OWASP OT Top 10

Andreas Happe
(andreas.happe@owasp.org)

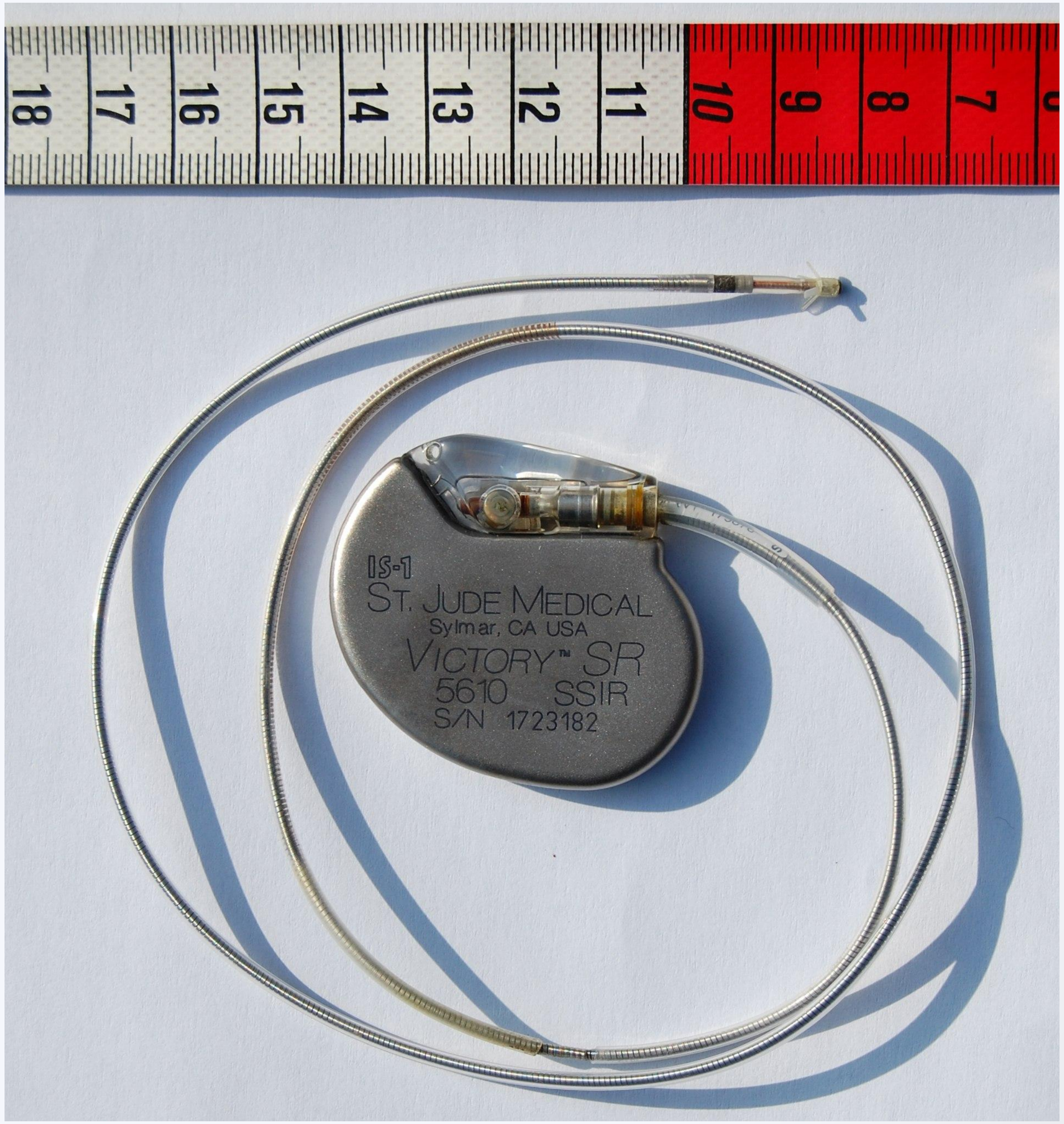
Agenda

- What is Operational Technology (OT)?
- Why is it important?

- What are the OWASP OT Top 10?
  - ..and why am I here?

- Cultural differences between OT and IT (Sec)

What is Operational Technology (OT)?


IS-1
ST. JUDE MEDICAL
Sylmar, CA USA
VICTORY™ SR
5610 SSIR
S/N 1723182

Why are they important?

OWASP OT Top 10

A Bit of Background

- quite new
  - started in summer 2024
  - hopefully there will be a beta release in 2025
  - video conference every two weeks

- identify top 10 threats for OT networks
- found ‘cultural’ problems between OT and IT Sec

- full disclosure: I am using you as alpha-testers

Cultural Differences between OT and IT (Security)

Safety/Availability vs. Security

- online shop vs. power plant
- what does the focus upon availability mean for us?
    - what does this mean for updates?
    - special case: regulations

- Simple examples
    - emergency stop switches

Lifecycles

- in the IT world: couple of years

- in the OT world: decades
  - think about power plants, cars, your pacemaker

- What security did we have 30 years ago?
  - do you still get software/hardware support for stuff you bought back then (if you were even alive)?
  - what network protocol security did we have 30 years ago?

