

15 april 2025

Beveiliging ontrafeld

Uitgelegd wat je altijd al wilde weten

Test strategieën voor IEC61850 in slimme hoogspanningstations





Wie zijn wij



Robbert Koenderman
Senior PAC Engineer bij Qirion (Alliander)



Milan Jankovski
Engineer Beveiligingssystemen bij Stedin



Inhoud

- 'Waarom' IEC61850 in hoogspanningsstation
- Testen van stationsautomatisering configuraties met IEC61850 (Qirion)
- Testen van beveiligingsfuncties met IEC61850 (Stedin)



Inleiding 'Waarom IEC61850'

- Toepassen van 'top-down engineering'. Eerst functioneel ontwerp maken hardware keuze komt later.
- Beter toepassen van systeem typicals en templates, snellere engineering/configureren van systemen.
- Interoperabiliteit, IED's van verschillende leveranciers kunnen met elkaar communiceren.
- Verminderde bekabelingskosten, informatie wordt uitgewisseld via een netwerk.

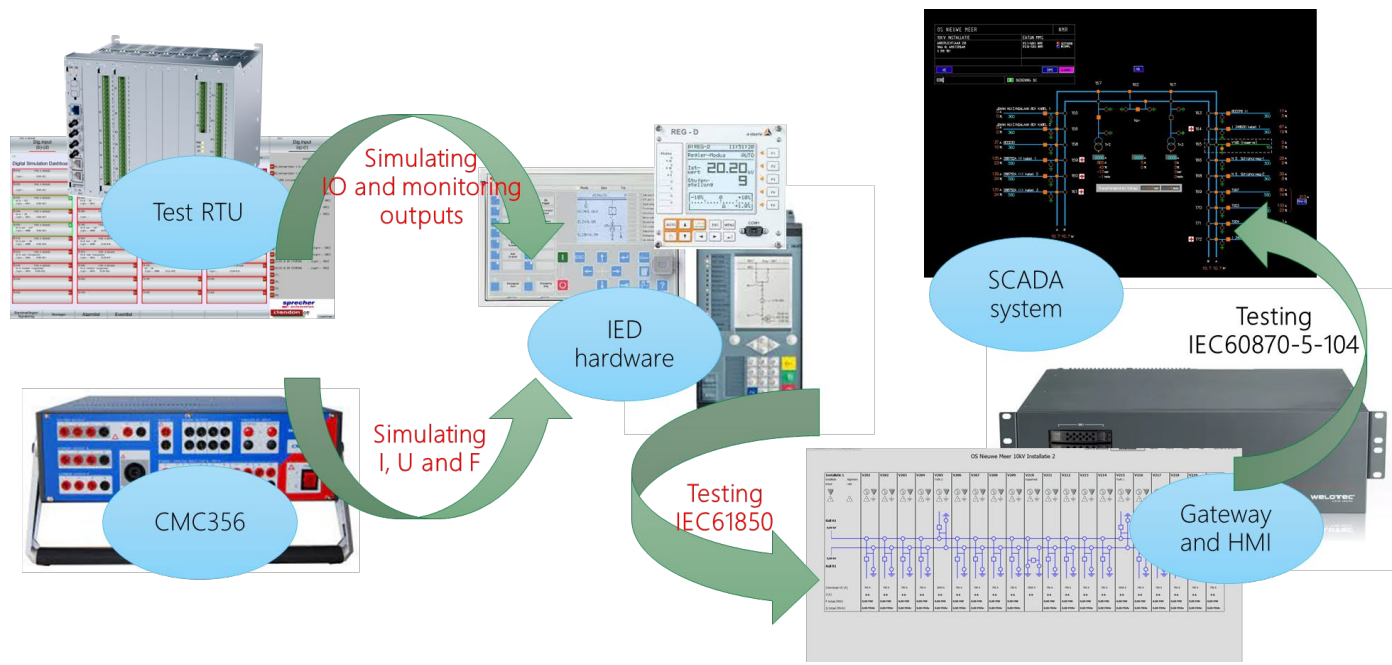


Testen van stationsautomatisering configuraties met IEC61850

- Conventioneel testen van SA systemen
- Testen op basis van IEC61850 m.b.v. stationscout
- Automatisch testen (closed loop) m.b.v. IEC61850



Conventioneel testen van SA systemen





Conventioneel testen van SA systemen

Voordelen;

