TESTING RELIABILITY PERFORMANCE OF IEC61850-BASED DIGITAL SUBSTATIONS

Rick Loenders[1], Dirk Van Hertem[1], Jef Beerten[1], Geraint Chaffey[1]and Li Yang[1]*

[1]Dep. of electrical energy and computer architectures, KU Leuven and EnergyVille, Thor Park 8310, Genk, Belgium
**rick.loenders@kuleuven.be*

Keywords: DIGITAL SUBSTATION, RELIABILITY, IEC 61850, PROTECTION

Abstract

In modern power systems, communication between multiple Intelligent Electronic Devices (IEDs) has opened up a number of new applications to protection, automation and control of substations. Many system operators are concerned about the reliability of this digital transition, specifically the complexity and the reliability of the protection in these digital substations. The IEC 61850 standard is the likely communication protocol for these substations; however, it still faces some issues regarding interoperability and reliability. Therefore, it is valuable to examine the reliability of the information exchange between IEDs, particularly fault triggered events transported through GOOSE-messages and analogue data sampling through Sample Values (SV). One important task within a reliability assessment is to evaluate the consequences of selected failure modes. This paper presents different failure cases in the overall communication network and proposes a practical evaluation of an IEC61850-based protection scheme under a selected failure condition. The paper reviews reliability requirements for a digital substation with regards to the operation speed and dependability. Tests are performed in a real-time simulation environment to which IEDs are physically interfaced. Performance data is statistically analysed to produce likelihood curves of the operation time to evaluate the reliability of the protection scheme.

1 Introduction

There is no standard definition of a digital substation, based on [1] a digital substation is defined as; "a substation that is heavily reliant on an automation system, using a digital communication bus to exchange data between multiple Intelligent Electronic Devices (IEDs), such as bay controllers or protection relays to perform its main functions". Digital substations provide many benefits over their traditional counterpart, as high-speed communication has paved the way for a fully automated system that can improve system operation. The availability of high-bandwidth communication has made it possible to transmit large quantities of data over a single fibre or Ethernet-cable, reducing the amount of wiring in a substation and allowing for real-time monitoring of the system. Despite the benefits, utilities remain hesitant to adapt to the idea of a full digital substation. The survey in [1] evaluates the reasons for the slow digital transition. Overall, many concerns still exist about the complexity and dependability of the protection devices in a digital substation. However, it is often stated that digital substations are more reliable. Since, dependability of protection is considered the most important function for utilities; this statement is often seen through the potential availability (A) increase of the system given by equation (1) [2]. The reasons for this apparent increase in availability are due to the inherent substation communication, which provides better observability and added functionality to automatically supervise, alarm and potentially self-heal failures. This can remarkably reduce the Mean Time To Repair (MTTR). Additionally, remote automatic testing as in [3] and [4], permits troubleshooting without a primary system outage. Intelligent systems are able to analyse more data and provide recommendations for maintenance and repair actions, enabling an increased Mean Time Between Failures (MTBF).

$$\mathrm{A} = \frac{\mathrm{MTBF}}{\mathrm{MTBF} + \mathrm{MTTR}} \tag{1}$$

Both arguments have the ability to increase the systems availability. However, these statements fail to mention the added failure probability due to additional electronic components, like switches, Merging Units (MU) etc. and their relative shorter lifetime. Additionally, the performance of multiple decentralized functions of IEDs might be affected by a failure on the communication bus, as delayed responsive actions of substation elements have a larger impact on total operation time of the protection system. This could potentially reduce the MTBF, reducing the systems availability. Out of scope of this paper is the influence of cyber security issues, which are a valid concern regarding the reliability of any communication network, jeopardizing grid operation in general. Standardized communication protocols improves the reliability and efficiency of data exchange between IEDs. Widely discussed is the IEC 61850, which is a prominent communication standard initially designed for substation automation, and later adapted for multiple smart grid applications. The standard provides comprehensive information models of each IED in the substation. Intended to improve the interoperability between devices, these models represent a virtual description of the devices and their relationship with other intelligent components in the substation. A full implementation of IEC 61850 in a digital substation for protection and automation indicates the use of

Authorized licensed use limited to: Electricity Generating Authority of Thailand. Downloaded on October 12,2021 at 04:14:53 UTC from IEEE Xplore. Restrictions apply.

both the station bus and the process bus, transmitting event-based signals through the GOOSE-messages and digitally converted analogue values through Sampled Values (SV). However, the standard IEC 61850 still faces some challenges regarding interoperability and its reliability.

