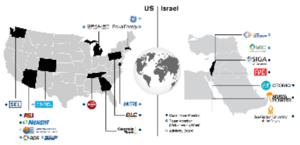
Task 2: Digital representation of physical processes and aggregation operational process modelling

Michael Faifer, Dr. Rami Puzis, Prof. Asaf Shabtai

BGU

The problem: missing the operational state situational awareness

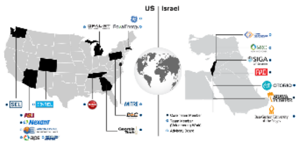


- Monitoring, detecting, and handling cybersecurity incidents in ICS
  - is based on data collected from the operational network and IT network
  - ignores (in most of the cases) the operational state or the ICS system

- Security personnel is not involved in defining and monitoring the operational processes of the ICS;
- Engineer and operators are not involved in monitoring and detecting the cyber attacks

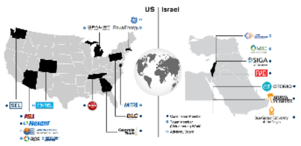
- This leads to potential false alarms, wasting time in investigating alerts, and applying wrong countermeasures

Proposed solution: ICS operations situational awareness



- Formulation of common operational process enumeration (COPE) for Industrial Control Systems (ISC)
- COPE for ICS will be used to represent the common operational processes
  - in a structured human readable manner
  - while specifying the data sources appropriate for monitoring the process
- Using COPE, stakeholders can understand at any point in time the state of the ISC system
  - Define a process signature and detect anomalies
  - Justify system behaviors and avoid false positives

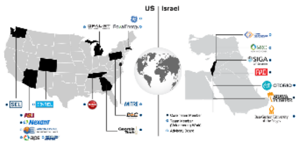
Current known data sources



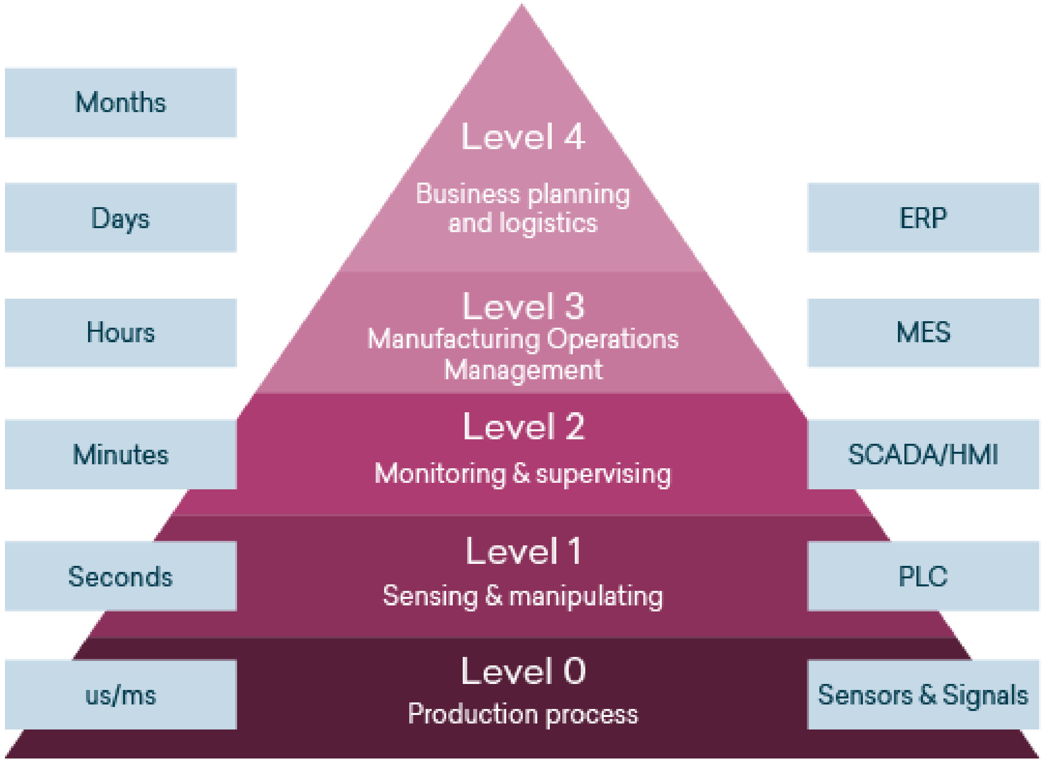
- CAPEC:
  - An enumeration of attack patterns, focused on application security.
    - Application threat modeling
    - Developer training and education
    - Penetration testing