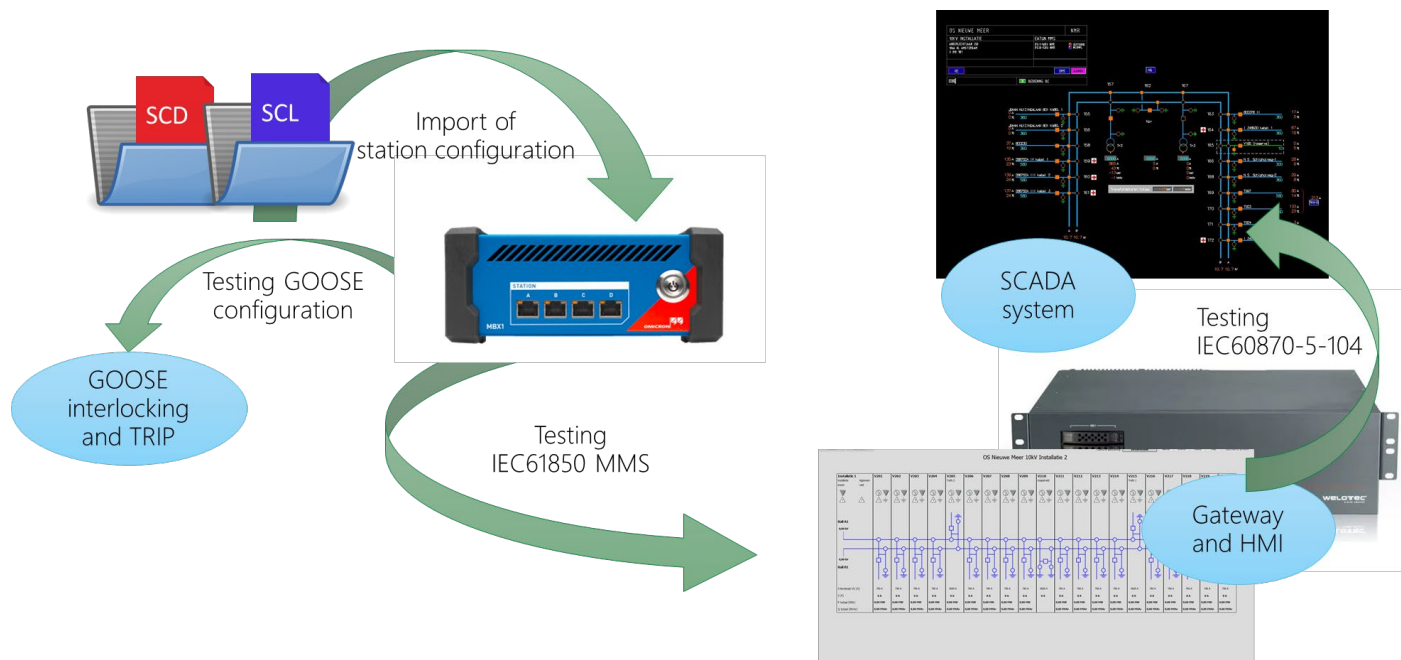
- Wanneer je een fysieke IED gebruikt, dan test je de volledige configuratie
- End-to-end test van hardware tot Scada
- Mogelijkheid tot testen logische blokken in IED
- Vooraf testen van een configuratie in een veilige omgeving
- Bij voorkeur toegepast voor testen nieuwe en aangepaste typicals
- Reduceert SAT test tijd

Nadelen;

- Test RTU is gelimiteerd tot vijf IEDs, na het testen dienen de IED opnieuw geladen te worden. Dit kost tijd
- GOOSE configuratie voor schakelvoorwaarden kan niet volledig getest worden.
- GOOSE configuratie in bestaande stations kan niet getest worden
- Het bouwen van een test omgeving kost tijd (en geld)



Testen op basis van IEC61850 m.b.v. stationscout







Testen op basis van IEC61850 m.b.v. stationscout

Voordelen;

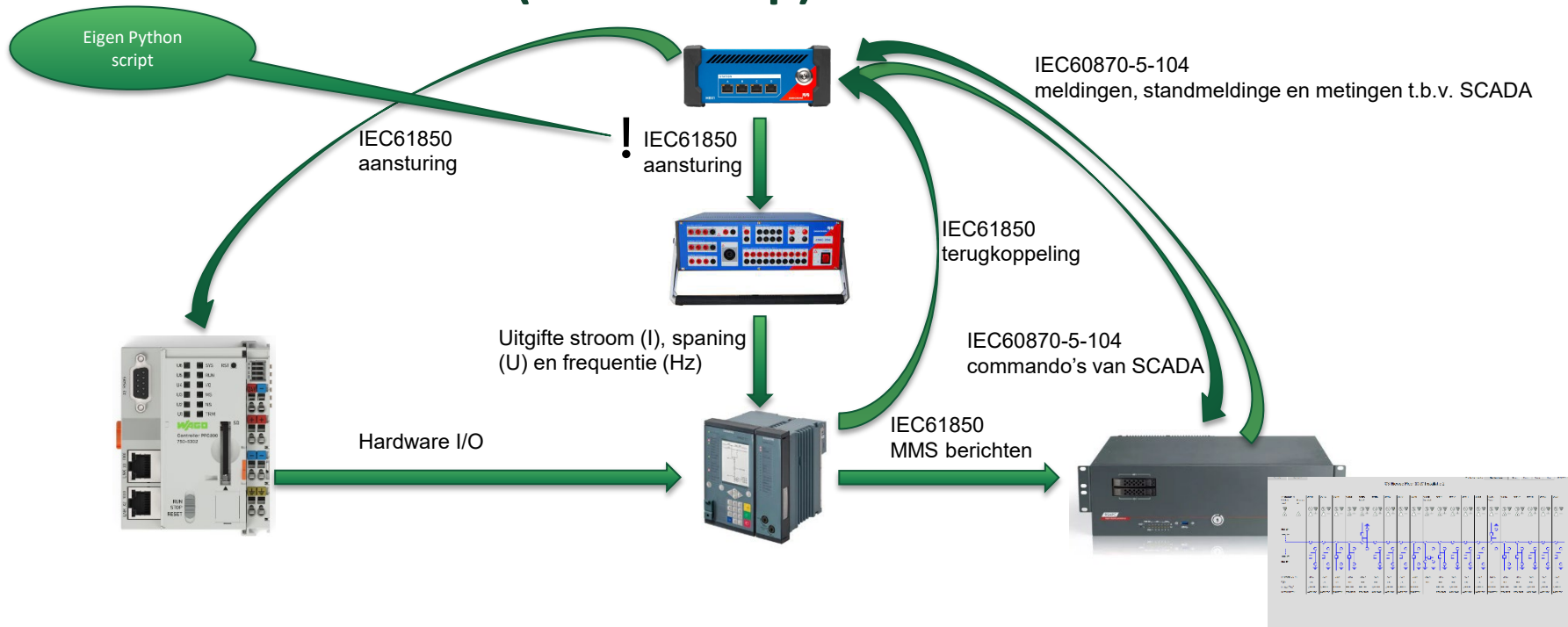
- Complete station simulatie voor het testen, dit scheelt tijd
- End-to-end test van software IED tot SCADA mogelijk, incl. IEC104 terug koppeling
- Geen fysieke componenten nodig, dit bespaart enorm budget
- Eenvoudig simuleren van signalen, metingen en status van IED
- Schakelvoorwaarden d.m.v. GOOSE kan eenvoudig getest worden
- Reduceert SAT test tijd
- Uitbreidingen in een bestaan IEC61850 station kan volledig getest worden. Ook als de bestaande IED niet meer voorhanden zijn.
- Vooraf testen van een configuratie in een veilige omgeving