It is therefore valuable to examine the reliability of digital substations and the methods by which the reliability is evaluated. Risk analysis is typically applied in the area of power systems, where often the first step is the evaluation of different failures. The paper first evaluates what constitutes as a failure in a digital substation by reviewing performance requirements set for transmission system protection and IEC 61850 communication. Next, different failure modes are examined and how they are implemented in a lab environment. A practical case is considered to illustrate the impact of different failures, and evaluated the consequences based on different performance tests. Based on the data the failure probability is plotted under a given failure mode.

2. Review of reliability performance requirements

2.1 Power system protection

The objective of the protection scheme is defined by its protective zone. This is an area of the power system established around a primary system component. In case of a system disturbance, it is the objective of the protection system to guarantee the safety to the direct environment, prevent hazardous situations by limiting damages to components within the protection zone and keep consequential effects perceived by grid users to a minimum. Therefore, any protection system should meet two main requirements [6]:

- Dependability: is the probability of the protection of not having a failure to operate under given conditions for a given time interval [5]. It is the measure for certainty of reaction and is the ability of the protection system to operate during a power system fault for which it is intended to operate
- Security: is the probability of the protection of not having an unwanted operation for a given time interval [5]. It is the measure for certainty of not overreacting and is the ability for the protection not to operate when it is not required

Reliability is both comprised of dependability and security requirements. A dependability issue may result in delayed fault clearing and could lead to back-up tripping, leading to undesirable loss of load or generation. A security issue always results in tripping unfaulted elements, but does not normally result in delayed fault clearing. There is generally a trade-off between dependability and security. Improving one typically degrades the other. In the misoperations report of NERC [7] it is stated that (94%) of recorded failures resulted in a false trip, concerning the security of protection. A power system fault generates high fault currents with potential destructive power. Among other effects, power plants close to short circuits may lose synchronism with the grid. It is therefore important to clear any faults as fast as possible within the transmission grid. Failure of a protection system to operate may have significant consequences related to equipment damage and power system performance. Even if dependability failure modes are less frequent, they represent more severe consequences over security failures. Therefore, protection systems are mainly designed for dependability, as any failure in the system could potentially lead to a failure to trip. Power system requirements are likely to be specified for digital substations in much the same manner as for conventional systems. Rather the assumption that digital substations perform at par or better in terms of performance than traditional wired substations is not generally accepted by end-users [9]. The impact of a failure mode in a digital substation can be associated with the following consequences [8]:

- Failure to trip
- Delayed trip
- Failure of back-up trip
- Delayed back-up trip
- Unnecessary trip due to failure

A failure mode in a protection scheme thus regards any defect or deviation resulting in the incapability to perform the intended protection function. Not all IED failures manifest in an undesired trip actions. The loss of some automation system functions may have marginal impact and do not affect the protection systems reliability. The first step in dealing with the reliability of the substation is to define the dependability and performance requirements by function. The primary protection function is expected to have priority in initiating the fault clearance actions. Protection designs generally provide for a contingency loss of a primary protective function by use of a secondary protective function that will adequately cover for the loss. This includes the operation of backup protection for fault clearing. The objective of each utility is to operate its power system with the necessary primary and back-up protection in order to automatically prevent the propagation of disturbances that could endanger the operational security of its own power system and that of any interconnected system. Any fault should be cleared within the Critical Fault Clearance Time (CFCT), this time is defined as “the longest duration to which a fault does not lead to any generator to lose synchronism with the system or any other inadmissible repercussion for the system” [6]. The performance of the protection system is compared with CFCT-calculations for three-phase faults on any point of the network in order to ensure sufficient security margins and to adapt actions if necessary. The performance is measured based on the total fault clearing time, which consists out of the sum of all delays that are part of the protection scheme to trip the circuit breaker. Within the standard IEC60834-1 [10] the total operation time ($t_{operation}$) is referenced as the sum of fault recognition (t_a), relay decision (t_b), relay-output (t_c) and circuit-breaker operation (t_d). For a digital substation, the total fault clearing time could also be concluded after the processing HMI indicates an alarm due to the state change of the breaker.

