Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch

CLAROTY SIEMENS

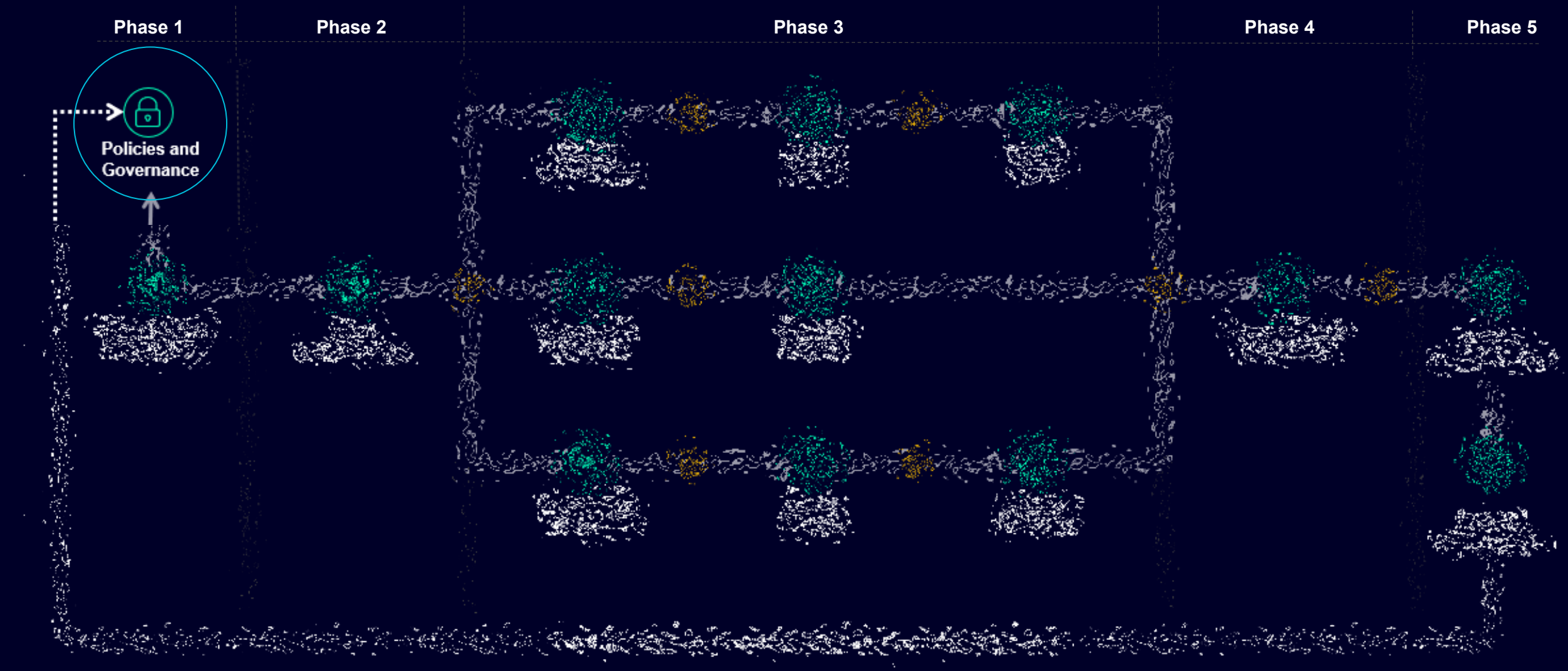
No technology without a plan

Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch

CLAROTY SIEMENS

OT security Journey



Industrial Cyber Security

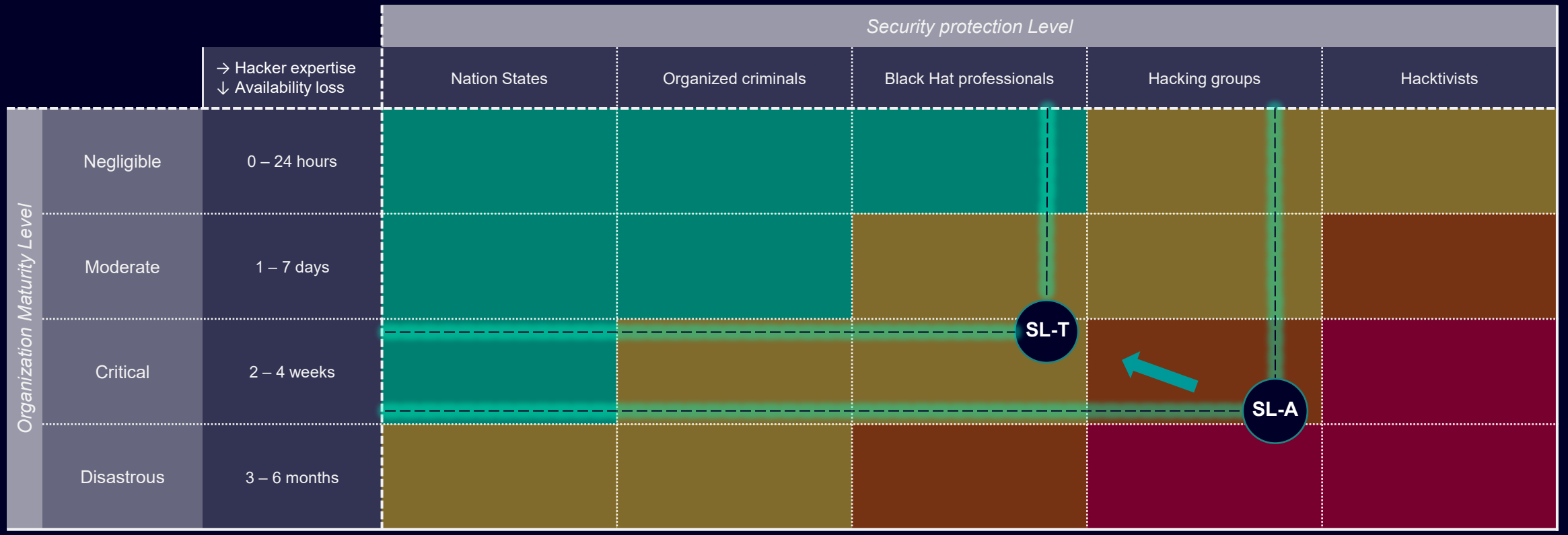
10 oktober 2023 | Congrescentrum 1931, den Bosch

CLAROTY SIEMENS

Beleid en organisatie

- Top down aanpak
- OT security programma manager
- Bepaal risico bereidheid
- Bekijk organisatie en technologie
- Betrek de productie sites

