# Reviewing the new IEEE C37.250 Guide for Engineering, Implementation, and Management of System Integrity Protection Schemes

## Power Systems Relaying and Control Committee

## Report of the Working Group C42 of the System Protection Subcommittee


Chair: Gene Henneberg  Vice Chair: Yi Hu

Members and Contributors

Robin Byun
Fernando Calero
Peiman Dadkhah
Alfredo De La Quintana
Ramakrishna Gokaraju
Erin Jessup
Vahid Madani
Mehrdad Majidi
Dean Miller
Wladimir Quishpe

## KEYWORDS

contingency

mitigation

power system protection

remedial action scheme

special protection system

system integrity protection scheme

system performance

# CONTENTS

## ABSTRACT

This paper summarizes the IEEE Std C37.250™-2020, "IEEE Guide for Engineering, Implementation, and Management of System Integrity Protection Schemes" (SIPS). SIPS have been widely used to address power system reliability and other power system operating problems. In the recent past, regulatory authorities such as NERC have developed reliability requirements that several types of SIPS, e.g. RAS, UVLS and UFLS, must meet. This new guide is the first that provides a comprehensive collection of the practical concepts and approaches used to engineer, implement, and manage highly dependable and secure SIPS to meet such regulatory reliability requirements. High reliability is critical for SIPS to avoid cascading outages, equipment damage from unanticipated power system conditions beyond equipment emergency ratings, voltage collapse, angular instability, or other system problems beyond clearing of equipment faults. In addition, the Guide outlines design processes and considerations that will facilitate continued SIPS operation, maintenance, and modifications over the life of the scheme.

## 1. Introduction

In June 2020 IEEE Standards Association published IEEE Std C37.250™-2020 "IEEE Guide for Engineering, Implementation, and Management of System Integrity Protection Schemes" (the Guide). This new Guide was the product of working group C21 of the Power System Relaying and Control Committee of the Power and Energy Society. This guide was produced to share the practical knowledge, innovations, and experience of individuals and companies that have applied in engineering, implementation, and management of reliable System Integrity Protection Schemes (SIPS).

SIPS are mainly applied to protect the integrity of the power system beyond fault clearing. SIPS are applied, for example, to avoid cascading outages, equipment damage from unanticipated power system conditions beyond equipment emergency ratings, voltage collapse, angular instability, or other system problems. SIPS enhance security and prevent propagation of disturbances caused by unacceptable operating conditions and are used to stabilize the power system by taking control action to mitigate those system conditions. The actions taken by the SIPS are independent but coordinated with conventional equipment protection and controls.

The Guide provides the following SIPS definition:

> **System Integrity Protection Scheme (SIPS):** serves to enhance security and prevent propagation of disturbances for severe system emergencies caused by unacceptable operating conditions and is used to stabilize the power system by taking control action to mitigate those system conditions. It also encompasses Special Protection Systems (SPS) and Remedial Action Schemes (RAS) as well as underfrequency (UF), undervoltage (UV), and out-of-step (OOS) protection schemes. [1]

The Guide describes design, application, deployment and operational management of SIPS. Best practices are presented along with the rationale for different methods and in some instances offering a discussion of different solutions. Consideration is given to reliability, architecture, scalability, equipment consideration, commissioning, maintenance flexibility, documentation and record management, and life cycle training. Other common power system control functions such as automatic generation control

(AGC) and power system stabilizers (PSS) are usually not considered to be a form of SIPS because they primarily provide control during the normal variability of power system operations.

## 2. SIPS Overview

SIPS addressed in the Guide are complex, multisite systems that usually require inputs from more than one location to execute mitigation actions. The mitigation actions may also be taken at multiple sites. It is likely that these SIPS are primarily applied to the transmission system.

A power system's needs for SIPS often emerges when the power system could not meet the established performance requirements under certain contingency conditions or other situations.

The need for a SIPS is generally determined through system studies using power flow, stability, and/or other modeling of the power system. The general objectives of this process are as follows:

- Identify all critical single- or multiple system contingencies that result in unacceptable system conditions.
- Identify the power system problem that results from the contingencies of concern.
- Identify any system configuration or system load or generation conditions that would make the system vulnerable to the critical contingencies.
- Identify a sequence of actions to mitigate the problem.
- Identify performance requirements and response to mitigating actions. These identified control actions are what the SIPS is then designed to accomplish.
- In conjunction with the system protection function, determine how the system problem will be identified.

