



IEEE Guide for Engineering, Implementation, and Management of System Integrity Protection Schemes

IEEE Power and Energy Society

Developed by the
Power System Relaying and Control Committee

IEEE Std C37.250™-2020

STANDARDS

IEEE Guide for Engineering, Implementation, and Management of System Integrity Protection Schemes

Developed by the

Power System Relaying and Control Committee
of the
IEEE Power and Energy Society

Approved 5 March 2020

IEEE SA Standards Board

Abstract: Guidance for engineering, implementation, and management of System Integrity Protection Schemes (SIPS) is provided in this guide. General concepts for architecture and communication design to achieve functionality and performance requirements are addressed. Principles for commissioning processes and strategies for life-cycle management are also discussed.

Keywords: contingency, IEEE C37.250™, mitigation, power system protection, Remedial Action Scheme, Special Protection System, stability, System Integrity Protection Scheme, system performance

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2020 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 17 June 2020. Printed in the United States of America.

IEEE and 802 are registered trademarks in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-1-5044-6559-5 STD24118
Print: ISBN 978-1-5044-6560-1 STDPD24118

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading “Important Notices and Disclaimers Concerning IEEE Standards Documents.” They can also be obtained on request from IEEE or viewed at <http://standards.ieee.org/ipr/disclaimers.html>.

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents (standards, recommended practices, and guides), both full-use and trial-use, are developed within IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (“IEEE SA”) Standards Board. IEEE (“the Institute”) develops its standards through a consensus development process, approved by the American National Standards Institute (“ANSI”), which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed through scientific, academic, and industry-based technical working groups. Volunteers in IEEE working groups are not necessarily members of the Institute and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. IEEE standards documents are supplied “AS IS” and “WITH ALL FAULTS.”

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to comments or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

Secretary, IEEE SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854 USA

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate fee, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit IEEE Xplore at <http://ieeexplore.ieee.org/> or contact IEEE at the address listed previously. For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website at <http://standards.ieee.org>.

Errata

Errata, if any, for IEEE standards can be accessed via <https://standards.ieee.org/standard/index.html>. Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in IEEE Xplore: <https://ieeexplore.ieee.org/browse/standards/collection/ieee/>. Users are encouraged to periodically check for errata.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at <https://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this IEEE guide was completed, the C21—Engineering, Implementation & Management of System Integrity Protection Schemes Working Group of the Power System Protection & Control Committee had the following membership:

Yi Hu, *Chair*
Gene Henneberg, *Vice Chair*

Laura Agudelo
Eric Allen
Alex Apostolov
Phil Beaumont
Robin Byun
Alfredo de la Quintana

Alla Deronja
Kamal Garg
Anthony Johnson
Vahid Madani
Heather Malson
Dean Miller

Manish Patel
Zuyi Ren
Tony Seegers
Bonian Shi
Roger Whittaker
Yu Xia

The following members of the individual balloting committee voted on this guide. Balloters may have voted for approval, disapproval, or abstention.

William Ackerman
Laura Agudelo
Ali Al Awazi
Phil Beaumont
Martin Best
William Bloethe
Brian Boysen
Sukumar Brahma
Gustavo Brunello
Demetrio Bucaneg Jr.
Paul Cardinal
James Cornelison
Luis Coronado
Randall Crellin
Randall Cunico
Ratan Das
Robert Dempsey
Alla Deronja
Michael Dood
Donald Dunn
Paul Elkin
Jean-Sebastien Gagnon
Rafael Garcia
Kamal Garg
Tim Godfrey

Randall Groves
Hamidreza Heidarisafa
Gene Henneberg
Werner Hoelzl
Yi Hu
Anthony Johnson
Brian Johnson
Laszlo Kadar
Innocent Kamwa
Piotr Karocki
John Kay
Yuri Khersonsky
James Kinney
Boris Kogan
Jim Kulchisky
Chung-Yiu Lam
Don Lukach
Bruce Mackie
Dean Miller
Adi Mulawarman
R. Murphy
Bruce Muschlitz
Anthony Napikoski
Arthur Neubauer

Ming Ni
James O'Brien
Lorraine Padden
Manish Patel
Farnoosh Rahmatian
Zuyi Ren
Charles Rogers
Tony Seegers
Robert Seitz
Jerry Smith
Gary Smullin
Gary Stoedter
Eric Thibodeau
Michael Thompson
Matthew Vacha
James Van De Ligt
Benton Vandiver
John Vergis
Quintin Verzosa
Christopher Walker
John Wang
Kenneth White
Roger Whittaker
Philip Winston
Haiyan Zhang

When the IEEE SA Standards Board approved this guide on 5 March 2020, it had the following membership:

Gary Hoffman, *Chair*
Jon Walter Rosdahl, *Vice Chair*
Jean-Philippe Faure, *Past Chair*
Konstantinos Karachalios, *Secretary*

Ted Burse
J. Travis Griffith
Grace Gu
Guido R. Hiertz
Joseph L. Koepfinger*
John D. Kulick
David J. Law

Howard Li
Dong Liu
Kevin Lu
Paul Nikolich
Damir Novosel

Dorothy Stanley
Mehmet Ulema
Lei Wang
Sha Wei
Philip B. Winston
Daidi Zhong
Jingyi Zhou

*Member Emeritus

Introduction

This introduction is not part of IEEE Std C37.250–2020, IEEE Guide for Engineering, Implementation, and Management of System Integrity Protection Schemes.

