
Verandering zonder Compromissen
PAC als Fundament van Betrouwbaarheid
8 april 2026
cigre
Nederland

Hoe check ik of mijn oplossing secure is?

Stefan Goeman, DNV

Ernst Wierenga, DNV

cigre Nederland

Context

Wat betekent een secure oplossing?

- Hardware security / software security / **communicatie beveiliging**
- Regelgeving (NIS2, CRA, NCCS)
- Internationale standaarden en best pratices
  - ISO 2700x reeks
  - IEC 62443 reeks
  - IEC 62351 reeks

Communicatie in elektriciteitsnetten

- Known vulnerabilities
- No encryption
- No RBAC
- …..

Grid operator
(DSO, TSO)

IEC 60870-5-101
IEC 60870-5-104
IEC 61850
DNP3

Substation

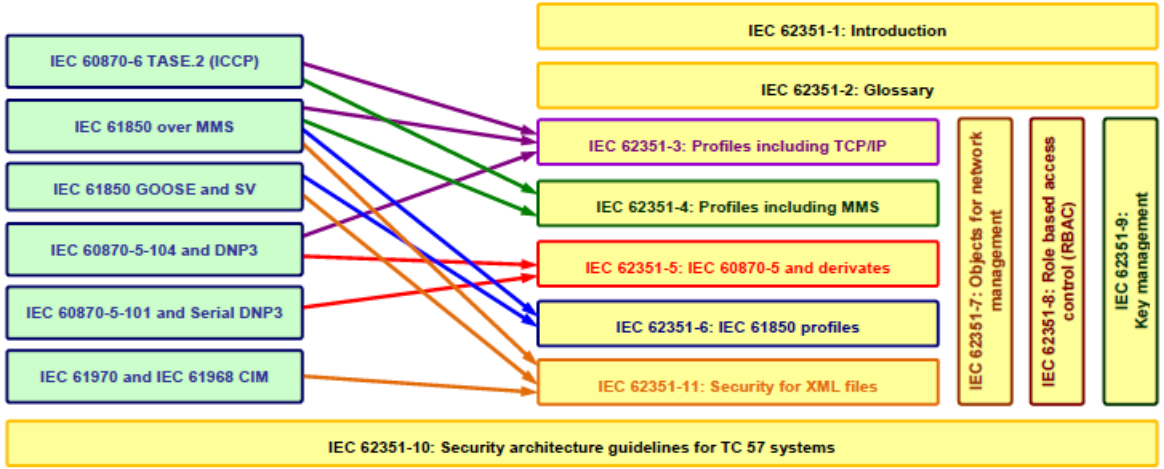
Distributes Energy Resources
(DER)

Storage

TC57/WG15: IEC 62351
Cyber Security

IEC 62351 - Beveiliging van communicatie in elektriciteitsnetten

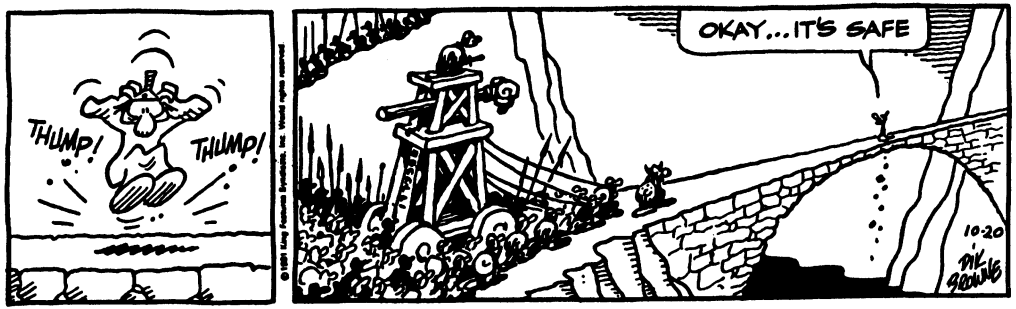
- Behandelt de beveiliging van de TC 57-protocollen.
  - IEC 60870-5 reeks
  - IEC 60870-6 reeks
  - IEC 61850 reeks
- Role-based Access Control
- Key management
- Security objectieven
  - Authenticatie van gegevensoverdracht
  - voorkomen van afluisteren
  - Voorkomen van afspelen en vervalsing…