- ATT&CK:
  - A knowledge base of cyber adversary behavior, focused on network defense
  - Comparing computer network defense capabilities
  - Defending against the advanced persistent threat
  - Hunting for new threats
  - Enhancing threat intelligence
  - Adversary emulation exercises

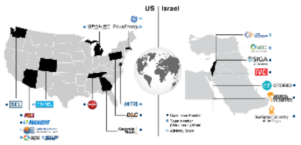
Selecting a modeling language



- UML -- too vague/generic
- ISO 62264 (ISA 95) - international standard for the integration of enterprise and control systems



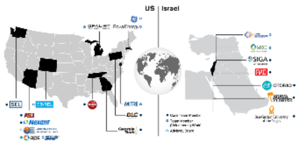
Selecting a modeling language – ISA95



- Level 0: Defines the actual physical processes
- Level 1: Defines the activities involved in sensing and manipulating the physical processes
- Level 2: Defines the activities of monitoring and controlling the physical processes
- Level 3: Defines the activities of workflow to produce the desired end products
- Level 4: Defines the business-related activities needed to manage a manufacturing operation

- Proprietary documents

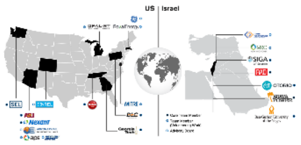
FPC – Flow Process Chart (ASME, 1947):



- Graphic representation of the sequence of all operations
- Used when observing a physical process
- Helps to analyze the steps in the process (usually to eliminate waste)

- Too old; although this modeling language matches our needs, it does not have any recent presence or documentation

WPML – Work Process Modeling Language (2011) [2]



- Built on top of the notation of the UML activity diagram
- Originally developed in order to describe the life cycle of a chemical plant
- Modeling processes that do not exist
- Can represent behavioral and functional aspects of a work process
- Hierarchical representation with varying levels of details

- Not security oriented
- Does not advance standardization of the process descriptions

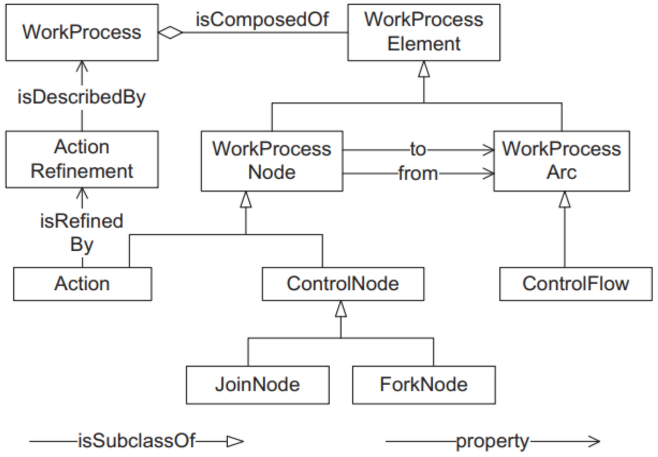
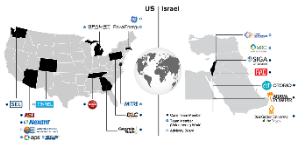


Fig. 1. Main classes of the WPML core.

[2] Hai, Ri, et al. "An ontology based approach for operational process modeling." Advanced Engineering Informatics 25, no. 4 (2011): 748-759.

