TITLE: IEMI test on a complex smart grid communication system, owned by SINTEF, by PETER project ESR2 as part of EriGrid 2 project.	**AUTHOR: Arash Nateghi** **DATE: 03/02/2022**

Object under Investigation (*OuI*)	**Test Objectives**	**System under Test** (*SuT*)
"The component(s) (1..n) that are to be qualified by the test” *Data communication channels of:* 1. *WLAN communication network* 2. *PLC communication network* 3. *Ethernet communication network* 4. *LAN communication network* 5. *IEC 61850* 6. *NTP* 7. *Modbus TCP* 8. *IEC 60870-5-104 of smart grid complex system.*	Why is the test needed? What do we expect to find out? *As part of PETER project, risk of Intentional electromagnetic Interference, IEMI, on a complex system of a critical infrastructure such as smart grid communication system need be assessed.* *IEMI signals need to be radiated and conducted to different part of the communication links of the smart grid communication system, such as WLAN and PLC communication channels. Then the behavior of each subsystem is assessed by monitoring the data or packet transfer rate between subsystems. Next, the measurement results are used as technical elements in combination with non-technical aspects of the IEMI risk assessment such as the mobility of the source or the accessibility to the location, where system is installed, as input for the risk assessment tool. Next, the risk from intentional electromagnetic interference is*	Systems, subsystems, components included in the test case or test setup. *Complex communication network system which links below subsystem and aggregated the data between within a smart grid system.* *Sub-systems:* • *SCADA & Monitoring* • *Automation Equipment* • *Wireless smart meter* • *PMU* • *Data Switches* • *Local HMI*
Function(s) under Investigation (*FuI*)		

"The referenced specification of a function realized (operationalized) by the object under investigation" *The data transmission rate against failure of the functionality of the communication of subsystems and thus of the complex smart grid system.*	*statistically evaluated using Monte Carlo simulations to identify the most threatening risks that need further investigation or mitigation.*	- *Protection devices* - *Metering devices* - *GPS*
Domain under Investigation (*DuI*): "The relevant domains of test parameters and connectivity" *Frequency domain to monitor power spectrum for Interference to Signal Ratio ISR.* *Time domain to monitor data transfer rate.*	**Purpose of Investigation** *(PoI)* The test purposes classified in with terms *Characterization*, *Verification*, or *Validation* *The connectivity of complex communication systems and the spread of IEMI due to the system properties must be assessed to ensure that the system structure is resistant to these attacks.* *The susceptibility of the subsystems and overall system due to IEMI attack on part of the system need to be verified.* *Statistical simulation results need to be validated after inserting the measurement results from the test.*	**Functions under Test** (*FuT*) Functions relevant to the operation of the system under test, including FuI and relevant interactions btw. OuI and SuT *System function failure behavior such as :* - *Short term disturbances* - *Long term disturbances* - *Automatic restart of the subsystems or the whole system* - *Manual restart of the subsystems or the whole system*
Target metrics (*TM*) Measures retrievable from SuT required to quantify each of the identified test criteria *Data transfer rate.* *Data packet transfer rate.* *Severity of Intentional Electromagnetic Interference and system behavior.* *Probability of breakdown failure of the subsystems and the overall system.*	**Test criteria** *(TCR)* formulation of criteria *for each PoI* based on properties of SuT; encompasses properties of test signals and output measures *Data transfer rate required for healthy communication.* *Probability of breakdown failure of subsystems due to resulting disturbances, including EMI field strength (E-field) (M-Field), Shielding factor and duration of disturbances.* **Quality attributes** *(QA)* Threshold levels for test result quality as well as pass/fail criteria *Fail:* - *Data transfer rate less than normal rate required for healthy communication.* - *Probability of breakdown failure if it higher than standards.* *Pass:* - *Otherwise*	**Variability attributes** *(VA)* Identify relevant controllable or uncontrollable factors of the SuT and their required variability; refer to PoI - *Uncertainties with measurement equipment* - *Existing EMI pollution apart from radiated or conducted IEMI within the system or in the vicinity* - *System robustness against IEMI based on its topology*

TITLE: CONSEQUENCE ANALYSIS OF IEMI ATTACKS ON A SMART GRID

AUTHOR: **Fernando Arduini**

DATE: **13.12.2021**

Object under Investigation (*OuI*)

It depends upon SINTEF available system. Among all subsystems we deem relevant when it comes to IEMI attacks, we think we should include the following in our investigations:

Protection Relays
Control Units
HMIs
Remote terminal units
Power Electronic Converters
Voltage regulators
Etc.

Function(s) under Investigation (*FuI*)

Still to be defined after knowledge of the system available at SINTEF.

Domain under Investigation (*DuI*):

Still to be defined after knowledge of the system available at SINTEF.

Test Objectives

The test is needed to assess the impact of successful IEMI attacks on a complex smart grid system that encompasses different Smart Electronic Devices (SEDs). We expect to find out how failures at a subsystem level can propagate to the system level, and how they can impact the system reliability.
We would like to introduce error states in some of the system parts, presumably by switching on and off some specific subsystems we expect to possibly be vulnerable to IEMI. In consequence, we would like to check and record the reaction of other subsystems to the induced disturbance mimicking an IEMI attack. In a further step, we would like to simultaneously trigger malfunctions in order to evaluate the system reaction to such a distributed attack scenario.