This guide is provided to share the knowledge, innovations, and experience of companies that have applied System Integrity Protection Scheme (SIPS) in certain contexts, such as in Remedial Action Scheme (RAS), Special Protection System (SPS), and so on. SIPS are mainly applied to protect the integrity of the power system. Unlike traditional localized equipment protection, 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 are applied for extreme contingencies when outages to critical high-voltage (HV) equipment, components, or elements of the power system have occurred.

This guide describes design, application, deployment, and operational management of SIPS. Best practices are presented along with the rationale for different methods, in some instances, offering a discussion of different solutions for user information. Consideration is given to reliability, design architecture, equipment consideration, deployment location, commissioning, maintenance flexibility, upgradability, documentation and record management, and personnel training.

This information is useful to planners, engineers, managers, system operators, owners, and technicians who are planning, designing, installing, testing, operating, maintaining, replacing, or retiring a SIPS.

Contents

1. Overview	10
1.1 General	10
1.2 Scope	10
1.3 Purpose	10
2. Normative references	10
3. Definitions, acronyms, and abbreviations	11
3.1 Definitions	11
3.2 Acronyms and abbreviations	11
4. System Integrity Protection Scheme overview	12
4.1 System Integrity Protection Scheme application overview	12
4.2 System Integrity Protection Scheme covered in this guide	15
4.3 Types of System Integrity Protection Scheme actions	16
4.4 System Integrity Protection Scheme life-cycle overview	16
4.5 General System Integrity Protection Scheme classifications	20
4.6 Classification of mitigation methods based on their characteristics	27
5. Engineering a System Integrity Protection Scheme	31
5.1 System Integrity Protection Scheme engineering design process	32
5.2 System Integrity Protection Scheme engineering design considerations	36
5.3 Engineering documents preparation	55
6. System Integrity Protection Scheme Implementation	56
6.1 System Integrity Protection Scheme implementation process overview	57
6.2 Testing before placing a System Integrity Protection Scheme in service	58
6.3 System Integrity Protection Scheme training	62
7. System Integrity Protection Scheme management	63
7.1 System Integrity Protection Scheme management philosophy	63
7.2 System Integrity Protection Scheme operation management	64
7.3 System Integrity Protection Scheme maintenance management	64
7.4 System Integrity Protection Scheme in-service assessment management	66
Annex A (informative) Bibliography	69

IEEE Guide for Engineering, Implementation, and Management of System Integrity Protection Schemes

1. Overview

1.1 General

Power system conditions requiring mitigation beyond fault protection often are unique problems. The difficulties magnify when the power system, or a section of the power system, is cascading rapidly and system integrity requires rapid detection and remedy. Since the power system and sequence of cascading conditions may vary, System Integrity Protection Schemes (SIPS) are intended to cover the specific circumstances necessary to protect the system. In most instances, however, general design concepts, commissioning principles, and management strategies are applicable to a wide range of SIPS. This guide documents concepts, principles, and strategies as applied in many deployed SIPS. Those responsible for system planning, engineering, implementation, and management of SIPS will benefit from the information provided in this guide.

Not all SIPS are intended to be covered by this guide. SIPS that are covered are those that have a wide-area impact, usually require information exchange among multiple locations, and generally require a complex architecture. See [4.2](#) for a list of SIPS that are covered by this guide.

1.2 Scope

This document provides guidance for engineering, implementation, and management of SIPS. General concepts for architecture and communication design to achieve functionality and performance requirements are addressed. The document also addresses principles for commissioning processes and strategies for life-cycle management.

1.3 Purpose

This guide provides information to help properly engineer, implement, and manage SIPS. The document addresses general concepts for architecture and communication design to achieve functionality and performance requirements and principles for SIPS implementation and management.

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is

explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

IEC 60870, A series of standards defining systems used for telecontrol (supervisory control and data acquisition).¹

IEC 61850, A series of standards defining communication protocols for intelligent electronic devices at electrical substations.

IEC 61970, A series of standards dealing with the application program interfaces for energy management systems (EMS).

IEEE Std C37.2TM, IEEE Standard Electrical Power System Device Function Numbers, Acronyms, and Contact Designations.^{2,3}

IEEE Std C37.94TM, IEEE Standard for N times 64 kbps Optical Fiber Interfaces between Teleprotection and Multiplexer Equipment.

IEEE Std C37.233TM, IEEE Guide for Power System Protection Testing.

ISA-99/IEC 62443, Industrial Automation and Control Systems Security” / “Cybersecurity Certificate Programs.⁴

ITU-T G.703, Physical/electrical characteristics of hierarchical digital interfaces.⁵

NERC TPL-001, Transmission System Planning Performance Requirements.⁶

3. Definitions, acronyms, and abbreviations

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.⁷

3.1 Definitions

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.

3.2 Acronyms and abbreviations

AGC automatic generation control

¹IEC publications are available from the International Electrotechnical Commission (<http://www.iec.ch>) and the American National Standards Institute (<http://www.ansi.org/>).