Hoe IEC 62351 helpt bij de implementatie van aspecten van IEC 62443

IEC 62443-4-2 Foundational Requirement	IEC 62351 series
FR1 – Identification and authentication	IEC 62351-5, IEC 62351-4, IEC 62351-9
FR2 – Use Control	IEC 62351-8
FR3 – System Integrity	IEC 62351-4, IEC 62351-5, IEC 62351-6
FR4 – Data Confidentiality	IED 62351-3, IEC 62351-4, IEC 62351-5, IEC 62351-6
FR5 – Restricted data flow	IEC 62351-10
FR6 – Timely response to events	IEC 62351-7, IEC 62351-14
FR7 – Resource availability	IEC 62351-7

Conformance testing



"To properly evaluate a system, this should be tested under conditions as close as possible to those under which it will ultimately be used"

How to test a device (62351-100 series)

DUT and PICS – verify all the DUT documents

→

Execution of the test procedures defined in IEC 62351-100-3

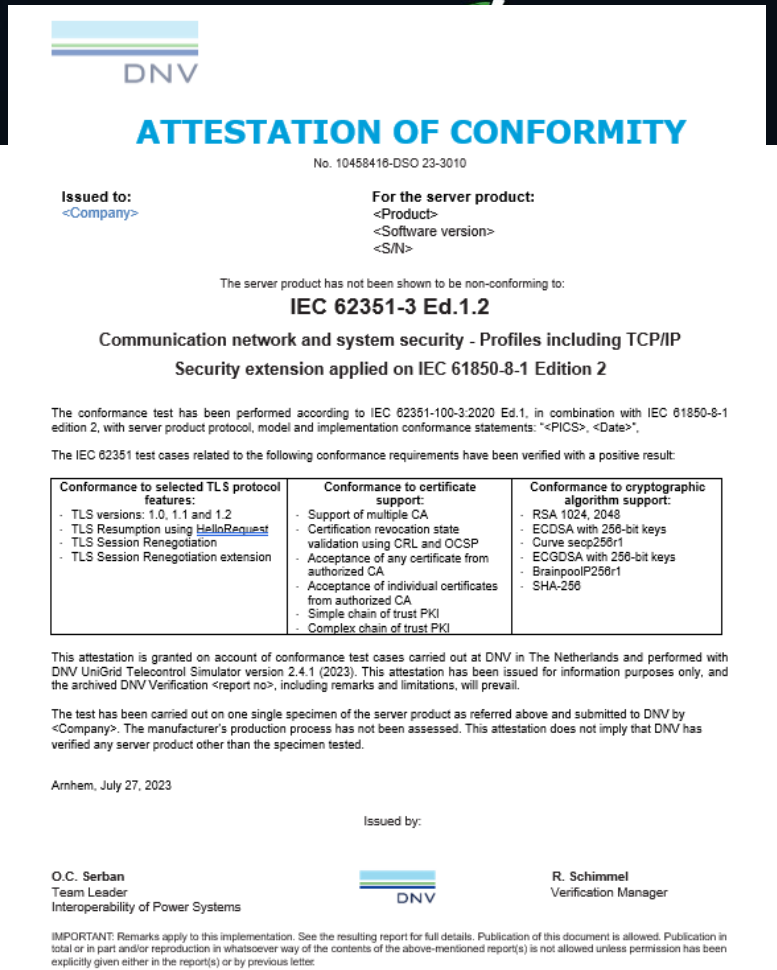
↓

Secure Application profile verification

IEC 61850-8-1

←

AoC and test report



DNV

ATTESTATION OF CONFORMITY

No. 10458416-DSO 23-3010

Issued to:
<Company>

For the server product:
<Product>
<Software version>
<S/N>

The server product has not been shown to be non-conforming to:

