Bieleschweig/fifth/download/B5-Ladkin.pdf>

[21] Dan Schoenecker, “*Determination of Financial Penalties*,” Midwest Reliability Organization, 2008, Available online: http://www.midwestreliability.org/01_about_mro/board_of_directors/presentations/Penalty%20tool%20determinants_MRO%20BOD.pdf

[22] “An operations view of special protection systems” *IEEE Trans. Power Syst.*, vol. 3, pp. 1078-1083, Aug. 1988

[23] *Nodal Operating Guides Planning section*, ERCOT, 2007, Available online: <http://www.ercot.com/content/mktrules/guides/noperating/2007/11/05/05-110107.doc>

[24] Balancing Authority/Transmission Operator Reliability Readiness Audit Report: British Columbia Transmission Corporation (BCTC), Burnaby, British Columbia, Canada, 2006, Available online: http://www.nerc.com/docs/rap/audits/BCTC_BA-TOP_ReadinessAuditReport.pdf

[25] Patricia L. Arons, *SCE Pilots the Next Level of Grid Protection*, Southern California Edison, Transmission and Distribution World, 2007, Available online: http://tdworld.com/overhead_transmission/power_sce_pilots_next/

[26] Transmission Constraints Management: RAS in the Planning Stage, AESO Discussion Paper, 2009 Available online: http://www.aeso.ca/downloads/RAS_Guideline_Discussion_Paper_July_03_2009.pdf

[27] T.J.Wang, C.W.Liu, and Y.H.Liu, “A PMU based Special Protection Scheme: a Case Study of Taiwan Power System”, *Electrical Power and Energy Systems* 27, pp.215-223, 2005

[28] Madani, V.; Adamiak, M.; Thakur, M., "Design and implementation of wide area special protection schemes," *Protective Relay Engineers, 2004 57th Annual Conference for* , vol., no., pp. 392-402, 30 Mar-1 Apr 2004

[29] *Procedure to submit a RAS for Assessment 2005*, WECC, Remedial Action Scheme Reliability Subcommittee, Available online: http://www.wecc.biz/library/Library/Remedial%20Action%20Schemes/RAS_Approval_Procedure-04-2005.pdf

[30] Reliability Coordinator, Reliability Readiness Audit Report, MISO, 2006, Available online: http://www.nerc.com/docs/rap/audits/MISO_RC_ReadinessEvaluationReport.pdf

[31] Document online: <http://www.ferc.gov/industries/electric/indus-act/reliability/blackout/ch5.pdf>

[32] Varghese, M.; Licheng Jin; Ghosh, S.; Lin, G.; Bunthath Pek; “The CAISO experience of implementing automated Remedial Action Schemes in Energy Management Systems” *IEEE power & energy society meeting* 2009

[33] BC HYDRO, Operations Support, 2009 Available online: <http://transmission.bchydro.com/nr/rdonlyres/f56489b9-f09a-452b-a0aa-6100a8f13aaf/0/7t18.pdf>

[34] Pai S.C., Sun J., “BCTC’s experience towards a smarter grid - increasing limits and reliability with centralized intelligence Remedial Action Schemes” *Electric Power Conference, 2008. EPEC 2008. IEEE Canada* ,no.,1-7,pp: 6-7 Oct. 2008

[35] R. Vinnakota, M. Yao, D. Atanackovic, A. Steed, and Q. Zhu, “Managing Contingencies in Real Time using EMS Advanced Network Applications,” *IEEE PES General Meeting 2009*, Slides available online: <http://www.ieee.org/organizations/pes/meetings/gm2009/slides/pesgm2009p-001028.pdf>

[36] Nodal Operating Guide, ERCOT, available online: http://www.ercot.com/content/meetings/owg/keydocs/2009/1021/029NOGRR-01_Synchronization_of_OGRR224_Special_Protection_S.doc

[37] C. W. Taylor, “*BPA’s Wide-Area stability and voltage Control System (WACS)*,” Imperial College, London, 2006, available online: <http://www3.imperial.ac.uk/pls/portallive/docs/1/4859962.PDF>

[38] *Talking points on RAS Arming and Ability to Schedule Generator Interconnection Projects*, BPA, 2008 available online: http://transmission.bpa.gov/business/generation_interconnection/documents/GI_talking_points_060508.pdf

