Test Case 01

Author Hristo Koshutanski Version 1.0
Project AID4EPES Date 21/09/2023

Name of the Test Case	**IEC-104-FDI**
Narrative Incl. use case and test objectives.	**Obj1**: Perform a **false data injection (FDI)** attack on the IEC-104 protocol in a power grid substation (both in process monitoring direction and in system control direction). **Obj2**: Define the **impact of an FDI attack** on the substation operation, define **indicators of compromise** (IoCs), and **record FDI traffic dataset**. **Obj3**: Validate the **efficiency of ATOS's anomaly and intrusion detection system** (called LADS) on the detection of the FDI. Define if any improvements based on IoCs.
Function(s) under Investigation (*Ful*) "the referenced specification of a function	**Ful1: Substation monitoring task**: RTU to SCADA communications based on IEC-104

realized (operationalized) by the object under investigation"	**FuI2: Substation control task:** SCADA to RTU communications based on IEC-104
Object under Investigation (*OuI*) "the component(s) (1..n) that are to be qualified by the test"	**OuI**: **Control centre (SCADA) – substation bus** communications
Domain under Investigation (*DuI*) "the relevant domains or sub-domains of test parameters and connectivity."	**DuI**: **Substation monitoring and control** under IEC-104 communication protocol.
Purpose of Investigation *(PoI)* The test purpose in terms of Characterization, Verification, or Validation	**PoI1**: Characterization (definition) of an FDI attack on FuI1 and FuI2. NOTE: Regarding FuI2, consider the FDI attack as **unauthorized access** attack. **PoI2**: Verification of an FDI attack impact on the substation monitoring and control tasks. **PoI3**: Validation of the efficiency the LADS anomaly & intrusion detection technology on the detection of an FDI attack.
System under Test (*SuT*): Systems, subsystems, components included in the test case or test setup.	**SuT**: consists of SCADA control centre (server), Substation bus (switch), RTU and IED, and LADS. Note: The SuT in this test case consists only of those components of the defined testbed that relevant for this type of attack.
Functions under Test (*FuT*) Functions relevant to the operation of the system under test, including FuI and relevant interactions btw. OuI and SuT.	**FuT1**: Any IEC104 ASDU typeID in the monitoring direction such as M_ME_NC_1, M_ME_TF_1, etc. At least **three** types of monitoring function codes should be targeted. **FuT2**: Any IEC104 ASDU typeID in the system control direction such as C_IC_NA_1, C_RP_NA_1, etc. At least **three** types of function codes in the control direction should be targeted, where at least **two** func. codes shall be under category of **unauthorized access**.
Test criteria *(TCR)* Formulation of criteria for each PoI based on properties of SuT; encompasses properties of test signals and output measures.	**TCR1**: Definition and implementation of an attack script capable to inject IEC-104 packets into a valid TCP session between a SCADA server and an RTU or IEC in a substation. At least three types of func. code packets in monitoring and three types of func. code packets injection in the control direction. [*Ref. PoI1, SuT*] **TCR2**: Document if PASS or FAIL an FDI attack, and impact of the FDI attack (ref. TCR1) on the SuT in terms whether the injected false data has been accepted by SCADA (ref. FuI1) or by the RTU/IED (ref. FuI2), and how this false data would impact a real substation behavior. [*Ref. PoI2*] **TCR3**: Quantify how efficient the LADS technology is for the detection of the FDI attacks. Meet at least all KPIs defined in the proposal of the AID4EPES for each of the FDI attacks.

	Target Metrics *(TM)* Measures required to quantify each identified test criteria	**TM1-TCR1**: At least **6 traffic captures** (pcaps) each at least **30 min** duration (of attack traces and normal traffic). Each traffic capture regards one type of func. code injection in either monitoring or control direction. **TM2-TCR2**: Document what percentage of **attacks succeed** (at least 15% PASS), and what % fail. For each of the FDI attacks (at least 6 FDI attacks), LADS shall meet the following TMs: **TM3-TCR3**: TPR > 94% **TM4-TCR3**: FPR < 9% **TM5-TCR3**: FNR < 5% **TM6-TCR3**: Accuracy ≥ 96% **TM7-TCR3**: Mean time to Detection < 1ms OR flows per second > 1000 (fps)
	Variability Attributes *(VA)* controllable or uncontrollable factors and the required variability; ref. to PoI.	**VA1**: The FDI attacks shall consider at least three func codes in the monitoring direction [*Ref. FuT1*] **VA2**: The FDI attacks shall consider at least three func codes in the control direction [*Ref. FuT2*]
	Quality Attributes *(QA)* threshold levels for test result quality as well as pass/fail criteria.	**QA**: At least **30 min** duration of traffic capture with **both** attack traces and normal traffic **per FDI type attack** [*Ref to TM1-TCR1*]