Figure 1 shows a typical SIPS life cycle including determining the power system needs, the conceptual design, recommended studies, engineering design, implementation and commissioning, and system management. For each stage, the inputs and outputs of each state are identified and the key activities to ensure the successful design, implementation, and management of a SIPS are described in the Guide.

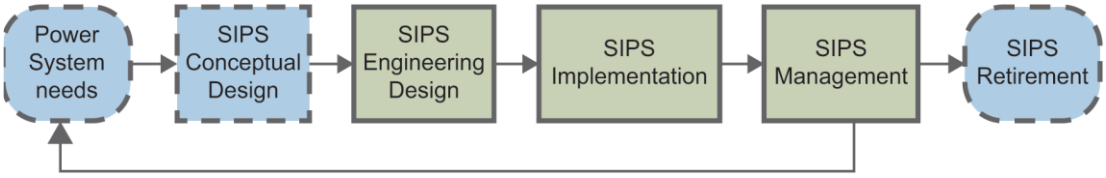


**Figure 1—**Typical SIPS life cycle [1]. *C37.250-2020 - Adapted and reprinted with permission from IEEE. Copyright IEEE 2020. All rights reserved.*

## 3. SIPS applications, actions, and mitigation methods

Unacceptable power system conditions that may require a SIPS to mitigate are discussed in the Guide. These unacceptable system conditions include rotor angle instability, frequency instability, voltage instability, abnormal voltage, and thermal overload. Depending on the condition, the SIPS needs to be designed to have the appropriate range of influence (i.e. local or wide area) and respond in different timeframes. An overview of these unacceptable power system conditions and mitigation strategies are outlined below and discussed in more detail in the Guide. SIPS are applied to mitigate unacceptable system conditions over time scales too fast or using actions too complex for a system dispatcher to do manually, as illustrated in Figure 2.

Actions taken for each of these unacceptable conditions are described in the following sub-sections.

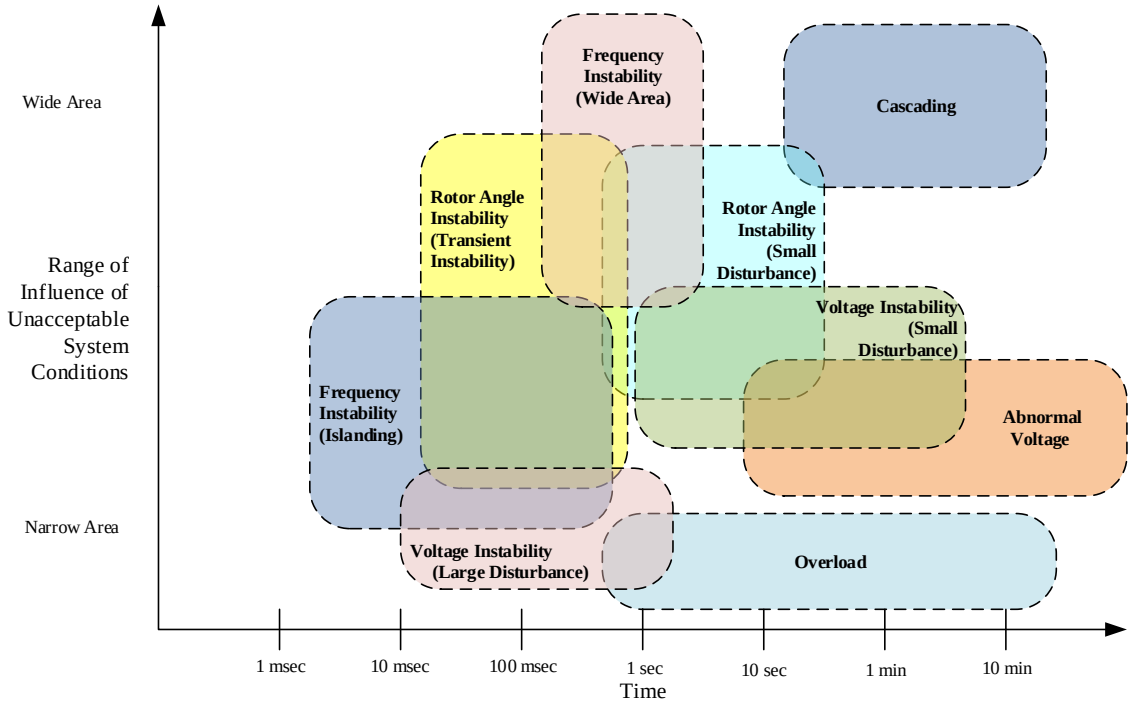


**Figure 2.** Typical range of influence and time scale for which SIPS are used to mitigate system conditions [1]. *C37.250-2020 - Adapted and reprinted with permission from IEEE. Copyright IEEE 2020. All rights reserved.*