- [39] A. Guzman, D. Tziouvaras, E. O. Schweitzer, and K. Martin, “Local and Wide-Area Network Protection Systems improve Power System Reliability,” available online: http://www.naspi.org/resources/archive/prtt/waps_wprc04.pdf
- [40] P. Arons, “Piloting a Centralized Remedial Action Scheme (C-RAS) with merging Telecom/Protection Technologies,” *Transmission & Interconnection Planning, SCE, VOTAGE2007*, available online: http://videostar.osisoft.com/uc2007/ppt/MO-02-04B_Arons_SCEd.pdf
- [41] E. O. Schweitzer, and D. E. Whitehead, “Real-Time Power System Control Using Synchrophasors,” *Schweitzer Engineering Laboratories, Inc., 61st annual conference for Protective Relay Engineers*, pp. 78-88, 2008
- [42] S. Wang, and G. Rodriguez (SCE), “Smart RAS (Remedial Action Scheme),” *Innovative Smart Grid Technologies*, Jan 2010.
- [43] K.E. Martin (BPA), “S4-I: Power systems operation control based on the phasor measurement technology,” *Phasor Measurement Systems in Western North America, Relay Protection and Substation Automation of Modern Power Systems*, Sept 2007
- [44] D. Karlsson, L. Messing, and M. Akke, “Wide Area Protection and Emergency Control,” *8th IEEE International conference on developments in Power System Protection*, Vol. 2, pp. 746-751, 2004
- [45] Northeast Power Coordinating Council, *Maintenance Criteria for Bulk Power System Protection*, 1996.
- [46] Northeast Power Coordinating Council, *Procedure for Reporting and Reviewing Proposed Bulk Power System Protection*, September, 1996.
- [47] S. Gillespie, *Safety Instrumented Systems*, available online: http://www.idc-online.com/technical_references/pdfs/instrumentation/Safety_Instrumented_Systems.pdf
- [48] ANSI/ISA Standard S84.01-1996, *Application of Safety Instrumented Systems to the Process Industries*, International Society for Measurement & Control, Research Triangle Park, NC, 1996
- [49] ISA-dTR84.02 (draft), The Instrument Society of America (ISA), September, 1997
- [50] IEC 61508 Parts 1-7: 1998, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*, International Electrotechnical Commission, Geneva, Switzerland.
- [51] *S 84/IEC 61511 Standard for SIS*, FAQ sheet Available online: http://www.primatech.com/info/faq_s84_standard_for_safety_instrumented_systems.pdf
- [52] *Guidelines for Cabinet Submissions and New Policy Proposals*, Department of the Prime Minister and Cabinet, Australian Government, available online: <http://www.dpmc.gov.au/implementation/policy.cfm>
- [53] Mike Scott and Bud Adler, “How to select a Safety PLC,” Available online: http://www.isa.org/Content/Microsites838/Safety_Division/Home818/ISA_2004_Safety_Papers/How_to_Select_a_Safety_PLC.pdf
- [54] *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*, International Electrotechnical Commission (IEC) Standard IEC 61508-1, 1st ed., Dec. 1998
- [55] *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*, International Electrotechnical Commission (IEC) Standard IEC 61508-2, 1st ed., May, 2000
- [56] *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*, International Electrotechnical Commission (IEC) Standard IEC 61508-3, 1st ed., Dec. 1998
- [57] *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*, International Electrotechnical Commission (IEC) Standard IEC 61508-4, 1st ed., Dec. 1998
- [58] *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*, International Electrotechnical Commission (IEC) Standard IEC 61508-5, 1st ed., Dec. 1998