Test Case 02

Author Hristo Koshutanski Version 1.0
Project AID4EPES Date 21/09/2023

Name of the Test Case	**IEC-104-DoS**
Narrative Incl. use case and test objectives.	**Obj1**: Perform a **Denial-of-Service** attack using the IEC-104 protocol in a power grid substation (both in process monitoring direction and in system control direction). **Obj2**: Define the **impact of a DoS attack** on the substation operation, define **indicators of compromise** (IoCs), and **record DoS traffic dataset**. **Obj3**: Validate the efficiency of ATOS's anomaly and intrusion detection system (called LADS) on the detection of the DoS. Define if any improvements based on IoCs.
Function(s) under Investigation (*FuI*) "the referenced specification of a function realized (operationalized) by the object under investigation"	**FuI1: Substation monitoring task**: RTU to SCADA communications based on IEC-104 **FuI2: Substation control task:** SCADA to RTU communications based on IEC-104
Object under Investigation (*OuI*) "the component(s) (1..n) that are to be qualified by the test"	**OuI**: **Control centre (SCADA) – substation bus** communications
Domain under Investigation (*DuI*) "the relevant domains or sub-domains of test parameters and connectivity."	**DuI**: **Substation monitoring and control tasks** under IEC-104 communication protocol.
Purpose of Investigation *(PoI)* The test purpose in terms of Characterization, Verification, or Validation	**PoI1**: Characterization (definition) of a DoS attack on FuI1 and FuI2. **PoI2**: Verification of a DoS attack impact on the substation monitoring and control tasks. **PoI3**: Validation of the efficiency the LADS anomaly & intrusion detection technology on the detection of a DoS attack.
System under Test (*SuT*): Systems, subsystems, components included in the test case or test setup.	**SuT**: Consists of SCADA control centre (server), Substation bus (switch), RTU and IED, and LADS. Note: The SuT in this test case consists only of those components of the defined testbed that are relevant for this type of attack.
Functions under Test (*FuT*) Functions relevant to the operation of the system under test, including FuI and relevant interactions btw. OuI and SuT.	**FuT1**: Use high volume of U-format (unnumbered) control functions, or any of ASDU typeID in the monitoring direction such as M_ME_NC_1, M_ME_TF_1, etc, to achieve DoS impact. At least **two** types of U-format and/or ASDU typeID monitoring function codes should be used to achieve a DoS. **FuT2**: Use high volume of U-format (unnumbered) control functions, or any of ASDU typeID in the control direction such as

	C_IC_NA_1, etc, to achieve DoS impact. At least **two** types of U-format and/or ASDU typeID control function codes should be used to achieve a DoS.
Test criteria *(TCR)* Formulation of criteria for each PoI based on properties of SuT; encompasses properties of test signals and output measures.	**TCR1**: Definition and implementation of an attack script capable to generate a high volume of U-format or I-format IEC-104 packets (into a valid TCP session) between a SCADA server and an RTU or IEC in a substation. [*Ref. PoI1, SuT*] **TCR2**: Document if PASS or FAIL an DoS attack, and impact of the DoS attack (ref. TCR1) on the SuT in terms whether the DoS has been achieved on the SCADA (ref. FuI1) or on the RTU/IED (ref. FuI2), and how this DoS would impact a real substation behavior. [*Ref. PoI2*] **TCR3**: Quantify how efficient the LADS technology is for the detection of the DoS attacks. Meet at least all KPIs defined in the proposal of the AID4EPES for each of the DoS attacks.
Target Metrics *(TM)* Measures required to quantify each identified test criteria	**TM1-TCR1**: At least **4 traffic captures** (pcaps) each at least **20 min** duration (of attack traces and normal traffic). Each traffic capture regards one type of DoS of U-format and/or I-format in either monitoring or control direction. **TM2-TCR2**: **At least 80% of attacks succeed** (PASS). At least 3 out 4 DoS attacks PASS, and less than 20% fail. For each of the DoS attacks (at least 4 DoS attacks), LADS shall meet the following TMs: **TM3-TCR3**: TPR > 94% **TM4-TCR3**: FPR < 9% **TM5-TCR3**: FNR < 5% **TM6-TCR3**: Accuracy ≥ 96% **TM7-TCR3**: Mean time to Detection < 1ms OR flows per second > 1000 (fps)
Variability Attributes *(VA)* controllable or uncontrollable factors and the required variability; ref. to PoI.	**VA1**: The DoS attacks shall consider at least two U-format and/or I-format IEC104 packets used in the monitoring direction [*Ref. FuT1*] **VA2**: The DoS attacks shall consider at least two U-format and/or I-format IEC104 packets used in the control direction [*Ref. FuT2*]
Quality Attributes *(QA)* threshold levels for test result quality as well as pass/fail criteria.	**QA**: At least **20 min** duration of traffic capture with **both** attack traces and normal traffic per DoS type attack [*Ref to TM1-TCR1*]