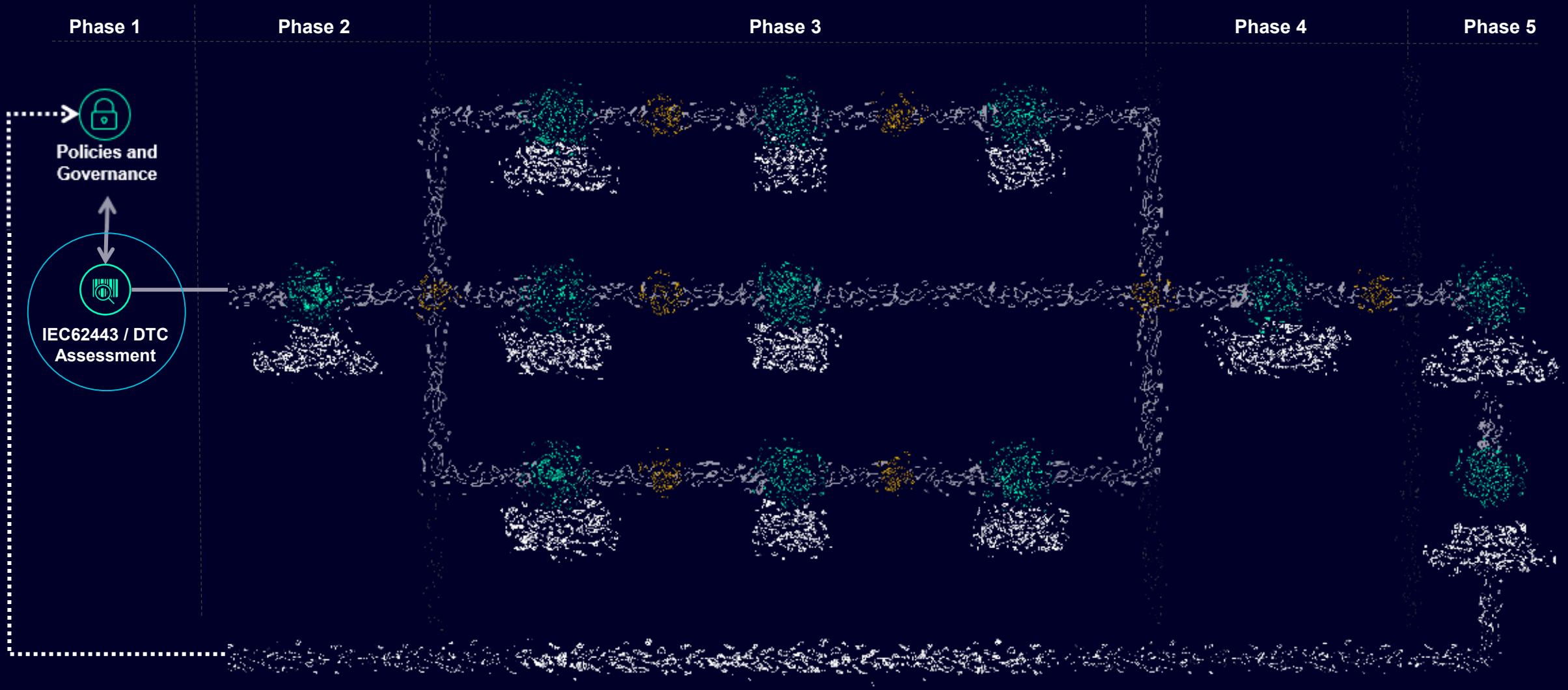
De mate van risico bereidheid



SL-A – Security Level Achieved
SL-T – Security Level Target

CLAROTY SIEMENS

OT security Journey



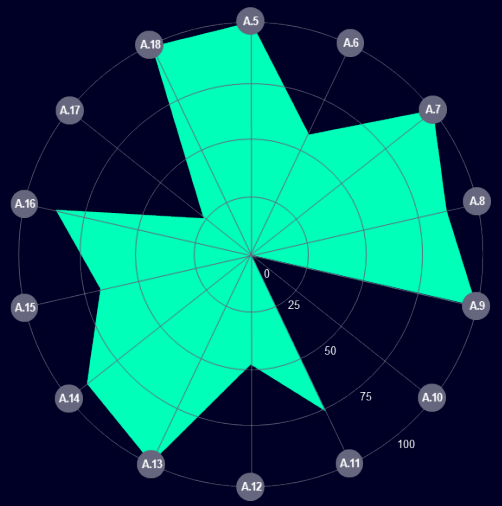
Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch

CLAROTY SIEMENS

IEC62443 Assessment

- Bepaal huidige risico’s
- Bepaal mate van volwassenheid
- Verkrijg inzicht in prioriteiten

