



DEFENSIFY
BUSINESS SECURITY SOLUTIONS

Introduction to OT

Ludwig Seitz, OT Security Specialist

June 2023

Agenda

1. OT – definition

02. OT hardware & software

ICS, SCADA, PLC, RTU, SIS, Historian MES

03. PERA model

Operational Technology – a definition

- Official:

“All IT monitoring or controlling physical processes”

- Inofficial:

“IT in the non-carpeted areas”



Where is Operational Technology?

- Everywhere



Power



Water



Transportation



Building Automation

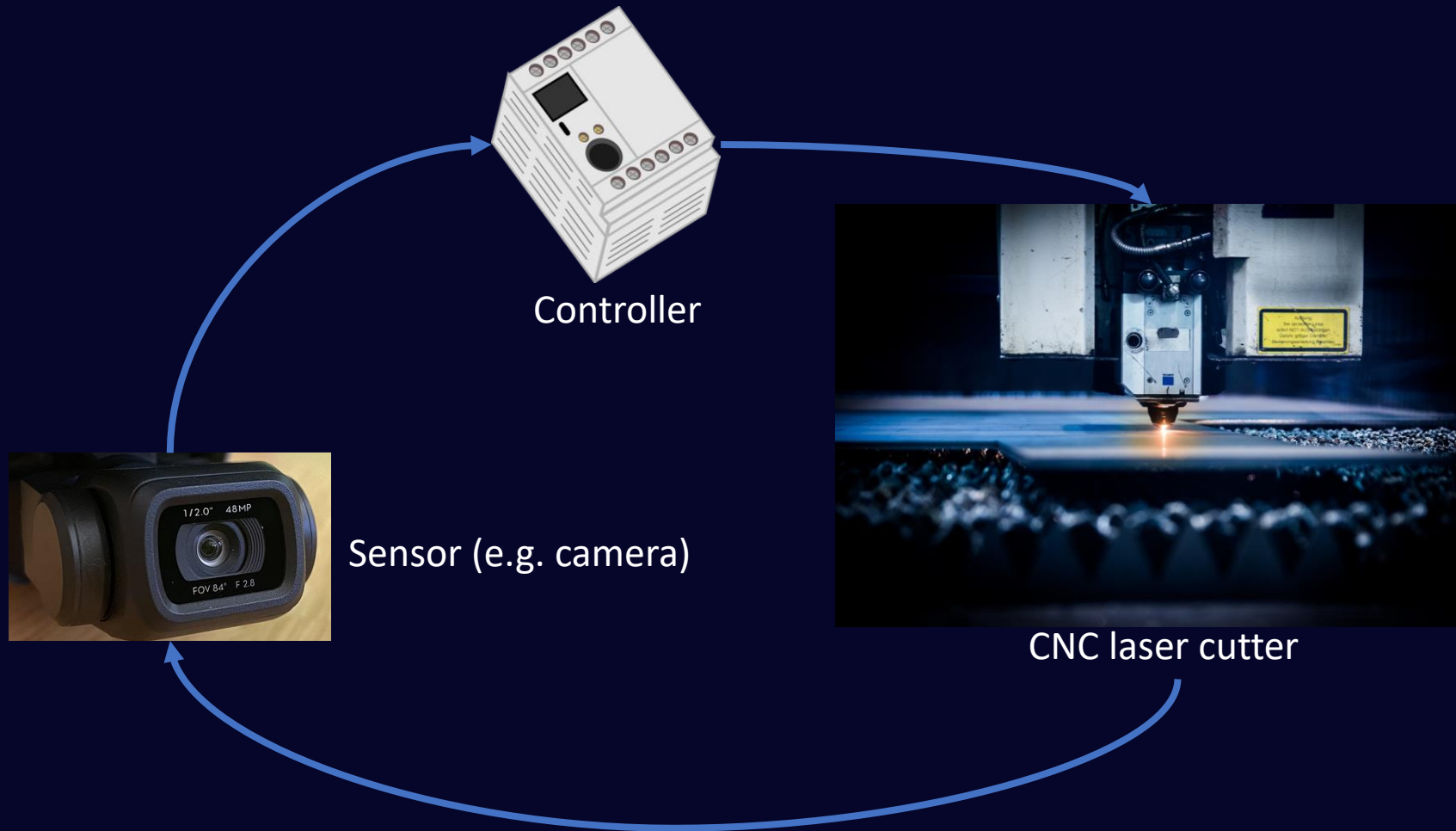


Manufacturing