IEC 62351-3 Ed.1.2

Communication network and system security - Profiles including TCP/IP

Security extension applied on IEC 61850-8-1 Edition 2

The conformance test has been performed according to IEC 62351-100-3:2020 Ed.1, in combination with IEC 61850-8-1 edition 2, with server product protocol, model and implementation conformance statements: "<PICS>, <Date>",

The IEC 62351 test cases related to the following conformance requirements have been verified with a positive result:

Conformance to selected TLS protocol features:	Conformance to certificate support:	Conformance to cryptographic algorithm support:
· TLS versions: 1.0, 1.1 and 1.2 · TLS Resumption using HelloRequest · TLS Session Renegotiation · TLS Session Renegotiation extension	· Support of multiple CA · Certification revocation state validation using CRL and OCSP · Acceptance of any certificate from authorized CA · Acceptance of individual certificates from authorized CA · Simple chain of trust PKI · Complex chain of trust PKI	· RSA 1024, 2048 · ECDSA with 256-bit keys · Curve secp256r1 · ECGDSA with 256-bit keys · BrainpoolP256r1 · SHA-256

This attestation is granted on account of conformance test cases carried out at DNV in The Netherlands and performed with DNV UniGrid Telecontrol Simulator version 2.4.1 (2023). This attestation has been issued for information purposes only, and the archived DNV Verification <report no>, including remarks and limitations, will prevail.

The test has been carried out on one single specimen of the server product as referred above and submitted to DNV by <Company>. The manufacturer's production process has not been assessed. This attestation does not imply that DNV has verified any server product other than the specimen tested.

Arnhem, July 27, 2023

Issued by:

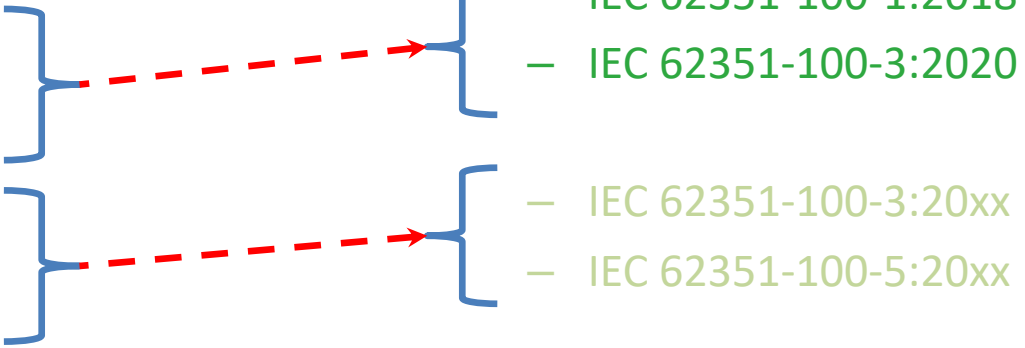
O.C. Serban
Team Leader
Interoperability of Power Systems