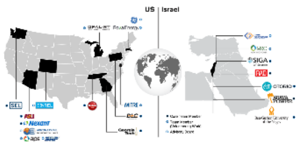
EPC - Event-Driven Process Chain (1992):



- Business process modeling oriented
- Ordered graph of events and functions
- Flow of events and activities

- Does not support the presentation of control flow

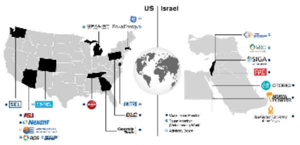
BPMN - Business Process Model and Notation (2004):



- Business processes oriented
- Depicts an end-to-end flow of a business process
- Describes the sequence of processes and message flow between process participants in set of activities
- Separates control flow from message flow
- Compatible with UML

- Still evaluating this model for our needs

I4PML (Petrasch & Hentschke, 2016):

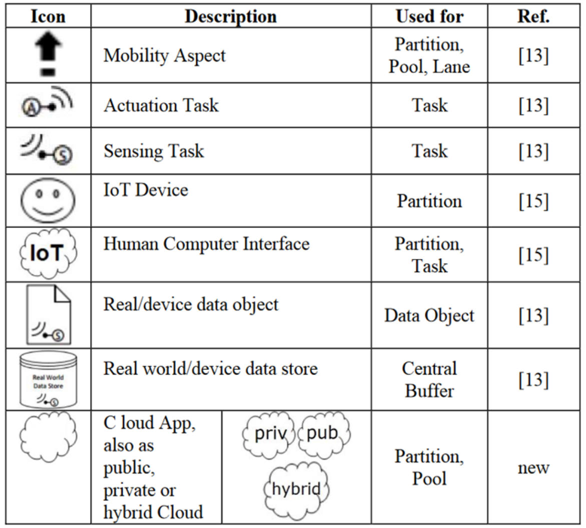


- I4PML is BPMN-based Language (OMG's BPMN 2.0)

- Can be used to model Cloud Apps, IoT devices, device data, actuation and sensing tasks, HCI, and mobility

- Still evaluating this model/language

TABLE I. ICONS TO BE USED FOR I4PML PROFILE



Icon	Description	Used for	Ref.
⬆	Mobility Aspect	Partition, Pool, Lane	[13]
	Actuation Task	Task	[13]
	Sensing Task	Task	[13]
☺	IoT Device	Partition	[15]
IoT	Human Computer Interface	Partition, Task	[15]
	Real/device data object	Data Object	[13]
Real World Data Store	Real world/device data store	Central Buffer	[13]
	C loud App, also as public, private or hybrid Cloud priv pub hybrid	Partition, Pool	new

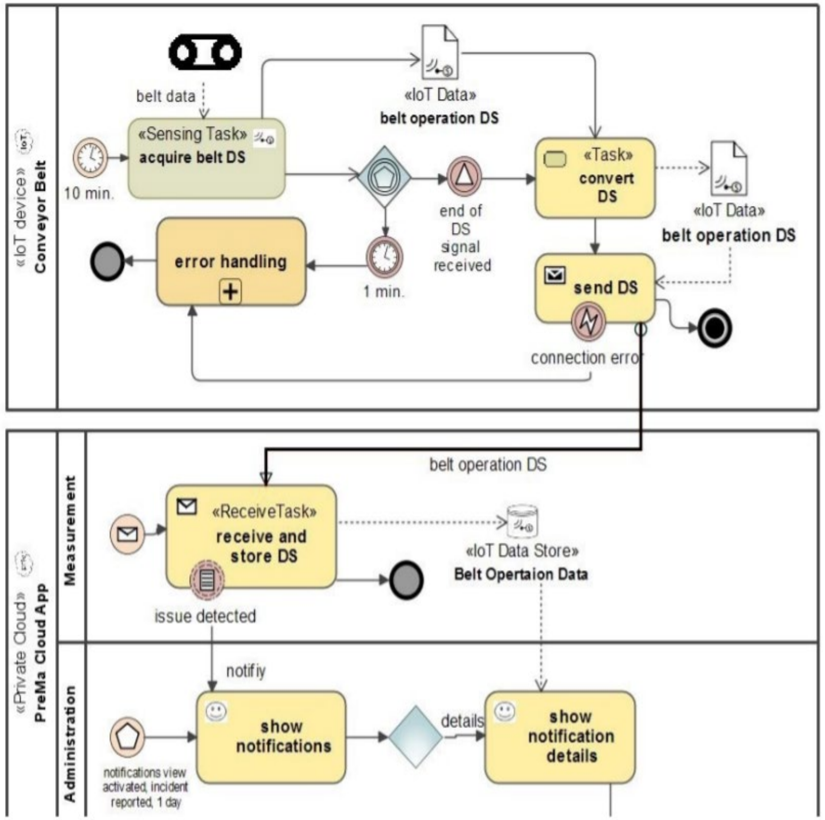
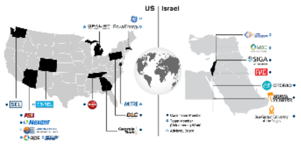


