Failure Modes in IEC 61850-Enabled Substation Automation Systems

Bamdad Falahati and Eric Chua
Schweitzer Engineering Laboratories, Inc.

This paper was presented at the 2016 IEEE PES Transmission and Distribution Conference and Exposition, Dallas, Texas, May 2–5, 2016, and can be accessed at: http://dx.doi.org/10.1109/TDC.2016.7520066.

Failure Modes in IEC 61850-Enabled Substation Automation Systems

Bamdad Falahati
Eric Chua
Engineering Services
Schweitzer Engineering Laboratories, Inc.
Pullman, WA, USA

***Abstract*—A substation automation system (SAS) is a digital communications network that facilitates control, protection, and monitoring. This new technology, however, has introduced a new set of failures that essentially differ from those of conventional control and protection systems. Because an SAS intrinsically follows the same rules as a communications network, the failure modes are similar. This paper studies the failures of SASs and proposes an all-inclusive categorization of failures that are likely to endanger the correct operation of a power system. Understanding different failure modes can contribute to the development of a model to evaluate the combined SAS and power network in a unique framework.**

***Index Terms*—Ethernet, Failure Mode, Substation Automation.**

I. Introduction

Modern substation automation systems (SASs) integrate advanced monitoring, protection, and control devices and operate as joint and multitask networks. IEC 61850, a novel standard for communication in substation automation, provides interoperability, reliability, and agility in a communications system [1]. In recent years, power equipment, such as circuit breakers, disconnecting switches (DSs), current transformers (CTs), and voltage transformers (VTs), have been equipped with digital transceivers, making the control and automation through the SAS more achievable [2].

The capabilities and power built into SAS designs are continually expanding. As more tasks are assigned to an SAS, system failures become more critical. Any failure in SAS operation can cause failures in the power network and can even disconnect power feeders in the substation [3].

Experience gathered during the development and operation of SASs over the years has proven that the performance of the associated communications systems plays an imperative role in the overall performance of the power system. In many cases, analysis of malfunctions involving protection and control systems points to failures in the communications network as the origin of the problem [4].

This paper introduces faults and failures of communications networks. The backbone of an IEC 61850-enabled SAS is an Ethernet network, so the focus of the paper is mostly on Ethernet faults and failures [5]. In addition, the faults and failures in three hierarchical layers of an SAS are discussed.

Network structure and data communications failures cover physical and logical integrity problems in network communication [6]. Software and operational failures are two newly introduced problems that do not have any equivalent in traditional hard-wired control, protection, and monitoring [7] [8] [9]. External faults are those that are not intrinsically related to a communications system but can lead to consecutive failures in an SAS [10].

II. Failures in Data Communications Networks

A. Failure in Ethernet Network

Two individual, independent Ethernet networks provide data communications among various levels of an SAS. Each interlevel network consists of connectors and switching devices.

Network connectivity problems occur for different reasons, such as a defective network interface card (NIC), faulty cable, inappropriate termination or splicing, or excessive cable length. This subsection discusses the physical faults and failures that can occur in the network structure.

1) Defective Network Interface Cards

The majority of problems that forestall data communication in an SAS occur at the lowest layer of the Open System Interconnection (OSI) model, the physical layer, which includes NICs, routers, and switches. Jabbering is a common network failure that usually results from faulty NICs. Although Ethernet networks establish themselves as reliable and fast networks, they are inherently vulnerable to jabbering [11]. Jabbering devices retransmit a packet that other devices do not understand, thus increasing network traffic and bringing the network to a halt.

2) Faulty Cables

If a cable (either copper or fiber-optic) between two nodes becomes disconnected or unplugged, a segment of the network is separated from the remaining part and loses its communications. The situation is better if the Ethernet network is equipped with a redundant path. In this case, only the network topology changes, and data communications systems must allocate another communications path. The Rapid Spanning Tree Protocol (RSTP) assigns an available path, if possible, based on the shortest path algorithm [5]. Fully redundant paths, which can be found in High-Availability Seamless Redundancy (HSR) protocol and Parallel Redundancy Protocol (PRP) topologies, are also

effective solutions to mitigate the risk of a single connection failure [4].

