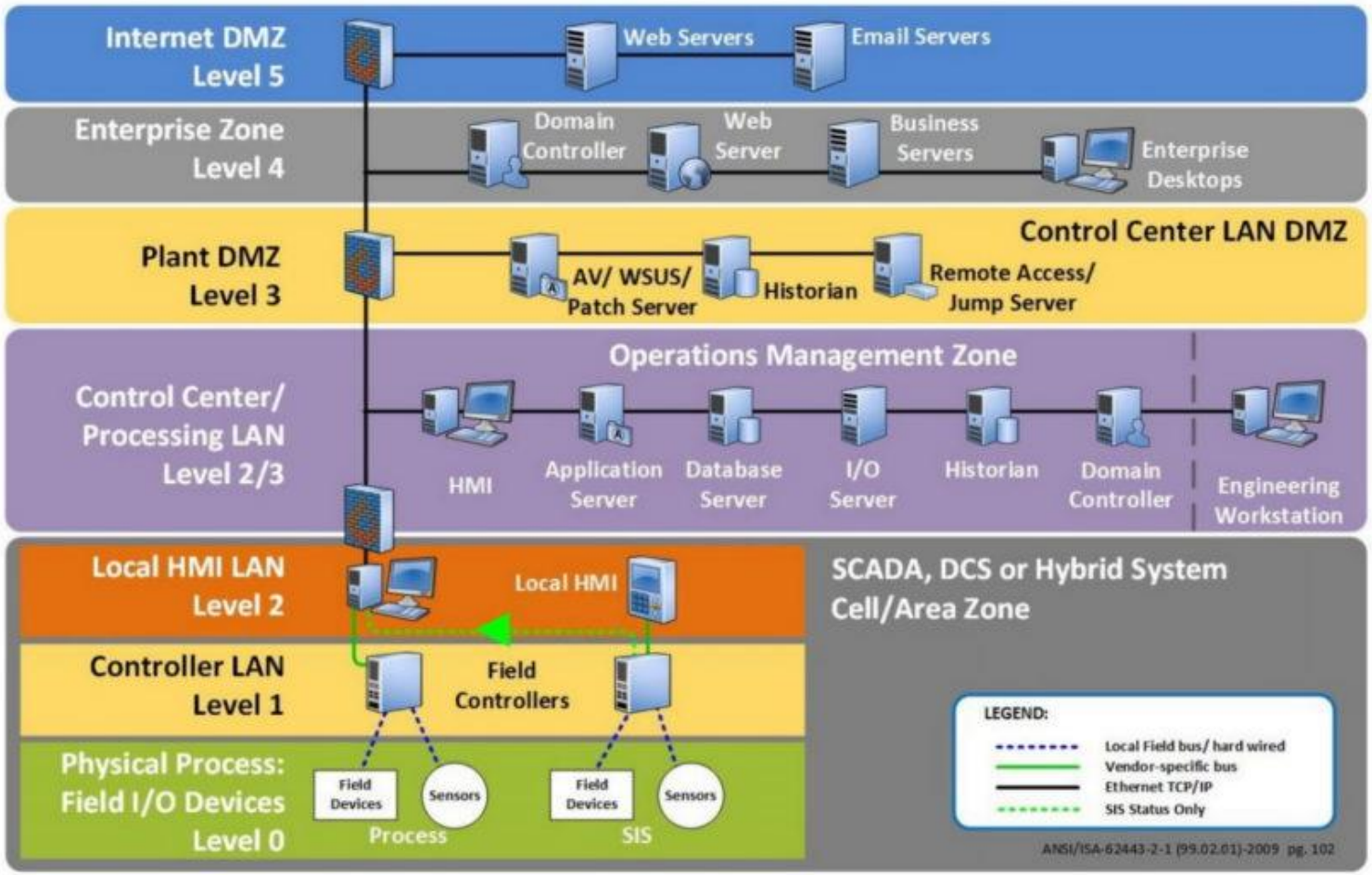
TRAFICOM
National Cyber Security Centre

Cybersecurity in Energy

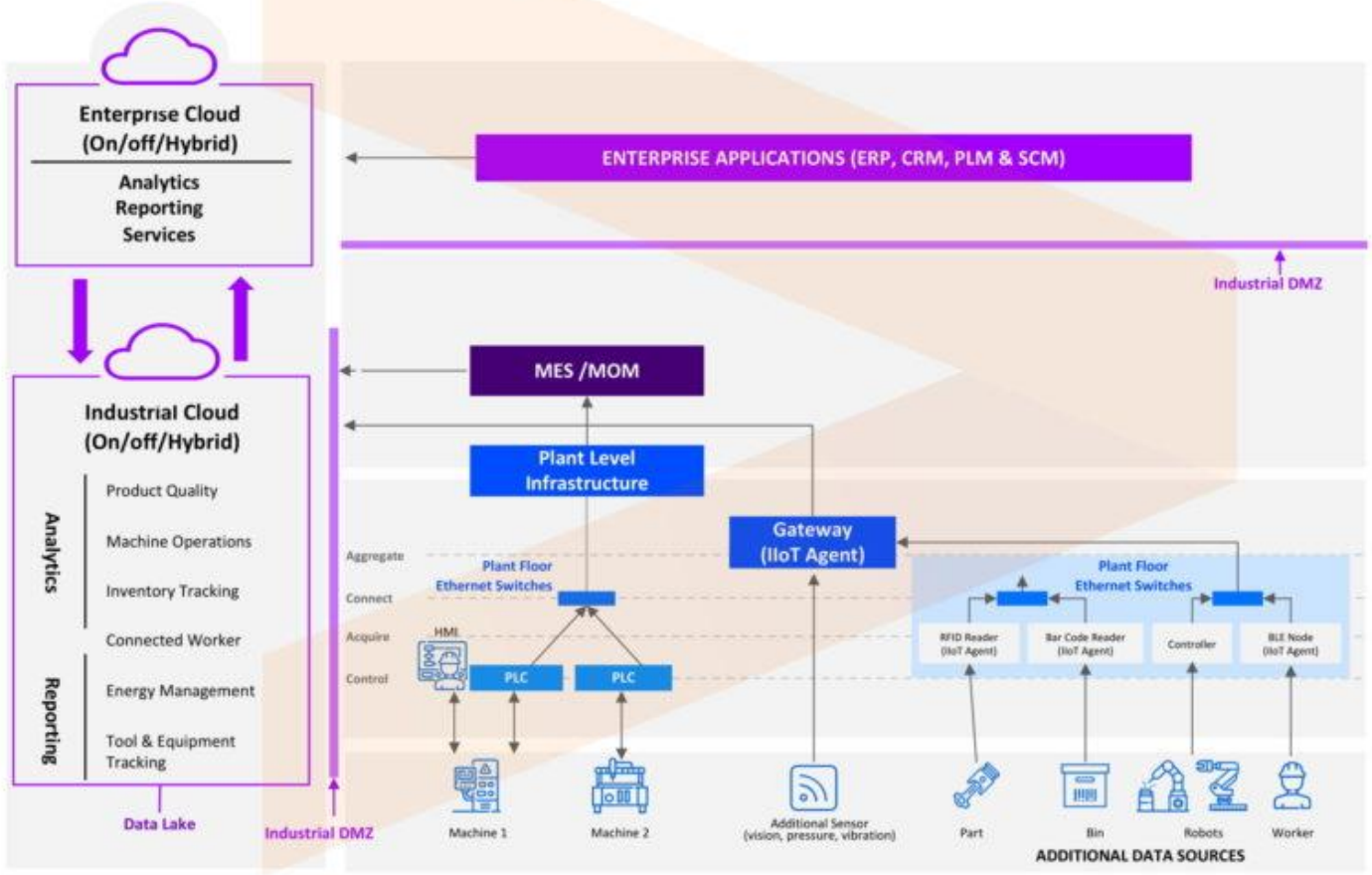
What is going on in the field?


Internet DMZ
Level 5
Web Servers
Email Servers
Enterprise Zone
Level 4
Domain Controller
Web Server
Business Servers
Enterprise Desktops
Plant DMZ
Level 3
Control Center LAN DMZ
AV/ WSUS/ Patch Server
Historian
Remote Access/ Jump Server
Control Center/ Processing LAN
Level 2/3
Operations Management Zone
HMI
Application Server
Database Server
I/O Server
Historian
Domain Controller
Engineering Workstation
Local HMI LAN
Level 2
Local HMI
SCADA, DCS or Hybrid System
Cell/Area Zone
Controller LAN
Level 1
Field Controllers
Physical Process:
Field I/O Devices
Level 0
Field Devices
Sensors
Process
Field Devices
Sensors
SIS
LEGEND:
Local Field bus/ hard wired
Vendor-specific bus
Ethernet TCP/IP
SIS Status Only
ANSI/ISA-62443-2-1 (99.02.01)-2009 pg. 102

Typical current problems

- Legacy systems
- Lack in system segregation
- Lack in understanding on systems and networks
- Control of outside dependencies
- Sharing of security data

