Application Considerations in System Integrity Protection Schemes (SIPS)

Vahid Madani
Pacific Gas & Electric Co.

Damir Novosel
Quanta Technology

Miroslave Begovic
Georgia Institute of Technology

Mark Adamiak
GE Digital Energy, Multilin

1. Abstract

This paper describes some of the critical engineering, design, and applications of the latest technology for the implementation of System Integrity Protection Schemes (SIPS). Applicability of the advanced analytical techniques for various types of SIPS applications on the basis of modern technology is also addressed. An overview is presented of traditional scheme requirements leading to the SIPS of the future. A new survey is described in the paper, which should provide valuable information about power industry trends and experiences in SIPS.

Keywords: Power system protection, emergency control, industry practice, SIPS.

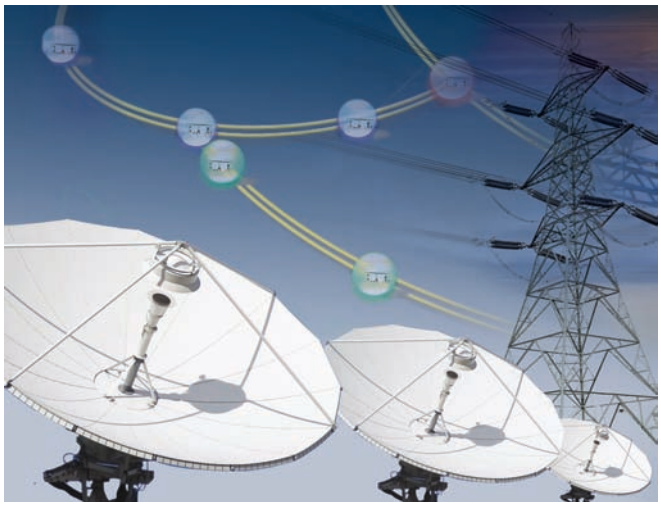
2. Introduction

The electric power grid is the "pivot point" that balances the generation and load. Maintaining the integrity of this pivot point is imperative for the effective operation of interconnected power systems. As such, the balance of power is only as reliable as the weakest pivot point in the system.

When a major disturbance occurs, protection and control actions are required to stop the power system degradation, restore the system to a normal state, and minimize the impact of the disturbance [1]. Control center operators must deal with a very complex situation and rely on heuristic solutions and policies [1], [2].

Local protection systems arrest the propagation of the fast-developing emergencies through automatic actions. Local protection systems, however, are not able to address the entire power system, which may be affected by the disturbance.

The trend in power system planning utilizes tight operating margins, with less redundancy in the grid. At the same time, addition of non-utility generators and independent power producers, an interchange increase in a growing competitive environment and introduction of fast control devices make the power system more complex to operate. This changing environment highlights the need for automated systems with advanced monitoring and intuitive interface tools to enable real-time operator interactions. On the other hand, the advanced measurement devices and communication technology in wide-area monitoring and controls,



FACTS devices (better operational and stability control), and new analytical and heuristic procedures provide better ways to detect and control an impending system collapse [3], [4], [5], [6].

Advanced detection and control strategies through the concept of System Integrity Protection Schemes (SIPS) offer a cohesive management of the disturbances. SIPS is a concept of using system information from local as well as relevant remote sites and sending this information to a processing location to counteract propagation of the major disturbances in the power system. With the increased availability of advanced computer, communication and measurement technologies, more "intelligent" equipment can be used at the local level to improve the overall response. Traditional contingency dependant / event based systems could be enhanced to include power system response based algorithms with proper local supervisions for security.

Decentralized subsystems that can make local decisions based on local measurements (system-wide data and emergency control policies) and/or send pre-processed information to higher hierarchical levels are an economical solution to the problem [7]. A major component of the SIPS is the ability to receive remote measurement information and commands via the data communication system and to send selected local information to the SCADA centre. This information should reflect the prevailing state of the power system.

This paper describes how SIPS help manage system disturbances and prevent blackouts. The design and architecture of a SIPS is addressed. The paper also discusses an effort underway to gather best practices and operational experiences globally [8].

