An idea of using a Digital Twin to perform functional safety and cybersecurity analyses

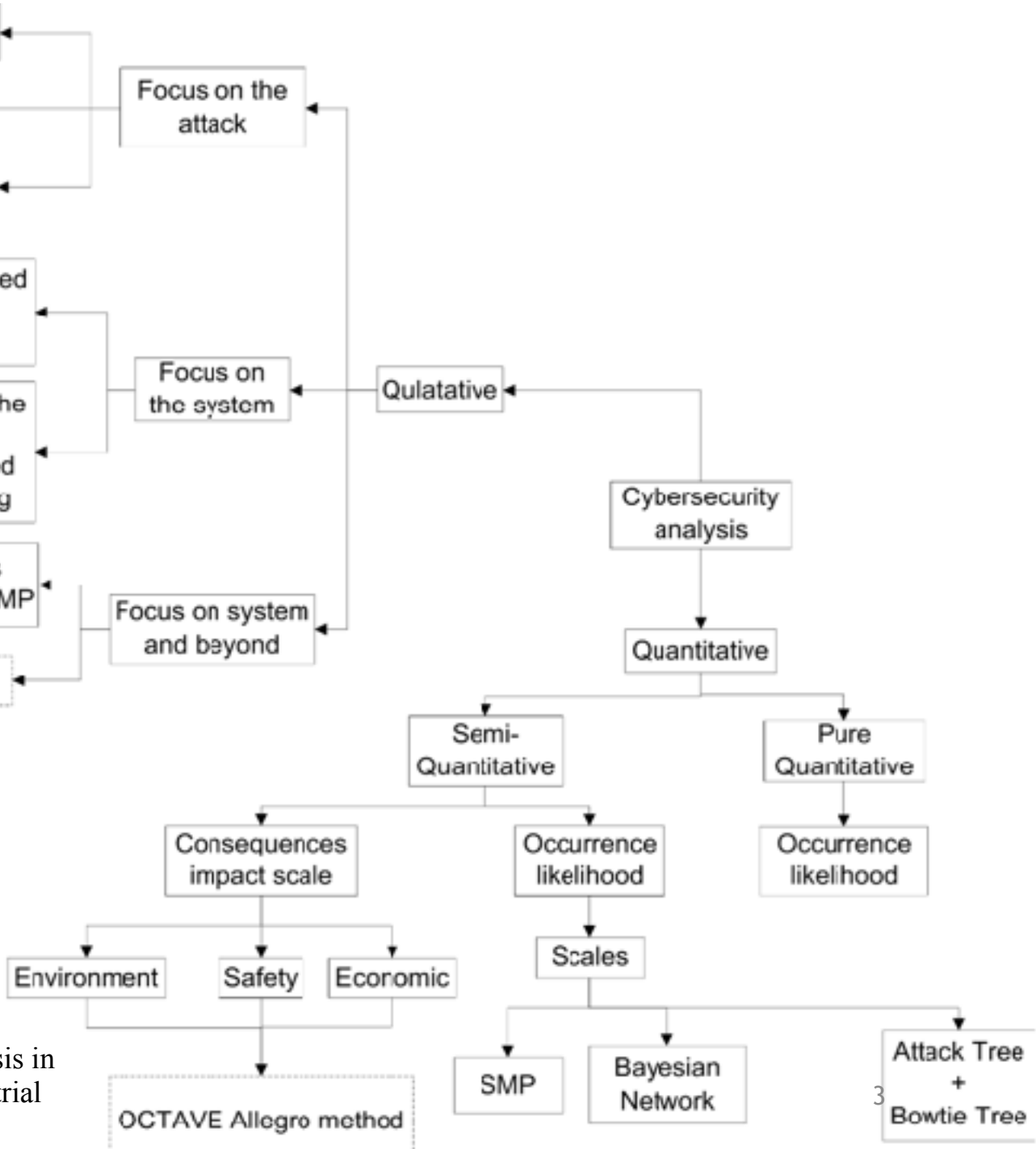
Xinxin Lou
Ph.D. Candidate
Kassel/Germany, 2019-09-24

Overview of this paper

- 1. Introduction
- 2. Required knowledge (background)
- 3. Our idea of building a Digital Twin (DT)
- 4. Performing Safety and Cybersecurity Analyses based on a DT
- 5. Advantages of doing analysis based on a DT
- 6. Conclusion

1. Introduction

- Current analysis approaches[1]