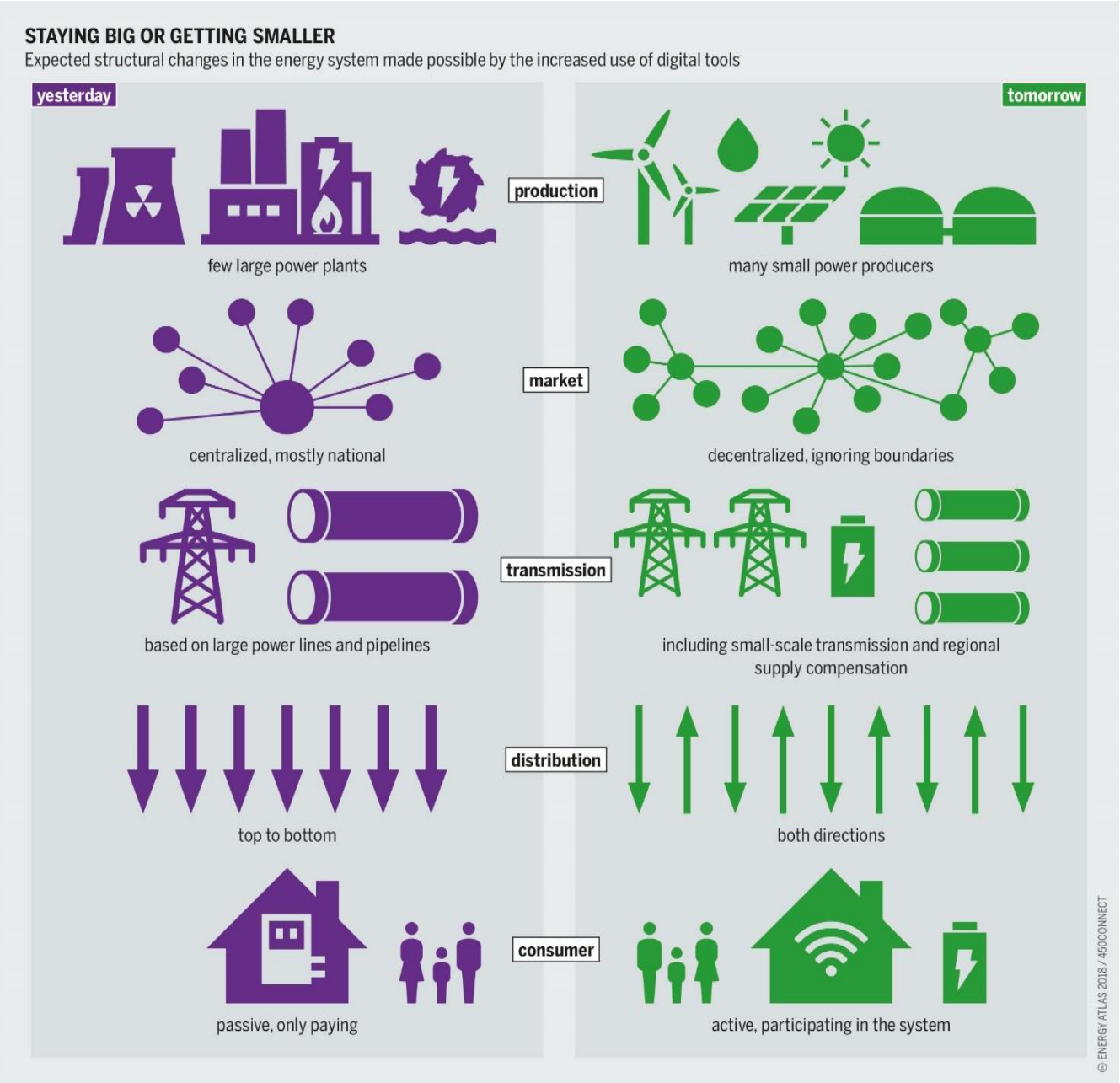
CLOUD-ORIENTED INDUSTRIAL ARCHITECTURE



Dale Peterson, https://dale-peterson.com/2019/02/11/is-the-purdue-model-dead/

Attack trends

- Consolidation of technologies -> commoditization of attacks
  - Same attacks can be used against any systems
- Faster cycle in deploying new attacks
  - Advanced attacks become public -> attacks in the standard toolbox
- Attacks to weak links in the supply chain
- Hybrid attacks and widespread scamming are the new normal