### 3.1 Rotor angle instability (also known as loss of synchronism or out-of-step)

Large generators may lose synchronism due to transient instability or small disturbance instability. After the disturbance occurs, if the system is accelerating (overspeed, overfrequency), a SIPS often mitigates this condition by tripping generation (also known as generation rejection). Other mitigation strategies include reducing mechanical inputs to the turbines, inserting a braking resistor, or system separation. The initial mitigation may trigger a need for load shedding.

### 3.2 Frequency instability

Power system equipment can be damaged during off-nominal frequency conditions. When a frequency deviation occurs due to an unbalance between generation and load, it typically causes a wide area disturbance which must be mitigated quickly. A SIPS may shed load for underfrequency conditions or shed generation for overfrequency conditions in coordination with local generation protection schemes.

### 3.3 Voltage instability

Voltage instability can be classified as either large-disturbance or small-disturbance voltage instability. Large disturbances may be caused by significant events such as tripping a transmission line while small disturbances may be caused by a transformer tap change. To prevent widespread voltage collapse, a SIPS may be designed to switch in shunt capacitors, SVCs, or synchronous condensers to provide reactive power supply.

### 3.4 Abnormal voltage

An abnormal voltage condition differs from voltage instability because it results in stable, yet unacceptable system condition. In an overvoltage condition, a SIPS can be applied to use the SVC reactive range and shunt reactors to return the system to an acceptable state. In an undervoltage condition, SVC capacitive range and shunt capacitors are used to increase the system voltage.

### 3.5 Overload

An overload condition happens when the current flowing through the equipment exceeds the rated steady state current. A SIPS can be used to monitor power system flows and respond to an overload condition by load shedding, generator rejection or system reconfiguration to mitigate the condition.

### 3.6 Mitigation methods

SIPS mitigation methods can be classified into three categories including fixed response type, pre-contingency calculation type, and post-contingency calculation type. A fixed response type uses a predetermined set of conditions and thresholds to determine when to take a control action. A pre-contingency mitigation method uses either online or offline models to determine what actions to initiate when a severe contingency occurs. Finally, a post-contingency mitigation method assesses the power system after a contingency occurs and then determines what control action to initiate.

## 4. Engineering a SIPS

### 4.1 Design process

Engineering a SIPS consists of two general phases: the identification of required functionality and the implementation of a physical design to accomplish the required functions. The initial studies identify system conditions which should trigger SIPS action, including arming and monitoring.

Large-scale SIPS tend to be complex, requiring detailed discussions and coordination among the personnel who perform the power system analysis and the engineers who design the components to implement necessary mitigation.

Often the consequences of SIPS failure to operate when required or inadvertent operation are so significant that dependability and security measures and supervisory parameters are included in the design. Operational availability requirements, or mission criticality, of the scheme often leads to redundancy for the SIPS.

### 4.2 Design considerations

It is important that SIPS design, functionality, and performance be validated through tests. Additionally, routine testing of in-service SIPS is important to validate the scheme functionality over its life cycle. Integrating measurement elements, preparing scenarios and simulations to verify the arming, and incorporating many of the elements that validate overall performance reduces the risk of inadvertent operations due to undiscovered failures.

The basic functional requirements for a SIPS include condition measurement of power system inputs (to determine arming and identify contingencies), operational calculations, mitigation action outputs, and communication to transport the inputs to the calculation platform and on to the control outputs. In the simplest case, this occurs at single facility; however, often various components must be located at different facilities with the critical input signals, operational calculations, and control outputs being telecommunicated between locations. In this more common case, a healthy communication system is vital. In addition, the response time of a SIPS including measurement time, processing time, communication channel delay, output control signal delay, and mitigation equipment operate time plays an essential role to handle transient stability issues which may occur within a few cycles. The speed of the SIPS can be less critical for reducing thermal overloads which may be tolerated in the range of seconds to minutes.