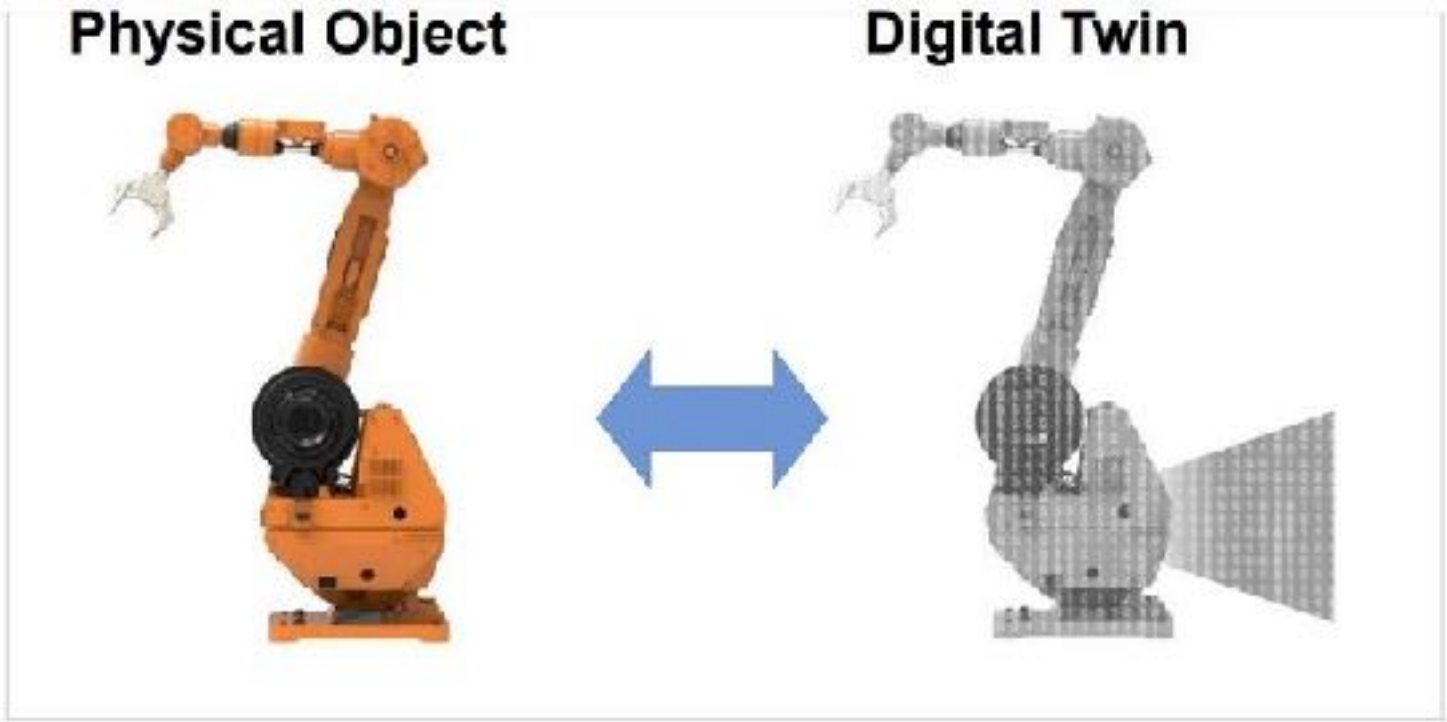
[1]. X. Lou and A. Talabi, “Chapter 4 Cybersecurity threats, vulnerability and analysis in safety critical Industrial Control System (ICS),” in Recent Developments on Industrial Control Systems Resiliency [preparing for publishing], 2019.

2. Required knowledge (Background)

- Digital Twin (DT)
- Automation ML (AML)
- Interoperability with OPC UA
- Functional specifications

2. Background -Digital Twin

- Real-time representation of physical assets in a digital world



Physical Assets → Visual Assets

Figure source: https://www.nanalyze.com/2019/01/what-is-digital-twin/

2 Background - Digital Twin

- Create a DT for various purposes
  - We use it to do safety and cybersecurity analyses
  - Other applications, e.g. what-if simulation, fault classification
- More than a model:
  - Real geometry size/data
  - Higher detail
  - Using real time data, history data to predicate the potential failures, faults
  - Prevent faults, failures in advance

2. Background - Digital Twin

- Digital Twin (DT)

- “thing” in the figure,
  - can be a component
  - system, sub-system etc.