Test Case 03

Author Hristo Koshutanski Version 1.0
Project AID4EPES Date 21/09/2023

Name of the Test Case	**IEC61850-GOOSE-FDI**
Narrative Incl. use case and test objectives.	**Obj1**: Perform a **false data injection (FDI)** attack on the IEC61850 GOOSE protocol in a power grid substation. **Obj2**: Define the **impact of an FDI attack** on the substation operation, define **indicators of compromise** (IoCs), and **record FDI traffic dataset**. **Obj3**: Validate the **efficiency of ATOS's anomaly and intrusion detection** system (called LADS) on the detection of the FDI. Define if any improvements based on IoCs.
Function(s) under Investigation (*FuI*) "the referenced specification of a function realized (operationalized) by the object under investigation"	**FuI: Substation monitoring and control task**: IED to RTU communications based on IEC61850 GOOSE.
Object under Investigation (*OuI*) "the component(s) (1..n) that are to be qualified by the test"	**OuI**: **Process/physical bus** communications of a power substation.
Domain under Investigation (*DuI*) "the relevant domains or sub-domains of test parameters and connectivity."	**DuI**: **Substation monitoring and control tasks** under IEC61850 GOOSE protocol.
Purpose of Investigation *(PoI)* The test purpose in terms of Characterization, Verification, or Validation	**PoI1**: Characterization (definition) of FDI attacks on FuI. **PoI2**: Verification of an FDI attack impact on the substation monitoring and control tasks. **PoI3**: Validation of the efficiency the LADS anomaly & intrusion detection technology on the detection of an FDI attack.
System under Test (*SuT*): Systems, subsystems, components included in the test case or test setup.	**SuT**: consists of a process/physical bus (switch), an RTU, two IEDs, and LADS. Note: The SuT in this test case consists only of those components of the defined testbed that relevant for this type of attack.
Functions under Test (*FuT*) Functions relevant to the operation of the system under test, including FuI and relevant interactions btw. OuI and SuT.	**FuT**: Monitoring of substation state changes, i.e. changes in stNum in GOOSE messages, from the IEDs to RTUs. At least **two types of changes** should be considered: unexpected changes in stNum values and unexpected changes in sqNum values.
Test criteria *(TCR)* Formulation of criteria for each PoI based on properties of SuT; encompasses properties of test signals and output	**TCR1**: Definition and implementation of an attack script capable to inject/broadcast GOOSE packets on the process bus under **three different types**: **replay** GOOSE packets from previous communications, **change stNum** with reset sqNum, and