SIPS equipment often includes typical protection components such as instrument transformers, cables, switchboard racks, panel segments, auxiliary relays, dc battery control sources, distribution panels, cutout switches, intelligent electronic devices (IED's), in addition to computers, and programmable logic controllers. SIPS will often have its own panel space separate from equipment protection panels.

The basic operational functions of a SIPS can be divided into four parts: arming, contingency detection, operational calculations, and control. Arming may be "always on," a simple determination based on equipment loading, or it may be a more complex calculation such as a nomogram. Arming enables the mitigating action after critical contingencies. Contingency detection is the recognition of critical system failures. Operational calculations are based on both the arming state of the SIPS and these contingencies. When these calculations indicate that an action is required, the control functions enable signals to operate necessary equipment (circuit breakers or other devices). The reliability of the control functions requires a robust communication system.

It is a good practice to monitor the health and relevant status of a SIPS through an Energy Management System (EMS) that is continuously staffed. The large concentration of data present in the EMS can be helpful. This allows for timely identification of SIPS issues so that personnel can be dispatched to perform repairs. SIPS are intended to operate autonomously without dispatcher action for event mitigation.

The SIPS must be coordinated with protective relay functions. A SIPS should be coordinated with auto-reclosing function of line relays to avoid any unnecessary action of SIPS for temporary faults. The SIPS actions should not cause relays to trip due to load conditions on the remaining power system components. The coordination between SIPS

and out-of-step blocking/tripping schemes should be checked. The SIPS may suspend the automatic generation control (AGC) of units in separate power system regions to prevent counterproductive action of AGC which would otherwise ramp up the reserve generation while the SIPS is tripping other units.

The main architecture choices for implementing a SIPS are distributed or centralized. A SIPS may include aspects of both architectures, depending on the scheme purpose and the designer's philosophy. The main SIPS decisions in a centralized scheme are processed at a single location. Remote measurements and control actions are telecommunicated to and from the remote locations. In most centralized designs, it is preferable to locate the SIPS operational controls where the majority of the input or output quantities reside to reduce the required communication infrastructure. In a distributed scheme, logic processing is done at multiple locations as near to measurement and/or control action equipment as possible.

An appropriate human-machine interface (HMI) design is needed to configure, operate, and maintain the SIPS. Manual intervention is needed to enable or disable the SIPS, access programming tools, update settings, change configurations, run test simulations, view event information, and perform troubleshooting. An HMI facilitates human awareness of SIPS alarms and enables human interaction with system diagnostics. It also provides a manual means to download, archive or view event information. A basic HMI consists of a personal computer and/or programmable logic controller (PLC), a PLC operating system, and an HMI configuration software for the controllers. The HMI display will indicate that the scheme is enabled and functioning, identify alarms, indicate control points, or target/flag the presence of a scheme operation. The HMI is also designed to interface with other systems such as the EMS.

Since the purpose of a SIPS is to detect critical system conditions and take control actions that will mitigate electric system performance that would be unacceptable, design reliability is crucial. Thus, SIPS design must satisfy dependability and security requirements. To achieve dependability, it is important to lower the number of failures that may occur. An effective approach is to reduce the number of hardware components by adopting simple scheme designs and follow quality control techniques. To meet the dependability requirements redundant independent systems are often applied. The object is that no single failure will prevent the SIPS from functioning. Security improvement measures include blocking operation after failures and series redundancy. Some schemes, like voting, can improve both dependability and security at the same time.

Automatic supervision (self-monitoring) functions can enhance reliability of the SIPS. Continuous monitoring is used to detect a complete cessation of the SIPS function, an abnormal operation, or other system degradation. Automatic checking assesses information that continuous monitoring cannot check for in sufficient depth, i.e. analog input circuits and output circuits. When a defect is detected by automatic supervision, the SIPS provides an alarm indication and blocks the final output.

