Electrical Power and Energy Systems 68 (2015) 15–25

Contents lists available at ScienceDirect

Electrical Power and Energy Systems

journal homepage: www.elsevier.com/locate/ijepes

Design of dependable and secure system integrity protection schemes

Mathaios Panteli [a,*], Peter A. Crossley [a], John Fitch [b]

[a] School of Electrical and Electronic Engineering, Electrical Energy and Power Systems Group, The University of Manchester, Oxford Road, Manchester M13 9PL, UK
[b] National Grid, Warwick Technology Park, Gallows Hill, Warwick CV43 6DA, UK

ARTICLE INFO

Article history:
Received 6 October 2014
Received in revised form 10 December 2014
Accepted 10 December 2014
Available online 29 December 2014

Keywords:
Dependability
Fault tree analysis
Reliability
Security
System integrity protection schemes

ABSTRACT

System Integrity Protection Schemes (SIPS) are traditionally designed with an emphasis on dependability. This ensures they operate when required to preserve system integrity and as a result, most SIPS are implemented as fully duplicated schemes. However, as the complexity and uncertainty of power systems increase, enhancing the security of SIPS becomes vitally important. This prevents spurious operations, which have a detrimental impact on system reliability. A procedure for designing SIPS that achieve an effective tradeoff between dependability and security is proposed in this paper. The proposed method uses fault tree analysis and the theory of minimal cut sets to break down the reliability analysis of the complete SIPS into the analysis of the individual operational phases of SIPS, which simplifies the analysis. Then, this study determines the minimum reliability requirements of each component, i.e. Mean Time To Failure (MTTF) and Mean Time To Fail Spurious ($\text{MTTF}^{\text{spurious}}$) and the optimum design of SIPS for realizing the desired level of dependability and security. It is illustrated using the Dinorwig Intertrip Scheme, which is located in North Wales and operated by National Grid (Great Britain transmission system operator).

Introduction

An increasing number of electrical utilities are using System Integrity Protection Schemes (SIPS) to minimize the risk of blackouts and to cope with the growing size, complexity and stress of modern power systems. SIPS are defined as the protection systems designed to detect predetermined conditions that have a high probability of causing unusual or excessive stress on the power system, and for which pre-planned remedial action is necessary to protect the integrity of the power system [1].

SIPS have been traditionally designed with a bias towards dependability, i.e. to ensure they operate when required. This resulted in fully duplicated and highly dependable schemes, when considered in terms of measuring equipment, communications, controllers and mitigation strategies. However, as power systems grow, they become increasingly complex and uncertain and a spurious operation of a SIPS can have a catastrophic impact on power systems reliability. This is evidenced by the island of Ireland disturbance of 2005, where an incorrect operation of a SIPS triggered a chain of events leading to the disconnection of numerous customers [2]. Therefore, the design approach necessary for future SIPS needs to ensure a balance between dependability and security.

The importance of SIPS reliability in maintaining the reliability of the entire power infrastructure was recognized by the IEEE Power System Relaying Committee (PSRC), which published a report on a SIPS-related survey in 2010 [3]. The aim of this survey was to provide guidelines for designing and operating SIPS in a reliable way. The reliability assessment of SIPS has also attracted the interest of several researchers, which resulted in the development of numerous reliability assessment techniques. McCalley and Weihui [4] discuss the importance in developing a comprehensive reliability assessment framework for SIPS and they present the methods that can be used for this purpose, including Markov modelling and fault tree analysis. In [5], the limitations, risks and management of SIPS are discussed, along with a SIPS-related risk assessment approach. A generic approach for assessing the risk introduced by SIPS is also presented in [6] using Markov modelling and failure mode and effect analysis. Tsun-Yu and Chan-Nan in [7] apply and compare the effectiveness and accuracy of the methods discussed in [4]. The same authors propose a risk informed design refinement of SIPS in [8], which uses fault tree analysis and it is applied on a local event-based SIPS operated by Taiwan Power Company. The above methodologies provide an effective and systematic way of estimating the probability of the SIPS failure modes and the risk introduced to the system by such undesirable events. This is critically important as it helps identify the key vulnerabilities of SIPS and it also helps enhance SIPS reliability, which contributes significantly to the reliability of a power system.

[*] Corresponding author. Tel.: +44 1613068721.
E-mail addresses: mathaios.panteli@manchester.ac.uk (M. Panteli), peter.crossley@manchester.ac.uk (P.A. Crossley), john.fitch@nationalgrid.com (J. Fitch).

http://dx.doi.org/10.1016/j.ijepes.2014.12.047
0142-0615/© 2014 Elsevier Ltd. All rights reserved.

A significant limitation of these methodologies (including previous work by the authors [9]) is that the reliability data of the SIPS components, i.e. Mean Time To Failure (or failure rate), are assumed for carrying out the reliability evaluation. This is mainly because of the difficulty in obtaining real data, which is a big challenge in such studies. The main reason behind this is that these data are not made publicly available by the SIPS manufacturers. However, even if the data were provided by the manufacturers, they would have to be calibrated based on actual experiences during their operational cycle using the historical database of the utility. Nevertheless, the frequency of SIPS components' misoperations is so low that it might not allow the accurate estimation of the components' reliability data that would reflect their real behaviour.