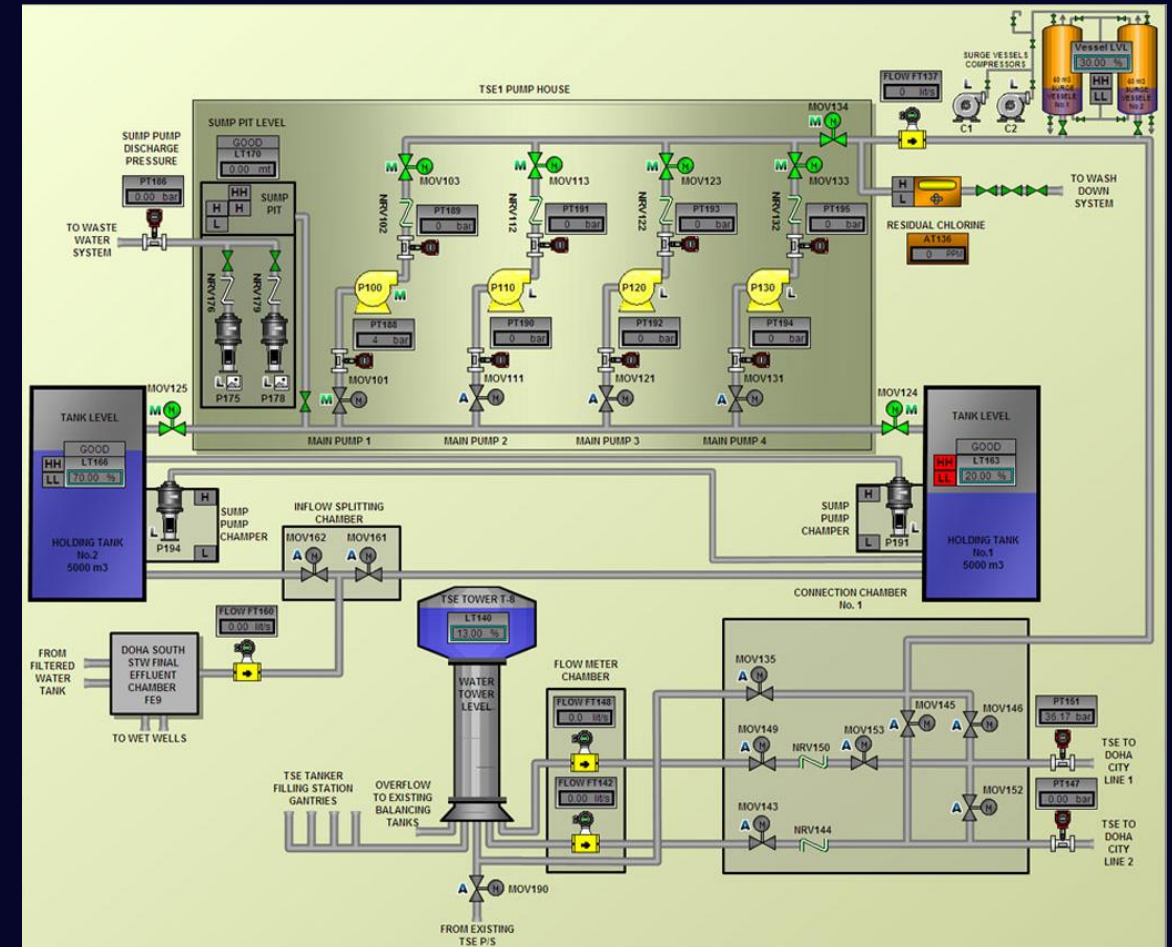
Laundry Rooms*

Industrial Control System



SCADA

- Supervisory Control and Data Acquisition
 - High-level system for supervision of industrial processes
 - Consists of computers, communication infrastructure and human-machine interfaces
 - Focus on supervision (not control)
 - Often event-driven



PLC

- Programmable Logic Controller
 - Computer for controlling industrial processes
 - Ruggedized
 - Real-time operating system
 - Provides inputs and outputs
 - Often modular
 - Support for various Industrial protocols