SIPS may take different actions depending on the power system conditions and the initiating event; these are referred to as "multi-action SIPS." Multi-action SIPS often monitor several components of the power system. Depending on which component is faulted or the specific fault, different actions are taken. For example, multi-action SIPS may trip generation, lines, transformers, or shed load. These actions are designed to deal

with a single contingency as well as double or triple contingency events that occur in rapid succession. These multi-action SIPS are much different than the typical protective relay system which monitors one piece of equipment. Once the action is taken by a relay, no additional action is required until the device being monitored is returned to service. The complex arrangement of a multi-action SIPS requires the use of power system simulation tests to verity the functionality of the SIPS for a wide variety of simulated feasible events.

### 4.3 Design document preparation

Creation of a SIPS requires comprehensive design documentation for the installation, commissioning, maintenance, periodic testing, and long-term operations of SIPS equipment. Examples of diagrams include: one-lines, schematics, communications, switchboard layout, wiring, and logic diagrams. SIPS equipment co-exists with and may share control circuits with other protection equipment. Documentation of the schematic, layout, and wiring interconnections of the SIPS equipment as well as its relation to existing non-SIPS equipment is necessary.

## 5. SIPS implementation

### 5.1 Process overview

Implementation and Engineering of SIPS are more tightly coupled than traditional protection and control in that selection and applications of equipment and interfaces as well as settings and testing involve engaging various lines of business. There are fewer discrete tasks and more collaboration amongst many different lines of business both during implementation and life-cycle operation of SIPS. For example, for a SIPS impacting only the entity that is implementing the specific scheme, the lines of business may include real-time generation asset, system planning, design engineering, protection and control, operation or Energy Management groups plus much broader IT groups depending on the technology and interfaces selected or whether cyber security is a consideration. For SIPS with wider interfaces outside of one entity, additional engineering and implementation and coordination steps may be involved as interactions with affected systems requires each respective entity's engagement.

As SIPS implementation requires a comprehensive understanding of intent of the scheme and its interactions with other protection and control systems (internal or with interconnected companies), it is most efficient that the implementation engineer is familiar with the hardware and technology used for the respective SIPS. All hardware used should meet every sensing element prerequisites, have compatible data formatting for interoperability, and sufficient data transfer speed. A good testing plan and personnel training are crucial parts of SIPS implementation. Commissioning tests plans must examine all functionality of the SIPS systems including cases where SIPS is not intended to take any action. Settings (pickup, arming, types of triggers), activation logic, interface with other systems and devices, operational alerts and testing are some of the tasks undertaken during implementation stages.

### 5.2 Testing before system implementation

Various tests are required for SIPS implementation based on project size, hardware, and other factors. Refer to IEEE Std C37.233™ for more guidance in these tests.

For localized SIPS that impact a small number of internal facilities, implementation test plans may involve fewer steps compared to SIPS with broader impact which require more comprehensive and coordinated testing of the equipment performance, operational and planning scenarios. Large SIPS have multiple decision branches which need to be tested independently and as a system, and overall throughput validated. System hardware needs to be tested and validated. If a system design is dependent on communications network, then its performance should be tested.

A key point to consider during SIPS original design is the commissioning and maintenance testing processes over the life cycle which will result in more through testing, less time consuming, and less prone to errors.

### 5.3 Types of testing

Successful SIPS implementation relies on comprehensive and coordinated test plans. Depending on the scheme purpose and technology, test plans may contain the following types:

- Proof-of-concept (POC)/laboratory testing
- Field commissioning testing
- Detailed system-wide performance testing (during maintenance intervals)
- Validation through state estimation
- Automatic and manual periodic testing of the entire scheme

This section explores the first two items.

Use of POC facility allows the implementors to validate intent of scheme, engage various lines of business or interconnected parties participating in the operation of the SIPS. POC facility allows for closed loop testing to validate overall performance on a smaller scale, make modifications in settings or logic, or various IT components prior to field deployment. POC also helps with developing test plans for later stages of field installations. Some examples of use of a POC facility may be for response-based scheme such as wide-area voltage control SIPS applied to bulk interconnected power systems or SIPS that use rate of change of power flow or rate of change of frequency (ROCOF) to trigger action. Use of a POC facility provides a venue to validate overall performance, engage others for their feedback, help develop life cycle asset strategy, provide a training test bed, and make evaluation and implementation agreements more effective and efficient.

### 5.4 SIPS training

SIPS training needs to be commensurate to the system's complexity. There are four important components to considered when creating SIPS training materials: overview of design elements, equipment used, system functionality, and expected system and human response to events.

It is essential that the designers note essential trainings for relevant personnel. Based on SIPS level of complexity the training might only include the system operators or if complex enough many other departments.