Authorized licensed use limited to: Electricity Generating Authority of Thailand. Downloaded on October 12,2021 at 04:14:53 UTC from IEEE Xplore. Restrictions apply.

2.2 Communication bus - IEC 61850

The flexibility offered by the communication bus gives the system designer a wider allocation of functions. The smallest entity that can exchange data in a digital substation that utilizes IEC 61850 is a Logical Nodes (LN), which represents a virtual description of the device functions. In the standard, these LNs are grouped by the provided services, divided under 19 different LN groups in [15]. Performance requirements of the data exchange between these nodes are defined under the standard in terms of the transfer time [13]. The transfer time is described as "the complete transmission of a message including necessary handling at both ends. The time counts from the moment the sending IED puts the data content on top of its transmission stack till the moment the receiving IED extracts the data from its transmission stack". This means that communication system delay is not only dependent on the local and the remote IED but also on the processing times of active components in the communication path, such as routers and switches. These components contribute a significant amount of delay to the network transfer time. Therefore functional performance is limited by the availability and latency imposed by the applied communication network and its configuration. Two mission critical networks are identified: the Ethernet-based substation LAN and the Time synchronisation network. Both of these networks must be operational at all times, and are often not segregated, which might make them prone to common failures.

Critical functionalities in smart grid, like protection require very high levels of reliability with an availability level greater than 99,99% [21], which cannot be obtained if the underlying communication infrastructure does not support very reliable communications. Within IEC 61850 transferred data is classified into different types and performance classes depending on their application. The most demanding messages with the shortest transmission time requirements are set for tripping, blocking and sampling [13], classified in the standard as type 1A, 1B and 4 respectfully. These message types are further sorted into performance classes. The performance classes P1 and P7 define total transmission time to be smaller than a quarter of a cycle (3ms), while performance classes P2 and P3 dictate a transmission times in the order of half a cycle and a full cycle respectfully (10ms or 20ms). When messages with different performance classes are transmitted over the same network segment, that network segment must be designed and configured to meet the most sensitive performance requirements. It is always possible for the user to specify different performance classes than those given in the standard. Alternate reference can be taken from IEC 61850-90-4 [19] or IEEE 2030 [20], which specify performance tiers to better satisfy network design, but lacks the necessary classification in terms of protection and automation. Other requirements for SV are considered under IEC 61869-9 [22] concerning digital interfaces for instrument transformers. Here, the total processing delay of a MU for a protection application should not exceed 2ms. Additional requirements are expected under IEC 61869-13 regarding stand-alone MU.

A full implementation of IEC 61850 in a digital substation for protection and automation indicates the use of both event-based information through messages from Generic Object Orientated Substation Events (GOOSE) [16] and a digital converted stream of analogue values from instrument transformers are transmitted through Sampled Values (SV) [17]. Both message types utilizes multicast services, meaning that each message on the network reaches a pre-defined group of IEDs within approximately the same timeframe. The inherent design of these messages do not provide acknowledgement of reception. The sending IED normally does not observe lost messages. However, attributes of functional health, the age and number of messages are able to verify the quality of the data. The value of the data quality attributes are jointly published as quality bits, potentially blocking functional operation. If packets are lost, the previous value of the input is retained. As SV provide a steady data stream, the loss of a packet is simply replaced by the next. Therefore, the impact of delays and network failures on the time and quality of reception is equally distributed for SV. GOOSE-messages are event based, and to increase reliable reception they are suited with a so-called retransmission scheme. Messages are transmitted cyclic, but when a defined substation event occurs (e.g. the short-circuit detection) the transmission of a message is changed from a cyclic mode to a burst mode. Messages are send immediately after the defined event, and the time between messages increases exponentially till a maximum defined time interval is reached.