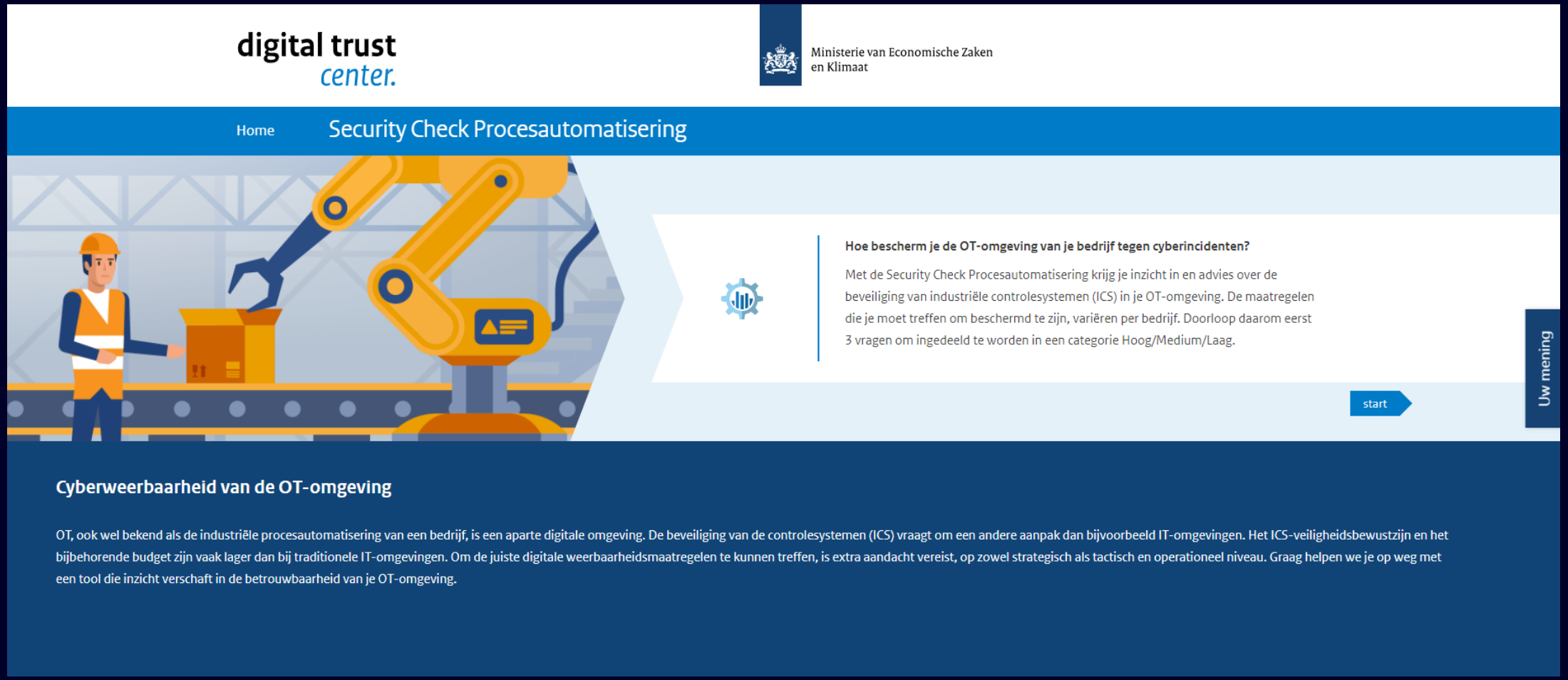


Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch

CLAROTY SIEMENS

Digital trust center

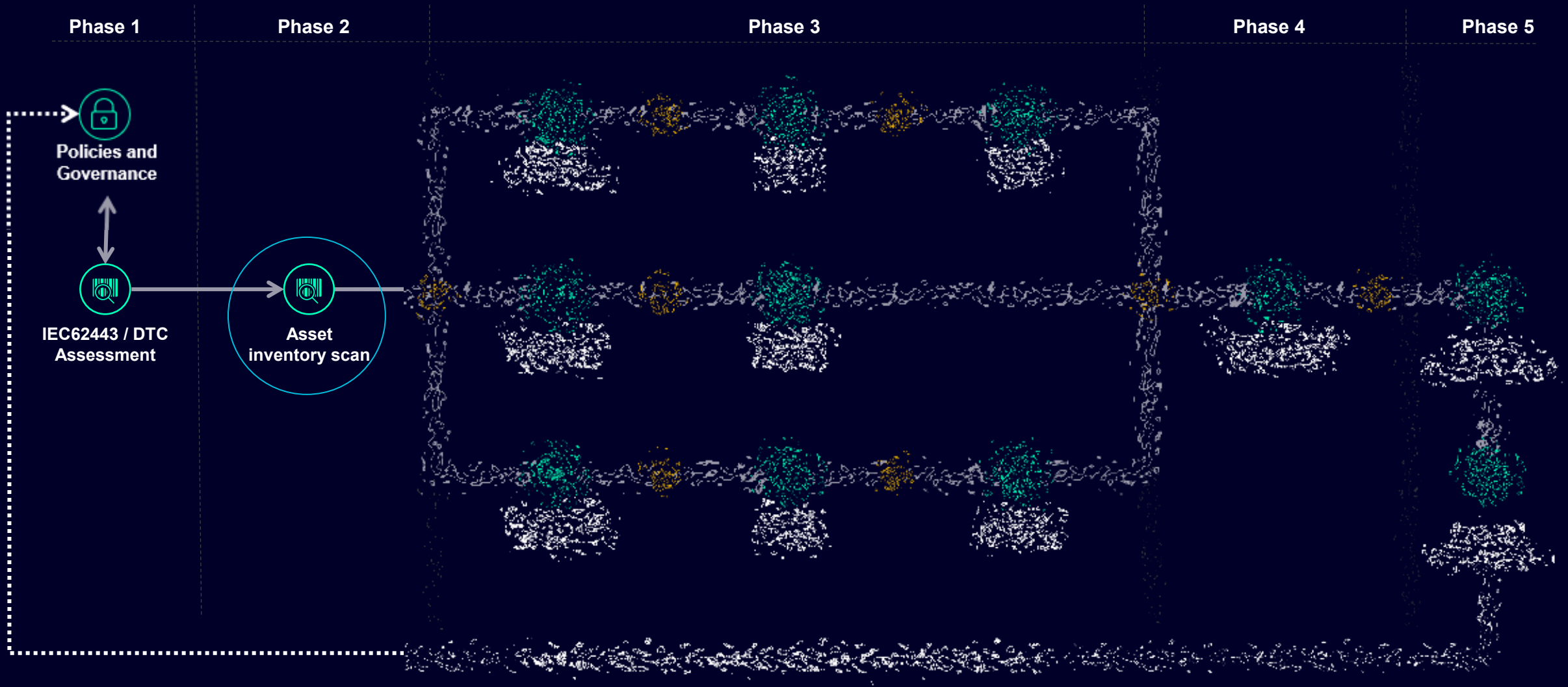


Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch

CLAROTY SIEMENS

OT security Journey



Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch

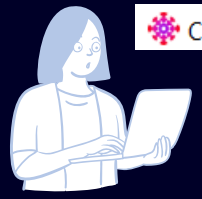
CLAROTY SIEMENS

Inventarisatie

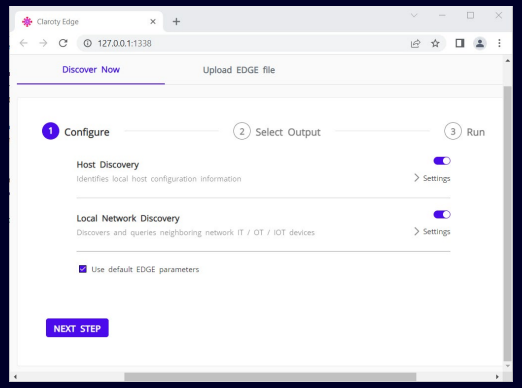
- Voor onderhoud of security?
- Via het netwerk… voorzichtig, voorkom schade
- Penetration testing is geen inventarisatie
- Gebruik leverancier neutrale OT scan tools
- Actief of passief, krijg alle device informatie

