

## Test Case 25

Author: Petra Raussi (VTT), Vetrivel Subramaniam Rajkumar (TUD)  
 Project: ERIGrid 2.0

Version 1  
 Date 19/4/2021

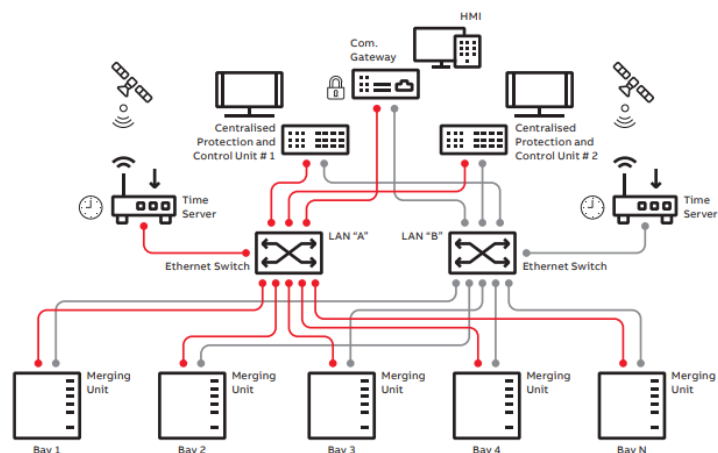
<b>Name of the Test Case</b>	Cyber Security of Digital Substations and Impact Analysis
<b>Narrative</b> Inc. use case and test objectives.	The energy transition towards a carbon neutral and clean energy system requires increased power grid digitalization. This is seen as the most cost-effective path in developing smart grids. An essential part of any functional power system are substations; thus, their digitalization is crucial. While the digitalization of power system brings several benefits from cost savings to more optimized operations and investments, it also raises concerns related to cybersecurity. To ensure safe and resilient operation of digital substations even in the case of cyber attacks or incidents, it is necessary to investigate their cyber resilience. This can aid in impact analysis of cyber attacks on digital substations, and help to gain deeper understanding of which components must be most secured
<b>Function(s) under Investigation (FuI)</b> "the referenced specification of a function realized (operationalized) by the object under investigation"	<ul style="list-style-type: none"> <li>• Grid stability and operation when impacted by cyber-attacks/incidents</li> <li>• Cyber resilience of digital substations</li> </ul>
<b>Object under Investigation (OuI)</b> "the component(s) (1..n) that are to be qualified by the test"	Digital substation components and communication systems: <ul style="list-style-type: none"> <li>• substation bays (busbars, disconnectors, circuit breakers, current and voltage transformers),</li> <li>• merging units,</li> <li>• Ethernet switches,</li> <li>• HMIs,</li> <li>• time servers,</li> <li>• IEDs,</li> <li>• centralized protection and control units,</li> <li>• station control systems,</li> <li>• process bus, and</li> <li>• communication gateways.</li> </ul>
<b>Domain under Investigation (DuI):</b> "the relevant domains or sub-domains of test parameters and connectivity."	<ul style="list-style-type: none"> <li>• ICT</li> <li>• Electrical power system</li> </ul>
<b>Purpose of Investigation (PoI)</b> The test purpose in terms of Characterization, Verification, or Validation	To carry out impact analysis of cyber-physical events on digital substations and quantify impact on grid operations.
<b>System under Test (SuT):</b> Systems, subsystems, components included in the test case or test setup.	In power system domain: digital substation including substation bays, merging units, Ethernet switches, HMIs, time servers and IEDs centralised protection and control units, station control systems, etc. A substation bay comprises of busbars,

disconnectors, circuit breakers, current and voltage transformers, etc.

In ICT domain: communication within the substation via local operating networks (process bus) at bay level using communication protocols such as IEC 61850 and LAN at the station level for communication with the control centre via dedicated communication gateway and protocols such as IEC 104 and DNP3. Hence, to realize this test case, the following components are required:

- Real-time grid simulator such as RTDS or OPAL-RT that supports Hardware-in-Loop (HIL) studies
- Substation network elements:
  - i. At least one ethernet switch and time server. At least two or more physical IEC 61850 capable IEDs
  - ii. RTUs, MUs, other HIL devices
- A dedicated communication network emulator to model disturbances/cyber attacks

The testing involves interfacing the real-time grid simulator with all hardware components in a HIL setup to mimic a digital substation. Furthermore, the real-time grid simulator also needs to be interfaced with the network emulator to model and input communication related effects such as latency, packet loss, loss of service, etc.