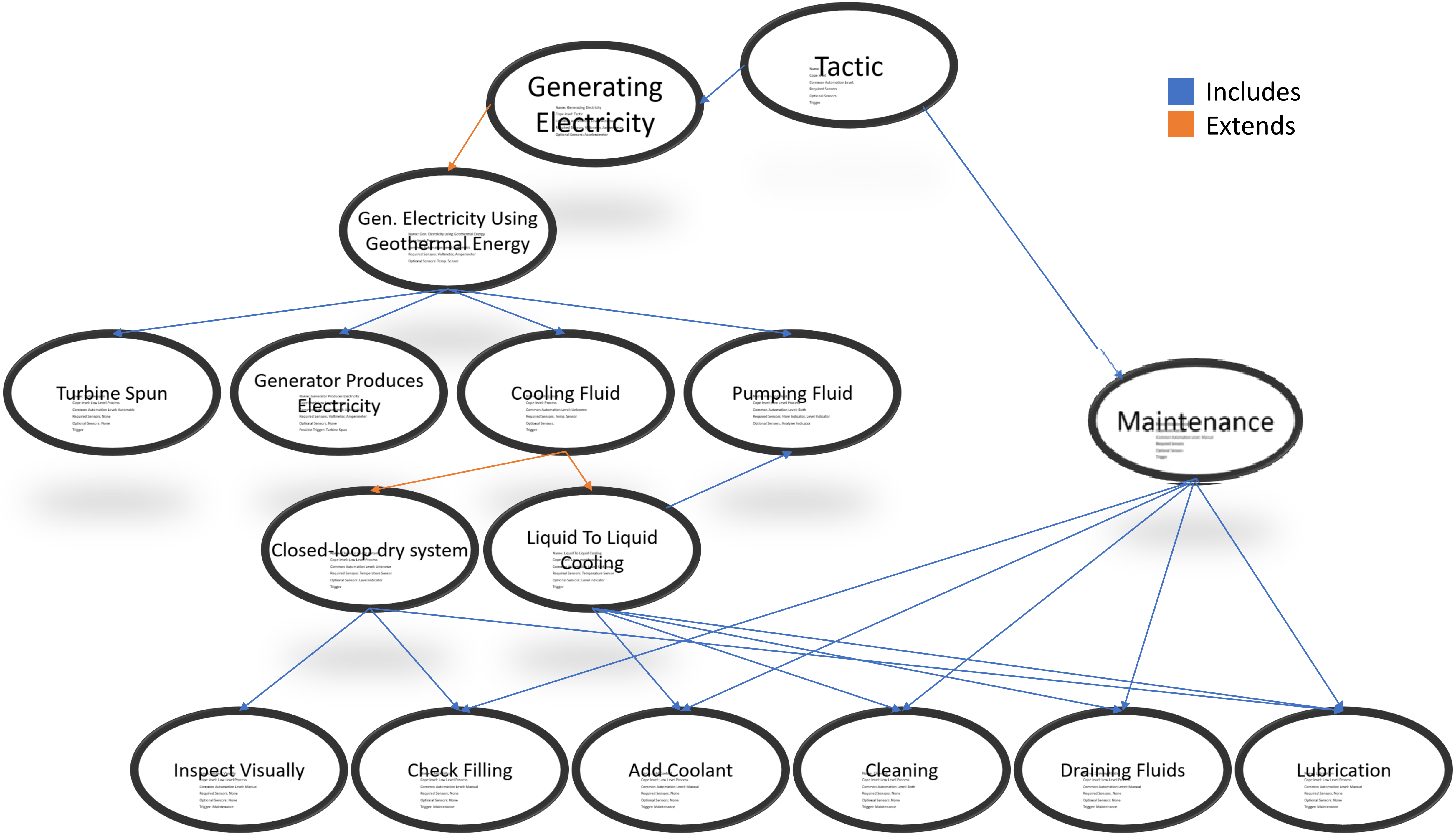
Figure 5. Process model for acquisition of belt operation data using the Industry 4.0 Process Modeling Language (I4PML)