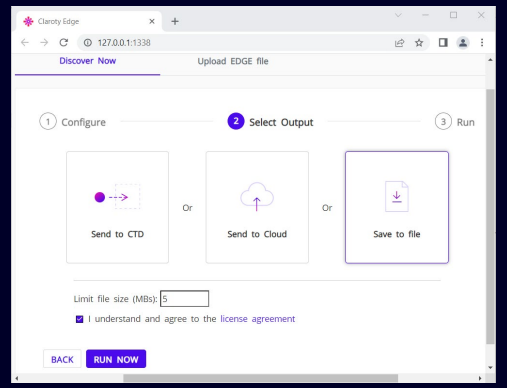
Inventarisatie scan

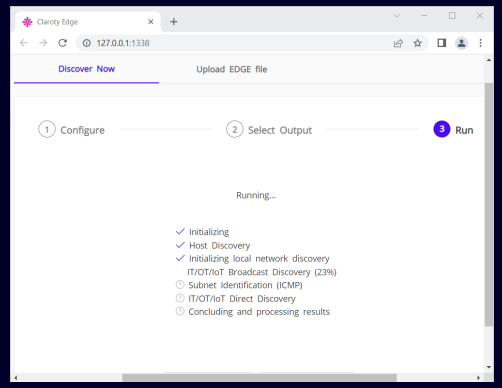
@ field

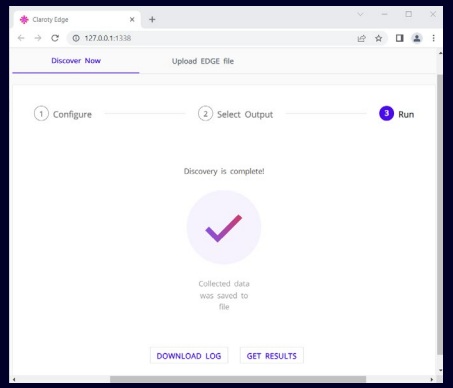


Claroty_Edge.exe



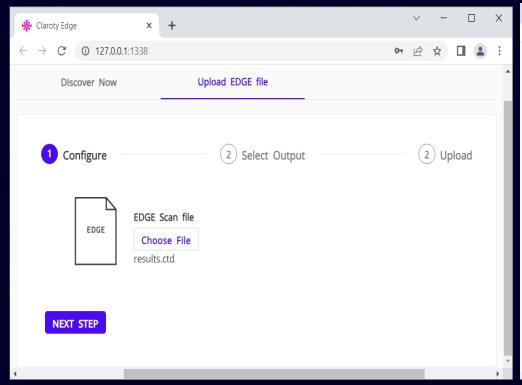


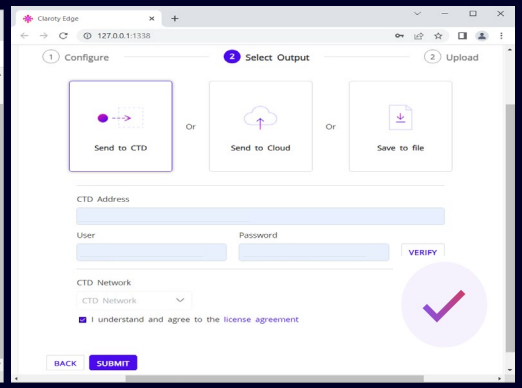


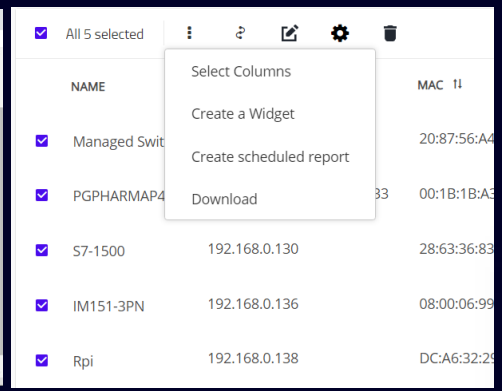


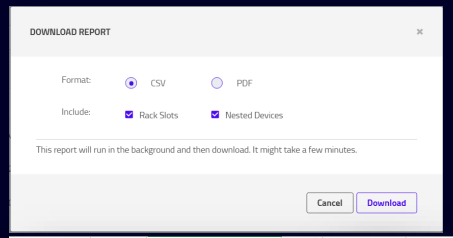
@ office

results.ctd





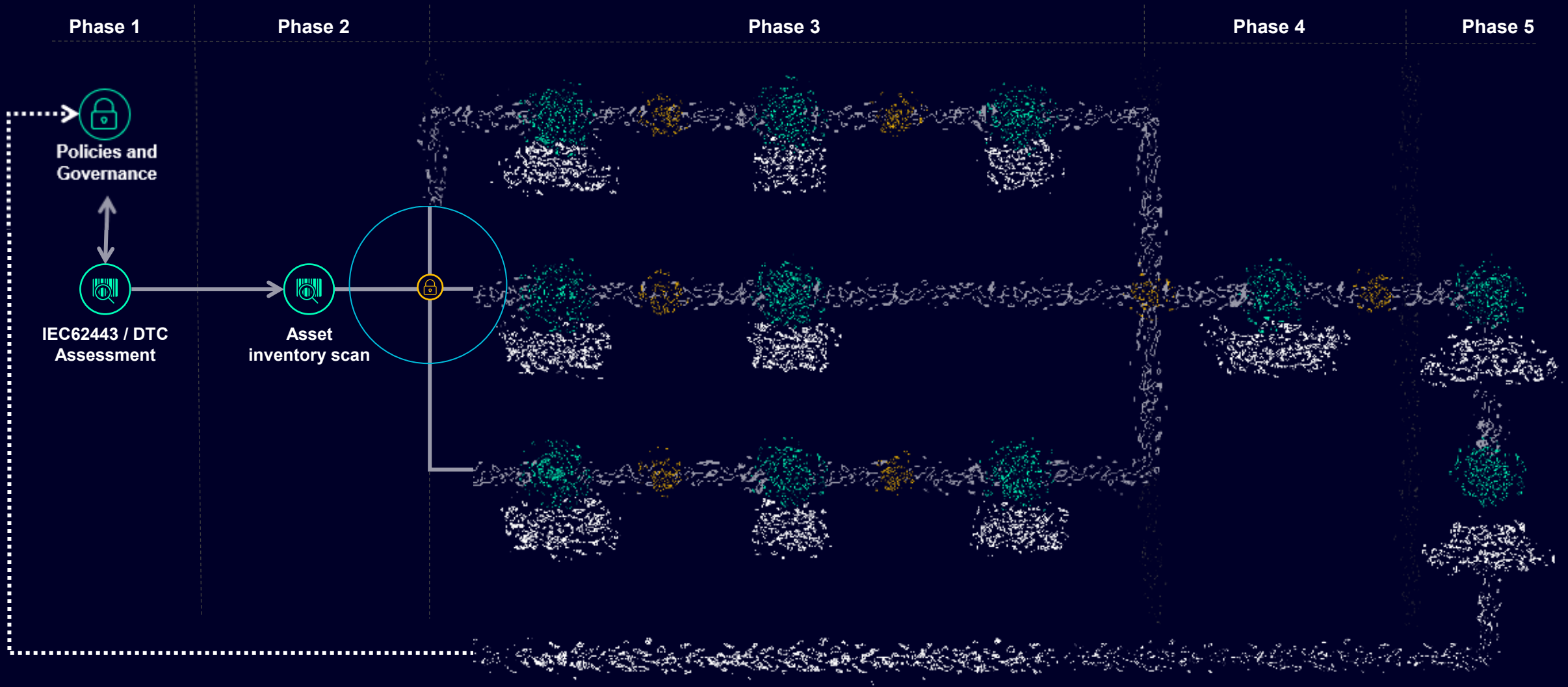




Asset Id	Site Id	Name	IP	Firmware	Order Number
111	1	PGPHARMAP4	192.	-	00330-80000-00000-AA572
112	1	Managed Switch	192.	V04.03.01	6GK5 206-2BS00-2AC2
113	1	IM151-3PN	192.	-	6ES7 151-3BA23-0AB0
114	1	S7-1500	192.	V1.6.0	6ES7 511-1AK00-0AB0
115	1	Rpi	192.	-	