- [59] *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*, International Electrotechnical Commission (IEC) Standard IEC 61508-6, 1st ed., Apr., 2000
- [60] *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures*, International Electrotechnical Commission (IEC) Standard IEC 61508-7, 1st ed., Mar., 2000
- [61] *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 0: Functional safety and IEC 61508*, International Electrotechnical Commission (IEC) Technical Report IEC/TR 61508-0, 1st ed., Jan., 2005
- [62] R. Bell, “Introduction to IEC 61508,” in: T. Cant, editor, *10th Australian Workshop on Safety Critical Systems and Software, Conferences in Research and Practice in Information Technology*, vol. 55, pp. 3-12, 2005
- [63] *Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems*, International Electrotechnical Commission (IEC) Standard IEC 61513, 1st ed., Mar., 2001
- [64] *Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions*, International Electrotechnical Commission (IEC) Standard IEC 61226, 3rd ed., Jul., 2009
- [65] *Nuclear power plants – Instrumentation and control systems important to safety – Separation*, International Electrotechnical Commission (IEC) Standard IEC 60709, 2nd ed., Nov., 2004
- [66] *Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems*, International Electrotechnical Commission (IEC) Standard IEC 60987, 2nd ed., Aug., 2007
- [67] *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions*, International Electrotechnical Commission (IEC) Standard IEC 60880, 2nd ed., May, 2006
- [68] *Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions*, International Electrotechnical Commission (IEC) Standard IEC 62138, 1st ed., Jan., 2004
- [69] *Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF)*, International Electrotechnical Commission (IEC) Standard IEC 62340, 1st ed., Dec., 2007
- [70] *Nuclear power plants – Instrumentation and control systems important to safety – Management of ageing*, International Electrotechnical Commission (IEC) Standard IEC 62342, 1st ed., Aug., 2007
- [71] *Nuclear power plants – Instrumentation and control systems important to safety – Surveillance testing*, International Electrotechnical Commission (IEC) Standard IEC 60671, 2nd ed., May, 2007
- [72] E. A. Corte, and J. P. Bouard, *International Standardisation in Nuclear I&C Engineering*, 2005, Available online: <http://www.yellowdocuments.com/6460428-international-standardisation>
- [73] *Safety of Nuclear Power Plants: Design – Safety Requirements*, International Atomic Energy Agency (IAEA), Safety Standards Series No. NS-R-1, 2000, Oct. 31, 2000
- [74] *Software for Computer Based Systems Important to Safety in Nuclear Power Plants – Safety Guide*, International Atomic Energy Agency (IAEA) Safety Standards Series No. NS-G-1.1, 2000, Nov. 14, 2000
- [75] *Instrumentation and Control Systems Important to Safety in Nuclear Power Plants – Safety Guide*, International Atomic Energy Agency (IAEA) Safety Standards Series No. NS-G-1.3, 2002, Apr. 17, 2002
- [76] *Design of Emergency Power Systems for Nuclear Power Plants – Safety Guide*, International Atomic Energy Agency (IAEA) Safety Standards Series No. NS-G-1.8, 2004, Oct. 13, 2004
- [77] G. Johnson, “Comparison of IEC and IEEE Standards for Computer-Based Control Systems Important to Safety,” in *Proc. 2001 IEEE Nuclear Science Symposium Conference Record*, vol. 4, pp. 2474-2481