3) Inappropriate Physical Network Design

In an appropriate communications network design, many limits must be considered. Otherwise, the network performance will be considerably less than expected.

The Ethernet network detects collisions in the network using carrier sense multiple access with collision detection (CSMA/CD) technology. When the length of a segment or network exceeds the IEEE standard maximum, the probability of collision increases. Collisions inside the Ethernet network cause runts (packets smaller than the minimum packet size) and giants (packets exceeding the maximum packet size) to be produced. Choosing proper cable lengths for an SAS minimizes the risk of such failures. For example, IEEE limits the 100BASE-TX segment in the Ethernet network to 80 meters [12]. Adding an additional switch decreases the length of the cables, thus decreasing the collision risk. On the other hand, the additional device has its own failure rate and therefore deteriorates the system reliability correspondingly.

B. Operational Failures

Operational failures include misoperations caused by erroneous and inaccurate SAS engineering and design that lead to inadvertent operations in the power system. Incorrect logic engineering causes the power system to incorrectly prevent or authorize requested commands.

1) Incorrect Configuration and Settings

Each device has a dedicated piece of configuration software. Assorted parameters, known as configurations and settings, must be precisely set to enable the device to work properly. Any incorrect or missed value can cause the device not to function, or even worse, to malfunction.

A key difference between electromechanical relays and intelligent electronic devices (IEDs) is the notably greater amount of data that need to be transmitted for stipulating settings. Although developing basic setting specifications for IEDs, for the most part, is relatively straightforward, it is a tedious and time-consuming process that requires significant input data.

A good tracking system is necessary to ensure that proper settings are applied to the IEDs and to provide troubleshooting when problems occur [8].

2) Commissioning Issues

When commissioning IEDs, the same objectives exist as for electromechanical relays. Testing of interlocking, control, or protection logic in IEDs requires validation and verification that all block diagrams, controls, inputs/outputs, indications, and switches function as intended. Testing is an unavoidable part of commissioning to verify the correct operation of the IEDs. Because of the nature and capabilities of IEDs, however, the scope and techniques necessary for the associated tests are different than those required for electromechanical relays and hard-wired circuits. Uncertainty in the commissioning of IEDs is the most common issue during commissioning and testing [9].

C. Data Communications Failures

The connection of two points in a digital network does not necessarily ensure correct data delivery; various prerequisites must be met to preserve correct communication. Data communications failures are different than network structure failures in that no metric or troubleshooting tool exists to identify them. As a result, logical connectivity problems usually are more intricate and difficult to diagnose, segregate, and resolve than network structure problems. The following subsections describe a few data communications issues in SASs.

1) Protocol Incompatibility

The foremost issue in an SAS is the variety of protocols used to perform communications between IEDs. Although IEC 61850 increases the interoperability among devices from different manufacturers, many devices still communicate with protocols that are not compatible with IEDs from other manufacturers. The addition of protocol converters, although inevitable, compromises SAS reliability because of the additional failure rate. The most effective solution is to deploy multiprotocol switches to provide full interoperability among all devices. Figure 1 shows a simple architecture with a multiprotocol switch that maintains the network integrity without compromising the reliability.

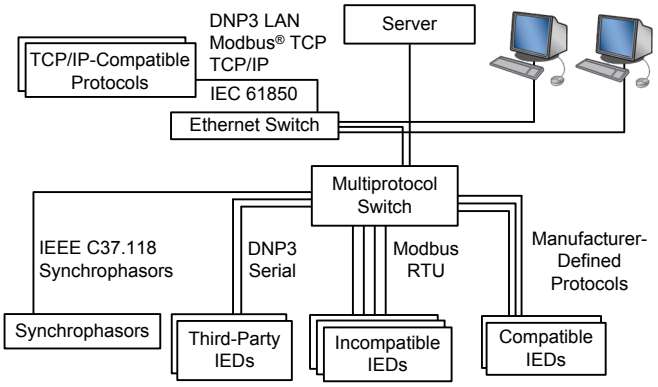

Figure 1. Multiprotocol Network Architecture to Resolve Protocol Incompatibilities

2) Upgrade and Compatibility Issues

Even if all of the configurations of two clients match, the two clients still may not receive identical responses when communicating with an individual node. Compatibility issues can occur because of upgrades in the hardware, software, or firmware of devices, such as IEDs, switches, or servers.