Nadelen;

- Logische blokken in een IED kunnen niet getest worden, maar in theorie is dat tijdens een typical test al gedaan



Automatisch testen (closed loop) m.b.v. IEC61850





Automatisch testen (closed loop) m.b.v. IEC61850

Voordelen;

- End-to-end test van software IED tot SCADA mogelijk, incl. IEC104 terug koppeling
- Eenvoudig simuleren van signalen, metingen en status van IED
- Wanneer je een fysieke IED gebruikt, dan test je de volledige configuratie
- Mogelijkheid tot testen logische blokken in IED
- Bij voorkeur toegepast voor testen nieuwe en aangepaste typicals
- Testen van typicals indien nieuwe firmware ge-released is door leverancier
- Volledige test van IED in 30 min mogelijk

Testscript op de Stationscout

CURRENTA			
1.2	stroom uitgang A L1	⌚ 01:00:00	1
0	stroom uitgang A L1 hoek	⌚ 01:00:00	
1	stroom uitgang A L2	⌚ 01:00:00	2
180	stroom uitgang A L2 hoek	⌚ 01:00:00	3
0	stroom uitgang A L3	⌚ 01:00:00	
0	stroom uitgang A L3 hoek	⌚ 01:00:00	

<- Control signals, naar CMC testkoffer

Testcase met alle test stappen ->

Group indicat.			
False	MST bev uitcommando [615] 1J- V501	⌚ 11:53:27	
True	MST bev fase 3 aangespr [603] 2J- V501	⌚ 11:55:21	
False	MST bev fase 7 aangespr [607] 2J- V501	⌚ 11:55:21	
False	MST bev fase 11 aangespr [611] 2J- V501	⌚ 11:55:21	
False	Aardfout bev aangespr [616] 2J- V501	⌚ 11:55:21	

<- Assessment signals, van IED

Overview		Watchlist
LIP_K05Q01A1		Control IO kar/IED 70
Details		
Status:	Passed	
Executed:	2025-04-07 11:55:28.408+02:00	
Settings		
Test type:	Logic	
Automated control:	On	
Automated assessment:	On	
Test steps		26
Test step 1	2025-04-07 11:54:17.652+02:00	
Test step 2	2025-04-07 11:54:19.893+02:00	
Test step 3	2025-04-07 11:54:22.066+02:00	
Test step 4	2025-04-07 11:54:24.224+02:00	
Test step 5	2025-04-07 11:54:26.385+02:00	
Test step 6	2025-04-07 11:54:28.545+02:00	
Test step 7	2025-04-07 11:54:30.709+02:00	
Test step 8	2025-04-07 11:54:32.881+02:00	
Test step 9	2025-04-07 11:54:36.063+02:00	
Test step 10	2025-04-07 11:54:38.351+02:00	
Test step 11	2025-04-07 11:54:40.505+02:00	
Test step 12	2025-04-07 11:54:42.670+02:00	
Test step 13	2025-04-07 11:54:44.913+02:00	
Test step 14	2025-04-07 11:54:47.078+02:00	
Test step 15	2025-04-07 11:54:49.254+02:00	
Test step 16	2025-04-07 11:55:10.736+02:00	
Test step 17	2025-04-07 11:55:13.027+02:00	
Test step 18	2025-04-07 11:55:15.300+02:00	
Test step 19	2025-04-07 11:55:16.408+02:00	
Test step 20	2025-04-07 11:55:17.526+02:00	
Test step 21	2025-04-07 11:55:18.621+02:00	
Test step 22	2025-04-07 11:55:19.744+02:00	
Test step 23	2025-04-07 11:55:20.834+02:00	
Test step 24	2025-04-07 11:55:22.007+02:00	
Test step 25	2025-04-07 11:55:27.225+02:00	
Test step 26	2025-04-07 11:55:28.408+02:00	
Execute test case		▶



System diagram

Search

Devices

IP - Substation generated ...