- [78] *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations*, Institute of Electrical and Electronics Engineers (IEEE) Standard IEEE Std 603-2009, Nov., 2009
- [79] *IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations*, Institute of Electrical and Electronics Engineers (IEEE) Standard IEEE Std 7-4.3.2-2003, Dec., 2003
- [80] *IEEE Standard Criteria for Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems*, Institute of Electrical and Electronics Engineers (IEEE) Standard IEEE Std 338-2006, Jun., 2007
- [81] *IEEE Guide for Installation, Inspection, and Testing for Class 1E Power, Instrumentation, and Control Equipment at Nuclear Facilities*, Institute of Electrical and Electronics Engineers (IEEE) Standard IEEE Std 336-2005, Feb., 2006
- [82] *IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems*, American National Standards Institute (ANSI) / Institute of Electrical and Electronics Engineers (IEEE) Standard ANSI/IEEE Std 352-1987, Nov., 1985 / Jun. 1985
- [83] *IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Facilities*, Institute of Electrical and Electronics Engineers (IEEE) Standard IEEE Std 577-2004, Aug., 2004
- [84] *Construction Codes and Standards: Avoidance of New Nuclear Power Plant Construction Delays*. Energetics Incorporated, The United States Department of Energy (DOE), Office of Nuclear Energy, Tech. Rep., Nuclear Energy Standards Coordination Collaborative (NESCC) Meeting Jun. 2009, Available online: <http://publicaa.ansi.org/sites/apdl/Documents/Meetings and Events/2009 NESCC/NESCC Meeting - June 1, 2009/NESCC 09-004 Mattson Report.pdf>
- [85] C. Lebrevelec, P. Cholley, J.F. Quenet, and L. Wehenkel, "A statistical analysis of the impact on security of a protection scheme on the French power system," *International Conference on Power System Technology, Proceedings, POWERCON '98*, Volume 2, pp. 1102 - 1106, 18-21 Aug. 1998
- [86] Y. Schlumberger, C. Lebrevelec, and M. De Pasquale, "Power systems security analysis-new approaches used at EDF," *IEEE Power Engineering Society Summer Meeting*, Volume 1, pp. 147 – 151, 18-22 July 1999
- [87] J. Pierre, C. Lebrevelec, and L. Wehenkel, "Automatic learning methods applied to dynamic security assessment of power systems," *International Conference on Electric Power Engineering. PowerTech Budapest*, pp.180, 29 Aug.-2 Sept. 1999
- [88] H. Martigne, P. Cholley, D. King, and J. Christon, "Statistical method to determine operating rules in the event of generator dropout on EDF French Guyana Grid," *IEEE Power Tech Proceedings, Porto*, Vol. 1, pp. 5, 10-13 Sept. 2001
- [89] J. Paul and K. Bell, "A Flexible and Comprehensive Approach to the Assessment of Large-Scale Power System Security Under Uncertainty," *Proc. of the 7th International Conference on Probabilistic Methods Applied to Power Systems*, Naples Italy, September 2002
- [90] S. Henry, J. Pompee, M. Bulot, and K. Bell, "Applications of statistical assessment of power system security under uncertainty," *International Conference on Probabilistic Methods Applied to Power Systems*, pp. 914-919, 12-16 Sept. 2004
- [91] S. Henry, J. Pompee, L. Devatine, M. Bulot, and K. Bell, "New trends for the assessment of power system security under uncertainty," *IEEE PES Power Systems Conference and Exposition*, vol.3, pp. 1380-1385, 10-13 Oct. 2004
- [92] S. Henry, E. Bréda-Séyès, H. Lefebvre, V. Sermanson and M. Béna, "Probabilistic study of the collapse modes of an area of the French network," *Proc. of the 9th International Conference on Probabilistic Methods Applied to Power Systems*, Stockholm, Sweden, June 2006
- [93] P. Cholley, C. Lebrevelec, S. Vitet, and M. de Pasquale, "Constructing operating rules to avoid voltage collapse: a statistical approach," *International Conference on Power System Technology, Proceedings, POWERCON '98*, Volume 2, pp. 1468-1472, 18-21 Aug. 1998