3. Blackouts - Cause and Effect

Reviewing examples of 1996 and 2003 system blackouts worldwide [9-10] reveal some similar patterns among such disturbances. Some common causes include:

- Pre-existing conditions, such as generator/line maintenance, heavy loading.
- Tripping lines due to faults and/or protection actions resulting in heavy overloads on other lines. Protection and control misoperation or unnecessary actions, which may contribute to disturbance propagation.
- Insufficient voltage (reactive power) support.
- Inadequate right-of-way maintenance.
- Insufficient alarms or monitoring to inform operators of equipment malfunctions.
- Inability of operators to respond to impending disturbances or to prevent further propagation of the disturbance and problems with EMS/SCADA systems to provide only important information when required.
- Inadequate planning/operation studies.
- Automated actions are not available/initiated to prevent further overloading of the lines, arrest voltage decline and/or initiate automatic and pre-planned separation of the power system.

While it is not realistically possible to completely eliminate blackouts (unless very large investments are made that would make the price of electricity unreasonable for end users) the above shows that by taking some reasonably cost-effective measures, occurrence of the blackouts could be reduced. We are focusing in this paper on the last of those issues, implementation of automated actions, the purpose of which is to prevent an imminent blackout, or at least arrest its propagation and mitigate some of its undesired consequences.

4. Technology for Modern Protection

SCADA/EMS system capability has greatly improved in the last few years, due to improved communication facilities and enhanced data handling capabilities. Improved EMS/SCADA systems require the ability to filter, display, and analyze only critical information and to increase availability of critical functions to 99.99% or better. Critical alarm monitoring systems must be maintained in top operating condition, and newer alarm analysis technologies should be deployed to detect and prevent the spread of major disturbances.

Modern technology, such as phasor measurement units (PMUs) and high bandwidth and high-speed communication networks, can provide time-synchronized measurements from all over the grid [1]. Based on those measurements, improved, faster and more accurate state estimators can be developed. In addition, advanced algorithms and calculation programs that assist the operator can also be included in the SCADA system, such as "faster than real-time simulations" to calculate power transfer margins based on various contingencies.

Development of system integrity protection schemes can help manage system disturbances and prevent blackouts. Those wide area protection schemes are based on pre-planned, automatic and corrective actions, implemented on the basis of system studies, with the goal to restore acceptable system performance. Although SIPS schemes can help increase the transfer limits, their primary goal is to improve security of the power system.

As system conditions change, it is necessary to perform studies and review protection designs on a regular basis to prevent protection misoperation. In addition, as protection systems are designed to be either more dependable (emphasis on making sure that protection acts when it should) or more secure (protection does not misoperate), designers can increase the security of protection design in the areas vulnerable to blackouts. As an example, transmission line pilot protection could be migrated to Permissive Overreach Transfer Trip scheme (POTT), which is more secure, compared to the more dependable Directional Comparison Blocking (DCB) scheme.

As hidden failures have been identified to be the significant contributors to blackouts [9], adequate testing of not only individual relays, but also overall relay applications, is crucial to reveal the potential failures. As system protection is generally intended to operate for rare events, and at the same time to mitigate a large number of potential disturbance conditions, a well developed automated testing plan which verifies inputs, logic, and output, is critical for proper maintenance of the scheme.

5. SIPS: Design and Architectures

The SIPS encompasses Special Protection Schemes (SPS), Remedial Action Schemes (RAS), as well as additional schemes such as, but not limited to, Underfrequency (UF), undervoltage (UV), out-of-step (OOS), etc., Figure 1.

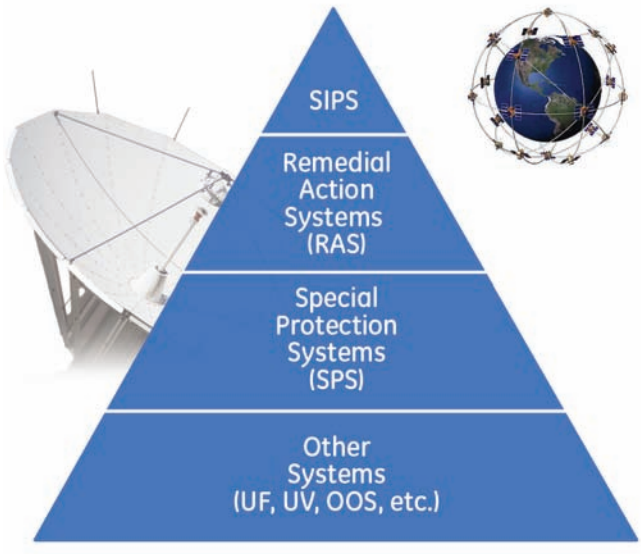


Figure 1.
SIPS, A Set of Automatic, Synchronized, and Coordinated Counter Measures