Common Attack Pattern Enumeration and Classification (CAPEC) vs Common Operational Process Enumeration (COPE)



- Attack Patterns (CAPEC)
  - Name, ID
  - Description
  - Likelihood of Attack
  - **Typical Severity**
  - Related Attack Patterns
  - Execution Flow
  - Prerequisites
  - Skills/Resources Required
  - **Indicators**
  - **Consequences**
  - Mitigations
  - Example Instances
  - Related Weaknesses

- Operational Processes (COPE)
  - **Name, ID**
  - **Description**
  - **Cope level (Tactic\Process\Low Level Process)**
  - **Common Automation Level (Automatic\Manual\Both)**
  - **Triggers**
  - **Includes**
  - **Extends**
  - Process prevalence
  - Impact modifiers (severity)
  - Related Processes
  - Execution Flow
  - Prerequisites
  - Skills/Resources Required
  - **Required sensors/telemetry**
  - **Optional Sensors**
  - Related past incidents
  - Example Instances
  - Related Weaknesses



🟦 Includes

🟧 Extends

Tactic

Name
Cope level
Common Automation Level:
Required Sensors
Optional Sensors
Trigger

Generating Electricity

Name: Generating Electricity
Cope level: Tactic
Common Automation Level: Automatic
Required Sensors: Voltmeter, Ampermeter
Optional Sensors: Accelerometer

Gen. Electricity Using Geothermal Energy

Name: Gen. Electricity using Geothermal Energy
Cope level: Process
Common Automation Level: Automatic
Required Sensors: Voltmeter, Ampermeter
Optional Sensors: Temp. Sensor

Turbine Spun

Name: Turbine Spun
Cope level: Low Level Process
Common Automation Level: Automatic
Required Sensors: None
Optional Sensors: None
Trigger

Generator Produces Electricity

Name: Generator Produces Electricity
Cope level: Low Level Process
Common Automation Level: Automatic
Required Sensors: Voltmeter, Ampermeter
Optional Sensors: None
Possible Trigger: Turbine Spun

Cooling Fluid

Name: Cooling Fluid
Cope level: Process
Common Automation Level: Unknown
Required Sensors: Temp. Sensor
Optional Sensors:
Trigger

Pumping Fluid

Name: Pumping Fluid
Cope level: Low Level Process
Common Automation Level: Both
Required Sensors: Flow Indicator, Level Indicator
Optional Sensors: Analyzer Indicator

Maintenance

Closed-loop dry system

Name: Closed-loop dry system
Cope level: Low Level Process
Common Automation Level: Unknown
Required Sensors: Temperature Sensor
Optional Sensors: Level indicator
Trigger

Liquid To Liquid Cooling

Name: Liquid To Liquid Cooling
Cope level: Low Level Process
Common Automation Level: Unknown
Required Sensors: Temperature Sensor
Optional Sensors: Level indicator
Trigger

Inspect Visually

Name: Inspect Visually
Cope level: Low Level Process
Common Automation Level: Manual
Required Sensors: None
Optional Sensors: None
Trigger: Maintenance