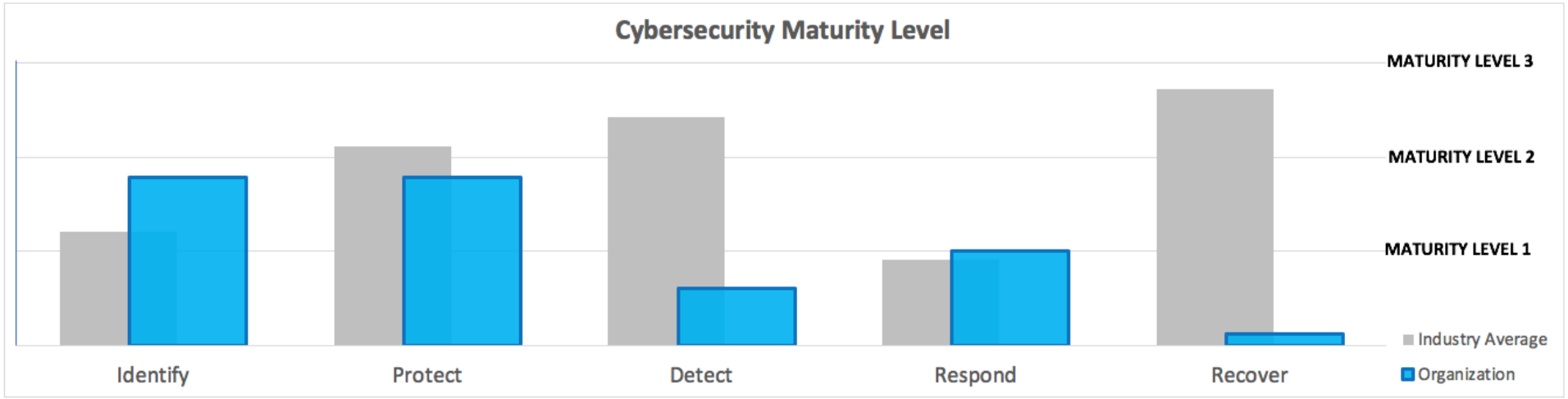


TRAFICOM
National Cyber Security Centre

Some NCSC-FI services

What are we doing in the field?

NCSC-FI Cyber Resilience Framework – Self Assessment Tool



Identify	Organization has a good capability to identify and manage cyber security risks to systems, people, assets, data and critical services, but some weak areas exist. This typically means that some unmitigated cyber risks remain that weaken the overall resiliency of the organization.
Protect	Organization has a good capability to protect its critical services from cyber security threats and incidents, but it still has some weak control areas. This typically means that while all critical services and information may be covered, the implementation leaves grey areas or gaps in the protection, leading to unnecessarily high cost and number of incidents.
Detect	Organization has a very limited capability to detect cyber incidents as they happen. Typically this means that response activities are delayed significantly and happen after major breach and damage an attacker wants to cause will realize in full.
Respond	Organization has a basic capability to initiate a timely response to a cyber incident, but the process may not be well coordinated and rehearsed. Typically this means that even if the detection has been done early, it is still likely that the response is not able to contain the breach and damage.
Recover	Organization has a very limited capability to initiate and execute recovery from the damage caused by a cyber incident. This typically means that the recovery will take unnecessarily long and therefore may significantly increase the brand damage, cost and impact of the incident.

Situational awareness

Situational awareness products provide up-to-date information on events and trends affecting cyber security.

Our industry-specific mailing lists are:

- State administration
- Public administration
- Defence industry
- Energy sector
- FSI
- Industrial automation
- Chemical and processing industry
- Logistics
- Food industry
- Healthcare
- Industrial enterprises
- Component and product manufacturers
- ICT sector
- Media
- Cyber security consultants and consulting firms
- Information security researchers
- CERT operators

Cooperation networks

Information sharing and analysis centres (ISACs) share information about cyber threats and trends.

Information sharing groups (ISACs) enable:

- Confidential information sharing and discussion about information security related matters
- Improving and enhancing information security know-how within participating organisations
- Developing the overall situational awareness of the NCSC-FI
- Developing the cyber security both within the industry and across the society.

ISACs have been established on the following industries:

- Central government
- Internet service providers (ISPs)
- Energy sector
- Chemical and forest industry
- Banks
- Media
- Food production and distribution
- Social welfare and healthcare
- Logistics
- Water
- (Software manufacturers)

Cyber exercises

- We support critical infrastructure providers' cyber preparedness by providing exercise support services.
- We offer professional support and materials both for conducting the exercise and for planning realistic scenarios, based on real-life cyber incidents.
- Organisation's ability to react to cyber incidents can be improved and practiced with cyber exercises. This helps in shortening and reducing the impact of the incident.
- https://www.kyberturvallisuuskeskus.fi/en/our-services/exercises

TRAFICOM
National Cyber Security Centre

Thank you!

Jussi Eronen
Chief Specialist, NCSC-FI
juhani.eronen@traficom.fi
@CERTFI || ncsc.fi