²The IEEE standards or products referred to in [Clause 2](#) are trademarks owned by the Institute of Electrical and Electronics Engineers, Incorporated.

³IEEE publications are available from the Institute of Electrical and Electronics Engineers (<http://standards.ieee.org/>).

⁴ISA publications are available from the International Society of Automation (<http://isa.org/>).

⁵ITU-T publications are available from the International Telecommunications Union (<http://www.itu.int/>).

⁶NERC publications are available from the North American Electric Reliability Corporation (<http://www.nerc.com/>).

⁷*IEEE Standards Dictionary Online* is available at: <http://dictionary.ieee.org>. An IEEE Account is required for access to the dictionary, and one can be created at no charge on the dictionary sign-in page.

CT	current transformer
DNP	Distributed Network Protocol
EMS	energy management system
FAT	factory acceptance test
GOOSE	Generic Object Oriented Substation Events
GUI	graphical user interface
HMI	human-machine interface
IED	intelligent electronic device
IP	Internet Protocol
NERC	North American Electric Reliability Corporation
OOS	out of step
PC	personal computer
PHIL	power hardware in the loop testing
PLC	programmable logic controller
PSS	power system stabilizer
RAS	Remedial Action Scheme
SAT	site acceptance test
SCADA	substation control and data acquisition
SIPS	System Integrity Protection Scheme
SONET	synchronous optical networking
SPS	Special Protection System
STATCOM	static synchronous compensator
SVC	static voltage-ampere reactive (VAR) compensator
UF	underfrequency
UV	undervoltage
VAR	voltage-ampere reactive
XML	Extensible Markup Language

4. System Integrity Protection Scheme overview

4.1 System Integrity Protection Scheme application overview

The power grid is a complex system with wide geographical reach and a large number of elements. A large-scale power system dynamic response can be very fast. A disturbance resulting from a critical contingency may quickly spread to have a larger impact, if not mitigated. A SIPS is often used to maintain the reliable operation of the power system for critical single or double (or additional) contingencies by enabling the system to achieve system performance objectives and preventing or minimizing large-scale power outages. The actions taken by the SIPS are independent from systems engineered to address conventional equipment protection, such as fault clearing or, for example, transformer or capacitor protection.

SIPS actions are normally required when a system operator should not be expected or is not able to take appropriate action within the required time. Within this guide, the term “system operator” is used to describe several functions that may have different job titles⁸ and varying duties in different companies.

The need for a SIPS and the actions it is intended to take are typically determined through system planning studies such as power flow, stability, and/or other modeling of the power system as part of the transmission operations function. For example, in North America, the system planning engineer typically models the contingencies specified in the North American Electric Reliability Corporation (NERC) standard TPL-001.⁹ System studies identify conditions when system performance is not acceptable. Although this process is not described here in significant detail, it is vital to recognize that this process identifies intent, high-level monitoring elements, and performance requirements for the scheme and is the basis for an engineering solution to implement the particular SIPS. System studies also assist in general understanding of monitoring and set points, arming and alarming elements to be engineered during the scheme design. The general objectives of this planning process are as follows:

- Identify all critical single- or multiple-system contingencies that result in unacceptable system conditions. Usually these involve the unplanned unavailability or incorrect operation of one or more elements resulting in unanticipated system conditions from which the system may not be able to recover. Mitigation will result in a stable system that avoids prolonged stress to any portion of the system that would lead to further problems.
- Identify the power system problem that results from the contingencies of concern. This problem is generally a violation of performance standards or other applicable planning or operating criteria. SIPS are typically designed to mitigate the effects of one or a limited set of specific contingencies that result in unacceptable system conditions.
- Identify any system configuration or system load or generation conditions that would make the system vulnerable to the critical contingencies. When such conditions exist, these represent “arming” conditions to enable SIPS action upon subsequent detection of the critical contingency. When system performance is vulnerable to the critical contingencies under any conditions, the SIPS may also be described as “always armed” to take action upon detection of the critical contingency.
- Identify a sequence of actions through further system modeling to mitigate the problem(s). These actions are the basis of (and may be) the appropriate SIPS actions.
- Identify performance requirements and response to mitigating actions. For example transient stability and some voltage stability problems may require rapid mitigation, whereas a thermal overload condition may accommodate some time delays.
- These identified control actions are what the SIPS is then designed to accomplish. The actions may include, but are not limited to, load shedding, generator rejection or ramping, system reconfiguration, or switching of series or shunt reactive devices such as static VAR compensator (SVC), synchronous condenser, STATCOM, and so on. A more detailed control action list is included in 4.4.
- In conjunction with the system protection function, determine how the system problem will be identified. This may be equipment status (out of service), fault detection, equipment loading, or other pertinent system conditions.

Generally, several defense lines are engineered to aid power system operation and to help ensure the security and the stability of the power grid. For example, protective relays isolate failed component(s) from the rest of the power system. Although fault clearing functions are not specifically part of SIPS and are beyond the

⁸These functions include but are not limited to 1) substation operator or control room operator for operational work performed at a specific site; 2) transmission operator to monitor the transmission system via data collected from SCADA and performs appropriate switching, and so on; 3) SIPS operator to monitor SIPS functions via substation control and data acquisition (SCADA) and perform any manual operations that may be required based on the specific SIPS designs; 4) dispatcher is often the same as transmission operator; or 5) generation dispatcher to schedule resources to supply power to the system to serve load requirements.