CLAROTY SIEMENS

OT security Journey



Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch

CLAROTY SIEMENS

A Roadmap to success – the OT security Journey

VALUE GENERATION

OT Check

Start to investigate your current level of OT security

OT Scan

Initial OT asset & network scan

OT Workshop

Cyber Security report from DTC & Inventory vulnerability insights

OT Plan

Implement the roadmap from the Cyber Workshop

Remote Industrial Operations Services

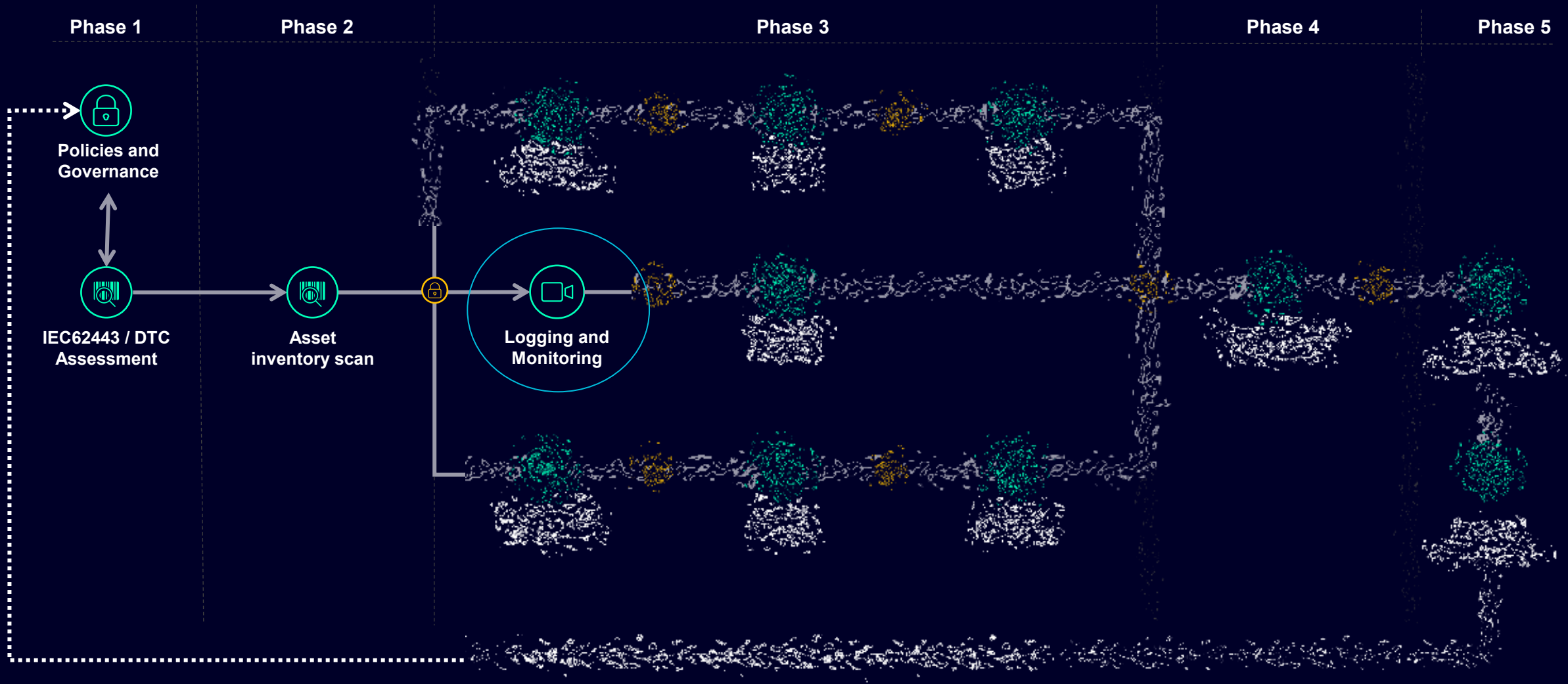
Visibility, monitoring, protection & threat detection across OT assets

SETTING A BASELINE | **OUTCOME** | **IMPLEMENTATION** | **CONTINUOUS IMPROVEMENT**

CYBER SECURITY JOURNEY

CLAROTY SIEMENS

OT security Journey



Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch

CLAROTY SIEMENS

De uitdaging binnen OT

- Binnen 24 uur rapporteren van incidenten
- Aantonen weerbaarheid onder controle
- Vervangen legacy equipement is geen optie
- Ook na segmentatie blijft rest risico over

CLAROTY SIEMENS

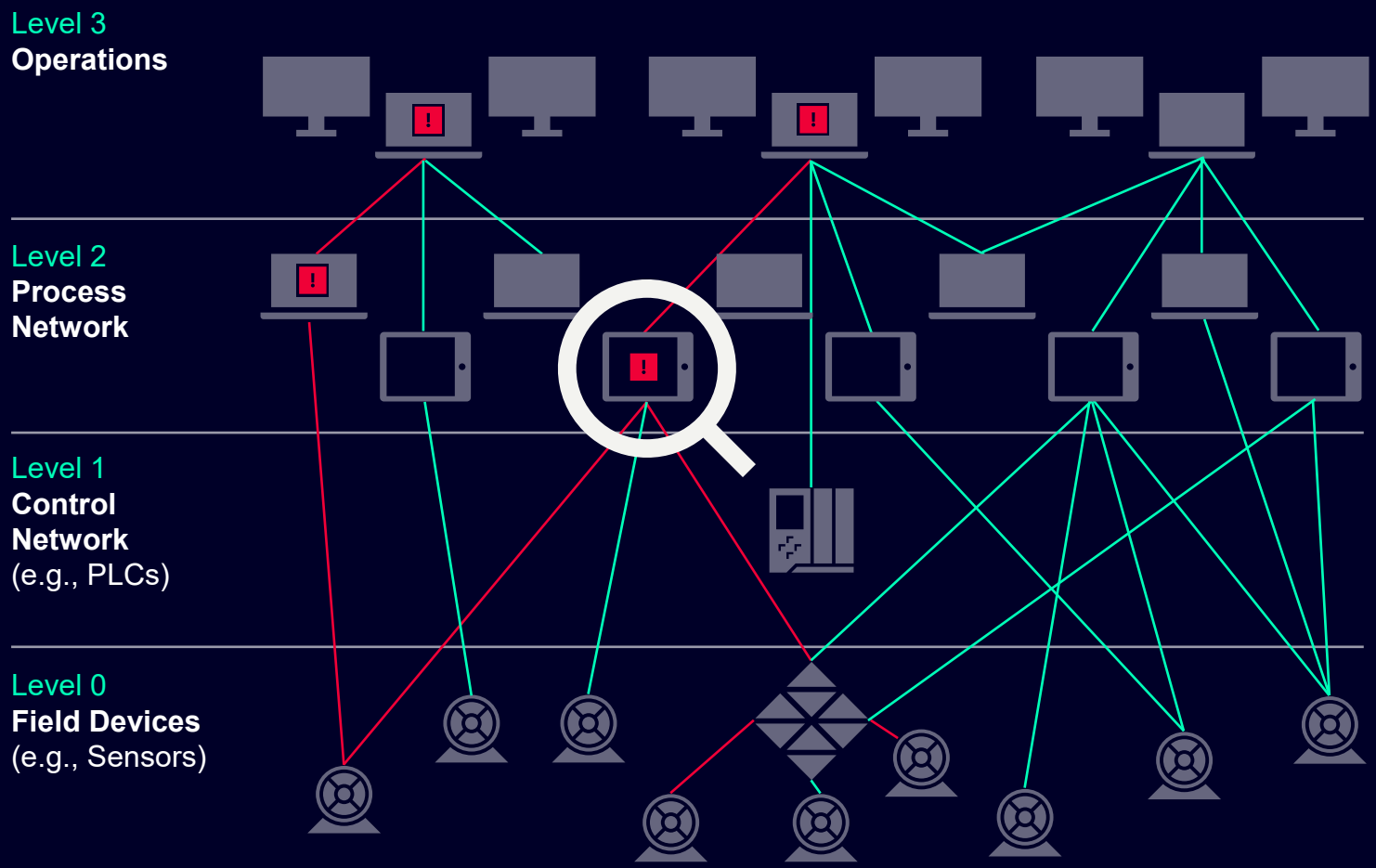

xDome

Inzicht in de “black box” van OT

- Inzicht in afwijkingen op normaal gedrag
  - Functieblok verandering
  - Virtual zone overschrijding
  - Andere devices met zelfde geaccepteerde protocol
  - Zelfde devices met ander geaccepteerd protocol
  - Andere gebruiker, route, tijdstip of combinatie
- Juist op kritische onderste lagen van OT
  - Aansturing en beveiliging van fysieke systemen
  - Eenvoudige ingang tot “alles” via industrie protocol

CLAROTY SIEMENS

Detect threats at an early stage to increase security and availability – with Industrial Anomaly Detection



Solution

Industrial Anomaly Detection provides transparency of connected assets and data exchange as well as enhanced security through continuous and proactive identification of changes in the system.

Artificial intelligence allows a self-learning system configuration: The software automatically analyzes the data traffic in the network in a "learning phase" and correlates the current traffic against that baseline to detects anomalies – for example, intrusion of hackers or data theft.