SIPS are installed to protect the integrity of the power system or its strategic portions. A SIPS is applied to the overall power system or a strategic part of it in order to preserve system stability, maintain overall system connectivity, and/or to avoid serious equipment damage during major events. Therefore, the SIPS may require multiple detection and actuation devices and communication facilities. Figure 2 shows SIPS classification.

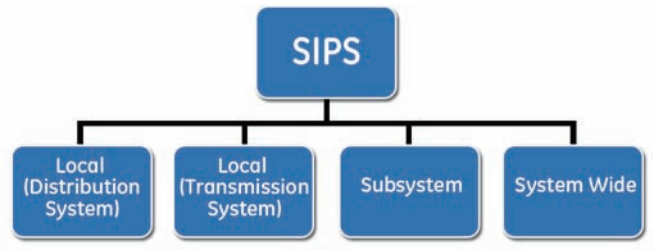


Figure 2.
SIPS Classification

SIPS classifications have been defined through a collective global industry effort by members of the IEEE and CIGRE [8]. Below is a summary.

Local (Distribution System) – SIPS equipment is usually simple, with a dedicated function. All sensing, decision-making and control devices are typically located within one distribution substation. Operation of this type of SIPS generally affects only a very limited portion of the distribution system such as a radial feeder or small network.

Local (Transmission System) - All sensing, decision-making and control devices are typically located within one transmission substation. Operation of this type of SIPS generally affects only a single small power company, or portion of a larger utility, with limited impact on neighboring interconnected systems. This category includes SIPS with impact on generating facilities.

Subsystem - The operation of this type of SIPS has a significant impact on a large geographic area consisting of more than one utility, transmission system owner or generating facility. SIPS of this type are more complex, involving sensing of multiple power system parameters and states. Information can be collected both locally and from remote locations. Decision-making and logic functions are typically performed at one location. Telecommunications facilities are generally needed both to collect information and to initiate remote corrective actions.

System wide - SIPS of this type are the most complex and involve multiple levels of arming and decision making and communications. These types of schemes collect local and telemetry data from multiple locations and can initiate multi-level corrective actions consistent with real-time power system requirements. These schemes typically have multi-level logic for different types and layers of power system contingencies or outage scenarios. Operation of a SIPS of this type has a significant impact on an entire interconnected system.

Failure of the SIPS to operate when required, or its undesired or unintentional operation will also impact balanced power system operation. Therefore, design of the SIPS may involve redundancy or some backup functions, and depending on the operational security requirements, may involve some form of voting or vetoing (fail-safe) based on the intended design.

The scheme architecture can be described by the physical location of the sensing, decision making, and control devices that make up the scheme and the extent of impact the SIPS has on the electrical system. SIPS are classified into two main types of architectures: flat and hierarchical.

Flat Architecture - the measurement and operating elements of the SIPS are typically in the same location. The decision and corrective action may need a communication link to collect remote information and/or to initiate actions.

Hierarchical Architecture - There are several steps involved in the SIPS corrective action. For example, local measurement, or a series of predetermined parameters at several locations are transmitted to multiple control locations. Depending on the intent of the scheme, immediate action can be taken and further analysis performed. The scheme purpose will drive the logic, design, and actions. Typical logic involves use of operating nomograms, state estimation and contingency analysis.