⁹Information on references can be found in [Clause 2](#).

scope of this guide, fault detection or the open-circuit breakers that are associated with fault clearing are often important parameters for event-based SIPS to determine loss of critical equipment leading to contingencies.

Another line of defense includes controls that “fine tune” system operations, such as transformer load tap changers and switching shunt capacitors and reactors based on local voltage or other local measurements. As with fault clearing, these local control devices and functions are also beyond the scope of this guide.

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, at least on their own. Such schemes can and do react when contingencies change system conditions, but they are primarily intended to provide control during the normal variability of power system operations. It is possible that SIPS action may suspend AGC if the scheme involves rejection or runback of generation. Such control schemes are discussed elsewhere in adequate detail (e.g., IEEE Power and Energy Society [B10] and Madani et al., *IEEE Transactions on Power Delivery* [B26]), and, therefore, are not discussed in this guide.¹⁰

SIPS are applied as another line of defense to mitigate a wide range of post-contingency power system problems, as outlined in 4.2. The more common problems include transient angular stability, prevention of or limiting the extent of cascading outages, wide area voltage collapse, and thermal overloads.

The SIPS may include multiple system condition detection levels and actions to mitigate the most severe power system disturbances, including islanding or other cascading conditions. Successful operation of the SIPS results in the power system returning to a new stable operating condition after the disturbance that it is designed to mitigate.

Often the consequences of SIPS failure to operate when required or inadvertent operation would be so significant that dependability and security measures and supervisory parameters from either local measurements or remote locations to validate the system impact are included in the design. Other possible solutions may be based on overall expected reliability, either part of the entire scheme or applied to specific parts, such as voting schemes. Voting schemes, as the term indicates, require more than one action to activate a portion or the entire scheme. Voting schemes may, therefore, need to address the maintenance or unavailability of one of the voting elements. Operational availability requirements, or mission criticality, of the particular scheme may also lead to redundancy for a particular SIPS. In some instances, there may also be regulatory requirements when applying engineered solutions for these schemes.

It is important that SIPS design, functionality, and performance be properly validated through appropriate tests. A SIPS design could be validated through the use of specialized test software and, hardware. Customized test plans that use simulation tools such as power-hardware-in-the-loop (PHIL) testing simulate the power system and use the SIPS equipment to allow their interactions to be observed.

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 help to reduce the risk of inadvertent operations due to undiscovered failures in the SIPS hardware, logic, wiring, and security, as well as help to ensure that the SIPS design meets the overall performance specifications. Carefully planned and prepared test plans also help to identify isolation points. SIPS may interface with power system equipment such as circuit breakers, or conventional protection schemes, for example, breaker failure, direct transfer trip, and reactive voltage equipment, so that test programs will isolate the SIPS while it is under test. Such assessments are vital as an ongoing part of managing SIPS because the electric power system in which a SIPS operates will often change over time.

¹⁰The numbers in brackets correspond to those of the bibliography in Annex A.

Even after a SIPS is placed in service, system planning engineers continue to play a vital role in periodic assessment of the particular SIPS such as in determining the continued need for the scheme or to update contingency tables or arming levels. These topics are discussed in more detail in 7.4.

Cyber-security issues are important from operations and maintenance perspectives when engineering solutions for many types of protection and control schemes, including SIPS. When the schemes are communication based, and in cases when a network is used for parts of the scheme, or when there is an interface between SIPS and the hardware or equipment common to SIPS and conventional protection, incorporating cyber-security measures is important. There are also SIPS that are response based. For example, such schemes incorporate power system parameters such as rate of change of power or reactive voltage support as part of either scheme supervision or arming circuits. There are also SIPS that use network-based precision timing such as IEEE Std 1588™, making cyber-security measures more critical in engineering and employing such solutions. As these topics are often part of solutions that encompass corporate policies, however, SIPS solutions would also be part of the overall strategy that is applied to other protection and control systems. This subject is not directly discussed in this guide.

4.2 System Integrity Protection Scheme covered in this guide

In general, the definition of SIPS encompasses SPS, RAS, as well as additional schemes such as UF, UV, OOS, and so on. Although all these SIPS are critical to the protection of the electrical grid, this guide will focus on a subset of them. Several are addressed in other IEEE publications or just require “simple” coordination. The SIPS that will be addressed in this guide are complex, multisite systems that require multiple inputs from more than one location for execution of the desired mitigation actions. The mitigation actions may also be taken at multiple sites. It is likely that the SIPS covered in the guide are primarily applied to the transmission system. The coordination aspect of the SIPS, however, can extend into distribution systems as renewable or other small-scale generation on the distribution system becomes more prevalent.