Overview

IP - MISC0001
Control IO kar/IED 70

Details

Status: Not executed

Settings

Test type: Single

Automated control: On

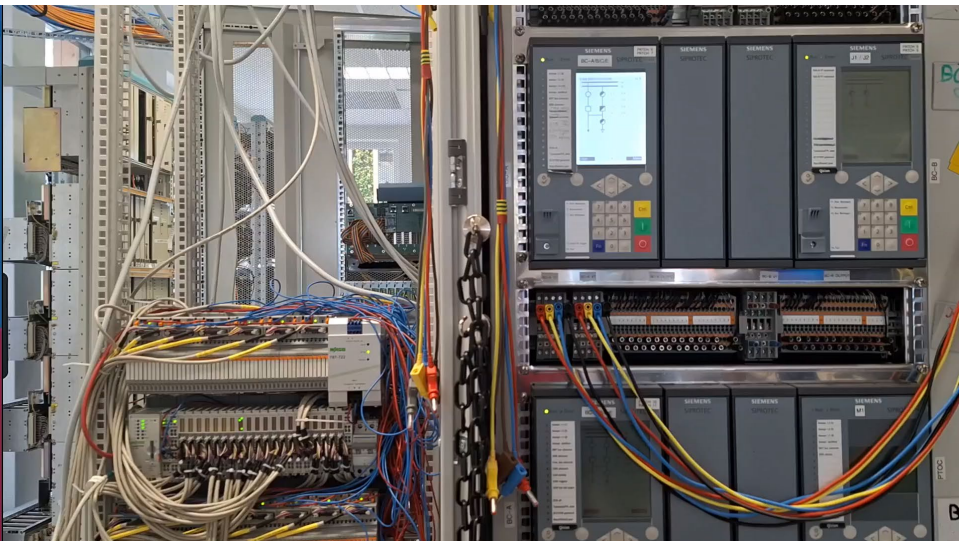
Automated assessment: On

Test steps

- Test step 1
- Test step 2
- Test step 3
- Test step 4
- Test step 5
- Test step 6
- Test step 7
- Test step 8
- Test step 9
- Test step 10
- Test step 11
- Test step 12
- Test step 13
- Test step 14
- Test step 15
- Test step 16
- Test step 17
- Test step 18
- Test step 19
- Test step 20
- Test step 21
- Test step 22
- Test step 23
- Test step 24
- Test step 25

Execute test case

Live status: On 15:48 CB235N



IEC 61850 in beveiliging testen

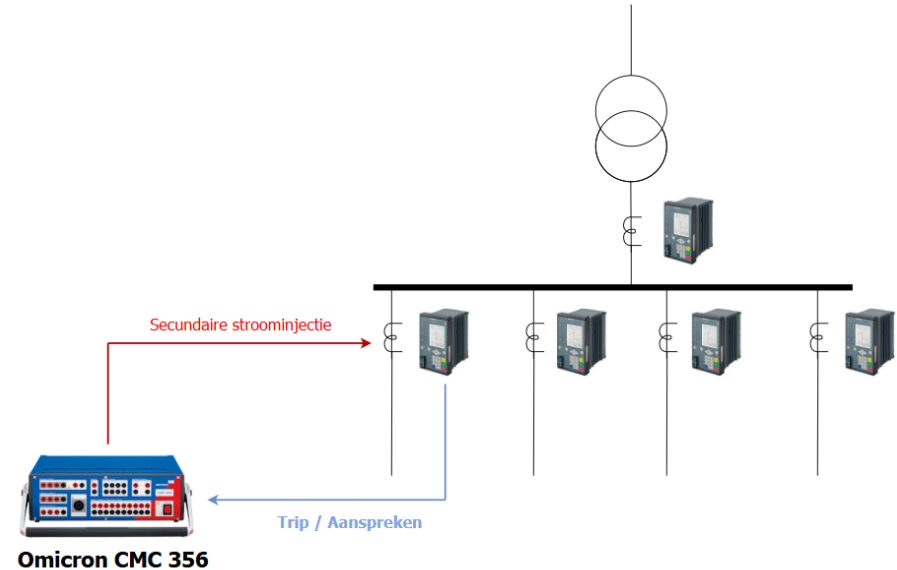
- Manieren van testen
 - Hoe gebruiken wij IEC 61850 voor slimme testen
 - Voordelen van IEC61850 gebaseerd testen
 - Voorbeeld
-
- **DISCLAIMER:** In deze presentatie, wij praten alleen over GOOSE berichten (nog niet over SV)

Beveiliging testen – wat willen wij testen?

- Of de beveiliging werkt of werkt niet – stabiel situatie vs fout
- Of de juiste beveiligingsfunctie werkt – trip signaal per functie
- Hoe snel werkt de beveiliging – tijd criteria