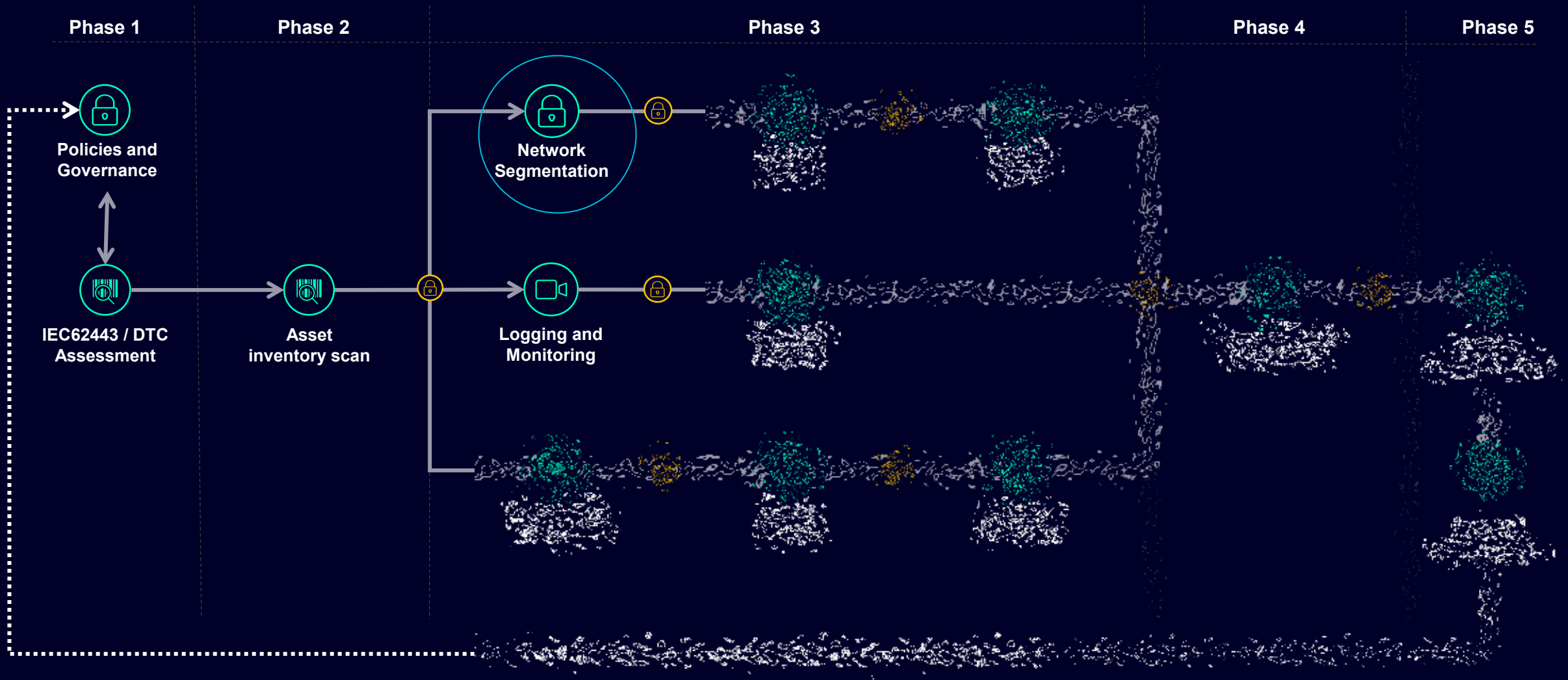
The 100% passive monitoring solution can be seamlessly integrated into industrial networks and control systems.

Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch

CLAROTY SIEMENS

OT security Journey



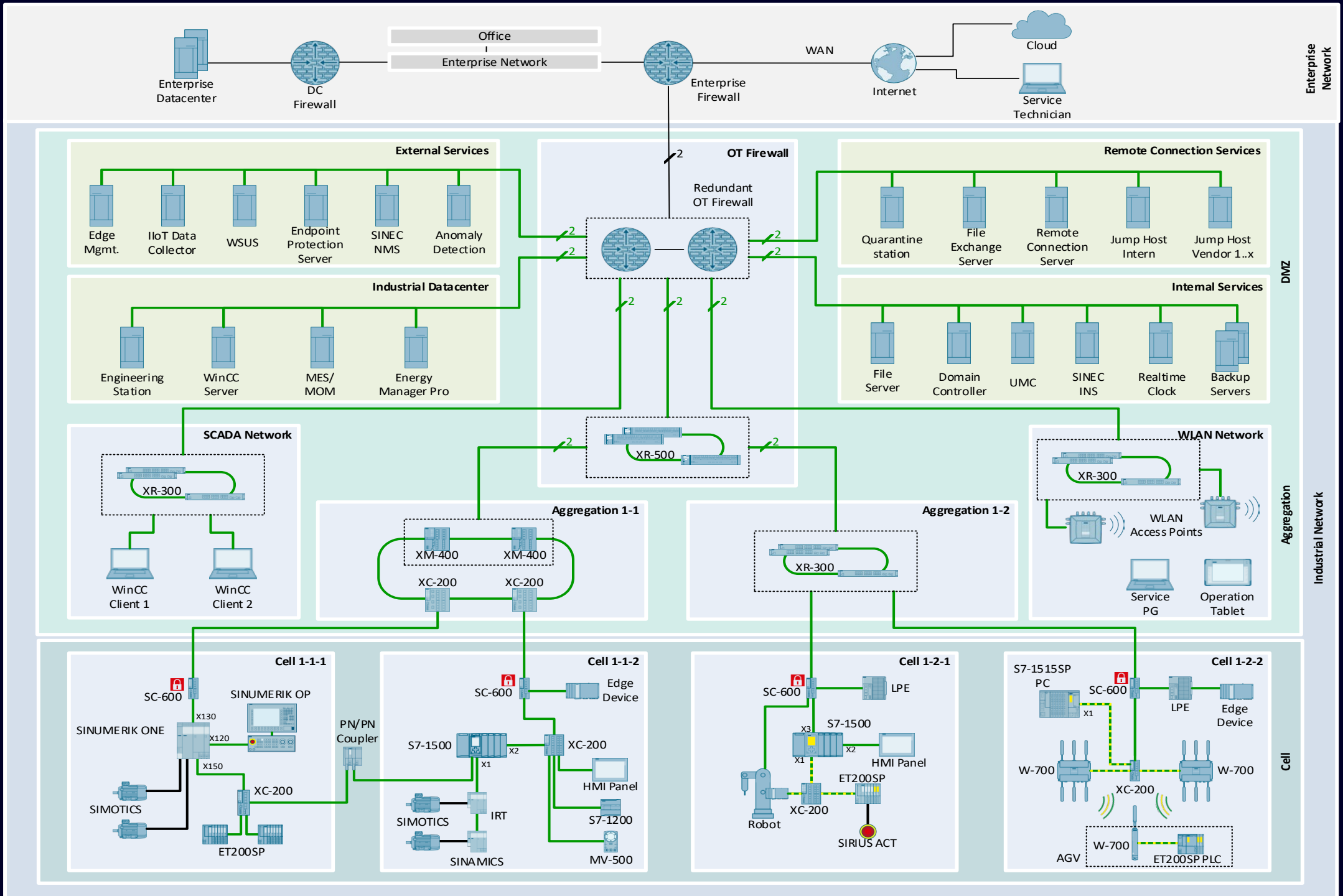
CLAROTY SIEMENS

How can we support you?