The SIPS covered in this guide typically include the following components:

- Arming functions*: These may be inputs from monitoring systems such as energy management systems (EMS) or be an integral part of the SIPS. The facilities may include SCADA systems. The arming/disarming facilities may be manual or automatic.
- Monitoring devices*: These will often be relays but may be other devices as well.
- Mitigation devices*: These will also likely be relays; they may or may not be the same devices as the monitoring device, and they may or may not be located at the same sites as the monitoring devices.
- Operational calculations controller*: This is often a computational platform, which could be a relay, programmable logic controller or a specialty computer-based controller system.
- Communication infrastructure*: This is a high-speed communication path or network that meets the performance requirements of the SIPS.

Examples of SIPS not covered by this guide are SIPS that are generally less complex or have a restricted scope of monitoring and action. The broad, general definition of SIPS includes many of these, although most are among the smaller scale SIPS that are not specifically intended to be described in this document. The concepts that define a SIPS may be applied at distribution voltage levels or elsewhere within a power system. Such schemes will generally be individually applied on a small scale, however, so they are not specifically covered by this guide.

4.3 Types of System Integrity Protection Scheme actions

The IEEE Power and Energy Society Report “Global Industry Experiences with System Integrity Protection Schemes (SIPS)” [B10] listed many types of SIPS functions in use by the global power industry. These and other possible actions are as follows:

- Generator rejection (also called generator shedding)
- Load shedding (also called load rejection)
- Underfrequency load shedding
- Undervoltage 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
- Load and generation balancing
- Shunt capacitor and reactor switching
- Tap-changer control
- SVC/STATCOM control
- Turbine valve control
- High Voltage Direct Current (HVDC) controls
- Power System Stabilizer Control
- Discrete excitation
- Dynamic braking
- Generator runback
- Bypassing series capacitor
- Black-start or gas-turbine start-up
- AGC actions
- Busbar splitting
- System reconfiguration
- Fast control to photovoltaic inverters
- Fast control to wind turbine controllers
- Fast control to energy storage controllers
- Synchronous condenser control

4.4 System Integrity Protection Scheme life-cycle overview

The typical life cycle of SIPS is illustrated in Figure 1.

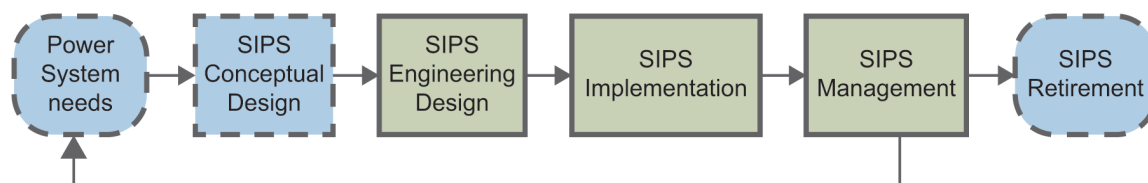


Figure 1—Typical System Integrity Protection Scheme life cycle

A SIPS is applied to address specific system needs. When such needs arise, a SIPS conceptual design study will identify the problems to be solved, types of mitigation actions to be taken by the SIPS, and any associated functional and performance requirements. The design study is followed by the engineering design and the implementation processes including commissioning the SIPS. Once commissioned, proper management is required until the SIPS is retired. In Figure 1, information within the boxes enclosed by solid lines is covered in detail in this guide. Information enclosed with dashed lines is not the focus of this guide, but it is briefly described to provide relevant background information. This guide also uses this formatting in Figure 1 through Figure 5, Figure 12, Figure 23, and Figure 24.

Each stage in the SIPS life cycle has multiple activities. The following is an overview of the main activities at each stage. The activities in the SIPS conceptual design stage also determine the input to the SIPS engineering stage. In the following overview, the input and output of each stage are shown in the following pertinent figures as parallelograms and the activities are shown as rectangles.

Considerations in the selection of types of SIPS actions that are part of the SIPS conceptual design process are described in 4.5.1.