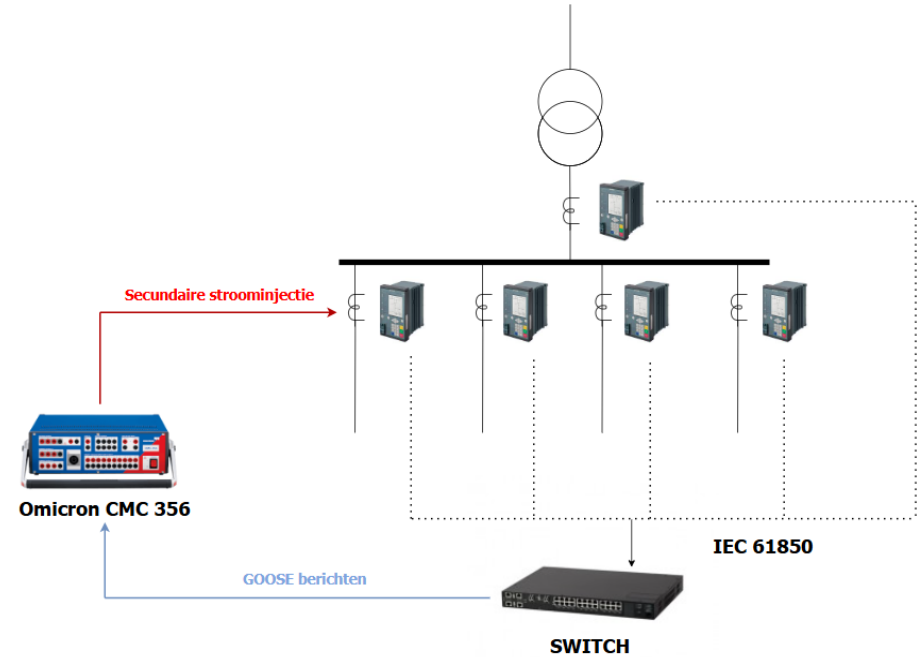
Manieren van testen

- Hard-wired
 - Elke functie (bv. $I>$, $Ie>$, $I>>...$) stuurt een Aanspreken (Start) en Trip (Operate) signaal
 - Het IED heeft meestal maar één Aanspreken en één Trip BO
 - Conflicterende functies moeten soms worden “uitgeschakeld” tijdens het testen
 - Testen van gedistribueerde beveiligingsconcepten is complex en kost veel tijd



Manieren van testen

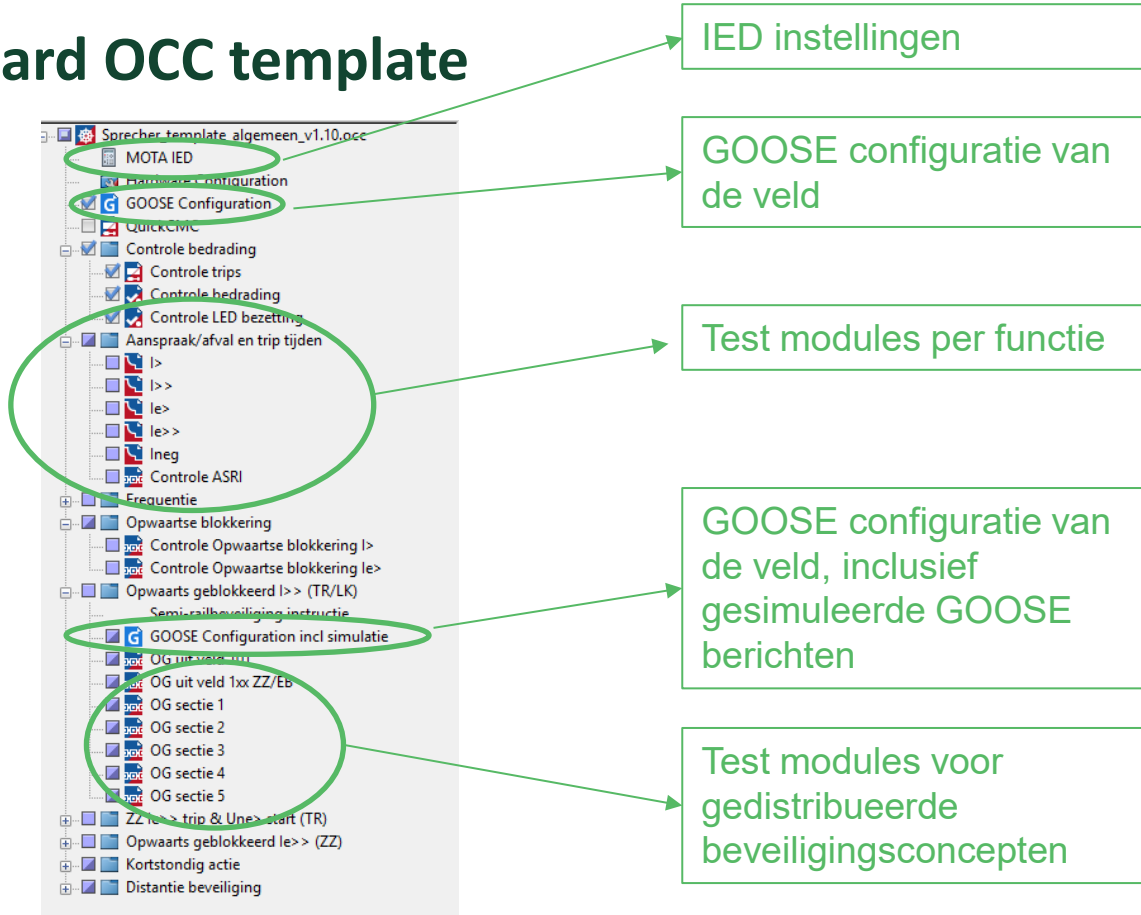
- IEC 61850
 - Elke functie (bv. $I>$, $Ie>$, $I>>...$) stuurt een Aanspreken (Start) en Trip (Operate) signaal die uniek voor de functie is – geen probleem met conflicterende functies
 - Subscription, maar ook simulatie van GOOSE berichten is wel mogelijk
 - Testen van gedistribueerde beveiligingsconcepten is makkelijker en kost minder tijd



Hoe gebruiken wij IEC 61850 voor beveiliging testen

- Standard OCC template – met IEC 61850 configuratie modules
- Python tooling – automatisatie van het process
- Subscription en simulatie van GOOSE berichten

Standard OCC template



Python tooling



GOOSE configuratie module

```
<?xml version="1.0" encoding="UTF-8"?>
<SCL xmlns="http://www.iec.ch/61850/2003/SCL" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" revision="B" version="2007">
  <Header id="" revision="1" toolID="SPRECON-E IEC61850 Mapper 2.34 SP1 (3099)" version="1">
    <History>
      <Item revision="1" version="1" what="Initial creation of model." when="2022-12-02 15:15:10" who="SPRECON-E IEC61850 Mapper 2.34 SP1 (3099)" user="Veikko.Pluijm" resources="com.sprecher.easyeng.resources-7.0.10.v2021112">
```