## 6. SIPS management philosophy

SIPS are installed for a wide variety of reasons with intent to maintain or improve the reliability of the power system. To support daily operation during life cycle, including SIPS

maintenance, testing, and upgrades, redundant systems are often deployed. Redundant SIPS consist of at least two independent schemes, each of which by itself can perform the full suite of functions required to assure reliable electric system performance. Depending on the purpose and overall throughput performance of a SIPS, there may be ways to achieve redundancy in addition to the traditional method of a second scheme having a full complement of measurements, actions, arming methods, and controllers where applied. One example might use out of step devices to locally provide back-up the SIPS.

Availability, reliability, and resilience of SIPS are part of the SIPS management. Operational aspects and performance assessment require a comprehensive plan which includes day-to-day operation, managing priority response to equipment failures requiring attention, analysis of events to determine overall performance based on system study requirements, and/or power system configuration changes that may require parts of the SIPS to be changed. For example, a new outage detection location or addition of an action site may need to be included based on new operational requirements. Corrective, diagnostic, or when needed, failure remediation corrective actions are performed after a problematic SIPS operation. For instance, failure to operate when intended, and/or test failure during planned maintenance schedule. This activity may include providing documentation to operational or oversight authorities where applicable, in particular when a SIPS underperforms or does not operate as intended.

## 6.1 SIPS operational management

The failure of a SIPS to operate correctly may result in system problems including some or all of the following: major system instability, voltage deviations, thermal overloads, equipment damage. Most SIPS do not operate as often as traditional protection schemes because their operation is often intended to remediate system problems of a wider scale. Therefore, when SIPS operate, it is important to determine whether the scheme operated correctly. Some of the criteria that can help judge whether SIPS operation is correct are:

- The power system events and/or conditions appropriately triggered the SIPS.
- The SIPS responded as designed.
- The SIPS was effective in mitigating power system performance for which it was designed.
- The SIPS operation resulted in any unintended or adverse system response.

Evaluation of the first two items can generally follow procedures similar to analyses of equipment protection operations. Analysis of the third and fourth items may require further evaluation using power flow, stability, or other system performance analysis tools. More detailed assessment would include throughput timing and comparison with either commission tests or historical operation if there have been previous operations under similar operating conditions.

Redundant SIPS are also used to improve both dependability and security to ensure correct operations even if one scheme fails. Non-redundant SIPS require mitigating measures to cover for conditions when the SIPS fails to operate, e.g. system operators could be required to modify operating procedures, such as re-dispatch of generation or arming of appropriate actions prior to the critical contingency that the SIPS is designed to detect.

## 6.2 SIPS maintenance management

Some hardware used for SIPS is similar to traditional protection systems equipment, using similar types of IEDs. Hence, parts of maintenance procedures for SIPS may look similar. It will often be possible to use the protection system maintenance procedures as a base on which to

design the SIPS maintenance procedures. However, the setpoints and logic may be completely different therefore, requiring independent SIPS maintenance procedure.

Generally, some standards impose specific requirements on both protection systems and SIPS maintenance activity. These may range from an owner's internal practices to national or international regulations.

Present day IEDs have self-check diagnostics and can be programmed to alarm. Device self-monitoring provides hardware and possibly communication inputs to the device. The user must determine whether user programmable logic or interface with other hardware require additional test procedures beyond device self-diagnostics.

Preventative or routine maintenance activity is usually performed on a specific, scheduled basis. Typical functions include but may not be limited to the following activities:

- Procedures to remove and restore the SIPS to service
- Battery maintenance
- Verification of ac system inputs and any thresholds
- Verification of DC control system inputs and outputs
- Communication channel health
- Verification that field device settings match the specified settings

Verification that each specified group of SIPS inputs produces the expected set of outputs for SIPS operations and data logging, for example, HMI and SCADA.

A SIPS functional test will usually be part of a testing program. The objective of functional testing is to verify the overall performance of the scheme. Functional tests validate SIPS operation by ensuring inputs, outputs, communication, arming, logic, and throughput timing provide the expected results. SIPS owners are best positioned to determine the specific tests that are appropriate for their schemes. An actual correct SIPS operation may be treated as a successful functional test (or a partial test depending on the SIPS as a single purpose or having multiple actions) if it could be demonstrated that all elements within the scheme performed as intended. It is a good practice to verify the entire SIPS response to a specific operating situation and to validate overall performance even for successful operations.