$$t_j = 2^{(i-1)} t_i \text{ with } i \epsilon [1, j_{t_{max}}] \quad (2)$$

Therefore, the impact of delays and network failures on GOOSE-messages will increase exponentially with the retransmission. Other elements such as the size of the message, type of data set elements, use of different constraints and attributes, number of subscribed messages and other communication on the network further impact the performance of GOOSE [17].

Previous requirements are specific to the performance of the substation automation system. Regarding reliability requirements reference is found in the standards IEC 60834-1 [10] and IEC 61850-90-1 [18], which define latency, dependability and security requirements for tele-protection functions, targeted to GOOSE-messages. Here, dependability and security requirements are defined based on the probability of missing a command (e.g. due to latency) or the probability of an unwanted command respectfully. The most stringent requirements are set for inter-trip signals. Here, a dependability requirement is the probability of countering a message delay greater than (>10ms) to be lower than 10^{-4}, while messages affecting security requirements should a probability of 10^{-8}.

Authorized licensed use limited to: Electricity Generating Authority of Thailand. Downloaded on October 12,2021 at 04:14:53 UTC from IEEE Xplore. Restrictions apply.

3 Practical lab testing

3.1 Lab environment

One technique to validate the performance of secondary substation equipment is by emulation in a test environment consisting of a real-time power system simulator. The primary system of the substation is simulated, while all secondary components of the substation automation under test are physically connected to the simulator. The IEDs are digitally interfaced with the communication bus and simulator through IEC 61850. Evaluation of consequences on complex systems requires the simulation of transient power system behaviour. Therefore, the use of real-time EMT simulations is of great importance for the understanding different failure modes of a protection scheme. A Real-Time Digital Simulator (RTDS) executes the EMT-simulations. Reasons for performing simulations of the failure modes are among others:

- To gather more information about the impacts of the failure modes.
- To evaluate causes and apply remedial actions
- To help in the development of backup sequences for different failure modes if needed

Additionally the simulation environment serves other purposes, such as pre-testing of IED functions prior to installing them in the field, troubleshooting of IEDs under different network configuration issues and the training of (new) engineers.