DNV

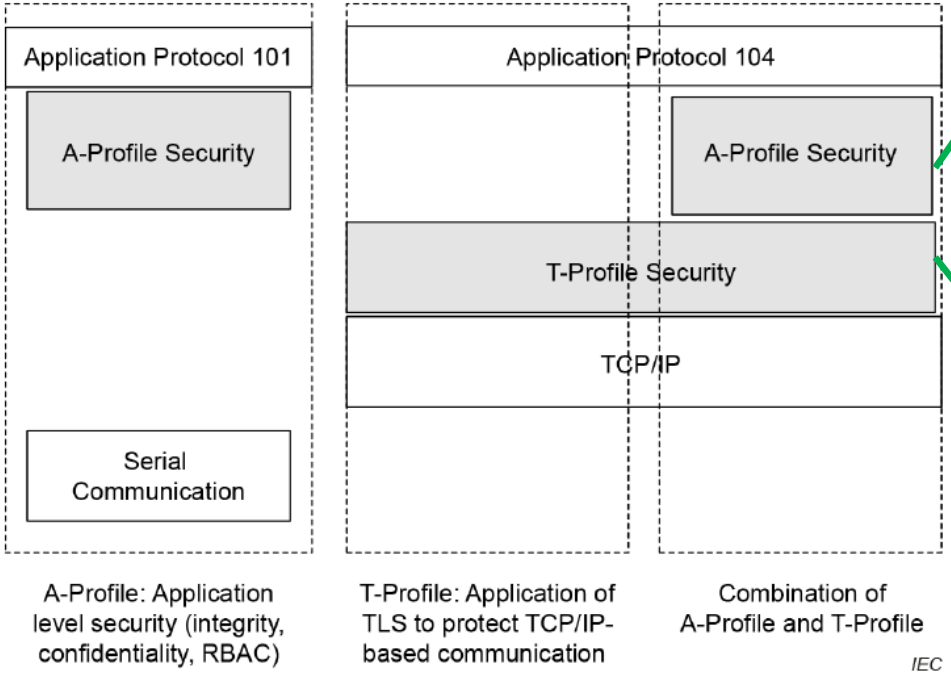
R. Schimmel
Verification Manager

Hoe IEC 60870-5-101/104 beveiligen?

- IEC 60870-5-101 & IEC 60870-5-104
  - Test procedures: IEC 60870-5-601 & IEC 60870-5-604
- Hoe IEC101 & IEC104 beveiligen wordt beschreven in
  - IEC 60870-5-7:2013
  - IEC 62351-3:2014
  - IEC 62351-5:2013
  - IEC 60870-5-7:2025
  - IEC 62351-3:2022
  - IEC 62351-5:2023
- Testen van de security uitbreidingen wordt beschreven in
  - IEC 62351-100-1:2018
  - IEC 62351-100-3:2020
  - IEC 62351-100-3:20xx
  - IEC 62351-100-5:20xx



Hoe IEC 60870-5-101/104 beveiligen?



IEC 62351-5:2023

- Eigen security procedures
- Station association procedure
- Session key change procedure
- Secure data exchange

IEC 62351-3:2022

- Profiel van TLSv1.2 en TLSv1.3

Hoe IEC 61850 MMS beveiligen?

- IEC IS 62351-4:2020 Ed. 1.0, “Power systems management and associated exchange – Data and communication security – Part 4: Profiles including MMS and derivatives”
- IEC TS 62351-100-6:2022 Ed. 1.0, “Power systems management and associated exchange – Data and communication security – Part 100-4: Cybersecurity conformance testing for IEC 62351-4”
- UCA – Conformance Test Procedures for IEC 61850-8-1 MMS Server Devices with IEC 62351-4 Edition 1 with Amendment 1 E2E security interface

Hoe IEC 61850 MMS beveiligen?

Application Security	A-security profile	None	A-security profile	E2E security without encryption	E2E security without encryption	E2E security with encryption	E2E security with encryption
Transport Security	none	TLS	TLS	none	TLS	none	TLS
Note	Note 1	Note 2		Note 3		Note 4	

For the application of the T-security, TLS is expected to be used as specified in 6.3 for the OSI operational environment. For other environments, TLS usage is outside the scope of this document and specified by the referencing standard.

Note 1: Using the A-security profile alone without TLS results in a non-secure system.

Note 2: Using TLS with or without the A-security profile gives a reasonable security assuming that all other security measures are observed, including use of secure TLS cipher suits and that the communication is peer-to-peer without intermediate entities. In addition to the authentication provided by TLS, the use of the A-security profile allows for authentication at the application layer of application entities.

Note 3: Using E2E security without encryption with or without TLS provides for mutual authentication and end-to-end integrity protection and thus reasonable security providing that confidentiality is not required and that other security measures are observed. Use of TLS fulfils confidentiality (encryption) an integrity protection on transport layer hops should the E2E security be compromised.

Note 4: As for note 3 with addition of end-to-end encryption (confidentiality).

Hoe IEC 61850 GOOSE en SV beveiligen?