Secure Reference Architecture

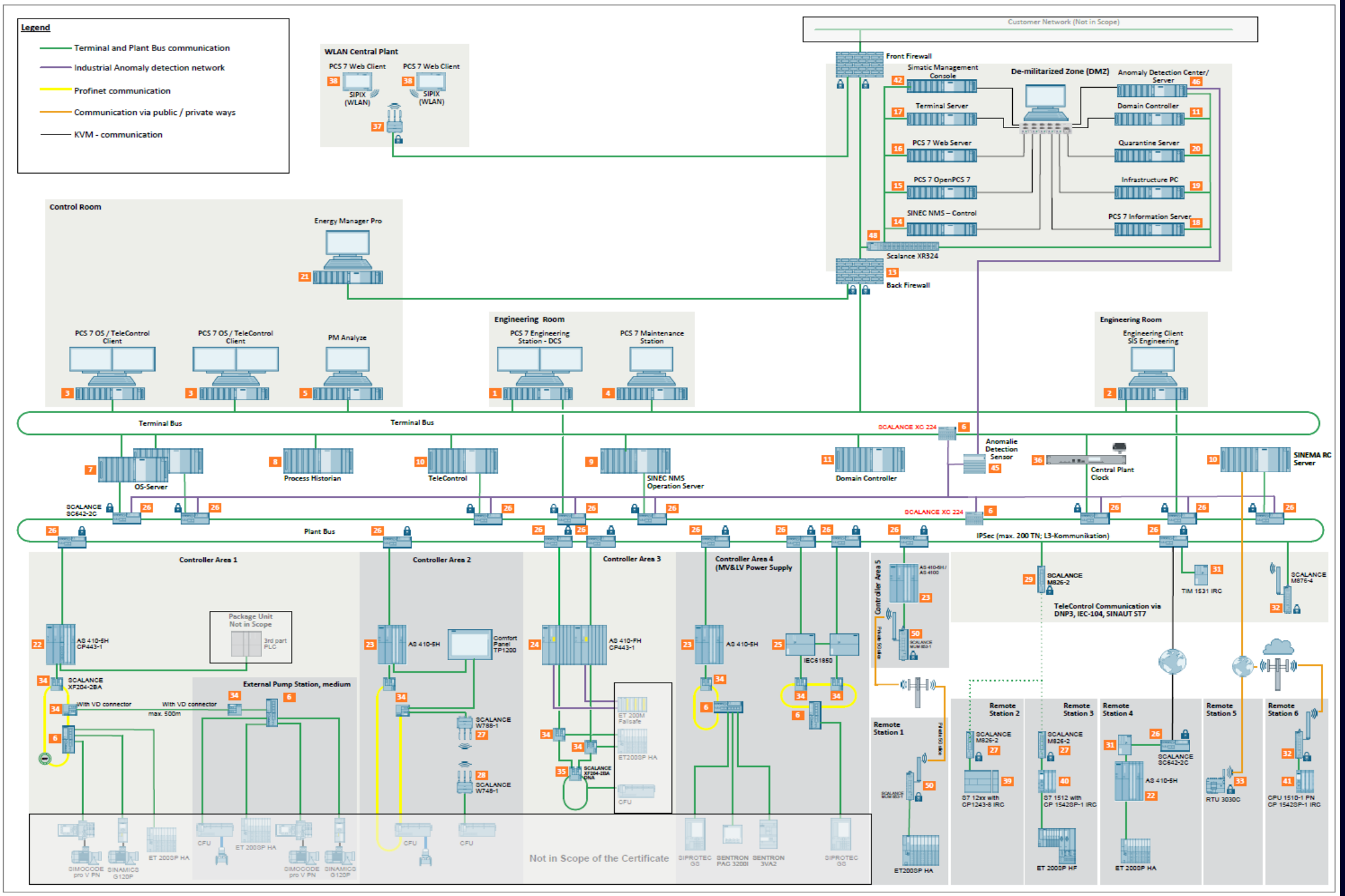
Generic network for OT
- Guidance document for IEC62443
- Applicable to all verticals
- For discrete manufacturing facilities
- For process plants

Guideline to be able to **comply** to IEC 62443-3-3


Enterprise Datacenter
DC Firewall
Office
Enterprise Network
Enterprise Firewall
WAN
Internet
Cloud
Service Technician
Enterprise Network
External Services
Edge Mgmt.
IIoT Data Collector
WSUS
Endpoint Protection Server
SINEC NMS
Anomaly Detection
OT Firewall
Redundant OT Firewall
Remote Connection Services
Quarantine station
File Exchange Server
Remote Connection Server
Jump Host Intern
Jump Host Vendor 1..x
Industrial Datacenter
Engineering Station
WinCC Server
MES/ MOM
Energy Manager Pro
Internal Services
File Server
Domain Controller
UMC
SINEC INS
Realtime Clock
Backup Servers
DMZ
SCADA Network
XR-300
WinCC Client 1
WinCC Client 2
XR-500
Aggregation 1-1
XM-400
XM-400
XC-200
XC-200
Aggregation 1-2
XR-300
WLAN Network
XR-300
WLAN Access Points
Service PG
Operation Tablet
Aggregation
Industrial Network
Cell 1-1-1
SC-600
SINUMERIK OP
SINUMERIK ONE
X130
X120
X150
SIMOTICS
XC-200
ET200SP
PN/PN Coupler
Cell 1-1-2
SC-600
Edge Device
S7-1500
X2
X1
XC-200
HMI Panel
S7-1200
SIMOTICS
IRT
SINAMICS
MV-500
Cell 1-2-1
SC-600
LPE
S7-1500
X3
X1
X2
HMI Panel
ET200SP
XC-200
Robot
SIRIUS ACT
Cell 1-2-2
S7-1515SP PC
X1
SC-600
LPE
Edge Device
W-700
XC-200
W-700
W-700
AGV
ET200SP PLC
Cell


SIEMENS
Secure Reference Architecture
Discrete Manufacturing Network

SIEMENS


Legend
Terminal and Plant Bus communication
Industrial Anomaly detection network
Profinet communication
Communication via public / private ways
KVM - communication
Customer Network (Not in Scope)
WLAN Central Plant
PCS 7 Web Client
PCS 7 Web Client
SIPIX (WLAN)
SIPIX (WLAN)
Front Firewall
Simatic Management Console
De-militarized Zone (DMZ)
Anomaly Detection Center/ Server
Terminal Server
Domain Controller
PCS 7 Web Server
Quarantine Server
PCS 7 OpenPCS 7
Infrastructure PC
SINEC NMS – Control
PCS 7 Information Server
Scalance XR324
Back Firewall
Control Room
Energy Manager Pro
PCS 7 OS / TeleControl Client
PCS 7 OS / TeleControl Client
PM Analyze
Engineering Room
PCS 7 Engineering Station - DCS
PCS 7 Maintenance Station
Engineering Room
Engineering Client SIS Engineering
Terminal Bus
Terminal Bus
SCALANCE XC 224
Anomalie Detection Sensor
Central Plant Clock
SINEMA RC Server
OS-Server
Process Historian
TeleControl
SINEC NMS Operation Server
Domain Controller
SCALANCE SC642-2C
SCALANCE XC 224
Plant Bus
IPSec (max. 200 TN; L3-Kommunikation)
Controller Area 1
Controller Area 2
Controller Area 3
Controller Area 4 (MV&LV Power Supply
Controller Area 5
Package Unit Not in Scope
3rd part PLC
AS 410-5H CP443-1
SCALANCE XF204-2BA
With VD connector
With VD connector max. 500m
External Pump Station, medium
AS 410-5H
Comfort Panel TP1200
SCALANCE W788-1
SCALANCE W748-1
AS 410-FH CP443-1
SCALANCE XF204-2BA DNA
ET 200M Failsafe
ET200SP HA
CPU
AS 410-5H
IEC61850
AS 410-5H / AS 4100
SCALANCE MUM 853-1
SCALANCE M826-2
TeleControl Communication via DNP3, IEC-104, SINAUT ST7
TIM 1531 IRC
SCALANCE M876-4
Remote Station 1
Remote Station 2
Remote Station 3
Remote Station 4
Remote Station 5
Remote Station 6
S7 12xx with CP1243-8 IRC
S7 1512 with CP 1542SP-1 IRC
AS 410-5H
RTU 3030C
CPU 1510-1 PN CP 1542SP-1 IRC
ET 200SP HA
SIMOCODE pro V PN
SINAMICS G120P
ET 200SP HA
CFU
ET 200SP HA
SIMOCODE pro V PN
SINAMICS G120P
CFU
CFU
Not in Scope of the Certificate
SIPROTEC GS
SENTRON PAC 3200I
SENTRON 3VA2
SIPROTEC GS