- [94] C. Lebrevelc, Y. Schlumberger, and M. de Pasquale, "An application of a risk based methodology for defining security rules against voltage collapse," *IEEE Power Engineering Society Summer Meeting*, Volume 1, pp.185-190, 18-22 July 1999
- [95] S. Henry, C. Lebrevelec, and Y. Schlumberger, "Defining operating rules against voltage collapse using a statistical approach: The EDF experience," *International Conference on Electric Power Engineering, PowerTech Budapest 99*, pp. 30, 29 Aug.-2 Sept. 1999
- [96] Y. Schlumberger, J. Pompee, and M. De Pasquale, "Updating operating rules against voltage collapse using new probabilistic techniques," *IEEE/PES Transmission and Distribution Conference and Exhibition: Asia Pacific*, Volume 2, pp. 1139-1144, 6-10 Oct. 2002
- [97] K. Sun, S. Likhate, V. Vittal, V.S. Kolluri, and S. Mandal, "An Online Dynamic Security Assessment Scheme Using Phasor Measurements and Decision Trees," *IEEE Trans. Power Systems*, Volume: 22, Issue: 4, pp. 1935-1943, Nov. 2007
- [98] R. Diao, K. Sun, V. Vittal, R.J. O'Keefe, M.R. Richardson, N. Bhatt, D. Stradford, and S.K. Sarawgi, "Decision Tree-Based Online Voltage Security Assessment Using PMU Measurements," *IEEE Trans. Power Systems*, Vol. 24, Issue 2, pp. 832-839, May 2009
- [99] V. Krishnan, J. D. McCalley, S. Henry, and S. Issad, "High Information Content Database Generation for Data Mining based Power System Operational Planning Studies," *IEEE PES General Meeting*, Minneapolis, July 2010
- [100] C. Singh, and J. Mitra, "Composite system reliability evaluation using state space pruning," *IEEE Trans. Power Systems*, Volume 12, Issue 1, pp. 471-479, Feb. 1997
- [101] J. Huang, G. Vanier, A. Valette, S. Harrison, F. Lévesque, and L. Wehenkel, "Operation rules determined by risk analysis for special protection systems at Hydro-Québec," *CIGRE*, 2004
- [102] J. Huang, G. Vanier, A. Valette, S. Harrison, and L. Wehenkel, "Application of data mining to optimize settings for generator tripping and load shedding system in emergency control," *The International Journal for Computation and Mathematics in Electrical and Electronic Engineering* Vol. 23 pp. 21-34 No. 1, 2004
- [103] N. Senroy, G. T. Heydt, and V. Vittal, "decision tree assisted controlled islanding," *IEEE trans. power syst.*, vol. 21, no. 4, November 2006
- [104] ASSESS, TROPIC, METRIX website: <http://www.rte-france.com/htm/an/activites/assess.jsp>
- [105] V. Vittal, J. McCalley, V. Van Acker, W. Fu, and N. Abi-Samra, "Transient instability risk assessment", *Proc. Of the 1999 IEEE PES Summer Meeting*, pp. 1999
- [106] "System disturbances," North Amer. Elect. Rel. Council, 1986–1995
- [107] P. M. Anderson, *Power System Protection*, Vol 111, Review Copy, 1996
- [108] W. M. Gable, *Evaluating Control Systems Reliability- Techniques and Applications*, The Instrument Society of America, (ISA), N. C., 1992
- [109] B. S. Dhillon, *Mechanical Reliability: Theory, Models and Applications*, American Institute of Aeronautics and Astronautics, Inc., Washington, DC, 1988
- [110] Peter Morgan, "Markov Modelling Primer- Calculating System PFDs for the design of Safety Instrumented Systems", available online: http://www.isa.org/filestore/Markov_Modelling.pdf
- [111] *Non-conventional instrument transformer solutions*, AREVA T&D, Available online: http://www.areva-t.com/solutions/liblocal/docs/NCIT/NCIT_BRen_1720.pdf
- [112] P. Zhang, J. Chen, and M. Shao, "Phasor measurement unit (PMU) implementation and applications," *Electric Power Research Institute (EPRI)*, Palo Alto, CA, Tech. Rep. 2007.1015511 Available online: http://my.epri.com/portal/server.pt?Abstract_id=000000000001015511
- [113] *Communication networks and systems in substation – Part 9-2: Specific communication service mapping (SCSM) – Sampled values over ISO/IEC 8802-3*, International Electrotechnical Commission (IEC) Standard IEC

61850-9-2, 1st ed., Apr. 2004.