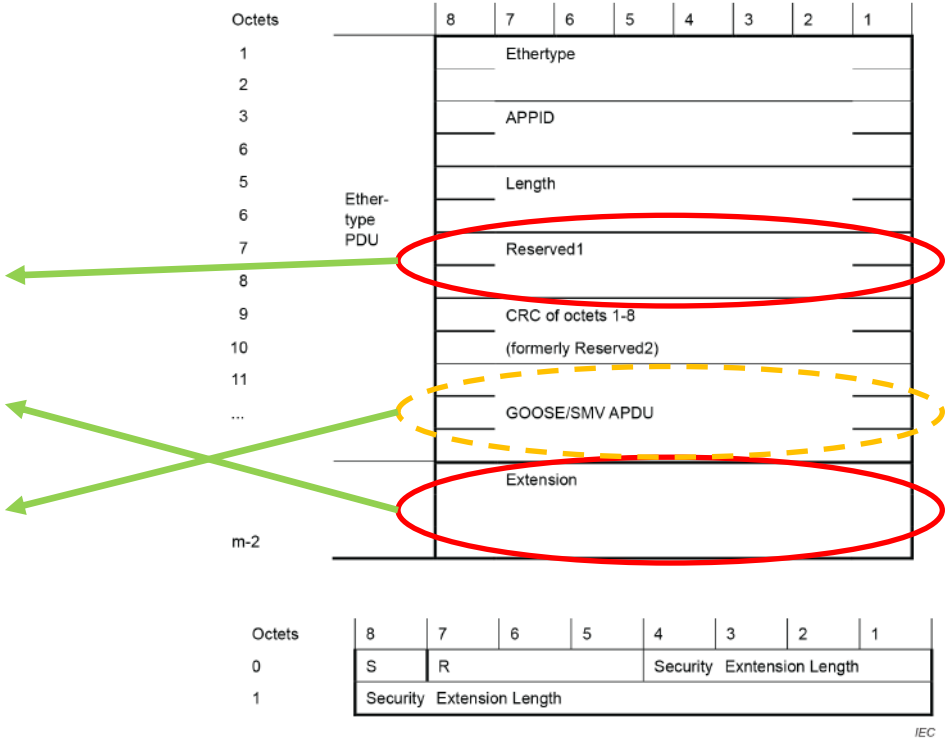
- IEC IS 62351-6:2020 Ed. 1.0, “Power systems management and associated exchange – Data and communication security – Part 6: Security for IEC 61850”
- IEC TS 62351-100-6:2022 Ed. 1.0, “Power systems management and associated exchange – Data and communication security – Part 100-6: Cybersecurity conformance testing for IEC 61850-8-1 and IEC 61850-9-2”

Hoe IEC 61850 GOOSE en SV beveiligen?

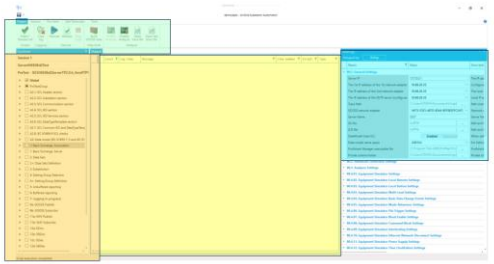
Aanpassingen in het ethernet frame

- Reserved1 veld geeft de lengte van het Extension veld
- Extenstion veld heeft een MAC waarde (authenticatie)
- Encryptie (AES-GCM) van GOOSE of SV enkel voor R-GOOSE en R-SV

(Zie IEC 62351-6)



IEC 61850: Test Plan



After the DUT documentation analysis:

- Test Plan definition
- Test selection from test the procedure:

UCA Conformance Test Procedures

Server Devices with IEC 61850-8-1 Edition 2 interface

Revision 2.0.6

Detailed test procedures

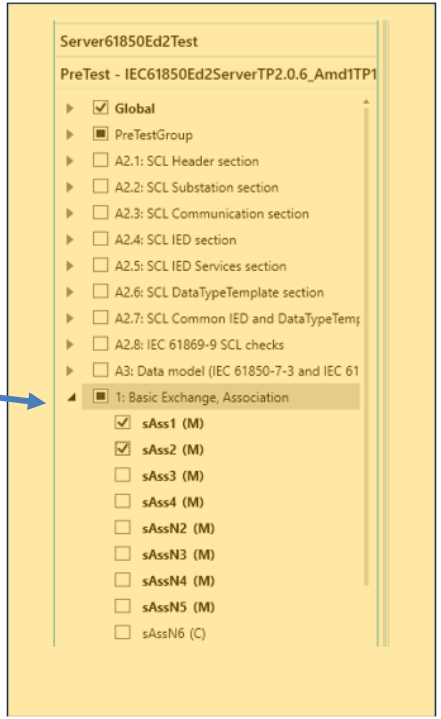
sAss1	Associate and client-release a TPAA association	☐ Passed ☐ Failed ☐ Inconclusive

IEC 61850-7-2 Subclause 8.3.2
IEC 61850-8-1 Subclause 10.2

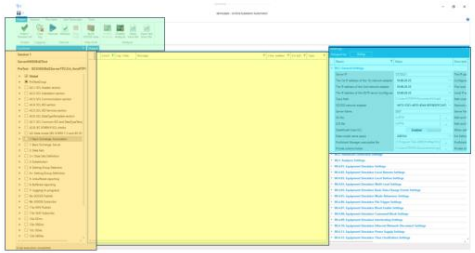
Expected result
2. DUT sends Associate response+
3. DUT sends Release response+

Test description
1. Configure the Client and DUT with the correct association and authentication parameters
2. Client request Associate
3. Client request Release
4. Repeat steps 2 and 3 250 times