Suppliers

- Difference between Plant Owner, Operators, Integrators

- shared responsibility

- few suppliers
  - can lead to security practises more fitting to ‘99
  - updates? notifications?

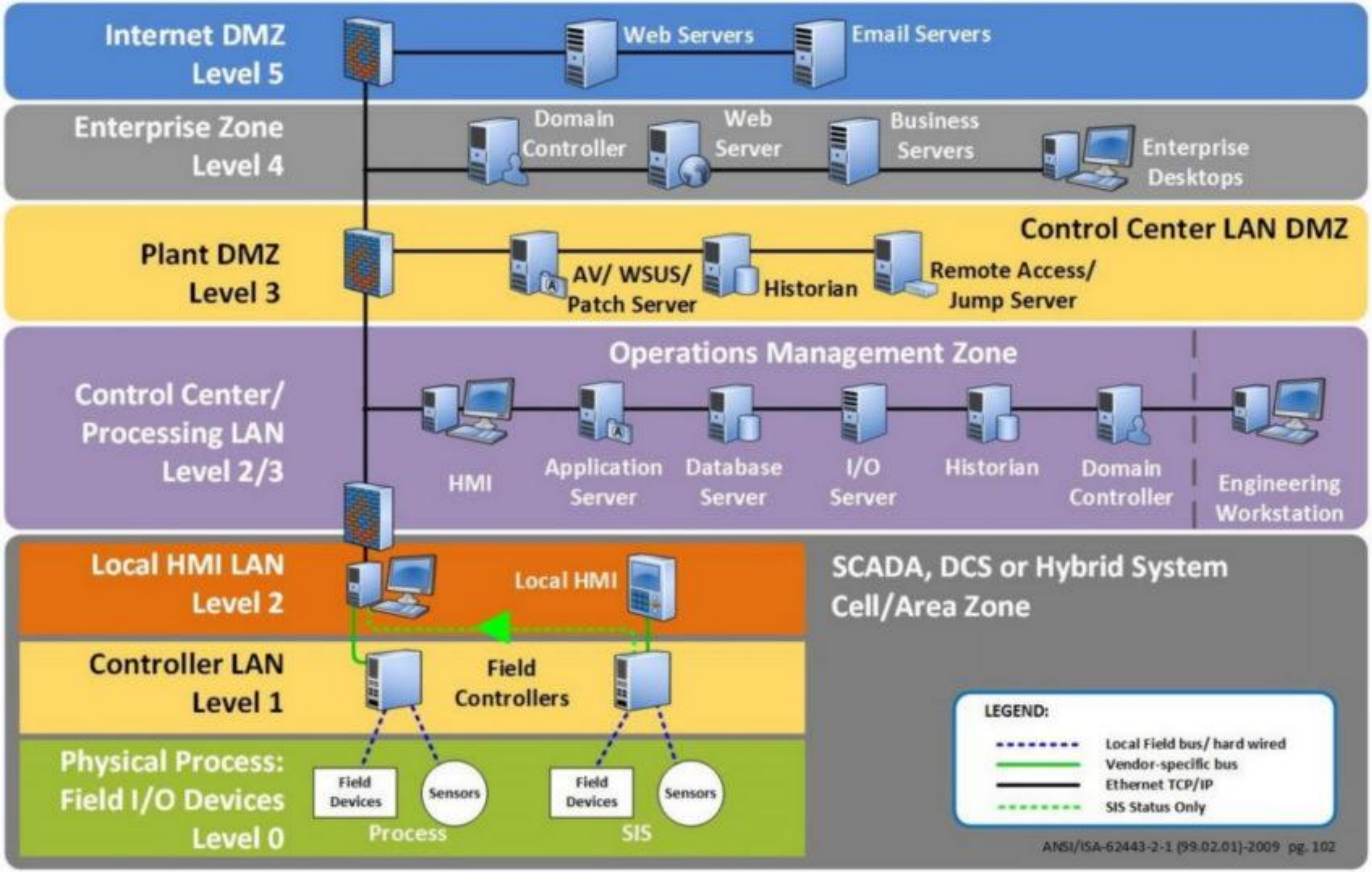
Devices must be Protected

Devices must be Protected

- network segmentation, physical access control, etc.
- problem: this does not come for free
  - complex architectures
  - more administration
  - people must heed security

What happens if Segmentation fails?