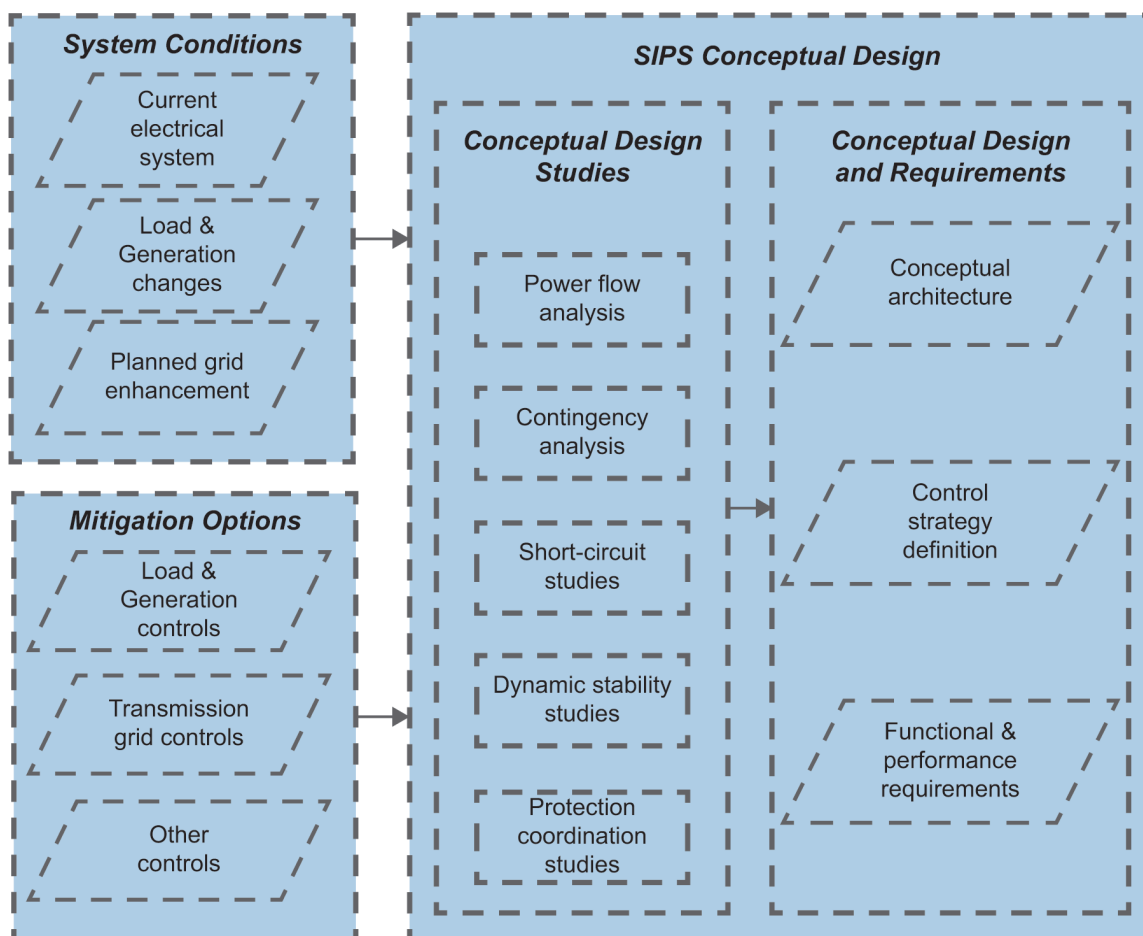


Figure 2—System Integrity Protection Scheme conceptual design

Figure 2 shows the main activities of the SIPS conceptual design stage, and the input and output of this stage. The conceptual design process involves performing contingency analysis, short-circuit, dynamic stability, and protection coordination studies to determine mitigation options to be used, selection of type of SIPS actions, overall control strategy, and identification of functional and performance requirements of SIPS. The studies include the current system conditions, forecasted load/generation growth, planned electric network expansion, and consideration of available mitigation options, such as load/generation controls, transmission network controls, and other types of controls such as those listed in 4.3. The conceptual design should also include an analysis of the SIPS architecture such that it is possible to intervene, upgrade, and service the SIPS without having to remove it from service.

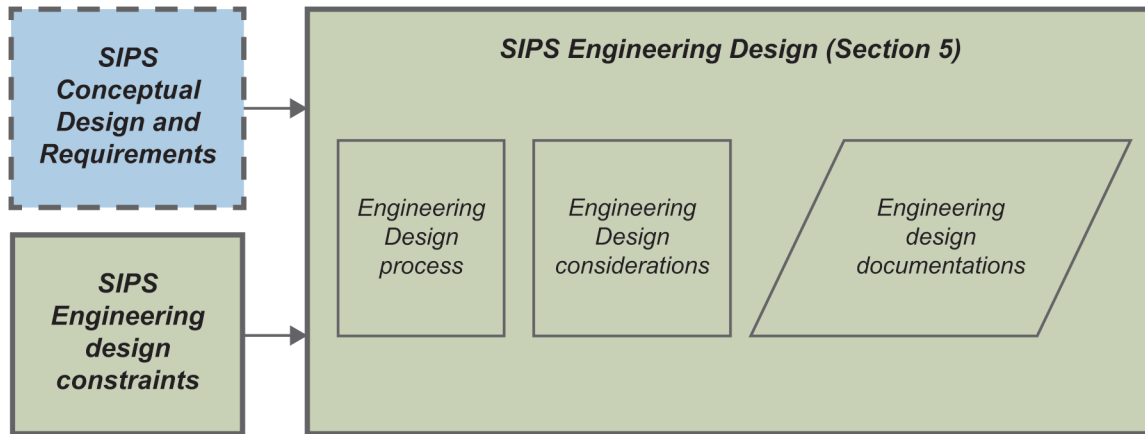


Figure 3—System Integrity Protection Scheme engineering design

Figure 3 shows the main activities of the SIPS engineering design stage. It takes the outputs of the SIPS conceptual design stage and generates the engineering design documentation as the output that will be used in the SIPS implementation stage. In addition to the output from the SIPS conceptual design stage, the SIPS engineering design must also take certain engineering design constraints into consideration, such as electricity supply system regulations and restrictions, product/technology availability, operational philosophy, architecture reliability analysis, and original installation drawings of facilities where SIPS components will be located. The SIPS engineering design process turns the conceptual SIPS design into detailed system design for subsequent implementation of the SIPS.

The process involves an initial interaction between engineering designers and conceptual designers to aid the former in understanding the conceptual design and to clarify the requirements, the initial selection and placement of the main functional components, and the communication network requirement specifications.