Check Filling

Name: Check Filling
Cope level: Low Level Process
Common Automation Level: Manual
Required Sensors: None
Optional Sensors: None
Trigger: Maintenance

Add Coolant

Name: Add Coolant
Cope level: Low Level Process
Common Automation Level: Manual
Required Sensors: None
Optional Sensors: None
Trigger: Maintenance

Cleaning

Name: Cleaning
Cope level: Low Level Process
Common Automation Level: Both
Required Sensors: None
Optional Sensors: None
Trigger: Maintenance

Draining Fluids

Name: Draining Fluids
Cope level: Low Level Process
Common Automation Level: Manual
Required Sensors: None
Optional Sensors: None
Trigger: Maintenance

Lubrication

Name: Lubrication
Cope level: Low Level Process
Common Automation Level: Manual
Required Sensors: None
Optional Sensors: None
Trigger: Maintenance

Gen. Electricity Using Geothermal Energy

Name: Gen. Electricity using Geothermal Energy

Scope level: Process

Common Automation Level: Automatic

Required Sensors: Voltmeter, Ampermeter

Optional Sensors: Temp. Sensor

Pumping Fluid

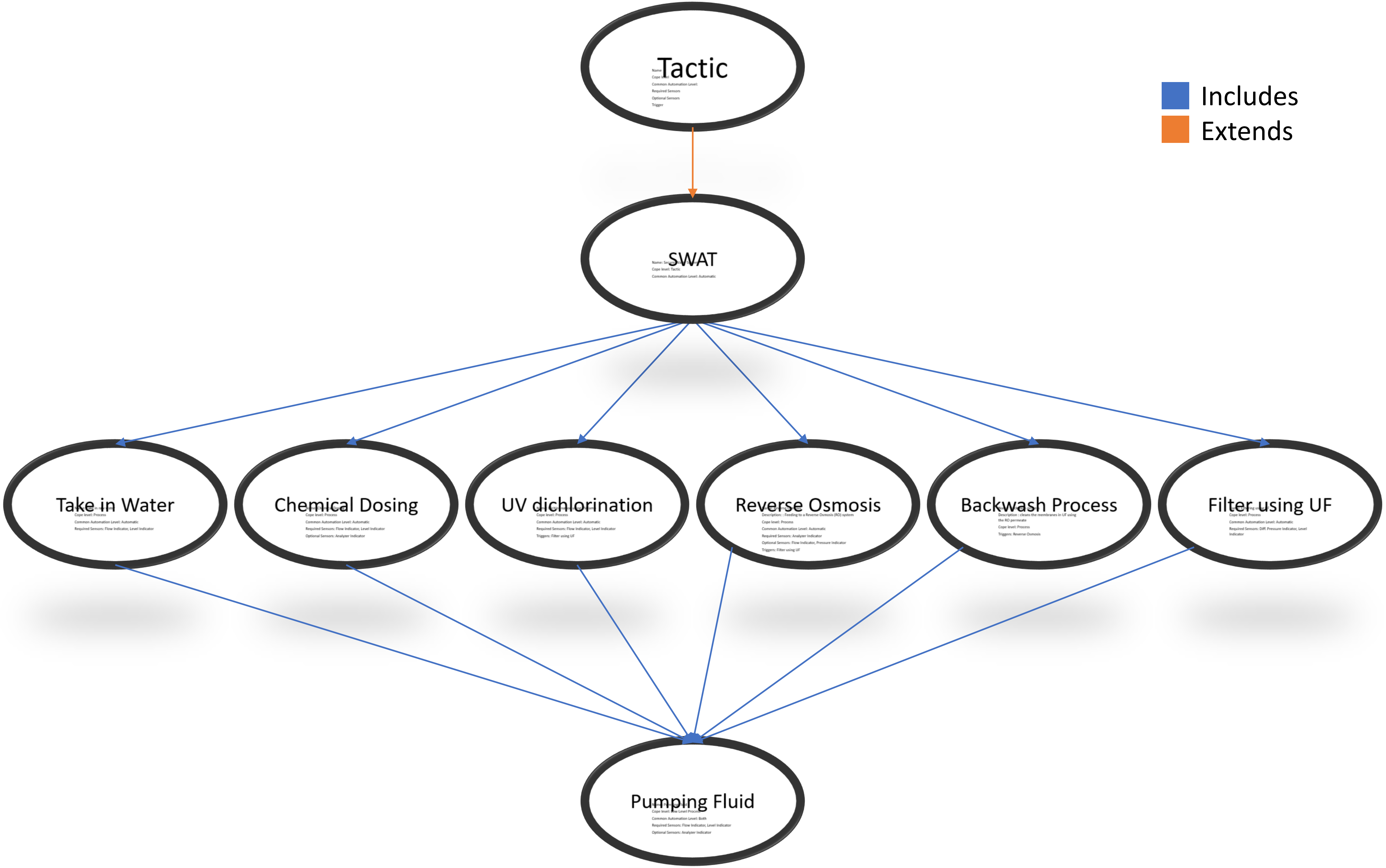
Name: Pumping Fluid

Cope level: Low Level Process

Common Automation Level: Both

Required Sensors: Flow Indicator, Level Indicator

Optional Sensors: Analyzer Indicator



🟦 Includes
🟧 Extends
Tactic
Name
Cope level
Common Automation Level:
Required Sensors
Optional Sensors
Trigger
SWAT
Name: Secure Water System
Cope level: Tactic
Common Automation Level: Automatic
Take in Water
Name: Take in raw water
Cope level: Process
Common Automation Level: Automatic
Required Sensors: Flow Indicator, Level Indicator
Chemical Dosing
Name: Chemical Dosing
Cope level: Process
Common Automation Level: Automatic
Required Sensors: Flow Indicator, Level Indicator
Optional Sensors: Analyzer Indicator
UV dichlorination
Name: Dichlorination using UV lamp
Cope level: Process