measures.		nications, and **change smpCnt** of new false value packets injection. [*Ref. PoI1*] **TCR2**: Document if PASS or FAIL an FDI attack, and impact of the FDI attack (ref. TCR1) on the SuT in terms whether the injected false data has been accepted by the IED (ref. FuI), and how this false data would impact a real substation behavior. [*Ref. PoI2*] **TCR3**: Quantify how efficient the LADS technology is for the detection of the FDI attacks. Meet at least all KPIs defined in the proposal of the AID4EPES for each of the FDI attacks.
	Target Metrics *(TM)* Measures required to quantify each identified test criteria	**TM1-TCR1**: At least **two traffic captures** (pcaps) each at least **20 min** duration (of attack traces and normal traffic). Each traffic capture regards one type of FDI attack [*Ref. TCR1*]. **TM2-TCR2**: Document what percentage of **attacks succeed** (at least 15% PASS), and what % fail. For each of the FDI attacks (at least 2 FDI attacks), LADS shall meet the following TMs: **TM3-TCR3**: TPR > 94% **TM4-TCR3**: FPR < 9% **TM5-TCR3**: FNR < 5% **TM6-TCR3**: Accuracy ≥ 96% **TM7-TCR3**: Mean time to Detection < 1ms OR flows per second > 1000 (fps)
	Variability Attributes *(VA)* controllable or uncontrollable factors and the required variability; ref. to PoI.	**VA**: The FDI attacks shall consider at least **two** different types of manipulation: replay packets from previously (but old) valid measurements, inject/broadcast new false SV packets with suitable smpCnt value (different or repeated from current communications) [*Ref. FuT, TCR1*]
	Quality Attributes *(QA)* threshold levels for test result quality as well as pass/fail criteria.	**QA**: At least **20 min** duration of traffic capture with **both** attack traces and normal traffic per FDI type attack [*Ref to TM1-TCR1*]

measures.	target the **same stNum but false sqNum**. [*Ref. PoI1*] **TCR2**: Document if PASS or FAIL an FDI attack, and impact of the FDI attack (ref. TCR1) on the SuT in terms whether the injected false data has been accepted by the RTU (ref. FuI), and how this false data would impact a real substation behavior. [*Ref. PoI2*] **TCR3**: Quantify how efficient the LADS technology is for the detection of the FDI attacks. Meet at least all KPIs defined in the proposal of the AID4EPES for each of the FDI attacks.
Target Metrics *(TM)* Measures required to quantify each identified test criteria	**TM1-TCR1**: At least **3 traffic captures** (pcaps) each at least **30 min** duration (of attack traces and normal traffic). Each traffic capture regards one type of FDI attack [*Ref. TCR1*]. **TM2-TCR2**: Document what percentage of **attacks succeed** (at least 15% PASS), and what % fail. For each of the FDI attacks (at least 3 FDI attacks), LADS shall meet the following TMs: **TM3-TCR3**: TPR > 94% **TM4-TCR3**: FPR < 9% **TM5-TCR3**: FNR < 5% **TM6-TCR3**: Accuracy ≥ 96% **TM7-TCR3**: Mean time to Detection < 1ms OR flows per second > 1000 (fps)
Variability Attributes *(VA)* controllable or uncontrollable factors and the required variability; ref. to PoI.	**VA**: The FDI attacks shall consider at least three different types of stNum manipulation (replay, false stNum, same StNum but false sqNum) in GOOSE messages [*Ref. FuT, TCR1*]
Quality Attributes *(QA)* threshold levels for test result quality as well as pass/fail criteria.	**QA**: At least **30 min** duration of traffic capture with **both** attack traces and normal traffic per FDI type attack [*Ref to TM1-TCR1*]

Test Case 04

Author Hristo Koshutanski | Version 1.0
Project AID4EPES | Date 21/09/2023

Name of the Test Case	**IEC61850-SV-FDI**
Narrative Incl. use case and test objectives.	**Obj1**: Perform a **false data injection (FDI)** attack on the IEC61850 SV protocol in a power grid substation. **Obj2**: Define the **impact of an FDI attack** on the substation operation, define **indicators of compromise** (IoCs), and **record FDI traffic dataset**. **Obj3**: Validate the **efficiency of ATOS's anomaly and intrusion detection** system (called LADS) on the detection of the FDI. Define if any improvements based on IoCs.
Function(s) under Investigation (*FuI*) "the referenced specification of a function realized (operationalized) by the object under investigation"	**FuI: Substation monitoring and control task**: MUs to IEDs communications based on IEC61850 SV.
Object under Investigation (*OuI*) "the component(s) (1..n) that are to be qualified by the test"	**OuI**: **Process/physical bus** communications of a power substation.
Domain under Investigation (*DuI*) "the relevant domains or sub-domains of test parameters and connectivity."	**DuI**: **Substation monitoring and control tasks** under IEC61850 SV protocol.
Purpose of Investigation *(PoI)* The test purpose in terms of Characterization, Verification, or Validation	**PoI1**: Characterization (definition) of FDI attacks on *FuI*. **PoI2**: Verification of an FDI attack impact on the substation monitoring and control tasks. **PoI3**: Validation of the efficiency the LADS anomaly & intrusion detection technology on the detection of the FDI attacks.
System under Test (*SuT*): Systems, subsystems, components included in the test case or test setup.	**SuT**: consists of a process/physical bus (switch), two IEDs, two MUs, and LADS. Note: The SuT in this test case consists only of those components of the defined testbed that are relevant for this type of attack.
Functions under Test (*FuT*) Functions relevant to the operation of the system under test, including FuI and relevant interactions btw. OuI and SuT.	**FuT**: Monitoring of substation real value measurements, i.e. any changes in SV messages with false data, from the MUs to IEDs. It should be monitored and considered unexpected changes in smpCnt values when injecting packets with false measurements.
Test criteria *(TCR)* Formulation of criteria for each PoI based on properties of SuT; encompasses properties of test signals and output	**TCR1**: Definition and implementation of an attack script capable to inject/broadcast SV packets on the process bus under **two different types**: **replay** SV packets from previous commu-