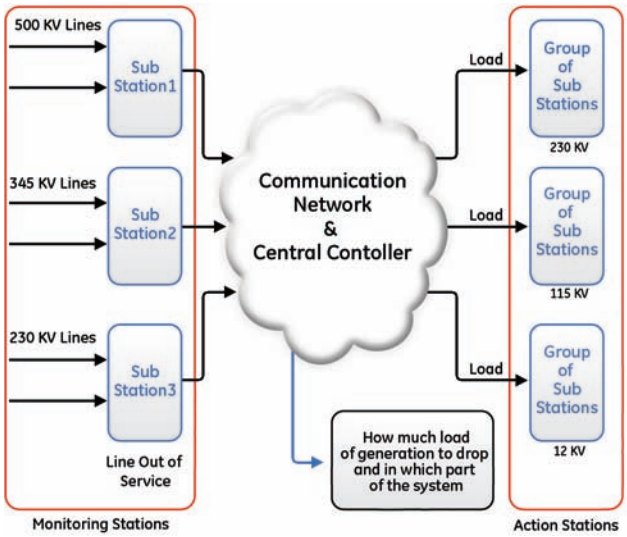


Figure 3.
System protection terminal [12]

The design should address all standard requirements for protection terminals [13], [14]. The terminal is connected to the substation control system. For time tagging applications, a GPS-based synchronization function is needed, Figures 1 and 3. The system protection terminal possesses a high-speed communication interface to transfer data between the terminal databases, which contain all updated measurements and binary signals recorded in that specific substation. The conventional substation control system is used for the input and output interfaces with the power system. The decision-making logic contains all the algorithms and configured logic necessary to derive appropriate output control signals, such as circuit-breaker trip, AVR-boosting, and tap-changer action, to be performed in that substation. The input data to the decision-making logic is taken from the continuously monitored data, stored in the database. A low speed communication interface for SCADA communication and operator interface should also be available as an enhancement for the SCADA state estimator. Actions ordered from SCADA/EMS functions, such as optimal power flow, emergency load control, etc., could be activated via the system protection terminal. The power system operator should also have access to the terminal, for supervision, maintenance, update, parameter setting, change of setting groups, disturbance recorder data collection, etc.

For local schemes, where monitoring and decision stations are within close proximity, there may still be a need for use of high-speed communication. Details of an extremely high speed vetoing scheme involving major generation and coordination against various types of protection schemes including out-of-step protection has been described in [13].

6. SIPS or RAS Application Definitions

The types of SIPS applications may vary based on the topology of the power grid. There may also be different views on the acceptability of the type of the application. For example, use of SIPS for generation shedding to balance grid performance may be viewed as unacceptable for certain levels of contingency in one network but a common practice in another interconnected grid. Consider power systems with limited transmission corridors where building a redundant and diverse interconnection outlet for a generating facility may not be physically practical or economically feasible to address variety of technically possible outlet outages. In such conditions, the generator owner may accept a certain level of risk so long as it can be demonstrated that such SIPS does not result in an unacceptable level of security for to other parts of the grid.

Table 1 shows the types of wide-are disturbances likely to occur in two different types of interconnected power grids, namely meshed network vs. an interconnected transmission system of narrow corridors consisting of extensive generation tied to the interconnection.

System Configuration	Densely meshed power system with dispersed generation and load		Lightly meshed transmission systems with localized generation and load	
Events	Located in a large interconnection	Not interconnected or by far the largest partner	Located in a large interconnection	Not interconnected or far the largest partner
Overloads	**	**	*	*
Frequency instability	*	**	*	**
Voltage instability	*	*	**	**
Transient angle instability	*	*	**	**
Small signal stability	*	*	*	*

Table 1.
Types of Wide-Area Events on two Different Interconnected Transmission Systems

The characteristics of the power system influencing the types of mitigation methods have been described in a variety of literature [15-19]. The mitigation measure to maintain grid integrity are described in a document under development by a collaborative effort of IEEE, CIGRE, and EPRI [8]. Below is a summary listing of the types:

- Generator Rejection
- Load Rejection
- Under-Frequency Load Shedding
- Under-Voltage Load Shedding
- Adaptive Load Mitigation
- Out-of-Step Tripping
- Voltage Instability Advance Warning Scheme
- Angular Stability Advance Warning Scheme
- Overload Mitigation
- Congestion Mitigation
- System Separation
- Shunt Capacitor Switching
- Tap-Changer Control
- SVC/STATCOM Control
- Turbine Valve Control
- HVDC Controls
- Power System Stabilizer Control
- Discrete Excitation
- Dynamic Breaking
- Generator Runback
- Bypassing Series Capacitor
- Black-Start or Gas-Turbine Start-Up
- AGC Actions
- Busbar Splitting