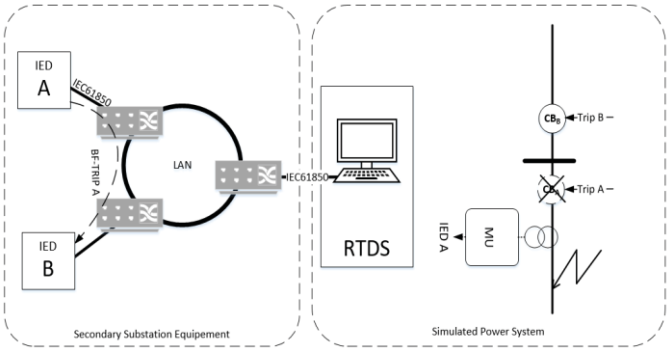

Fig. 1 Test set-up

Fig. 1 shows the simplified layout of the test environment. Failure modes are examined on a case protection scheme, which consists out of two IEDs (A and B) on a 380 kV substation bus configuration. Distance protection relaying is widely used for protection of transmission lines; therefore, both IEDs are equipped with a distance protection algorithm. Distance relays measure the ratio of voltage and current to determine the line impedance until the fault, in order to discriminate between internal and external faults. To obtain selective discrimination relay operation is limited to certain ranges of impedances or so called protection zones. If the measured impedance during a fault is lower than a predefined zone, the distance protection will send a trip signal to the associated circuit breaker. The operation of the breakers at the bus are supervised by both IEDs, as the measured current through the breaker determines if the primary trip signal failed to open the breaker or in case the current flow continues due to arcing. In either case, within a given time period the breaker failure function of the IED is activated. Afterwards, the IED issues a direct transfer trip to the remaining IEDs at the bus, in order to trip the transmission lines feeding the fault. Each IED is attained from a different vendor, allowing for investigation of interoperable systems. All IEDs are interfaced with the real-time simulator through a Gigabit-Transceiver Network interface card (GTNET) that exchanges digital messages through IEC 61850 GOOSE and SV. The real-time simulator thus performs the role of the breaker control and MU. Both IEDs are connected to a separate Ethernet-switch, configured in a ring bus with the simulator, which converges redundant data paths through the Rapid Spanning Tree Protocol (RSTP).

3.2 Proposed failure analysis

A failure is defined as "the inability to perform as required" [5]. In general, system failure can occur during one of several failure modes. The treatment of multiple failure modes requires modelling the behaviour of the entire system. Any failure can vary from a complete loss of the protection function, to a partial degradation of its expected performance. The failure probability or failure rate can thus be determined by analysing the physical process and uncertainty associated with a failure mode. Testing for reliability and the severity caused by the failure mode requires observing when the performance of a function associated with the (random) variable X is above or below a pre-defined value. Calculations require estimating the probability that X would surpass a critical defined threshold. This probability would represent the failure probability and the potential consequence during the failure mode.

In this paper, the considered critical threshold is the CFCT, associated with the variability of operation time of the protection scheme. The CFCT is dependent on the state of the power system, which includes; difference in network topology, generation availability and system load. The threshold for the European transmission grid is usually regarded to be less than 150ms. While the total action time initiated by a back-up function e.g. during a breaker failure is expected to be below 250ms [11]. Breaker operation time (t_d) generally varies between two to three cycles. This time is considered static, and after trip confirmation, a delay of 40ms is added. Additionally, the performance of any protection system ($t_a + t_b$) is dependent on the nature and features of the system disturbance (e.g. pre-fault system parameters, fault location and fault type). The test standard IEC 60255-121 [24] characterize the performance of distance protection IEDs under different grid parameters. While the standard requires adaptation for digital communication [12], characterized performance tests can set the prior probability distribution.

3.3 Failure modes

Testing of all conceivable failure modes is not feasible. A test concept includes a certain set of devices, configurations, and scenarios using well-defined dynamic cases. Categorizing

Authorized licensed use limited to: Electricity Generating Authority of Thailand. Downloaded on October 12,2021 at 04:14:53 UTC from IEEE Xplore. Restrictions apply.

different failure modes helps to evaluate different failure types and the likelihood of endangering the operation of the power system. Reported in NERC [8], almost 65% of all maloperations of protection systems are grouped under three main cause types: Incorrect device errors (e.g. settings, logic or design), relay failures and communication failures. Other failures are appointed to hidden failures and maloperations caused by human errors. For digital substations the impact of communication network related issues could be more severe. The work presented in [23] sums different type of failures in a digital substation and categorizes the failures based on:

- Failure on the Ethernet network
- Device failure
- Data communication failure
- Loss of synchronization
- Software failure
- Externally caused failures.

The basic assumption is that failure modes are independent from each other. While failure tests can evaluate the performance of redundant systems, failure of software and device are not addressed. Other hidden or external failures are hard to interpret and are not covered in the lab tests. A failure mode on the Ethernet network remains a likely cause for common failures, therefore this paper investigates both heavy network loads and packet losses for SV as a case study.