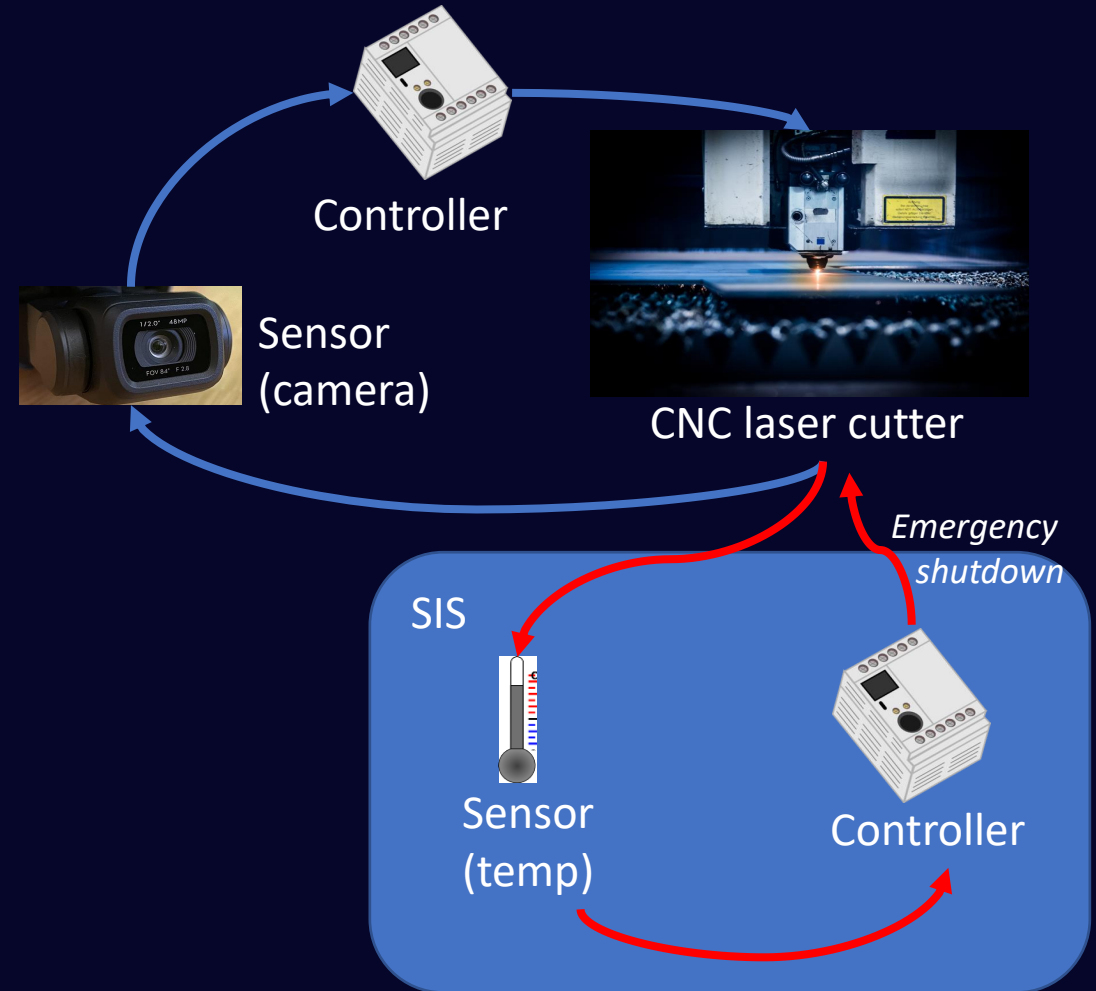
RTU

- Remote Terminal Unit
- Device for interfacing between automation equipment and control systems
- Used to gather data and transmit control signals
- Very similar to PLC



Wikimedia commons: FernaCM

- Safety Instrumented System
 - Software or hardware system for keeping an industrial process safe
 - Automatically intervenes with corrective action
- Side-node: Safety vs Security
 - Automation engineers often focus on safety
 - See: Triton attack → No safety without security



Historian

- Database
 - Collects industrial process data
 - Time-stamped
 - Real-time operations
 - Often provides data aggregation functions
- Often connected to ERP
 - Main reason why OT systems rarely can be air-gapped