- 9 - Bin. In. 9
- 10 - GOOSE Prot ready
- 25 - GOOSE CO1
 - Boolean - RDM_ALX_023_Veld405_C_PROT/CO1PTRC1.Op.general
- 26 - GOOSE Start L1
 - Boolean - RDM_ALX_023_Veld405_C_PROT/VSPTOC1.Str.phsA
- 27 - GOOSE Start L2
 - Boolean - RDM_ALX_023_Veld405_C_PROT/VSPTOC1.Str.phsB
- 28 - GOOSE Start L3
 - Boolean - RDM_ALX_023_Veld405_C_PROT/VSPTOC1.Str.phsC
- 29 - GOOSE Start I>
 - Boolean - RDM_ALX_023_Veld405_C_PROT/IGPTOC1.Str.general
- 30 - GOOSE Trip I>
 - Boolean - RDM_ALX_023_Veld405_C_PROT/IGPTOC1.Op.general
- 31 - GOOSE Start I>>
- 32 - GOOSE Trip I>>
- 33 - GOOSE Blok I>>
- 34 - GOOSE Start Ie>
- 35 - GOOSE Trip Ie>



<P type="APPID">0008</P>

- GOOSE signalen per functie
 - Kunnen als “triggers” in verschillende beveiligingen modules gebruikt worden
- an de IEC 61850 in het station
- De module reageert alleen op de I> functie

Maar ook.... Simulatie van GOOSE berichten

Test View: GOOSE Configuration incl simulatie in Station _TT071_SG1_10_V107

Subscriptions Simulations

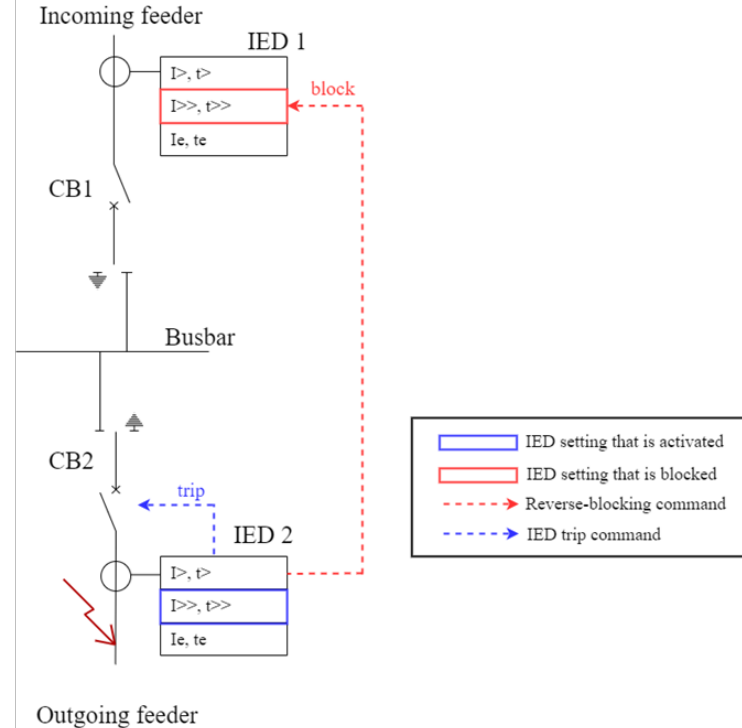
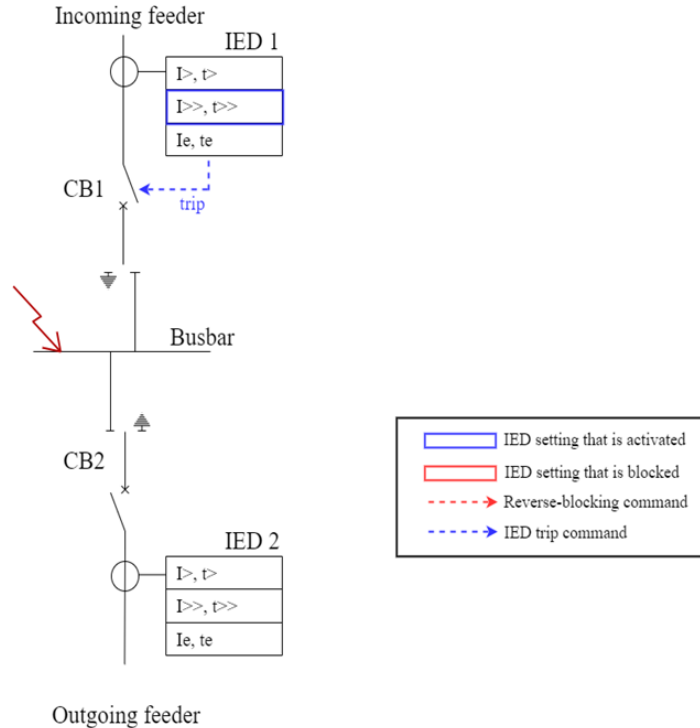
Outputs