3.3.1 Heavy network load

The bandwidth of the substation automation network is the maximum transfer rate of data across a given path. For most applications, a 100Mbps process bus is sufficient. Regarding occupation, SV messages will take up a majority of the bandwidth. Generally, messages from a single SV stream consist out of 160 octets at 80 samples per cycle, which roughly occupies 5% of the total bandwidth. The two key factors that affect the remaining bandwidth are the size and publication rate of the GOOSE messages published by IEDs. To emulate the published background data, a network traffic generator can dump random data, or if available generate additional GOOSE or SV messages. Within IEC 61850-10 [17], simple performance tests are described. The standard describes a test where the performance of the IED is measured with 300 unsubscribed background messages per second. These unsubscribed messages contain 20 double points and 20 Booleans, including respective data quality values. It is specified that each second the data changes state every 10ms. Depending on the remaining frame size, the occupied bandwidth of 300 messages has a measured average of 327 bytes per second would cumulate to an additional 0,79Mbps. Means to increase the reserved bandwidth can be achieved by either changing the scheduled retransmission time (cfr. 2.2), or decrease the interval of state changes. Additionally the total data size can be increased, beware that maximum defined capacity of the Ethernet frame for GOOSE-message is 1522 bytes.

3.3.2 Packet loss - SV

A packet loss condition occurs when an SV message published by an MU does not reach the subscribing SV relay. This may occur because of congestion on the process bus network, a device failure in the system, or bad network cabling. A sample counter (SmpCnt) indicating the amount of samples taken within a one-second window is encoded in the SV message. Depending on the system frequency and publication rate (e.g. 50Hz and 80 samples/cycle), this sample counter increments from 0000 to 3999, and resets at the top of every second. The relay leverages the sample counter information published in the SV message to identify packet loss. For SV messages, packet loss on the network causes analogue data loss at the SV relay. Packet loss may also cause a reduced magnitude, which may prevent or delay protection actions. How many consecutive missing (or invalid) samples are tolerable, will deviate between IEDs and between different functions. The limit is crossed when either an invalid quality attribute (DO) is published or in case reduced voltage levels initiate the Loss-Of-Potential (LOP) logic, blocking protective functions during a few cycles or until the filter produces a stable signal. For protection cases subscribed to multiple SV-streams (e.g. in case of differential protection) the impact is more apparent when apparent delays causes a maximum relative time delay between differential streams. Nevertheless, any packet loss leads to a shift in processing time, also influencing the total trip time.

4 Results

For each failure mode, it is necessary to choose an appropriate probability distribution to represent the random variability of the operation time (T). The actual value of T is unknown and the likelihood of different possible outcomes P(T = t) should be therefore considered. Observations of the arrival time of both the primary trip (IED A) and the back-up trip from the remote IED B (cfr. 3.1), are modelled using a gamma distribution. Observations of each failure mode were repeated 200 times. The operation time was matched with the proposed failure analysis in (cfr. 3.2).

4.1 Heavy network load

The test ran several cases between 0 and 90 Mbps, measuring the operation time against the cumulative distribution, the tests showed that probability of failure was low below 50 Mbps. As more data occupied the bandwidth, the probability of failure increased exponentially. Based on the data, fug.2 shows a fitted exponential curve.

Authorized licensed use limited to: Electricity Generating Authority of Thailand. Downloaded on October 12,2021 at 04:14:53 UTC from IEEE Xplore. Restrictions apply.