Common Automation Level: Automatic
Required Sensors: Flow Indicator, Level Indicator
Triggers: Filter using UF
Reverse Osmosis
Name: Reverse Osmosis
Description: : Feeding to a Reverse Osmosis (RO) system
Cope level: Process
Common Automation Level: Automatic
Required Sensors: Analyzer Indicator
Optional Sensors: Flow Indicator, Pressure Indicator
Triggers: Filter using UF
Backwash Process
Name: Backwash process
Description : cleans the membranes in UF using the RO permeate
Cope level: Process
Triggers: Reverse Osmosis
Filter using UF
Name: Filtering using UF
Cope level: Process
Common Automation Level: Automatic
Required Sensors: Diff. Pressure Indicator, Level Indicator
Pumping Fluid
Name: Pumping Fluid
Cope level: Low Level Process
Common Automation Level: Both
Required Sensors: Flow Indicator, Level Indicator
Optional Sensors: Analyzer Indicator

Chemical Dosing

Name: Chemical Dosing

Cope level: Process

Common Automation Level: Automatic

Required Sensors: Flow Indicator, Level Indicator

Optional Sensors: Analyzer Indicator

Reverse Osmosis

Name: Reverse Osmosis

Description: : Feeding to a Reverse Osmosis (RO) system

Cope level: Process

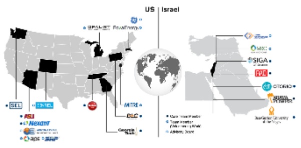
Common Automation Level: Automatic

Required Sensors: Analyzer Indicator

Optional Sensors: Flow Indicator, Pressure Indicator

Triggers: Filter using UF

Next steps



- Ongoing process of defining COPEs for the two environments and for additional ones with the support of the consortium partners

- Automatic COPE extraction using project files (with OTORIO) - TIA Portal of Siemens S7-1200 engineering file of the Meptagon lab project

- Use SWAT dataset in order to show that COPEs can be identified within the data

- Emulation of a system in order to show that we are able to identify COPEs within data

- Then,… integrating COPEs with IDS/Anomaly detectors