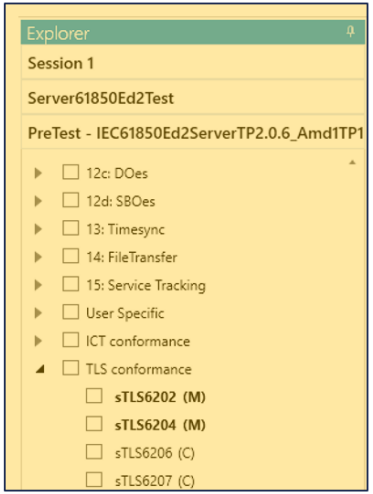
Comment

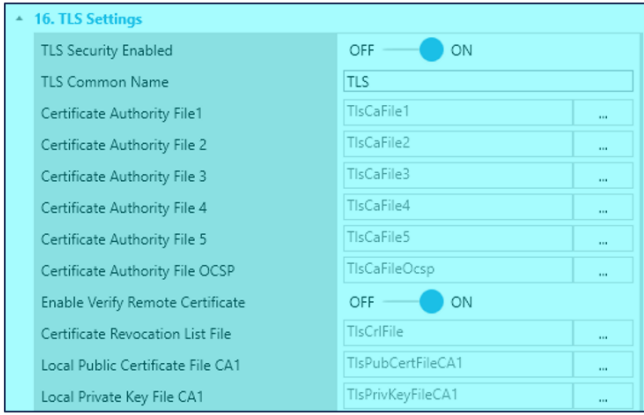


IEC 62351-100-3 Test Plan



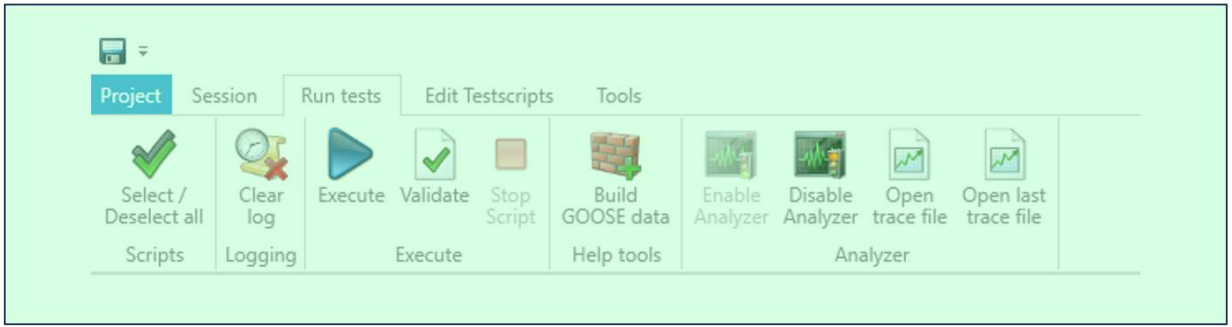
- IEC 62351-3 provides a TLS layer
- IEC 61850 run on top of the TLS layer
- The test tool and the DUT are configured with IEC 62351-3 settings
- IEC 61850 can be tested in the same way showed in the previous slides
- IEC 62351-3 can be tested according to its test procedure (IEC 62351-100-3)

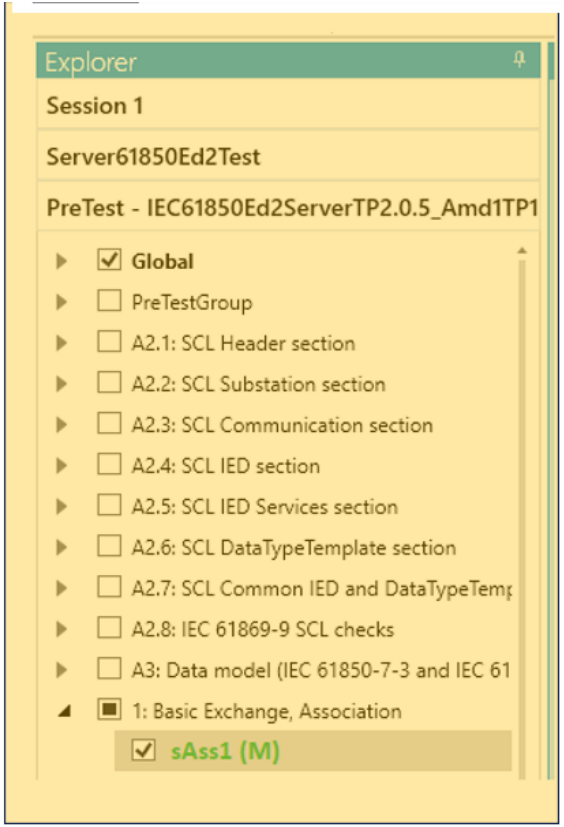




Test tool execution

- Test run/stop
- Packet Analyzer: Traces
- Test result (green - passed, red – failed)





Status DNV Test tools – security uitbreidingen (planning)

- TLS module: Eind 06/2026. Deze is nodig voor secure IEC101/IEC104 en secure MMS
- Secure IEC101/104: Eind 07/2026
- Secure MMS: Eind 11/2026
- Secure R-GOOSE (+KDC client): 09/2026

IEC security testing standaarden losen niet alles op

IEC IS 62351-9:2020 Ed. 1.0, “Power systems management and associated exchange – Data and communication security – Part 9: Cybersecurity key management for power system equipment”

- Certificate management (kan mbv EST en SCEP)
  - Momenteel geen interesse om hier testen voor te ontwikkelen
- Group key management (nodig voor secure SV en secure GOOSE)
  - In de toekomst zal er een test standard komen
- IEC 62351-100-9? Wat en wanneer?

Dus, geen testen voor het beheren van certificaten?

- Volgens IEC 62351-9 kan/moet het beheer van certificaten m.b.v. EST (of SCEP)
- Maar,
  - EST is slechts een protocol dat de berichten beschrijft die worden uitgewisseld tussen een EST-client en een EST-server.
  - EST specificeert geen clienttoepassing voor het beheren van (apparaat)certificaten.
  - Het apparaat moet zelf op tijd een nieuw certificaat aanvragen. Wil je dat?
- Wat gebeurt er bij CA roll-over? (tikkende tijdbom?)

BEDANKT VOOR JULLIE AANDACHT

cigre Nederland