CPU319-3 PN/DP
BF 1
BF 2
BF 3
SF
DC5V
FRCE
RUN
STOP
PUSH
RUN
STOP
MRES
SIEMENS
SIMATIC
S7-300
2
318-3EL00-0AB0
SM323
DI16/DO16xDC24V
4
323-1BL00-0AA0
SM322
DO 32xDC24V/0.5A
5
322-1BL00-0AA0
SM322
DO 32xDC24V/0.5A
6
322-1BL00-0AA0



ANSI/ISA-62443-2-1 (99.02.01)-2009 pg. 102

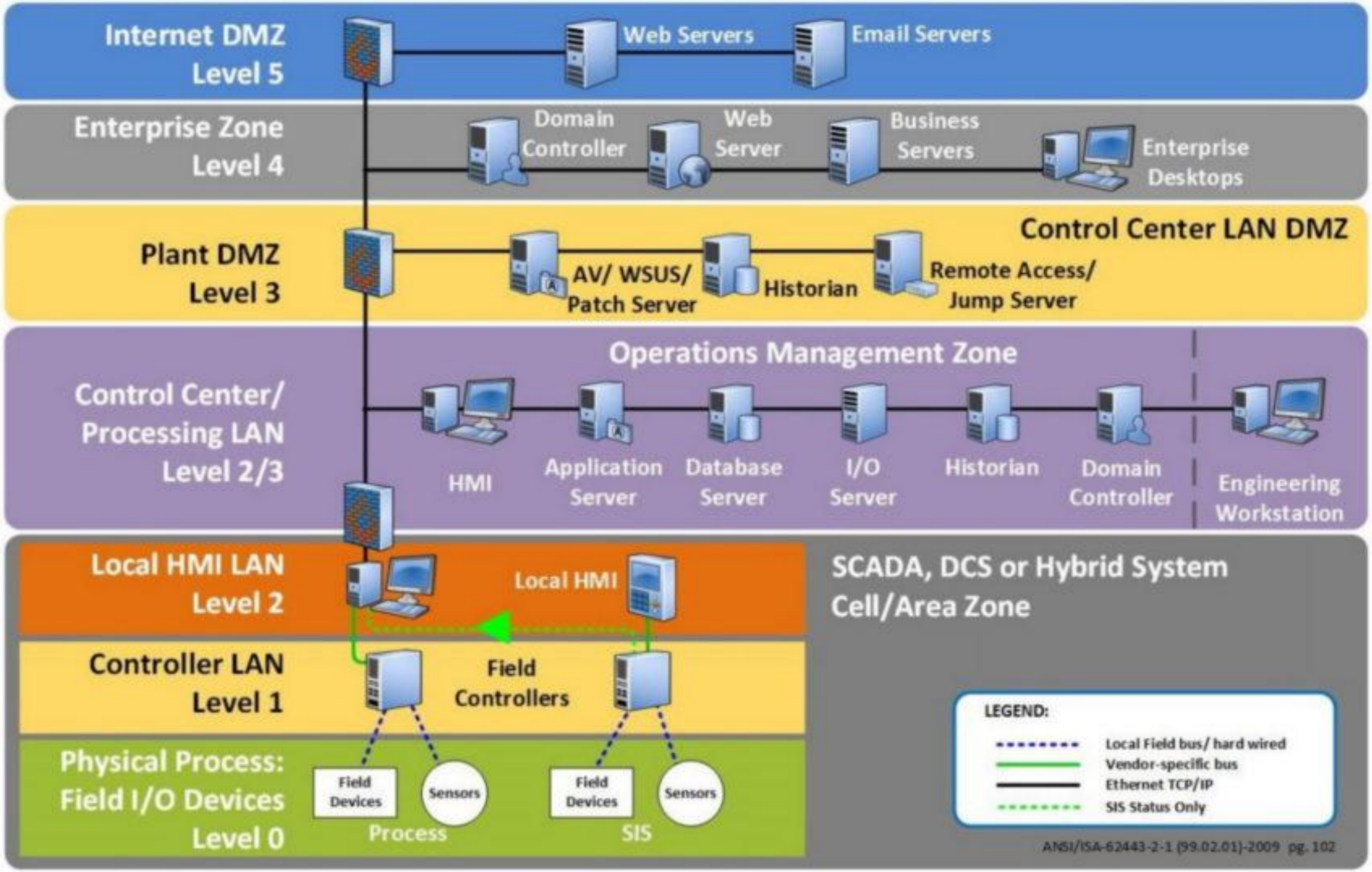
Problem: Blast Radius

How to recover from an incident?

What are common problem?

- missing configuration backups
- missing recovery options
    - how to you restore a pacemaker?

IT and OT are converging


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

How to involve OT people?

Currently working on this..

- availability/safety needs security
- convenience
- functional requirements
- regulatory pressure

The OWASP OT Top 10 (WIP)

- https://ot.owasp.org