Test Case 05

Author Hristo Koshutanski
Project AID4EPES
Version 1.0
Date 21/09/2023

Name of the Test Case	**IEC61850-PTP-Desynchronization**
Narrative Incl. use case and test objectives.	**Obj1**: Perform a **desynchronization** attack using the PTP protocol (IEEE 1588-2008) in a power grid substation. It is in the context of IEC61850 standard which adopts PTP. **Obj2**: Define the **impact of a desynchronization attack** on the substation operation, define **indicators of compromise** (IoCs), and **record attack traffic dataset**. **Obj3**: Validate the **efficiency of ATOS's anomaly and intrusion detection** system (called LADS) on the detection of a desynchronization attack. Define if any improvements based on IoCs.
Function(s) under Investigation (*FuI*) "the referenced specification of a function realized (operationalized) by the object under investigation"	**FuI: Substation monitoring and control task**: MUs to IEDs, and IEDs to RTU communications using PTP.
Object under Investigation (*OuI*) "the component(s) (1..n) that are to be qualified by the test"	**OuI**: **Process/physical bus** communications of a power substation.
Domain under Investigation (*DuI*) "the relevant domains or sub-domains of test parameters and connectivity."	**DuI**: **Substation monitoring and control tasks**
Purpose of Investigation *(PoI)* The test purpose in terms of Characterization, Verification, or Validation	**PoI1**: Characterization (definition) of a desynchronization attacks on FuI. **PoI2**: Verification of a desynchronization attack impact on the substation monitoring and control tasks. **PoI3**: Validation of the efficiency the LADS anomaly & intrusion detection technology on the detection of the desynchronization attack.
System under Test (*SuT*): Systems, subsystems, components included in the test case or test setup.	**SuT**: consists of a process/physical bus (switch), two IEDs, two MUs, Master Clock with a GPS-based network synchronization, and LADS. Note: The SuT in this test case consists only of those components of the defined testbed that relevant for this type of attack.
Functions under Test (*FuT*) Functions relevant to the operation of the system under test, including FuI and relevant interactions btw. OuI and SuT.	**FuT**: Monitoring of substation state and physical grid real value measurements. It should be considered any behavior deviation on MUs and IEDs from inability to achieve necessary network clock synchronization.

Test criteria *(TCR)* Formulation of criteria for each PoI based on properties of SuT; encompasses properties of test signals and output measures.	**TCR1**: Definition and implementation of an attack capable to introduce false communications from another Master Clock entity in the process bus to deviate IEDs from the original master clock synchronization. [*Ref. PoI1*] **TCR2**: Document if PASS or FAIL the desynchronization attack, and impact of the attack (ref. TCR1) on the SuT (ref. FuI), and how such desynchronization would impact a real substation behavior. [*Ref. PoI2*] **TCR3**: Quantify how efficient the LADS technology is for the detection of the desynchronization attack. Meet all KPIs defined in the proposal of AID4EPES.
Target Metrics *(TM)* Measures required to quantify each identified test criteria	**TM1-TCR1**: At least **1 traffic capture** (pcap) at least **20 min** duration (of attack traces and normal traffic). [*Ref. TCR1*]. **TM2-TCR2**: Document what percentage of **attack instances succeed** (at least 15% PASS), and what % fail. For this attack, LADS shall meet the following TMs: **TM3-TCR3**: TPR > 94% **TM4-TCR3**: FPR < 9% **TM5-TCR3**: FNR < 5% **TM6-TCR3**: Accuracy ≥ 96% **TM7-TCR3**: Mean time to Detection < 1ms OR flows per second > 1000 (fps)
Variability Attributes *(VA)* controllable or uncontrollable factors and the required variability; ref. to PoI.	**VA**: The desynchronization attack shall consider at least one false Master Clock device and its corresponding traffic injected to the process bus communications. [*Ref. FuT, TCR1*]
Quality Attributes *(QA)* threshold levels for test result quality as well as pass/fail criteria.	**QA**: At least **20 min** duration of traffic capture with **both** attack traces and normal traffic. [*Ref to TM1-TCR1*]