During our investigations, such induced malfunctions might include:

- Switching on or off of components
- Plugging/Unplugging of network cabling
- Possibly introducing our own intentionally and physically damaged cabling we bring with us to reduce transmission bandwidth and/or reliability of the subsystem connections.

Purpose of Investigation *(PoI)*

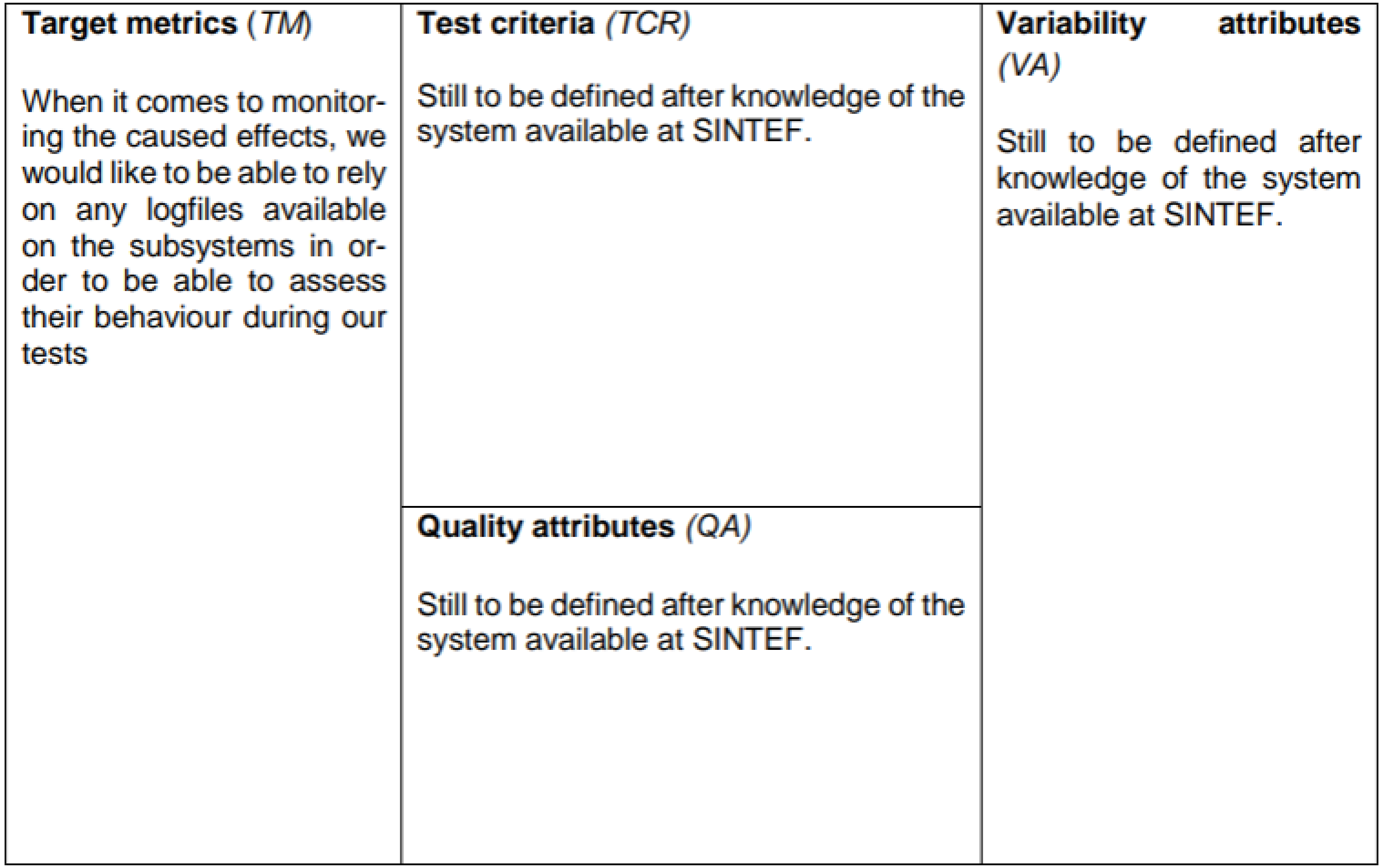
The purpose of investigation is to validate one of the steps of the IEMI risk management framework. This step consists of determining the consequences of IEMI attacks at a system level in order to estimate the risk of this threat.

System under Test (*SuT*)

The typical smart grid configuration will be agreed with SINTEF.

Functions under Test (*FuT*)

Ideally, the consequence analysis could be carried out considering the main operational modes of the system to be defined.



<table>
<tr>
<td rowspan="2"><b>Target metrics</b> (<i>TM</i>)

When it comes to monitoring the caused effects, we would like to be able to rely on any logfiles available on the subsystems in order to be able to assess their behaviour during our tests</td>
<td><b>Test criteria</b> <i>(TCR)</i>

Still to be defined after knowledge of the system available at SINTEF.</td>
<td rowspan="2"><b>Variability attributes</b> <i>(VA)</i>

Still to be defined after knowledge of the system available at SINTEF.</td>
</tr>
<tr>
<td><b>Quality attributes</b> <i>(QA)</i>

Still to be defined after knowledge of the system available at SINTEF.</td>
</tr>
</table>