- 1 - Bin. Out. 1
- 2 - Bin. Out. 2
- 3 - Bin. Out. 3
- 4 - Bin. Out. 4
- 5 - Bin. Out. 5
- 6 - Bin. Out. 6
- 7 - Bin. Out. 7
- 8 - Bin. Out. 8
- 25 - 101 Start
- Boolean - UTR_BLMD_010_Veld101_C_PROT/IGPTOC1.Str.general
- 26 - 101 prot ready
- Boolean - UTR_BLMD_010_Veld101_C_PROT/GLOBALGGIO1.SPCSO7.stVal
- 27 - 102 Start
- Boolean - UTR_BLMD_010_Veld102_C_PROT/IGPTOC1.Str.general
- 28 - 102 prot ready
- Boolean - UTR_BLMD_010_Veld102_C_PROT/GLOBALGGIO1.SPCSO7.stVal
- 29 - 103 Start
- 30 - 103 prot ready
- 31 - 104 Start

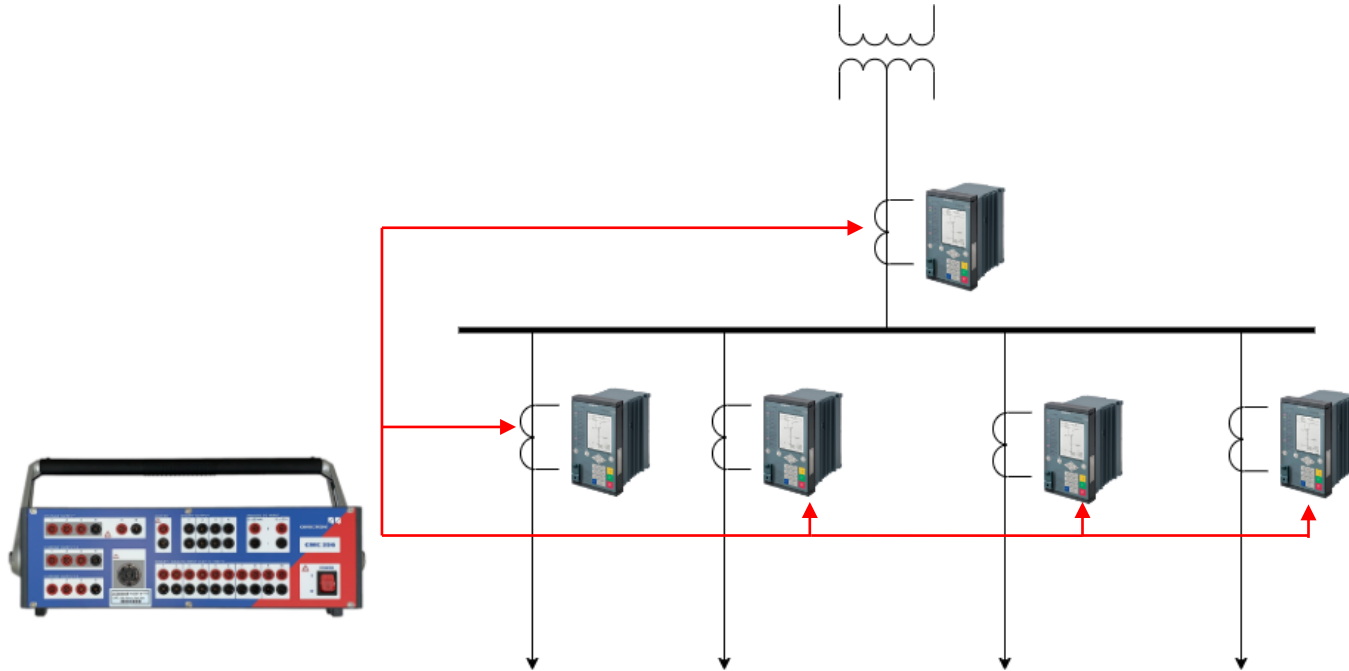
DA DA

- Simulatie van andere IEDs van het station
- Mogelijk "manipulatie" van verschillende IEDs

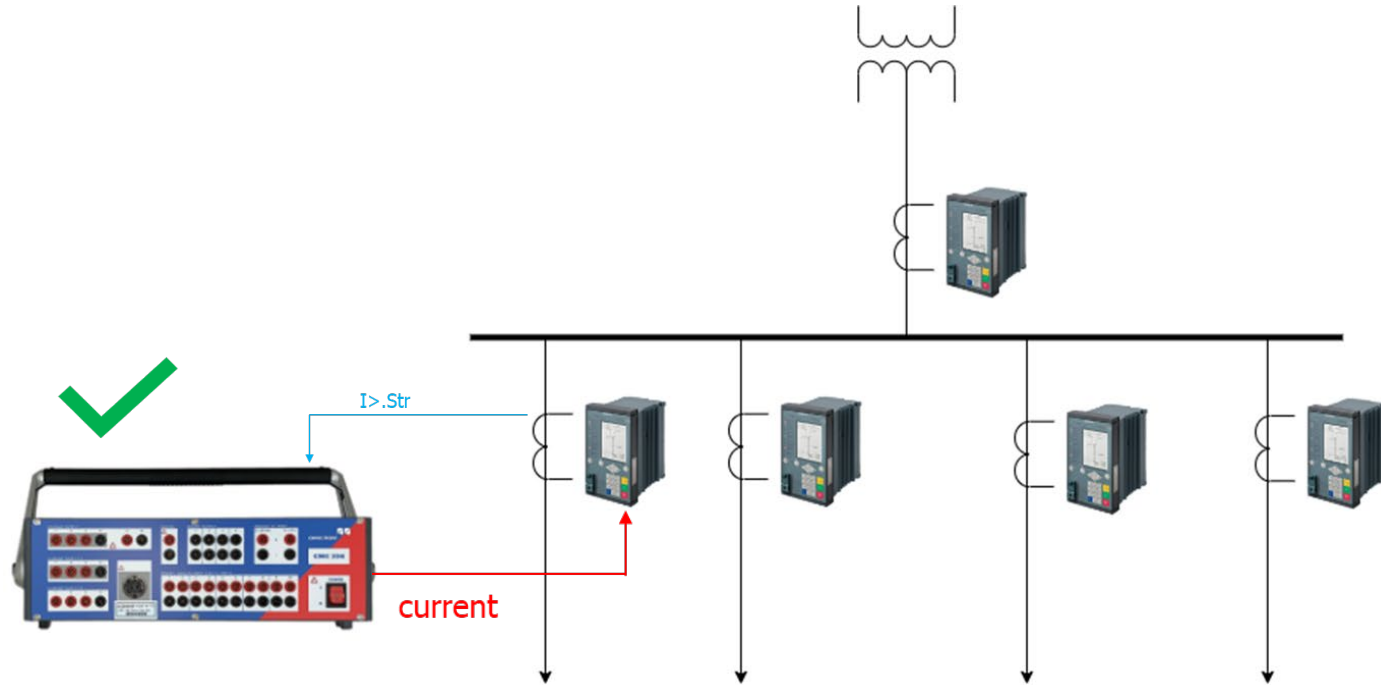
Voorbeeld: Opwärts-blokkering scheme (theorie)