Qualification Strategy

The Qualification strategy is heavily based on the final collection of attack datasets and on real time on premise validation of LADS technology. These datasets (curated traffic captures) will represent high impact attacks traces from a realistic HW-in-the-loop environment on four EPES protocols IEC-104, IEC61850 GOOSE, IEC61850 SV, and PTP. The captured dataset will allow to perform the necessary validation of the LADS technology and its efficiency in the detection of these attacks.
The datasets will also be published in a well-known dataset repository to allow other cybersecurity researchers to validate their AI/ML algorithms for anomaly or intrusion detection.

Across all test cases above, the PoI are defined along the three main lines:
PoI1: Characterization (definition) of a cyber attack on FuI.
PoI2: Verification of a cyber-attack impact on the substation monitoring and control tasks.
PoI3: Validation of the efficiency the LADS anomaly & intrusion detection technology on the detection of the given attack.

Thus, each test case will contribute to the generation of a dataset for the attack and protocol under consideration, and a short documentation on how to identify an attack and detect it. It will also include LADS validation results (KPI evaluation).

Test Specification

Reference to Test Case	Test Cases: 01, 02, 03, 04, 05
Title of Test	Validation of cybersecurity in a multi-substation environment.
Test Rationale	Define and learn the normal operation (traffic footprint) of a multi-substation environment. Detect and explain attacks on a SCADA digital substation by observing deviation from the normal operation.
Specific Test System (graphical)	Refer to next section.
Target measures	Collect datasets across the four EPES protocols IEC104, IEC61850 GOOSE, IEC61850 SV, and PTP. Validate LADS technology on these attacks and EPES testbed.
Input and output parameters	Input: Emulated substation traffic (normal legitimate), and Synthetic attack traffic injected into the substation normal traffic. Output: Datasets collected (from traffic captured), and Validation results of LADS performance on the detection of these attacks.
Test Design	See next section of topology.
Initial system state	Normal substations behavior and traffic
Evolution of system state and test signals	Traffic footprint changes under the four attack scenarios in the different test cases above.
Other parameters	N/A
Temporal resolution	N/A
Source of uncertainty	Devices firmware or manufacturer specific configurations
Suspension criteria / Stopping criteria	Attacks affect device's state significantly

Mapping to Research Infrastructure

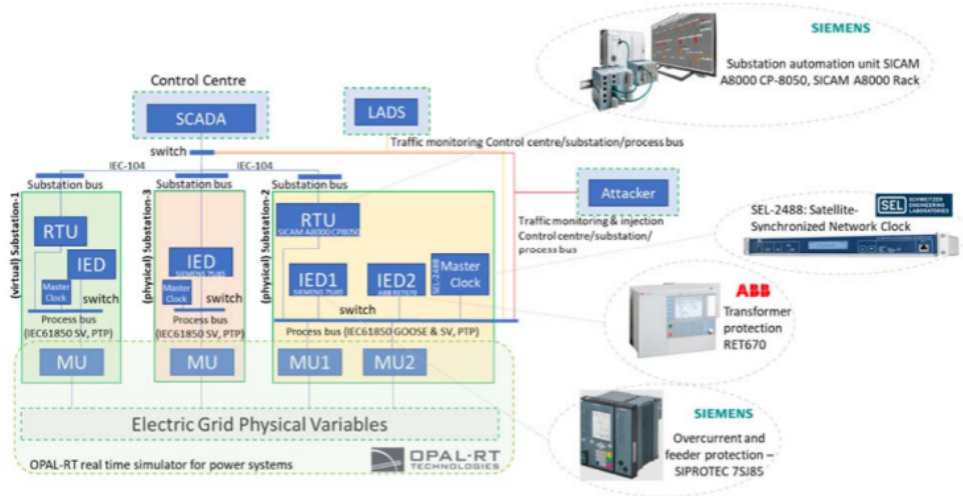

Figure 1. AID4EPES Research Infrastructure Architecture of a Multi-substation Environment (including hard-ware-in-the-loop workflow)