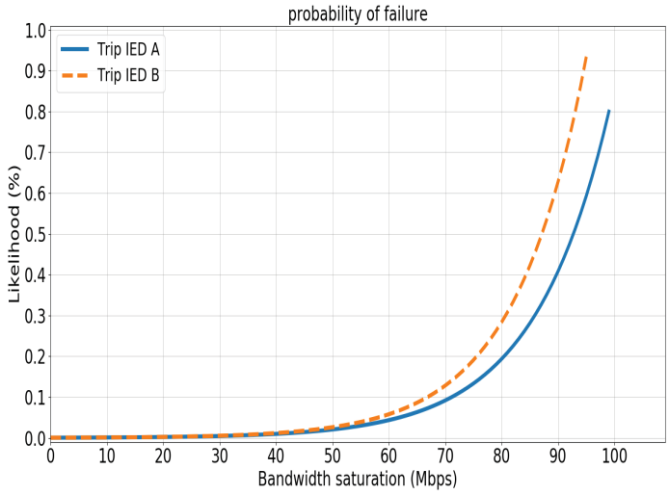

Fig. 2 Failure probability during heavy network loads

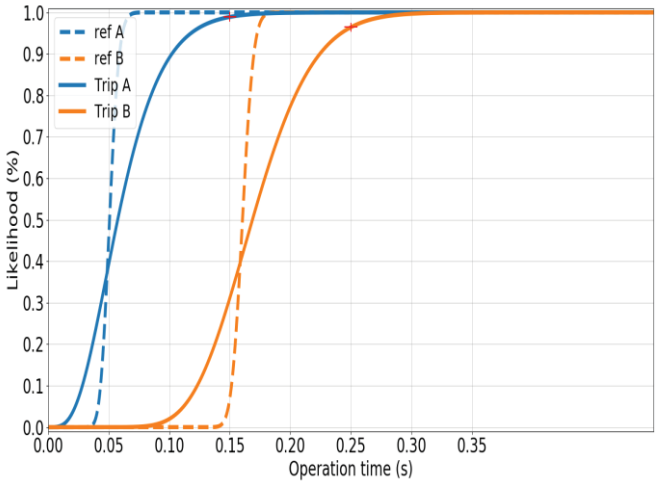

Fig. 3 Operation time under loss of SV-packets

Not confined in the data but observed during tests was an occasional premature reset from the breaker failure function due to consecutive loss of packets. Since the simulated short-circuit was persistent this was not recorded properly. However, premature resetting of protection functions can potentially cause erroneous system behaviour. To increase system reliability, is to prevent or minimize overloads. Unnecessary traffic should therefore be limited in the network. It is possible to segregate IEC 61850 data through the use of a Virtual LAN (VLAN) and provide the necessary priority tagging for time critical information (e.g. trip commands) to specific switch ports so relevant messages are forwarded first.

4.2 Packet loss - SV

The simulator is able to dynamically suppresses any published packet. SV data are deterministic on the process bus, and thus the loss of a packet would have no impact on the travel time considered under IEC 61850. Observations showed that the loss of one packet per cycle, either at a static point or at a random point on the waveform had no real observable impact. Multiple consecutive packets were not simulated as this caused an invalid data quality attribute, blocking the sampled cycle. However, this effect is not negligible as delayed readout of an entire cycle causes a maximum operation delay of 20ms. The worst case considered without affecting the quality is a cyclic suppression after each published message. This results in the loss of 2000 packets for an initial data stream of 4000 packets. A cumulative distribution curve (Fig.3) shows the reference ideal curve (dashed) when no packet is lost, against the stringent condition for both a trip received from IED A and IED B.

$$\mathrm{P}(\mathrm{T} < 0.15)_{\mathrm{A}} = 0.9891\% \quad (3)$$
$$\mathrm{P}(\mathrm{T} < 0.25)_{\mathrm{B}} = 0.9642\% \quad (5)$$

The result shows a larger deviation and decreased dependability, as tripping exceeds the threshold in a few cases. However, given a one-sided confidence interval of 5%, the mean operation time of during the failure mode is still within the confidence interval of the ideal reference. Therefore, a H_0-hypothesis that the mean of the failure mode is taken from the same sample than its ideal behaviour is not rejected.

4 Conclusion

In this paper a practical test method is described for evaluating the reliability of protection in a digital substation based on a review of performance requirements for protection systems and IEC 61850 communication. Reliability is tested during a given failure mode. As failure modes on the communication bus are likely to cause common failures, two practical cases of heavy network loads and loss of SV are tested. Given the know CFCT, one could assess the impact the failure mode on the total operation time. A cumulative gamma distribution measures the probability of failure against the pre-defined threshold as to rate the severity of the failure mode. It is shown that the impact for both cases under low stress-conditions are negligible. As presented for the case of heavy network data, the probability of failure increases exponentially with the increase of background data. As to fully test reliability requires to assess operation to other requirements set in IEC 61850. The set-up provides the ability to test other failure modes and mitigation actions.