SIEMENS
PCS 7 Cyber Security Blueprint for Water Plants
Guideline for Secure Configuration


CERTIFICATE
No. IITS3 050774 0007 Rev. 00
Holder of Certificate: Siemens AG DI PA SO
Siemensallee 84 76187 Karlsruhe GERMANY
Site(s): Siemens AG DI PA SO Siemensallee 84, 76187 Karlsruhe, GERMANY
Certification Mark:
Type: Industrial IT Security
Scope of Certificate: Security Program for the Blueprint "Water Plants"
Tested according to: IEC 62443-2-4:2015/AMD1:2017 IEC 62443-3-3:2013/COR1:2014 PPP 150118:2021 (IEC 62443-2-4: Full ML2 Process Profile for a Blueprint)
Test report no.: 23CR045026
Valid until: 2026-04-06
Date, 2023-05-15
(Markus Müller)
ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ CERTIFICADO ◆ CERTIFICAT

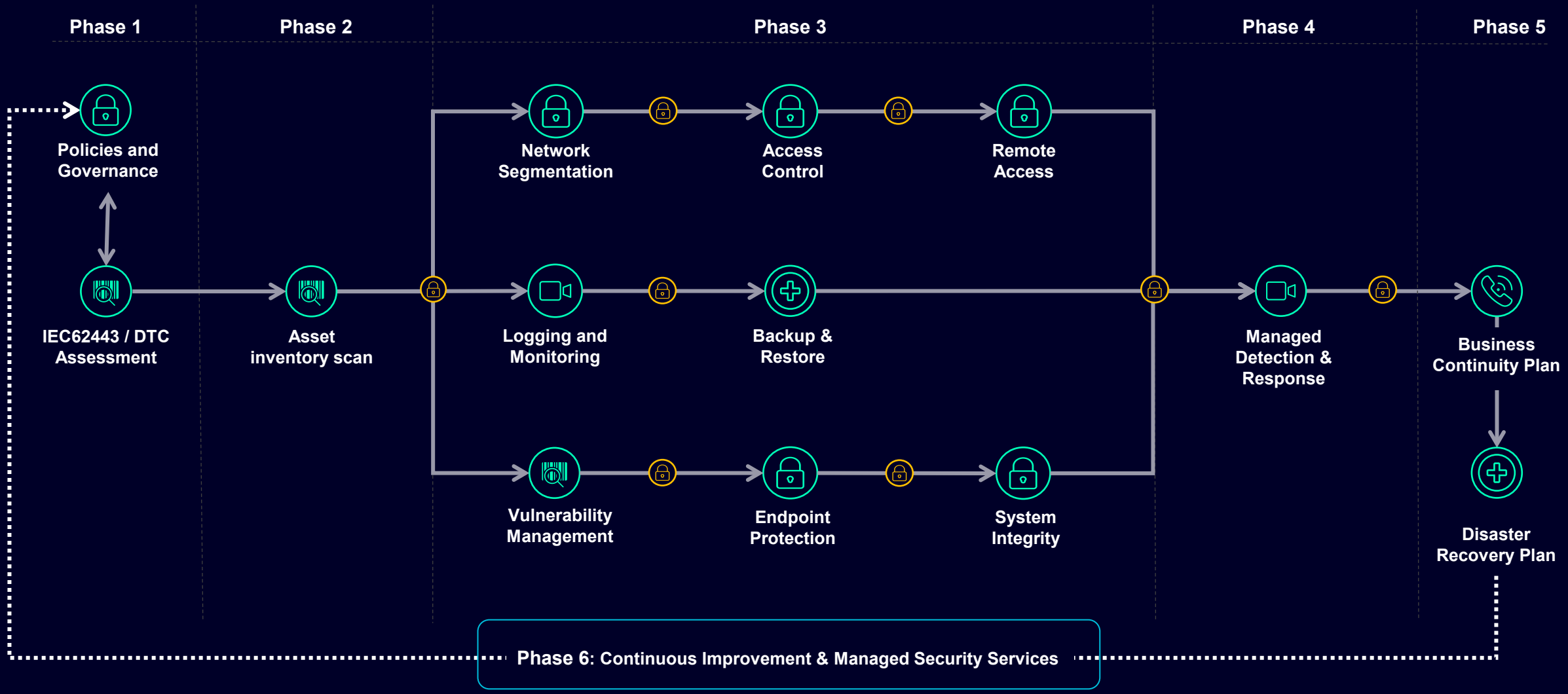
SIEMENS

Mijn fabriek is niet met internet verbonden…

uw mening over deze “AIRGAP”

- echt veilig
- schijn veilig

OT security Journey



CLAROTY SIEMENS

Nu voorbereiden op …

Technologische complexiteit & vergrijzing

Het samengaan van IT en OT

Voldoen aan OT Security wetgeving

Grip krijgen op de gehele OT infrastructure

CLAROTY SIEMENS

Bedankt voor uw aandacht

Uitnodiging: Digital Experience Center

OT Security onder de aandacht brengen van uw MT?
U bent van harte welkom!

Contact: Ruud.Welschen@Siemens.com
Contact: erwin.s@claroty.com
Follow: #OTSecurityJourney

linkedin.com/in/ruudwelschen

Industrial Cyber Security
10 oktober 2023 | Congrescentrum 1931, den Bosch

CLAROTY SIEMENS

Main references for more information:

• Claroty	Claroty.com
• Siemens Security portfolio	siemens.com/industrialsecuritservices
• Compendium Part F “Industrial Security	support.industry.siemens.com/cs/nl/nl/view/109756871/en
• Manual Security concept PCS 7	support.industry.siemens.com/cs/nl/nl/view/60119725/en
• Digital Trust Center	tools.digitaltrustcenter.nl/security-check-procesautomatisering
• Industrial Vulnerability Manager	demo.server-ivm.siemens.cloud
• Central User Management (UMC)	support.industry.siemens.com/cs/ww/en/view/109780337
• Product CERT	siemens.com/cert
• Discrete reference architecture	support.industry.siemens.com/cs/us/en/view/109802750
• Process reference architecture	water.c2.dc.siemens.com/en