Test Case 23

Authors: Tesfaye Amare Zerihun
Steffen Vogel
Version 1
Project: ERIGrid 2.0
Date: 10/05/2020

Name of the Test Case	Verification of the reliability of a redundant system or algorithm (e.g. failover)
Narrative	The aim of this test case is to assess and verify the reliability of failover systems in smart grids that relies on putting redundancy. Redundancy is mainly used for critical smart grid applications such as protection in substations. In general, the redundancy can be either for control systems (such as the SCADA controller), communication networks or network controller (such as SDN controller), or a redundancy in the sensors and actuators (CT/PTs, Merging units, Breakers). Specifically, this test case looks into the reliability of failover systems with a redundancy in the communication networks. The ICT support system/communication network may fail due various reasons for e.g., component (hardware) failures, environmental failures (such as weather disruption failing multiple components), a power outage, overloading of the network (capacity shortage) or cyber-attack. A fail-over system tries to quickly detect failures and switch to backup systems (smooth transition in the case of active standby systems) or it tries to recover the system after experiencing some performance glitch (the case of passive standby system). Unlike active backup systems, in the case of passive redundant systems, there can be small system down time until the backup system is powered on and takeover. The test case investigates the reliability of active or passive fail over systems to verify if these systems can meet the requirements (delays, packet loss or system down time) specified by the smart grid application considered or requirements set by the standards and protocols such as IEC 61850.
Function(s) under Investigation (*FuI*) “the referenced specification of a function realized (operationalized) by the object under investigation”	• Exchange of data (measurement and control commands) through the communication network • Control functions on the local controllers / IEDs • Protection functions on the local controllers / IEDs
Object under Investigation (*OuI*) "the component(s) (1..n) that are to be qualified by the test”	Communication Network (network devices, switches, network links), control devices or IEDs
Domain under Investigation (*DuI*): “the relevant domains or sub-domains of test parameters and connectivity.”	• Information & Communication System • Control system • Power system
Purpose of Investigation *(PoI)* The test purpose in terms of Characterization, Verification, or Validation	• **PoI#1:** Characterization of the performance of failover systems with a varying degree of redundancy. - **PoI#1.1:** Characterization of the performance of

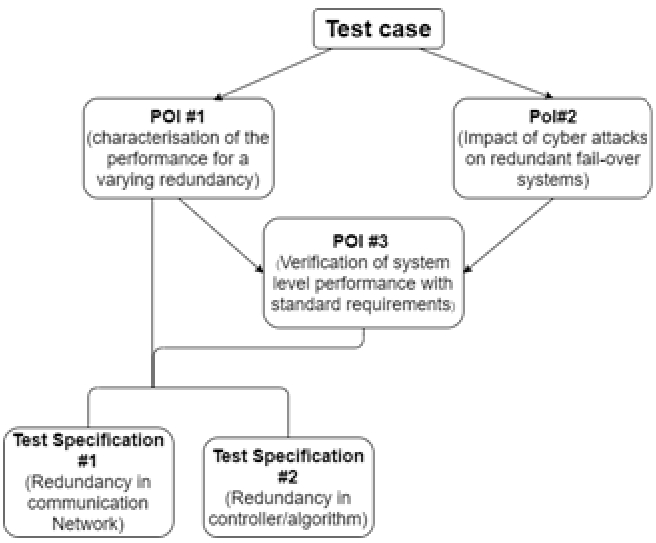
	fail-over systems with redundancy in the communication network. - **PoI#1.2:** Characterization of the performance of fail-over systems with redundancy in the controller/IED • **PoI#2:** Characterization of the redundant communication/control system for its vulnerability towards cyber attacks • **PoI#3:** Verification of the system level performance with standard requirements (if it complies with the minimum expected KPIs e.g., down time, packet loss or delay)
System under Test (*SuT*): Systems, subsystems, components included in the test case or test setup.	• Communication network (Switches, routers, network links) • Sensors (voltage sensors, CT/PT basic control), Actuators (breakers, intelligent switches) • SCADA Controller (for e.g., FLISR, voltage control, monitoring functions) or local controllers/IEDs • Power transmission system (substations, transmission lines)
Functions under Test (*FuT*) Functions relevant to the operation of the system under test, including FuI and relevant interactions btw. OuI and SuT.	• Capability of the communication network/ devices to facilitate data exchange between controllers/IEDs, sensors and actuators (breaker, disconnectors) • Control and Protection functions • Monitoring capability of sensors (devices such as Merging units, PMUs) • Actuator (breaker, disconnector) functions
<u>Test criteria</u> *(TCR)* Formulation of criteria for each PoI based on properties of SuT; encompasses properties of test signals and output measures.	• Run the system without introducing faults, and measure the communication network's performance during the normal operating condition… • Introduce a fault and measure the communication network performance degradation right after a failure/fault occur/injected. • Calculate and obtain the overall system performance (availability, reliability).