Even though assuming the reliability data simplifies the reliability analysis, it increases the uncertainty which affects the accuracy of the output results and leads to extensive sensitivity studies. Motivated by this limitation of the existing techniques, the methodology presented in this paper aims to deal with these challenges by estimating the required reliability of the individual components, i.e. Mean Time To Failure (MTTF) and Mean Time To Fail Spurious ($\text{MTTF}^{\text{spurious}}$), necessary to achieve the desired dependability and security respectively. The desired dependability and security levels are determined here using Safety Integrity Level (SIL) and Spurious Trip Level (STL), which express the dependability and security as a function of the scheme's Probability of Failure on Demand (PFD) and to Fail Safe (PFS) respectively. Therefore, if the desired PFD and PFS are known, then the components' reliability data can be accurately calculated for achieving the predetermined SIL and STL levels. Differently from existing methodologies, no assumptions are thus made regarding the reliability data used, which increases the confidence in the procedure. Since the components' reliability data are quantified using the systematic approach presented in this paper, they can then be used by the electrical utility to decide on the most suitable components for realizing the scheme and for improving the accuracy of the SIPS-related reliability assessment procedures.

An additional significant challenge in such studies is the incorporation of all the possible individual component failure modes in the reliability analysis, and the assessment of their impact on the overall scheme reliability. This is mainly because of the complexity and the number of elements involved in the logic operation of SIPS. In this paper, the reliability analysis of SIPS is broken down into the reliability analysis of each individual SIPS operational phase; arming, activation and actions implementation. Next, the expected overall reliability of the scheme is distributed to the operational phases and then to the individual SIPS components using fault tree analysis and the theory of minimal cut sets (MCS). This helps quantify the reliability required for each SIPS components necessary to fulfil the overall SIPS reliability requirements.

The aim of the proposed procedure is to determine the optimum scheme design and the minimum reliability requirements for each of the SIPS components necessary for developing a scheme that is highly dependable and secure. The paper is structured as follows. The methodology is presented in Section 'description of proposed methodology' and illustrated in Section 'method numerical illustration using Dinorwig Intertrip scheme, UK' using the Dinorwig Intertrip Scheme, which is located in North Wales, UK, and operated by National Grid. Section 'reliability comparison of different scheme designs' provides a reliability comparison of different architectures applied in this reliability analysis. Section 'discussion' discusses the cost of implementing these architectures and the requirements for designing a dependable and secure Dinorwig Intertrip scheme. Section 'conclusions' concludes the paper.

Description of proposed methodology

According to the Western Electricity Coordinating Council (WECC) standard PRC-004-WECC-1 [10] and to a review conducted in [9], the main failure modes of SIPS are:

A. *Failure on demand*, which reflects the dependability of the scheme and refers to its failure to operate when required. It is expressed using the Probability of Failure on Demand (PFD).

B. *Fail Safe*, which reflects the security of the scheme and refers to an operation of the scheme when there is no relevant disturbance in the system. It is expressed using the Probability to Fail Safe (PFS). Other names often used for safe failure include nuisance failure and spurious failure [11].

The proposed procedure, depicted in Fig. 1, aims to optimize the dependability and security of SIPS by determining the following:

- the reliability requirements of SIPS components: dependability – MTTF, and security – $\text{MTTF}^{\text{spurious}}$ [12], which is also the aim of safety integrity evaluation techniques used in the process control industry [11],
- the optimal scheme design and components to be used in the scheme implementation based on the desired reliability requirements.

Fig. 1 shows that it is composed of the following steps:

A. Scheme specification and logic design

Extensive reliability and risk studies of the network determine the weak areas for which the installation of SIPS is considered necessary. Next, the purpose and intended function of the scheme have to be determined. Finally, the logic of the scheme has to be defined since this determines the events and conditions for which the SIPS will and will not operate. For example, if (X AND Y) is true,

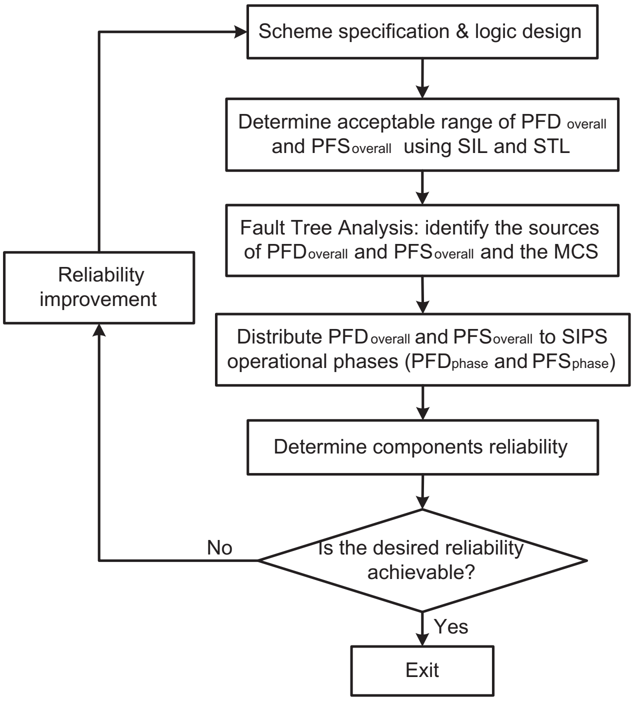
Scheme specification & logic design
Determine acceptable range of PFD overall and PFSoverall using SIL and STL
Fault Tree Analysis: identify the sources of PFDoverall and PFSoverall and the MCS
Distribute PFDoverall and PFSoverall to SIPS operational phases (PFDphase and PFSphase)
Determine components reliability
Is the desired reliability achievable?
No
Yes
Exit
Reliability improvement

Fig. 1. Flowchart of the proposed methodology.