Source: *Centralized Protection and Control*. ABB Whitepaper, 2020. Link:

[https://library.e.abb.com/public/6b20916a4d2e412daabb76fba4a1268e/Centralized\\_Protection\\_and\\_Control\\_White\\_paper\\_2NGA000256\\_LRENA.pdf](https://library.e.abb.com/public/6b20916a4d2e412daabb76fba4a1268e/Centralized_Protection_and_Control_White_paper_2NGA000256_LRENA.pdf)

#### Functions under Test (FuT)

Functions relevant to the operation of the system under test, including Ful and relevant interactions btw. Oul and SuT.

- Capability of test setup to exchange data using IEC 61850 and IEC 60870-5-104
- Automation and protection functionality realized by Oul

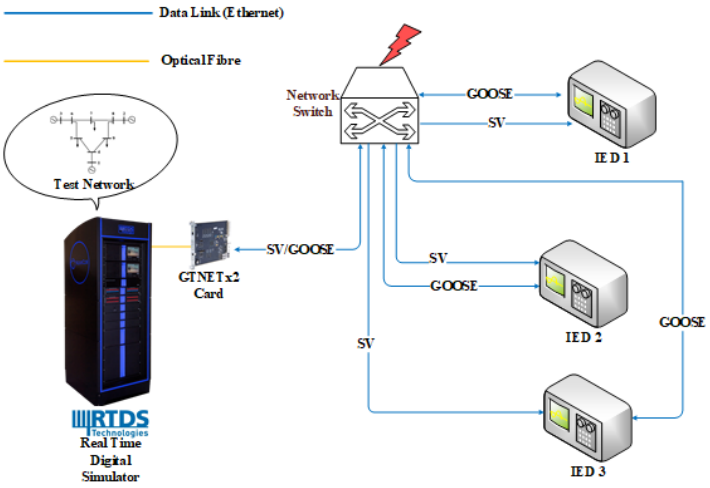
	<ul style="list-style-type: none"> <li>Behaviour and performance of substation, when subjected to specific cyber attacks/threats</li> </ul>
<b>Test criteria (TCR)</b> Formulation of criteria for each Pol based on properties of SuT; encompasses properties of test signals and output measures.	<ul style="list-style-type: none"> <li>Equipment response and performance under normal operating conditions</li> <li>Equipment response and performance when subjected to specific cyber attacks/threats.</li> <li>Impact of particular attack/threat on overall system performance</li> </ul>
<b>Target Metrics (TM)</b> Measures required to quantify each identified test criteria	Cyber security performance and resilience testing <ul style="list-style-type: none"> <li>This TC assumes that the substation is conformant to IEC 62351-6 and tests its implementation for resiliency.</li> <li>For e.g., through Denial-of-Service attacks, malformed authentication codes, etc.</li> </ul> Impact on Power system <ul style="list-style-type: none"> <li>KPIs: loss of load, voltage deviations, frequency fluctuations, etc.</li> </ul>
<b>Variability Attributes (VA)</b> controllable or uncontrollable factors and the required variability; ref. to Pol.	<ul style="list-style-type: none"> <li>Overall substation configuration and topology</li> <li>Network emulator characteristics</li> <li>Redundancy (N-1, N-2.... N-k): Number of components or communication links which can fail before system operation is at risk</li> <li>Topology and type of simulated power system (transmission vs distribution)</li> </ul>
<b>Quality Attributes (QA)</b> threshold levels for test result quality as well as pass/fail criteria.	<ul style="list-style-type: none"> <li>System performance under cyber attacks</li> <li>Pass: all KPIs within maximum limits/bounds</li> <li>Fail: at least one KPI maximum limits</li> </ul>

### Qualification Strategy

The Pol are mainly addressed by characterizing and verifying the impact of cyber attacks in digital substations on grid operations. This can be achieved by determining how substation functionality and thereby power system stability and operations are directly affected by cyber-physical attacks.