The main design activities include the selection of solution architecture, human-machine interface (HMI) design, communication network design, and various interface designs. These designs are affected by considerations such as the level at which SIPS will need to interact with system operators, coordination with other protection, and amount of control versus scale of the disturbance. The completed designs should be evaluated to help ensure the availability, testability, and maintainability requirements of the SIPS are satisfied.

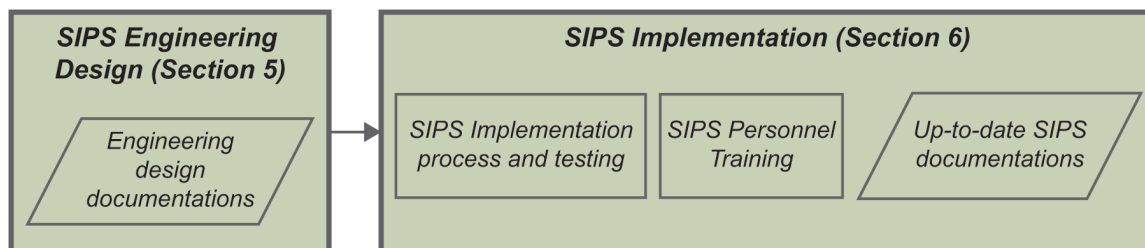


Figure 4—System Integrity Protection Scheme implementation

Figure 4 shows the main activities of the SIPS implementation stage. It takes the outputs of the SIPS engineering design stage and generates the final implemented SIPS documentation as the outputs that will be used in the SIPS management stage.

Implementing a SIPS generally involves the programming and configuration of the processing unit(s), which may involve the development of some software programs. If the entire SIPS is supplied by a contracted supplier, typically a factory acceptance test (FAT) will need to be performed before field installation. When a SIPS is implemented by a utility itself, laboratory tests for the SIPS that correspond to a FAT may also be conducted before the field installation. In either case, it is preferable to perform FAT or laboratory tests using a real-time simulation platform that has the facility to run PHIL-type tests (Power Hardware in the Loop) or other tests that simulate the critical contingencies off line that the SIPS is intended to mitigate.

Once the field installation is completed, a site acceptance test (SAT) or system acceptance test will be performed. The SIPS may go through a trial-run period after it has passed all SAT tests. Adjustments and corrections can be made during this period if any issues are identified.

Before the SIPS is commissioned, proper training for end users including those who will provide the support to the SIPS should be performed.

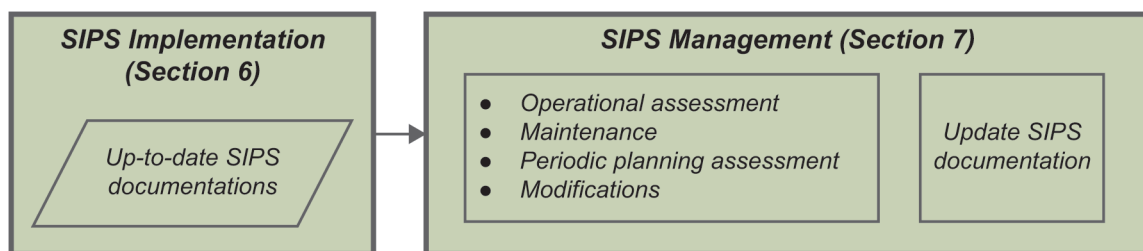


Figure 5—System Integrity Protection Scheme management

Figure 5 shows the main activities of the SIPS management stage. It uses the final documentation of the SIPS implementation stage, and updates the documentation when any changes need to be made. Typical documentation for the SIPS may include an overall scheme description, main requirements of scheme, logic diagrams, and setting and scheme test results. SIPS management involves several aspects governed by the overall management philosophy:

- Operation management: manage SIPS operations
- Change and maintenance management: manage changes in hardware and software and the periodic maintenance and testing of the SIPS
- In-service operational assessment: perform power system operation condition analysis to help ensure SIPS operation is adequate under various scheduled/unscheduled outage conditions, as well as whether the SIPS is performing as expected
- Periodic planning assessment: periodically check to see if changes in the power system warrant modification or retirement of the SIPS
- Special procedures, such as reinstatement of the SIPS operation after a contingency

4.5 General System Integrity Protection Scheme classifications

A single SIPS can be classified in several ways, in part, based on the actions listed in 4.3. For example, a SIPS may initiate both generator rejection and load shedding to balance the demand and supply in different areas affected by a major disturbance. There are additional ways to classify SIPS, several of which are described as follows. These classifications may include, but are not limited to the following:

- The contingency level for which mitigation is designed, for example, single, double, or other multiple contingencies related to line, transformer, generator, or other equipment outages.

- The type of problem the SIPS mitigates, for example, transient instability, thermal overload, transient or postevent voltage control, and so on.
- The geographic scale of the event that the SIPS is intended to mitigate, for example, “local” versus “wide area.”
- The electrical scale of the event that the SIPS is intended to mitigate, for example, the level of load or generation affected or at risk.
- Event-based versus condition-based SIPS operation, for example, taking action upon an unscheduled equipment outage event versus reacting to an overload condition.
- The type of action taken by the SIPS, for example, load shedding, generation rejection, and voltage control.