The overall objective is to discover any latent failures or hidden failures that could cause an incorrect operation or failure of the SIPS to operate.

Depending on the type and complexity of a SIPS, it may be more feasible to use a segmented functional testing approach. Overlapping tests of individual SIPS segments, when properly arranged, can thoroughly test a SIPS. Care should be exercised to track the throughput timing of segmented tests to assure that overall scheme timing is satisfactory.

Often SIPS cover a large area and have a significant impact on system operation. Therefore, functional tests are often scheduled at a time when the scheme operation would not be required if the critical contingency occurred, or in situations when the power system flows can be adjusted in order to accommodate a window of time when tests are conducted.

Often large SIPS use predefined simulated system conditions and contingencies in an automated, on-site test system to allow the overall SIPS to remain in service while individual redundant components are removed, modified, and any necessary setting changes are made and tested. The basic intent is to isolate the modular components of the SIPS by blocking control actions while observing their behavior as the inputs are subjected to predefined contingencies and simulated power system values.

### 6.3 SIPS corrective maintenance

Corrective, diagnostic, or failure maintenance is performed after a problematic SIPS operation, failure to operate when intended, or test failure during routine maintenance. The specific issue is documented, and repairs performed. This activity may include providing documentation to operational or oversight authorities, when required, depending on the nature of the failure and whether the failure had a negative impact on the power system.

### 6.4 SIPS operational assessment management

Operational studies of the electric system are performed on time scales ranging from real-time contingency analysis (RTCA), day ahead, week ahead. Potential SIPS operations are included in these analyses to ensure these impacts will be understood and anticipated by the system operators. This knowledge enables economic system operation through optimized generation dispatch as well as secure operation for both scheduled and forced equipment outages.

### 6.5 Periodic planning assessment

Electric systems change over time as lines, transformers, and generators are added or retired and loads are added or shut down. Such changes may directly or indirectly impact appropriate operation of the SIPS. Therefore, system configuration changes need to be evaluated for their impact on existing SIPS.

SIPS need to be reviewed when major system changes are planned. Incremental system changes, however, may also impact SIPS operation, so that periodic assessment is important. The assessment period is generally specified by local standards, which typically range from annually to five years or longer. These assessments are substantially a “rerun” of the original power system analysis studies on which the SIPS was originally designed but with current base cases that include all subsequent and planned system changes in the power system analysis models.

Some of the important issues that need to be reviewed by a periodic assessment include:

- Review the SIPS purpose and impact to ensure proper classification (when classification is pertinent).
- Is the SIPS still necessary?
- Does the SIPS still serve the intended purposes?
- Will the SIPS intended operation comply with performance requirements?
- Are there any coordination problems between this SIPS and other SIPS, protection, or control systems?
- If the assessment shows that the SIPS operation no longer complies with standards or has coordination problems with other systems, develop a plan to update the SIPS that will recover its necessary functionality.

It is also important to have a retirement plan for SIPS that are no longer operationally necessary for the system to meet performance requirements.

## 7. Summary

The recently published IEEE Std C37.250™-2020 “IEEE Guide for Engineering, Implementation, and Management of System Integrity Protection Schemes” provides a comprehensive look at managing the life cycle of SIPS. The Guide includes definitions with a brief review of system planning and system performance requirements before discussing in more detail the engineering, commissioning, testing, documentation, operations, and life cycle management processes of SIPS.

## 8. References


[1] IEEE Std C37.250™-2020, “IEEE Guide for Engineering, Implementation, and Management of System Integrity Protection Schemes”

[2] IEEE Std C37.233™-2009, “IEEE Guide for Power System Protection Testing”

[3] V. Madani, D. Novosel, S. Horowitz, M. Adamiak, J. Amantegui, D. Karlsson, S. Imai, A. Apostolov, IEEE PSRC Report on Global Industry Experiences With System Integrity Protection Schemes (SIPS), IEEE Transactions on Power Delivery, Vol. 25, NO. 4, October 2010, pp. 2143-2155

[4] North American Electric Reliability Corporation, Standard PRC-012-2, Remedial Action Schemes

[5] Western Electricity Coordinating Council, RWG and RASRS, RAS Design Guide, 2021