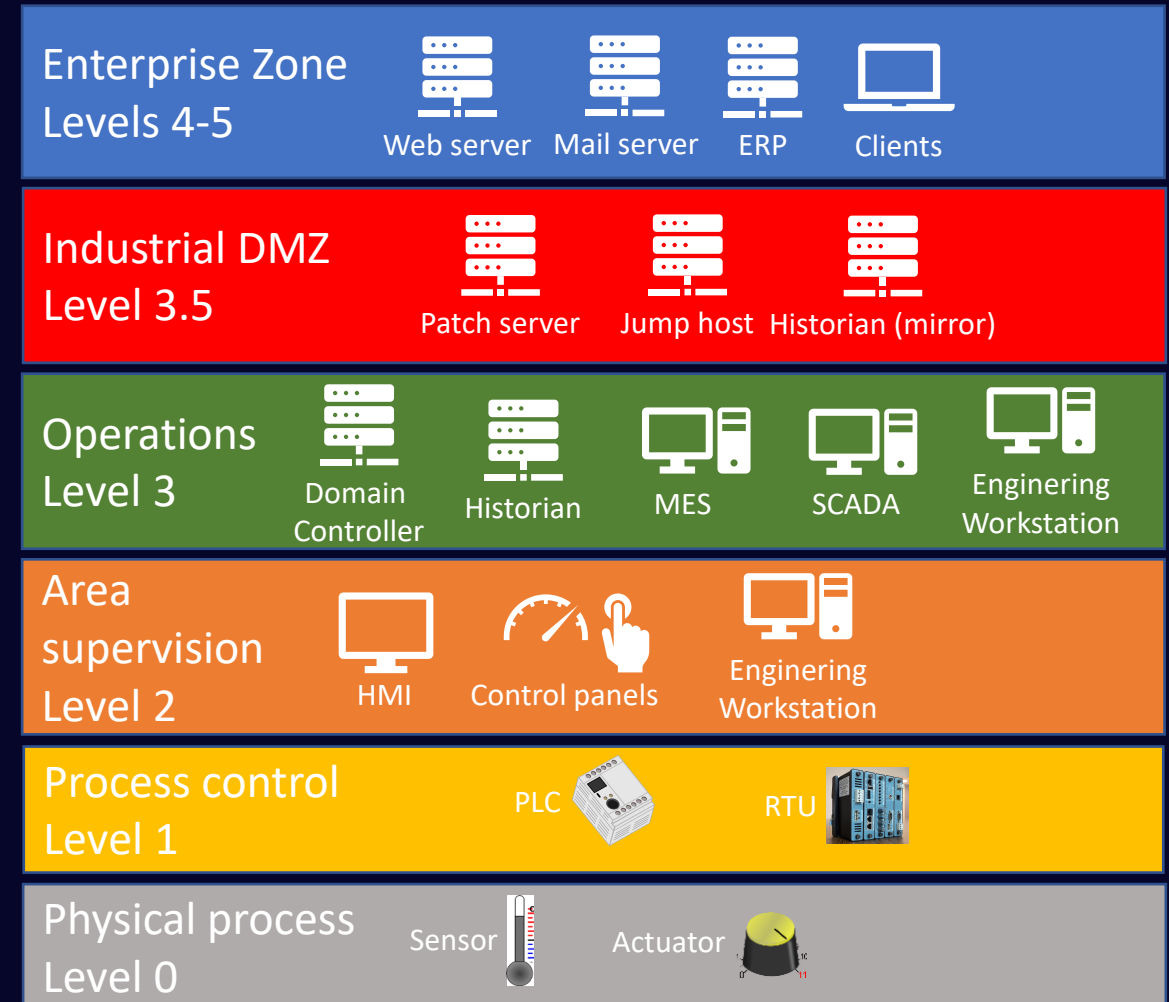
MES

- Manufacturing Execution System
 - Software for tracking production
 - Many possible applications
 - E.g., order handling, quality control, tracking effectivity, manage drawings
 - Often interfaced with ERP
 - Can be custom-build or off-the-shelf



Purdue Enterprise Reference Model

- Reference architecture
 - Used to describe OT systems
 - Not security specific
 - Level 3.5 is an add-on ☺
 - Note: Many different interpretations online





DEFENSIFY
BUSINESS SECURITY SOLUTIONS

THANK YOU!

Ludwig Seitz

E: ludwig.seitz@defensify.se

W: www.defensify.se

June 2023