7. SIPS or RAS: Industry Experience

In August of 1996, a seminal article [20] was published as a result of the activity of the joint Working Group of IEEE and CIGRE, the purpose of which was to investigate the special protection schemes then in existence worldwide and to report about various aspects of their designs, functional specifications, reliability, cost and operating experience. The report encompassed over 100 schemes from all over the world and provided a wealth of information on the direction the industry was taking in coping with ever larger disturbances.

In 2004, the System Protection Subcommittee of the IEEE Power System Relaying Committee started an initiative to update the industry experience on RAS, SPS and SIPS by creating and widely disseminating a new survey, which would attempt to attract as wide a response from the industry worldwide as the original report did. The authors of this paper are amongst the many industry recognized members that have generated a survey of industry experiences [16]. After considerable effort to incorporate in the framework of the new survey most of the advances which have occurred in the last decade, coupled by design considerations for natural calamity phenomenon such as tsunami or hurricanes, or seismic events, the revised survey has been completed and has distributed globally to professional audience with an intention to solicit as wide a response.

8. Structure of the Survey

The survey is divided into two parts: Part 1 identifies the "Purpose" of the scheme with subsections of "Type" and "Operational Experience" - For that part, a series of questions are repeated for each type of scheme which is reported.

Part 2 concerns Engineering, Design, Implementation, technology, and other related sections such as cyber security Considerations. This series of questions are asked only one time. The respondents are asked to answer those questions based on most common practice in their companies.

The survey also asks respondents to identify the system integrity protection schemes that exist on their systems, the design and implementation, and the operation experience as applicable. Results of the survey are expected to assist the respondents in:

- The application, design, implementation, operation, and maintenance of new and next generation SIPS.
- Understanding feasible alternatives applied to extending transmission system ratings without adding new transmission facilities.
- Applicability of delayed enhancement of transmission networks to the respondent's system.
- Providing reasonable countermeasures to slow and/or stop cascading outages caused by extreme contingencies (safety net).

The survey is intended for power system professionals involved in the Planning, Design, and Operation of SIPS. Specific skill required to complete the survey include, protection, telecommunication and system planning. The survey is distributed through CIGRE, IEEE, and EPRI. Among the questions found in Part II of the survey are the following issues:

- System Studies Done Prior to Deploying the SIPS
  - Planning criteria
  - Types of planning studies
  - Real-time operational studies
  - Protection and control coordination studies
- Coordination with other Protection and Control systems
- Types of protective relaying technology used
- Existence of standards for SIPS applications
- Hardware Description and Outage Detection
  - Outage detection Method
  - Questions on use of programmable logic controllers
- Scheme Architecture
  - Objective: decision making
  - Redundancy needs/implementation - Both telecommunication and hardware
  - Redundancy philosophy
  - Questions on use of the voting schemes
  - Questions about control: event based, or response based
  - Questions on Breaker Failure
  - Performance requirements:
    - Throughput timing: entire scheme
    - Throughput timing of the controller
- Data acquisition and related tools
  - Measured Quantities
  - Time synchronization requirements
  - Use of SMART SIPS / Intelligent SIPS
  - Blocking (by the scheme) of any automatic reclosing
  - Restoration Issues and Planned Mechanisms
- Communication, Networking, and Data Exchange
  - Architecture of the communication
  - Communication medium and protocols
  - Information about shared communication (with other applications)
  - Impact of communication failure on reliability index and availability
  - Cyber security implementation and protection features
  - Operability of the scheme with a communication channel failure
  - Control Area Visibility
- Arming methodology
- Implementation issues
  - Multi-functionality of the scheme
  - Design: Centralized or Distributed Architecture
  - Availability of event reconstruction or system playback capability
  - Description of event records and their availability within the organization
- Testing Considerations
  - Testing procedure
  - Periodicity of testing
  - Maintenance issues
- Cost Considerations
  - Approximate cost
  - System information (infrastructure)

The survey is currently being disseminated and responses are being collected. When sufficiently large sample of responses is received, a report will be compiled which is expected to answer many questions about current industry practices, regional differences in system protection philosophy and experience with such designs.