4.5.1 System conditions typically mitigated by System Integrity Protection Scheme actions

This subclause describes common abnormal power system conditions that are often intended to be mitigated by control actions of SIPS and control methods used to mitigate such phenomena.

Power system stability is the ability of an electric power system, for a given initial operating condition, to regain a state of operating equilibrium after being subjected to a physical disturbance, with most system variables bounded so that practically the entire system remains intact (Kundur, et al. [B25]). This general description covers essentially all power system conditions that result in stable operation. Conversely, the following individual phenomena are described as various causes of power system instability (rotor angle and voltage instability descriptions are adapted from Kundar, et al. [B25]):

- a) *Rotor angle instability* refers to the loss of ability of synchronous machines of an interconnected power system to remain in synchronism after being subjected to a disturbance:
 - 1) *Small-disturbance (or small-signal) rotor angle instability* is concerned with the inability of the power system to maintain synchronism under small disturbances.
 - 2) *Large-disturbance rotor angle instability or transient instability*, as it is commonly referred to, is the inability of the power system to maintain synchronism when subjected to a disturbance, such as a short circuit on a transmission line.
- b) *Frequency instability* (overfrequency or underfrequency) is the movement of the system frequency outside of predefined limits that specify the maximum allowable magnitude and time duration of frequency excursions. Such instability is caused by a significant unresolved imbalance between supply and demand of the active power in the system.
- c) *Voltage instability* refers to the loss of the ability of a power system to maintain steady voltages at all buses in the system after being subjected to a disturbance from a given initial operating condition. Power system voltage deviations from normal may be caused by power system faults, sudden increase in power demand, and so on.
 - 1) *Small-disturbance voltage instability* refers to the system’s inability to maintain steady voltages when subjected to small perturbations such as incremental changes in system load.
 - 2) *Large-disturbance voltage instability* refers to the system’s inability to maintain steady voltages after large disturbances such as system faults, loss of generation, or circuit contingencies.
- d) *Abnormal voltages* may include overvoltage, undervoltage, or voltage deviation (change from pre-event to post-event). These conditions are typically caused by loss of major equipment due to faults or other switching events.
- e) *Overloads* occur when the current flowing through power system facilities exceeds the rated capacity. This can be caused by power flowing through healthy facilities after the sudden unavailability of other power system facilities such as transmission lines and transformers that are isolated due to a fault.

f) *Cascading* is the uncontrolled successive loss of power system facilities triggered by an incident at any location. Cascading results in widespread electric service interruption that cannot be restrained from sequentially spreading beyond an area predetermined by studies (see “Glossary of Terms” by NERC [B29]).

This classification of unacceptable system conditions, also known as “abnormal phenomena,” is shown in Figure 6.

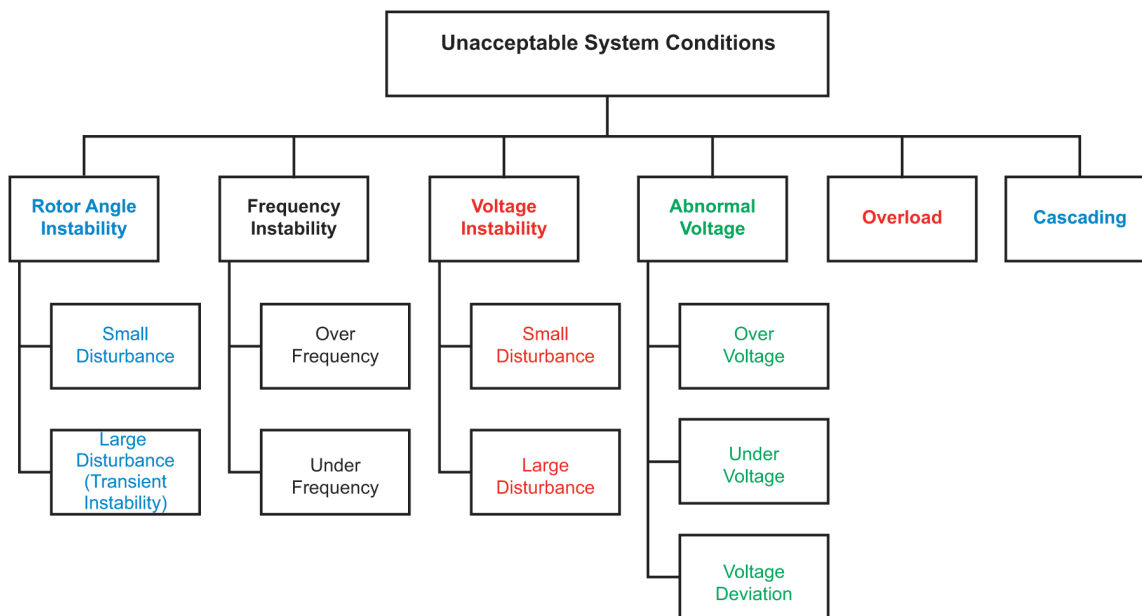


Figure 6—Unacceptable system conditions commonly mitigated by the System Integrity Protection Scheme

The relationship between the time frame when SIPS controls typically are expected to act and the system impact or range of influence of particular system conditions are illustrated in Figure 7.