Firmware is supposed to remain unchanged for a long time, but upgrades are often issued by manufacturers to improve the operational features of the IEDs or to fix defects that have been revealed after release. Upgrading the firmware by itself is a time-consuming task that halts the operation of an SAS for several hours. More importantly, when the firmware of an IED is upgraded, there is a possibility that the IED will not be able to establish effective communications with existing IEDs [8].

3) Latency

As Figure 2 illustrates, two intrinsically different types of latency exist in the network. The first type is constant latency, which is related to inherent delays in nodes and connections. Constant latency depends on the physical structure of the network and the bandwidth, and it is calculable and predictable. The second type, variable latency, depends on the traffic and present loading of the network. Simultaneous communications among devices in a shared bandwidth or a failure inside the network significantly degrades the throughput and increases the variable latency [6] [12].

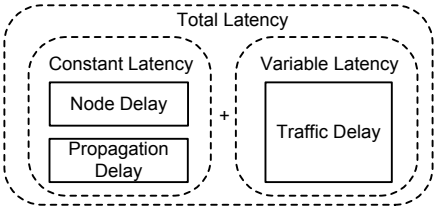

Figure 2. Components of Latency

Each task has acceptable latency limits. In time-critical tasks, such as power system protection, the protective devices must operate in a fast, reliable, and time-deterministic way; thus, latency is a crucial issue.

The latency of the network increases even more when a failure occurs in an intermediary device or connector. In such scenarios, the data must travel an alternate, nonoptimal path that can increase the hop count (number of intermediary devices). Moreover, some intermediary nodes need to transmit more packets to compensate for the out-of-service node, which causes more traffic delays [12].

D. Loss of Synchronization

In recent years, high-precision synchronization among devices has become a top priority. Synchronized recorded data from all substations are collected in a single device, known as a phasor data concentrator, for additional analysis. Also, IEC 61850 specifies that binary and Sampled Values gathered from the process level must be synchronized.

When the synchronization source is lost or malfunctions, the devices in an SAS are not synchronized with each other or with devices in other substations. In that case, the data are not valuable for wide-area monitoring and control. Figure 3 shows a data diagram of a synchronization system.

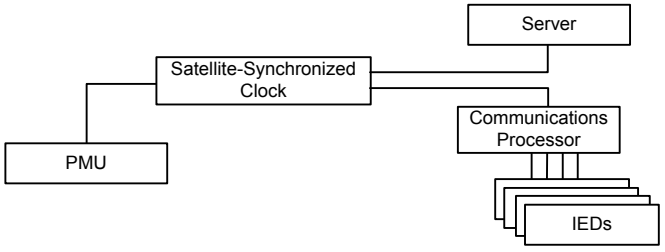

Figure 3. Synchronization Architecture

E. Software Failures

In modern relay technology and supervisory control and data acquisition (SCADA) control systems, software is an undeniable independent element with an intrinsic risk of failure that does not have an equivalent in a traditional hard-wired system. The following subsections describe the two most dominant types of software failure in SASs.

1) Code Faults

Each IED has a dedicated software tool to implement logic. Deep knowledge of programming procedures is necessary to effectively use the many features and the flexibility designed into modern IEDs. Programming tools available for IEDs include Boolean operators, control equation elements, binary elements, analog quantities, and math operators [8]. The probability of future failures is related to various factors, including but not limited to the number of variables, arguments (inputs and outputs), operation codes, operands, subroutines, and keywords. More complicated software designs lead to more expected failures. The sophistication of logic is doubled when latches and time-delay units are incorporated to build up protection and control logic [7] [9].

2) Database Failures

Each piece of software contains a database that is specifically designed to collect a massive amount of data. The size of the database increases gradually when new datasets are collected from the power system. These datasets need to be dumped in a safe, reliable, and spacious drive. Any unexpected disruption or data mismatch occurring in the database impacts the software operation directly. Moreover, crashes in the database structure cause a large amount of data to be lost, which is a disaster in the data storing task. From a cybersecurity viewpoint, connection to a database must be secure enough to avoid any unauthorized access (either read or write) [10].