9. Conclusions

The paper describes some of the critical design considerations and applications of latest technology for SIPS. Applicability of the advanced analytical techniques for various types of SIPS applications on the basis of modern technology is also addressed as part of the overview. An overview is presented of traditional scheme requirements leading to the SIPS of the future. In the light of fast changing operating conditions in power systems (ever smaller security margins and transmission capacity, aging infrastructure, etc.) and quickly changing enabling technologies for power system control and protection, the industry landscape is changing quickly and adapting to the conditions imposed by new business practices. The new survey should provide valuable information to industry practitioners and researchers alike about the trends and experiences in system protection. The readers are encouraged to assist the authors in disseminating the survey across the globe for maximum impact.

10. References

[1] D. Novosel, M. Begovic, V. Madani, "Shedding Light on Blackouts", IEEE PES Power & Energy, January / February 2004.

[2] K. Walve, "Modelling of Power System Components at Severe Disturbances", CIGRE paper 38-17, 1986, Paris, France.

[3] V. Madani, D. Novosel, A. Apostolov, S. Corsi, "Innovative Solutions for Preventing Wide Area Disturbance Propagation - Protection and Control Coordination Impact and Other Considerations In Cascading Disturbances ", International Institute for Research and Education in Power Systems Symposium Proceedings, August 2004.

[4] "Wide Area Protection and Emergency Control", Working Group C-6, System Protection Subcommittee, IEEE PES Power System Relaying Committee, January 2003.

[5] V. Madani "Understanding and Preventing Cascading Failures in Power Systems", National Science Foundation, October 2005.

[6] P. Kundur, Power System Stability and Control, McGraw-Hill, 1994.

[7] K. Vu, M. Begovic, D. Novosel and M. Saha, "Use of Local Measurements to Estimate Voltage-Stability Margin," Power Industry Computer Applications Conference (PICA), May 1997.

[8] "Global Industry Experiences with System Integrity Protection Schemes" – Survey of Industry practices – IEEE PES Power System Relaying Committee - Work in progress.

[9] Union for the Coordination of Transmission of Electricity (UCTE), Press Release, September 29, www.ucte.com.

[10] FERC, U.S./Canada Power Outage Task Force, "Initial Blackout Timeline," Press Release, September 12, 2003, www.ferc.gov.

[11] WECC, Coordinated Off-Nominal Frequency Load Shedding and Restoration Plan, November, 1997 and 2004.

[12] V. Madani, M. Adamiak, Engineering and Implementation of Wide Area Special Protection Schemes; Clemson, March 2008.

[13] V. Madani, M. Adamiak; et al. "High-Speed Control Scheme to Prevent Instability of a Large Multi-Unit Power Plant", Georgia Tech Protective Relaying Conference; May 2007.

[14] M. Begovic, V. Madani, D. Novosel, "System Integrity Protection Schemes (SIPS)", International Institute for Research and Education in Power Systems Proceedings, August 2007.

[15] S.H. Horowitz and A.G. Phadke, "Boosting Immunity to Blackouts," Power & Energy Magazine, September/October 2003.

[16] I. Dobson, J. Chen, J. Thorp, B. Carreras, D. Newman, "Examining Criticality of Blackouts in Power System Models with Cascading Outages", Proc. 35th Hawaii International Conference on System Science, Hawaii, January 2002.

[17] "Guide for the Application of Protective Relays Used for Abnormal Frequency Load Shedding and Restoration", IEEE PES PC37.117 System Protection Subcommittee, May 2004.

[18] CIGRE WG38.02.19, D. Karlson, et al., System protection schemes in power, June 2001.

[19] WECC Voltage Stability Methodology – May 1998 and May 2004.

[20] "Industry Experience with Special Protection Schemes" IEEE/CIGRE Special Report, P. Anderson, B.K. LeReverend, IEEE Transactions on Power Systems, Vol. 11, No. 3, Aug. 1996, pp. 1166-1179.