### Test Specification TC25.TS1

<b>Reference to Test Case</b>	TC25
<b>Title of Test</b>	Impact analysis of Denial-of-Service (DoS) attack in a digital substation
<b>Test Rationale</b>	A digital substation is realised by the IEC 61850 standard which mandates a common Ethernet based communication infrastruc-

	ture within a substation. This experiment seeks to analyse the impact of a DoS attack that successfully compromises the substation communication infrastructure. This may lead to delayed or loss of trip, block commands, thereby directly impacting grid operations.
<b>Specific Test System</b> (graphical)	<p>The test system comprises of a real-time grid simulator, at least one Ethernet switch, and multiple IEC 61850 compliant devices interconnected in a HIL setup. (See SuT for further information)</p> 
<b>Target measures</b>	<ul style="list-style-type: none"> <li>KPIs: loss of load, voltage deviations, frequency fluctuations on simulated system under a DoS attack</li> <li>Time taken and quality of service for IEC 61850 based communication under a DoS attack</li> </ul>
<b>Input and output parameters</b>	<p>Input parameters:</p> <ul style="list-style-type: none"> <li>Type of power system simulated</li> <li>Network topology of substation</li> <li>Protection schemes applied through the relays</li> <li>Fault type and duration</li> <li>Type of attack: DoS</li> </ul> <p>Output parameters:</p> <ul style="list-style-type: none"> <li>KPIs: loss of load, voltage deviations, frequency fluctuations on simulated system under a DoS attack</li> <li>Avg time for intra substation communication and communication quality of service (jitter, packet loss, latency, throughput, availability)</li> </ul>
<b>Test Design</b>	<p>The test is a HIL experiment as described in the SuT and specific test system. The test consists of a reference test for the baseline measurements and repeat of this test with the DoS attack. The test design is as follows:</p> <ol style="list-style-type: none"> <li>1. Start the system with all devices functioning as required and the system is stabilized.</li> <li>2. Run a test simulation with a short-circuit or fault condition at location monitored by relay.</li> <li>3. Note that the appropriate relay communicates trip signal via IEC 61850 GOOSE message. Note this time as reference time T1.</li> <li>4. Circuit breaker is opened, and the fault is cleared.</li> <li>5. Carry out DoS attack via external emulator/device to tar-</li> </ol>

	get specific IED/relay. 6. Repeat steps 2 to 3 and note the new time T2. 7. Quantify impact of attack through KPIs and note down targeted device. 8. Repeat for additional target devices at different locations to identify most critical digital asset.
<b>Initial system state</b>	<ul style="list-style-type: none"> <li>• All devices are ON and running</li> <li>• Real-time grid simulator can send and receive messages to and from the hardware devices</li> <li>• IEDs receive messages from the real-time grid simulator</li> </ul>
<b>Evolution of system state and test signals</b>	Successful recording of KPIs for each targeted device. The fault event generated by the real-time grid simulator has predetermined fault duration and wait time. The DoS attack operates independently of the HIL experiment sequence and can occur at any moment of time in the sequence.
<b>Other parameters</b>	N/A
<b>Temporal resolution</b>	Order of tens of seconds
<b>Source of uncertainty</b>	Configuration of HIL test setup, quality of time synchronization.
<b>Suspension criteria / Stopping criteria</b>	Suspension criteria: Errors in devices/misconfiguration Stopping criteria: the experiment can be concluded when the KPIs for various target devices are noted. Alternatively, if the attack causes cascading effects or a blackout, it can be stopped.

### Mapping to Research Infrastructure

Trying known cyber-attack malware, etc. on the digital substation and seeing the impacts of that, which components should be the most heavily guarded. What are the impacts of cyber-attack on the power system, in which components are influenced?

### Experiment Specification ##.##.##

<b>Reference to Test Specification</b>	
<b>Title of Experiment</b>	
<b>Research Infrastructure</b>	
<b>Experiment Realisation</b>	
<b>Experiment Setup</b> (concrete lab equipment)	
<b>Experimental Design and Justification</b>	
<b>Precision of equipment and measurement uncertainty</b>	
<b>Storage of experiment data</b>	