Target Metrics *(TM)*
Measures required to quantify each identified test criteria
	1. End to end delay, packet loss
	     During a normal operating condition
	     After introducing a fault
	2. Up time, down time, availability and reliability
	    • After introducing a fault

	Variability Attributes *(VA)* controllable or uncontrollable factors and the required variability; ref. to PoI.	• Redundancy type and degree (active-active, active-standby, active-inactive)
		• Number of simultaneous (component) failures
		• Communication network traffic situation (background traffic)
		• Communication topology
		• Failure type
		  ○ Cascading (from PS to CS)
		  ○ Hardware
		  ○ Software

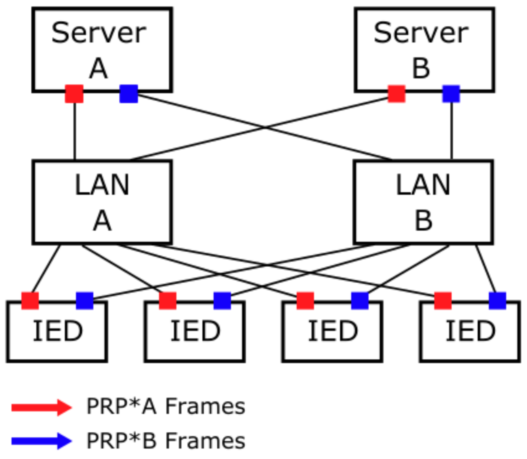
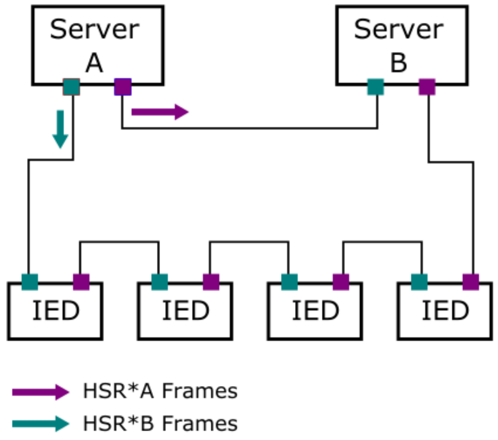
	Quality Attributes *(QA)* threshold levels for test result quality as well as pass/fail criteria.	**Pass:** End to end delay (average, maximum) and packet loss are within the maximum limit or threshold values set by specifications on standard communication protocol or the smart grid application (such as protection) considered. OR, the availability, reliability measures are within the limit on the specification requirement set by system administrator. • Packet loss > **T**, where T is a threshold value set according to the application (protection) type considered. • Packet delay larger than **D** ms, where **D** is the delay tolerance which depend on the application (protection) type considered. The delay tolerance varies from 1 ms (for bus bar protection), 4 to 8 ms (for other type of protection schemes) up to 800 ms for IED to SCADA communication. **Fail:** If the measured metrics (delay, packet loss, availability, or reliability) exceeds the threshold values.