5 Acknowledgements

The project has received research funding from VLAIO and support from Flux50

6 References

[1] CIGRE, ‘Experience concerning availability and reliability of digital substation automation systems’, 2017

Authorized licensed use limited to: Electricity Generating Authority of Thailand. Downloaded on October 12,2021 at 04:14:53 UTC from IEEE Xplore. Restrictions apply.

[2] IEEE 493: ‘IEEE recommended practice for the design of reliable industrial and commercial power systems’, 2007
[3] Schossig, T., Klien, A, and Steinhauser, F, ‘Methods for testing automation and control’, at DPSP, Belfast, UK, 2018
[4] Schossig, T., ‘Functional testing of substations according to IEC 61850 - a new approach’, Omicron, at DPSP, Birmingham, UK, 2014
[5] IEC 60050: ‘International electro-technical vocabulary’, Available: http://www.electropedia.org/
[6] ENTSO-E, ‘Best protection practices for HV and EHV AC-transmission systems of ENTSO-E electrical grids’, Ver. 2, 2018, Available: https://www.entsoe.eu/publications/system-operations-reports/
[7] NERC, ‘Misoperations report’, 2013
[8] NERC, ‘Analysis of system protection misoperations’, 2015
[9] Loenders, R., Van Hertem, D., and Beerten, J., ‘Control hardware in the loop for IEC 61850 GOOSE performance testing’, IEEE YRS, Brussel, 2018
[10] IEC 60834-1: ‘Teleprotection equipment of power systems - Performance and testing - Part 1: Command systems’, 1999
[11] ENTSO-E, ‘Determining generator fault clearing time for the synchronous zone of Continental Europe’, 2017
[12] Leitloff, V., Chen, H., Chen, D., Bonetti, A., Xu, L. and Mohamed, A., ‘Standardisation challenges for digital inputs and outputs of protection functions in IEC 60255 series’, 2019
[13] IEC 61850-5: 'Communication networks and systems for power utility automation – Part 5: Communication requirements for functions and device models’, 2013
[14] IEC 61850-7-3: ‘Communication networks and systems for power utility automation - Part 7-3: Basic communication structure - Common data classes’, 2010
[15] IEC 61850-7-4: ‘Communication networks and systems for power utility automation – Part 7-4: Basic communication structure - Compatible logical node classes and data object classes’, 2010
[16] IEC 61850-8-1: ‘Communication networks and systems for power utility automation – Part 8-1: Specific communication service mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3’, 2011
[17] IEC 61850-9-2: ‘Communication networks and systems for power utility automation – Part 9-2: Specific communication service mapping (SCSM) - Sampled values over ISO/IEC 8802-3’, 2011
[17] IEC 61850-10: ‘Communication networks and systems for power utility automation – Part 10: Conformance testing’, 2012
[18] IEC 61850-90-1: ‘Communication networks and systems for power utility automation – Part 90-1: Use of IEC 61850 for the communication between substations’, 2010
[19] IEC 61850-90-4: ‘Communication networks and systems for power utility automation – Part 90-4: Network engineering guidelines’, 2013
[20] IEEE 2030: ‘IEEE guide for smart grid interoperability of energy technology and information technology operation with the electric power system (EPS) end-use applications and loads’, 2011
[21] Takuro, S., Kammen, D. M., and Duan, B., et al., ‘Smart Grid Standards: Specifications, Requirements, and Technologies’ (Wiley), 2015
[22] IEC 61869-9: ‘Instrument transformers - Part 9: Digital interface for instrument transformers’, 2016
[23] Falahati, B., and Chua, C., ‘Failure modes in IEC 61850-enabled substation automation systems’, IEEE PES T&D, Dallas, USA, 2016
[24] IEC 60255-121: ‘Measuring relays and protection equipment - Part 121: Functional requirements for distance protection’, 2014

Authorized licensed use limited to: Electricity Generating Authority of Thailand. Downloaded on October 12,2021 at 04:14:53 UTC from IEEE Xplore. Restrictions apply.