F. External Failures

External failures are failures outside the scope of the SAS that impact the operation of digital devices and networks. In other words, all parts of the network are perfectly designed to cooperate with each other, but some special conditions can cause nontechnical failures.

1) Loss of Power

The most likely and crucial external failure is power loss. Power loss typically results from a failure in the distribution power system, a switchover among sources, or surges or intolerable voltages on the power supply. Even a momentary loss of power to any part of the data communications system resets and de-energizes devices and can cause the system to fail. The loss of power in IEDs is more destructive compared with electromechanical relays. Note that an IED, in addition to providing an array of protective functions, is capable of fulfilling most of the control and data acquisition requirements at substations [8]. The same discussion is valid for network switches; a power loss in a switch causes the disconnection of all connected IEDs.

A small-capacity external backup battery can keep the system running during a transitory power loss. Nevertheless, for longer power outages, a redundant power source, such as a battery station, is necessary. Providing a redundant battery

charger and inverter to equip key devices, such as servers and switches, with dual power supplies is also possible.

2) Aging and Environmental Conditions

Ambient conditions, such as temperature, can also cause environmental failures in an SAS. In large facilities, the loss of air conditioning can cause system components to overheat and can damage temperature-sensitive elements. The network performance may be degraded by severe ambient conditions as well.

Communications equipment, associated wiring, and connectors deteriorate over time, causing a gradual reduction of network performance. Likewise, dirt and dust are long-term threats to the reliability of electronic equipment. A build-up of dirt on electronic components puts components at risk by decreasing the effectiveness of the cooling system, allowing the components to overheat and, in extreme conditions, initiate a fire.

III. Failures in Hierarchical Levels of an SAS

Each SAS consists of three hierarchical levels, as shown in Figure 4. The station level encompasses devices at the station, SCADA center, or remote user. The main IEDs, such as bay control units (BCUs), bay protection units (BPUs), phasor measurement units (PMUs), and measuring centers (MCs), are located at the bay level. The process level connects the SAS and the power equipment.

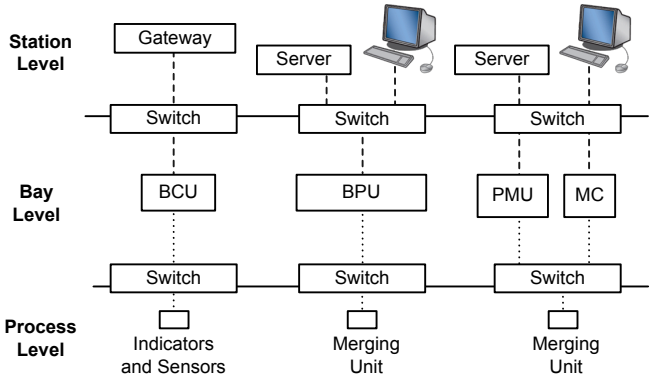

Figure 4. Three Distinct Levels in an SAS

A. Station-Level Failures

Station-level failures are failures that occur at the station level (e.g., SCADA center or remote access user) and are then transferred to the SAS. Station-level failures are challenging because their origin is hard to recognize.

Implementing redundant content sources, which consist of redundant human-machine interfaces (HMIs), servers, and gateways, in the SAS is the best practice to minimize the risk of station-level failures.

A server is the most important piece of station-level equipment. The loss of a server can cause permanent data loss in the SAS. All SAS schemes include redundant servers to maintain required reliability. Nevertheless, the failure of a server still causes data loss in the network until the backup server substitutes for the failed server.

If the main server stops responding, its workload must be transferred expeditiously and seamlessly to the standby server [10]. Mirroring is a method to provide hot standby redundancy between servers and involves the active server copying all of its contents to the redundant server. When one server fails, the standby server takes over in a few minutes [13]. Figure 5 shows a network with mirrored servers.