Qualification Strategy



Test Specification TC23.1

Reference to Test Case	*TC23*
Title of Test	**Verification of the reliability of Substation Automation Systems (SASs) with *redundancy in the communication network***
Test Rationale	With the use of IEC 61850 standard, substations are nowadays becoming digitized and automated with digital relays/IEDs and a LAN based communication network for connecting these IEDs. Failure of the communication, even for the few milliseconds, may jeopardize critical functions such as protection and lead to catastrophic effects within or beyond the substation impacting the operation of grid. New redundant architectures, notably parallel redundancy protocol (PRP) and high High-Availability Seamless Redundancy (HSR) from IEC 62439-3, have been used to increase the reliability of IEC 61850 LAN based substation automation communication networks [1]. PRP provides high reliability through two independent LAN networks. The PRP enabled nodes are connected to these two isolated networks, which operate in parallel as shown below in Fig. 1 below. Frames are duplicated in the source and are sent over both networks; the destination PRP enabled node receives packets from the first network and accepts it, if it is correct, and then the copy from the second network will be discarded as duplicate. HSR operation is similar to PRP but HSR uses a single LAN with a ring topology and it uses two independent paths (clockwise and counterclockwise). Both architectures aim to provide an ideal "zero recovery time" with no packet loss. This test aims to investigate the reliability of these two recent redundant communication networks in substation automation. [1] International Electrotechnical Commission *IEC 62439-3:2016 Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)* [2] S. Kumar, N. Das and S. Islam, "High performance communication redundancy in a digital substation based on IEC 62439-3 with a station bus configuration," *2015 Australasian Universities Power Engineering Conference (AUPEC)*, 2015, pp. 1-5, doi: 10.1109/AUPEC.2015.7324838.
Specific Test System (graphical)	The specific test system consists of a real-time grid simulator, protection IEDS, Ethernet switches (x2), communication cables (x2). The real-time simulator is used to model the power system dynamics as well as some IED functions such as Merging unit (generating sampled values), circuit breaker functionality. The physical IEDs (for protection) will be connected to the real-time simulator through the two redundant communication networks in a C-HIL setup.

	 Fig. 1: PRP Network Topology  Fig. 2: HSR Network Topology
Target measures	• End to end delay and packet loss of IEC 61850 GOOSE and sampled value (SV) messages after the introduction of fault. • Availability and Mission reliability (ability to continually deliver service) of the communication network after the introduction fault.
Input and output parameters	**Input parameters:** • Failure type • Failure rate of components • Repair rate of components • Communication network topology • Background traffic rate • Degree of redundancy **Output parameters:** • Maximum packet delay • Packet loss • Time duration of service interruption
Test Design	The test design is as follows. 1. System starts with normal operating conditions, no fault and there will be a normal GOOSE and SV stream (every 10 ms and 0.25 ms respectively) 2. Add some background traffic to the ethernet switches

	accounting for traffic from other IEDs or other devices in the substation. 3. Introduce faults in the system. This could be: 4. Failure in the communication network 5. OR, simultaneous failure in the communication network and the power system 6. During a failure in the communication network, the fail-over algorithm is activated and the system switches to the backup network with the redundant switches and network links. 7. If there is also a failure in the power system right before or after the failure of the communication system failure, it will also change the GOOSE traffic behavior (burst of GOOSE messages will be transmitted). 8. Collect the target measurements/metrics 9. end to end delay of GOOSE and SV streams between the IEDs and the virtual devices (MUs) in the Opal RT. 10. Down time of the communication between the IEDs and virtual MUs (if any) 11. Repeat these steps by varying the failure scenarios, background traffic, redundancy type and degree.
Initial system state	Normal system state where there is no failure in the power and communication system. There will be a normal GOOSE (status update) between IEDs (also between IED and breakers), and SV streams from OPAL virtual MUs to the physical IEDs.
Evolution of system state and test signals	1. Initial state where there is no failure in the system (Normal GOOSE and SV streams) 2. Failure of network components and/or the power system occur. 3. The GOOSE and SV traffic pattern will change (for power system failures). The IEDs will send burst of GOOSE messages for a certain duration to make sure that faults are cleared on time. 4. When the IEDs or the PRP enabled ethernet switches detect a failure on the primary communication path (network), a fail-over function will be activated (in response to failure in the communication system) 5. The IEDs start to accept GOOSE and SV packets coming through the secondary path (network). 6. GOOSE data rate will return to the normal rate. 7. After a recovery of failed nodes (the communication network), IEDs and PRP enabled ethernet switches will revert back to accepting packets from the primary communication network.

Other parameters	• Temporal order of contingency events
	    ○ ICT failure causes PS fault
	    ○ PS fault causes ICT failure
	    ○ PS fault and ICT failure coincident

Temporal resolution	100 us
Source of uncertainty	Background traffic data rate, configuration of the communication network (ethernet switches), Network devices or IED's capability to support the PRP/HSR architectures.
Suspension criteria / Stopping criteria	Exceeding of quality attributes: • Communication is down for 200 milliseconds (protection related applications) or 3 second for SCADA- IED communication.