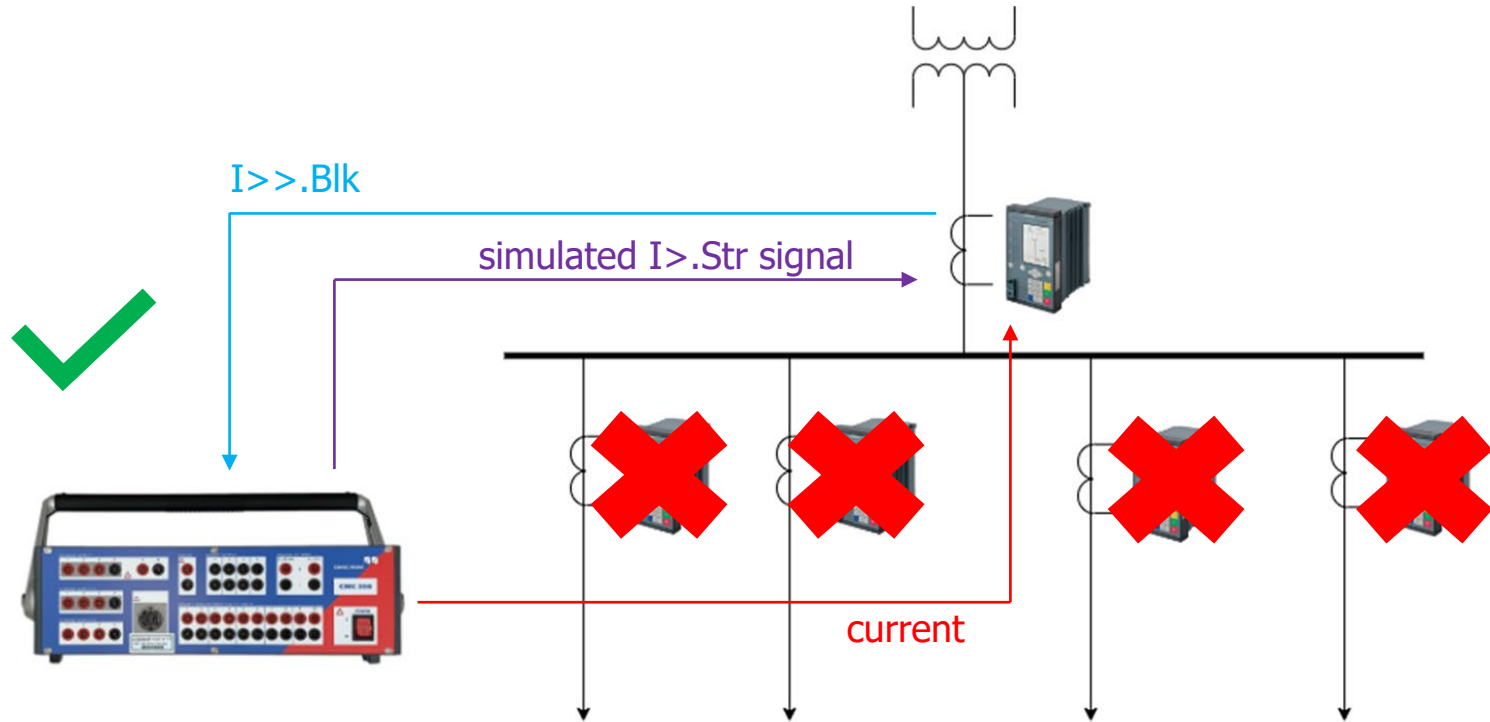
Opwards-blokkering scheme – Hard-wired testing



Opwards-blokkering scheme – GOOSE testing



Opwards-blokkering scheme – GOOSE testing





Samenvatting

- IEC 61850 is de "nieuwe" realiteit – ook tijdens testen
- SA testen kunnen worden uitgevoerd zonder alle fysieke componenten
- Automatisch end-to-end (IED tot en met SCADA) SA testen is mogelijk, op een snelle en eenvoudige manier
- Sneller en gevoeliger testen van beveiligingsfuncties door gebruik te maken van GOOSE-signalen als triggers
- Het testen van gedistribueerde beveiligingsconcepten is eenvoudig en snel (met de juiste testopstelling en plan)

**BEDANKT
VOOR UW
AANDACHT**