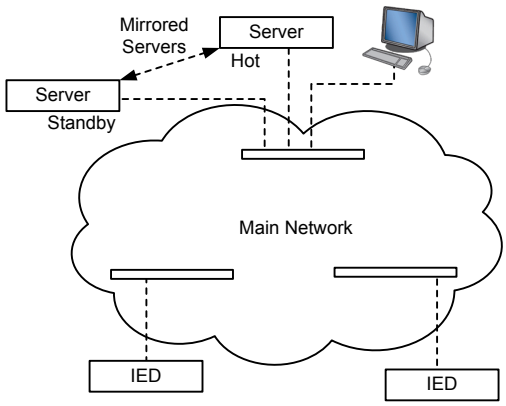

Figure 5. Server Mirroring Technique

B. Failures at the Bay Level

The bay level is the backbone of an SAS, and the corresponding IEDs are usually responsible for collecting data, running commands, and protecting and controlling the power network. Therefore, compared with the station and process levels, failures at this level impact the operation of the power network more severely. The failure of a protective relay, BCU, or MC is considered a bay-level failure. Failures of different components cause different effects and therefore entail different solutions. Failures at this level are divided into two categories, which are described in the following subsections.

1) Revealed Failures

IEDs collect data from the electrical switchgear and send them to the server. They also transfer the commands received from HMIs to the interface devices. The main concern with multifunctional IEDs is reliability. With complete protection and control contained within one IED, a single failure can cause all functions provided for a system facility to become disabled.

2) Hidden Failures

Hidden failures remain hidden during the normal operation of a power system, and they are exposed when failures occur. These failures cause the system to not operate when required and/or inadvertently operate when not required [14]. Protective relay failures are mostly hidden failures, which means that a failure in the power system occurs but the relay either cannot detect it or cannot respond to it. The concern is that failures can remain hidden and, even when revealed, can be hard to repair.

To avoid hidden failures, IEDs usually integrate self-testing and diagnostic and watchdog facilities to help with preventive failure detection [15].

C. Failures at the Process Level

The SAS and power networks are interconnected through the process level. The process level is the lowest level, and it connects directly to the power equipment. The proper control, protection, and monitoring of the power system strongly rely on the data collected at the process level from power equipment [2]. Similarly, digital data must be received by devices placed at the process level, and the system must operate in a timely manner [16]. Any failures in the process-level equipment units prevent the power networks and SAS from interacting properly. Redundancy is easy to achieve at the process level. The following subsections introduce some well-known process-level elements.

1) Merging Units

Merging units (MUs) gather multiple analog and binary inputs from switchgear equipment, such as CTs, VTs, and circuit breakers, through copper wiring. They then produce multiple time-synchronized serial unidirectional multidrop outputs, transmitting them to the process bus as data through the digital network [1].

In Figure 6, SCBR, TCTR, and TVTR are the IEC 61850 dedicated code for the status of breakers, the sample current of the CTs, and the sample voltage of the VTs, respectively. Any interruption in data transmission from the MUs to the BCUs and BPUs causes malfunctions in control (e.g., interlock logic) and protection (e.g., autoreclosing).

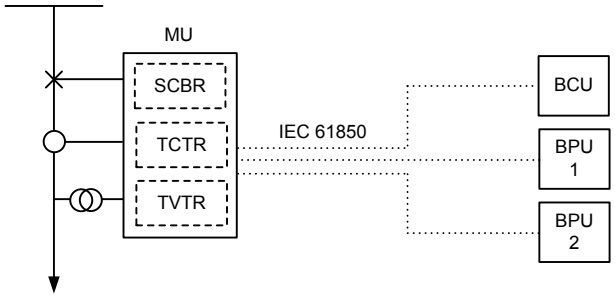

Figure 6. MU as an Interface Device

2) Sensors and Indicators

Sensors detect or measure physical properties in the power system and record, indicate, and report to the SAS. These devices are responsible for monitoring key power system equipment, such as transformers and breakers, to forecast any incipient failures. Sensor and indicator failures cause problems in system monitoring, which impacts the reliability of the power network indirectly [17].

IV. Conclusion

The categorization discussed in this paper empowers engineers to further develop a detailed model to assess the reliability of an SAS by considering all possible failures. Physical and logical failures can cause problems in data communications through the SAS. Software failure has emerged as a failure mode that is completely different than other existing modes and needs more study to develop corresponding numerical indices. The network structure, the main part of the network integration, enables data communications among the three hierarchical levels of an SAS: the station, bay, and process levels.