Figure 1 shows the research infrastructure of AID4EPES. It consists of a SCADA Control Center that communicates with three substations through the IEC104 protocol for monitoring and control tasks. There are two physically emulated substations with real HW-in-the-loop workflow specification, and one virtual substation with simulated components and traffic. We deployed three substations to present a wider and more appealing environment.
Each test case 01—05 above has been defined, i.e. its system under test (SuT) and function under investigation (FuI), according to the architecture in Figure 1. The figure illustrates where the LADS solution is morning on substation and process buses, where the attacker compromised machine is attacking on substation and process buses, and what devices and components the three substations consist of. We describe below the main components and interactions for each substation.

SETUP SUBSTATION-2 (physical):

- IED1 and IED2 publish GOOSE messages and an RTUs is a subscriber to those.
- MU1 and MU2 publish SV messages and IED1 and IED2 are the consumers of those.
- SV publisher for MU1 and MU2 is the real time simulator.
- RTU performs monitoring and control tasks with the SCADA control centre.
- RTU is a subscriber to GOOSE messages in the substation.
- PTP is available from the master clock device in the architecture.
- The subscriber for this PTP master clock is the IED1 (called "transparent clock")
- IED2 is communicated with the Master Clock with a direct (non-switch-based) line due to the ABB brand device setting.
- MU1 and MU2 are responsible for their breakers, respectively.

SETUP SUBSTATION-3 (physical):

- IED maps SV messages to IEC104 and communicates with the SCADA control centre for the monitoring and control tasks.
- IED is the responsible for the breaker in the substation.
- MU publishes SV messages and IED is the consumer.
- The real time simulator is the publisher of SV messages (on behalf of MU).
- PTP is available from a physical master clock device in the architecture.

SETUP SUBSTATION-1 (virtual): Monitoring and Control Tasks

- Virtual RTU, mapping of GOOSE to IEC104, and communicating with the SCADA control centre for monitoring and control tasks.
- RTU a subscriber for GOOSE messages.
- IED a publisher of GOOSE messages.
- MU publishes SV messages, and IED is the consumer.
- IED is a subscriber for SV.
- The real time simulator is the publisher of SV messages.

Experiment Specification

Reference to Test Specification	Test cases 01, 02, 03, 04, and 05
Title of Experiment	Validation of cybersecurity in a multi-substation environment.
Research Infrastructure	A Multi-substation Environment with hardware-in-the-loop workflow specification
Experiment Realisation	Collection of datasets representing a normal state, and state under different attacks (according to test cases 01, 02, 03, 04, 05). Each test case will realise: - Normal traffic collection (dataset, a pcap), - Attack traffic collection (dataset with more than one pcap of the different variances of the attack), - Attack definition, impact targeted by an attacker, indicators of compromise (IoCs on how to detect the attack), - LADS validation results on efficiency of detection (KPIs)
Experiment Setup (concrete lab equipment)	Figure 1 shows the equipment defined for the experimental setup. The various HW devices, real time simulator, and protocols used.
Experimental Design and Justification	The design is driven by the need to access and perform experiments on a realistic hardware-in-the-loop multi-substation environment. The aim is to determine how attack traffic footprint represents in such environment and differentiates from normal state. An attacker may target simultaneously multiple substations but different devices or protocols in each. The defined design will allow is to determine if we can detect such attacks. The targeted datasets of traffic capture will allow us to replay attacks and reevaluate results over time.
Precision of equipment and measurement uncertainty	PTP protocols is used to achieve the desired precision of time. The selected devices' HW allow to achieve certain level of precision as well, for instance on implementation of the IEC61850 GOOSE and SV protocol.
Storage of experiment data	Requires storing traffic capture of attacks from test cases 01, 02, 03, 04, 05. Approximately 20 GB+ of data storage is needed for the raw PCAP files, which will be curated to reduce size and unnecessary noise when published in a public repository.