- [114] D. Chatrefou, J. P. Dupraz, and G.F. Montillet, "Interoperability between non-conventional instrument transformers (NCIT) and intelligent electronic devices (IED)," in *Proc. 2005/2006 IEEE Power Engineering Society (PES) Transmission and Distribution Conf. and Exhibition*, pp. 1274-1279, May 2006
- [115] B. Kasztenny, J. Whatley, E. A. Udren, J. Burger, D. Finney, M. Adamiak, "Unanswered questions about IEC 61850: What needs to happen to realize the vision?" 32nd Annual Western Protective Relay Conference, 2005
- [116] Y. Wang, W. Li, and J. Lu, "Reliability Analysis of Phasor Measurement Unit Using Hierarchical Markov Modeling," *Electric Power Components and Systems*, 37, pp. 517-532, 2009
- [117] Y. Wang, W. Li, J. Lu, and H. Liu, "Evaluating multiple reliability indices of regional networks in wide area measurements system," *Electric Power Systems Research*, 79, pp. 1353-1359, 2009
- [118] Y. Wang, W. Li, and J. Lu, "Reliability Analysis of Wide-Area Measurement System," *IEEE Trans. Power Delivery*, Vol. 25, No. 3, July 2010
- [119] P. Zhang, L. Portillo, and M. Kezunovic, "Reliability and component importance analysis of all-digital protection systems," in *Proc. 2006 IEEE Power Engineering Society (PES) Power Systems Conf. and Exposition*, pp. 1380-1387, Oct. 2006
- [120] C. Singh and R. Billinton, "Frequency and duration concepts in system reliability evaluation," *IEEE Trans. Reliability*, vol. R-24, no. 1, pp. 31-36, Apr. 1975
- [121] C. Singh and R. Billinton, *System Reliability Modeling and Evaluation*, London, UK: Hutchinson Educational Publishers, 1977, pp. 48-59, Available online: <http://www.ece.tamu.edu/People/bios/singh/sysreliability>
- [122] C. Singh, "A matrix approach to calculate the failure frequency and related indices," *Microelectronics and Reliability*, vol. 19, pp. 395-398, 1979
- [123] J. Walseth, J. Eskedal, and O. Breidablik, "Analysis of misoperations of protection schemes in the Nordic Grid," Protection, Automation, and Control World, March 2010
- [124] T. Van Cutsem, C. Moors, D. Lefebvre, "Design of load shedding schemes against voltage instability using combinatorial optimization," IEEE PES Winter Meeting, Vol.2 2002
- [125] V. Sermanson, and a. Giard, "Dynamic voltage security assessment in operational planning at RTE, a way to improve the power system security," *Securing Critical Infrastructures*, Grenoble, October 2004
- [126] T. Y. Hsiao, C. N. Lu, Y. H. Liu, "Defense plan design in a longitudinal power system," PSCC 2002, in Sevilla, Session 25, Paper 5, 2002
- [127] W. T. Tsai and C. R. Chen, "A Special Protection System Implementation-Based on an Isolated and Longitudinal Power System," *International Conference on Power System Technology, POWERCON*, 21-24 November 2004
- [128] H. Seyedi, M. Sanaye-Pasand, "Design of New Load Shedding Special Protection Schemes for a Double Area Power System," *American Journal of Applied Sciences* 6 (2): 317-327, 2009
- [129] T.Y. Hsiao, C.A. Hsieh, and C. N. Lu; "A risk-based contingency selection method for SPS applications," *IEEE Trans. Power Sys.*, Vol. 21, issue. 2, pp. 1009 – 1010, 2006
- [130] B. D. Ripley, *Stochastic Simulation*, Wiley: New York, 1987
- [131] G. Papaefthymiou, and D. Kurowicka, "Using Copulas for Modeling Stochastic Dependence in Power System Uncertainty Analysis," *IEEE Trans. Power Systems*, Vol. 24, Issue 1, pp. 40 – 49, 2009
- [132] W.G. Wyss, K.H. Jorgensen, "A User's Guide to LHS: Sandia's Latin Hypercube Sampling Software," *Sandia National Laboratories Report SAND98-0210*, Albuquerque, NM, 1998.
- [133] R. Billinton, R.N. Allan, *Reliability evaluation of power systems*, Second Edition, New York: Plenum Press, c1996

- [134] R. Billinton, and W. Li, *Reliability assessment of electric power system using Monte Carlo methods*, Springer
- [135] *20% Wind Energy by 2030*, Increasing Wind Energy's Contribution to U.S Electricity Supply, DOE/GO-102008-2567, July 2008, available online: <http://www.energy.gov>
- [136] Paul Davidson, "Wind energy confronts shortage of transmission lines," USA Today, 2008, available online: http://www.usatoday.com/money/industries/energy/environment/2008-02-25-wind-power-transmission_N.htm
- [137] Phadke, A.G.; Thorp, J.S., "History and Application of Phasor Measurements," *IEEE Power Systems Conference and Exposition, 2006. PSCE '06*. Oct. 29 2006-Nov. 1 2006 pp. 331 – 335
- [138] Weaver, Warren (1948), "Science and Complexity", *American Scientist* 36: 536
- [139] *Highlights of the Midwest ISO 2003 State of the Market Report*, Independent Market Monitor, Midwest ISO, 2004, available online: www.ferc.gov/EventCalendar/Files/20040915134723-A-3-MISO.pps
- [140] N. Cetinkaya, *Optimization Algorithm for Combined Economic and Emission Dispatch with Security Constraints*
- [141] Zhu J.; Momoh J.A, "Optimal VAR pricing and VAR placement using analytic hierarchical process," *Electric Power Systems Research*, Volume 48, Number 1, 1 December 1998 , pp. 11-17