Understanding different failure modes can contribute to the development of an all-inclusive model to evaluate SASs and power networks in a unique framework. Fault tree analysis (FTA) can be studied to show how these failure modes affect the availability of different SASs.

References

[1] IEC 61850 Communication Networks and Systems in Substations. Available: http://www.iec.ch.

[2] C. Singh and A. Sprintson, "Reliability Assurance of Cyber-Physical Power Systems," proceedings of the 2010 IEEE Power and Energy Society General Meeting, Minneapolis, MN, July 2010.

[3] B. Falahati, Z. Darabi, Y. Fu, and M. Vakilian, "Quantitative Modeling and Analysis of Substation Automation Systems," proceedings of the 2012 IEEE PES Transmission and Distribution Conference and Exposition (T&D), Orlando, FL, May 2012.

[4] C. M. De Dominicis, P. Ferrari, A. Flammini, S. Rinaldi, and M. Quarantelli, "Integration of Existing IEC 61850-Based SAS Within New High-Availability Architectures," proceedings of the 2010 IEEE International Workshop on Applied Measurements For Power Systems (AMPS), Aachen, Germany, September 2010.

[5] M. P. Pozzuoli, "Ethernet in Substation Automation Applications – Issues and Requirements," July 2007. Available: http://www.energycentral.com/.

[6] B. Falahati, M. J. Mousavi, and M. Vakilian, "Latency Considerations in IEC 61850-Enabled Substation Automation Systems," proceedings of the 2011 IEEE Power and Energy Society General Meeting, San Diego, CA, July 2011.

[7] L. L. Pullum, *Software Fault Tolerance Techniques and Implementation*, Artech House, Norwood, MA, 2001.

[8] J. L. Blackburn and T. J. Domin, *Protective Relaying: Principles and Applications*, Fourth Edition, CRC Press, Boca Raton, FL, 2014.

[9] K. Zimmerman, "Commissioning of Protective Relay Systems," proceedings of the 61st Annual Conference for Protective Relay Engineers, College Station, TX, April 2008.

[10] T. Dean, *Network+ Guide to Networks*, Fourth Edition, Course Technology, 2005.

[11] A. L. de Carvalho Klingelfus and W. Godoy, Jr., "Mathematical Modeling, Performance Analysis and Simulation of Current Ethernet Computer Networks," proceedings of the 5th IEEE International Conference on High Speed Networks and Multimedia Communications, Jeju Island, South Korea, July 2002.

[12] B. Falahati, Z. Darabi, M. J. Mousavi, and Y. Fu, "Stochastic Latency Assessment in Substation Automation Systems," proceedings of the 2012 IEEE Power and Energy Society General Meeting, San Diego, CA, July 2012.

[13] J. M. Rhee, H. Pham, S. M. Kim, Y. M. Ko, and D. H. Lee. "Issues of Fail-Over Switching for Fault-Tolerant Ethernet Implementation," proceedings of the 2009 International Conference on New Trends in Information and Service Science, Beijing, China, June–July 2009.

[14] D. C. Elizondo, J. De La Ree, A. G. Phadke, and S. Horowitz, "Hidden Failures in Protection Systems and their Impact on Wide-Area Disturbances," proceedings of the 2001 IEEE Power Engineering Society Winter Meeting, Columbus, OH, January–February 2001.

[15] F. Yang, P. S. Meliopoulos, G. J. Cokkinides, and Q. Binh Dam. "Bulk Power System Reliability Assessment Considering Protection System Hidden Failures," proceedings of the 2007 iREP Symposium, Charleston, SC, August 2007.

[16] F. Katiraei, R. Iravani, N. Hatziargyriou, and A. Dimeas, "Microgrids Management," *IEEE Power and Energy Magazine*, Vol. 6, Issue 3, May–June 2008, pp. 54–65.

[17] B. Falahati and Y. Fu, "Reliability Assessment of Smart Grids Considering Indirect Cyber-Power Interdependencies," *IEEE Transactions on Smart Grid*, Vol. 5, Issue 4, July 2014, pp. 1677–1685.

Previously presented at the 2016 IEEE PES Transmission and Distribution Conference and Exposition, Dallas, TX, May 2016.