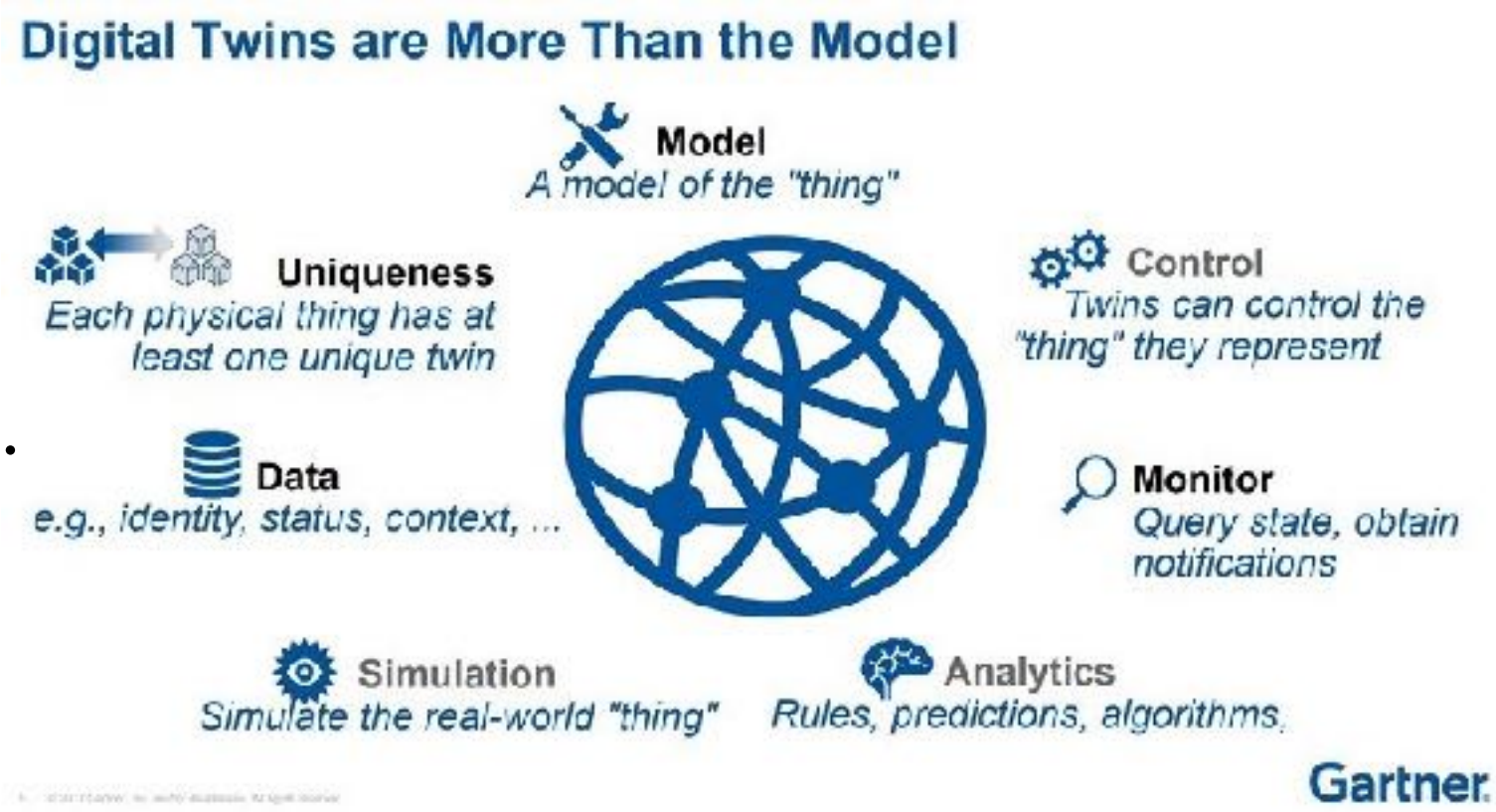


Figure source: https://www.nanalyze.com/2019/01/what-is-digital-twin/

2. Background -Automation ML

- The Automation ML (AML)—IEC 62714
  - a data format
  - to support the data exchange in a heterogeneous engineering tools
  - interconnect engineering tools from different disciplines,
    - e.g. mechanical plant engineering,
    - electrical design,
    - process control engineering etc.

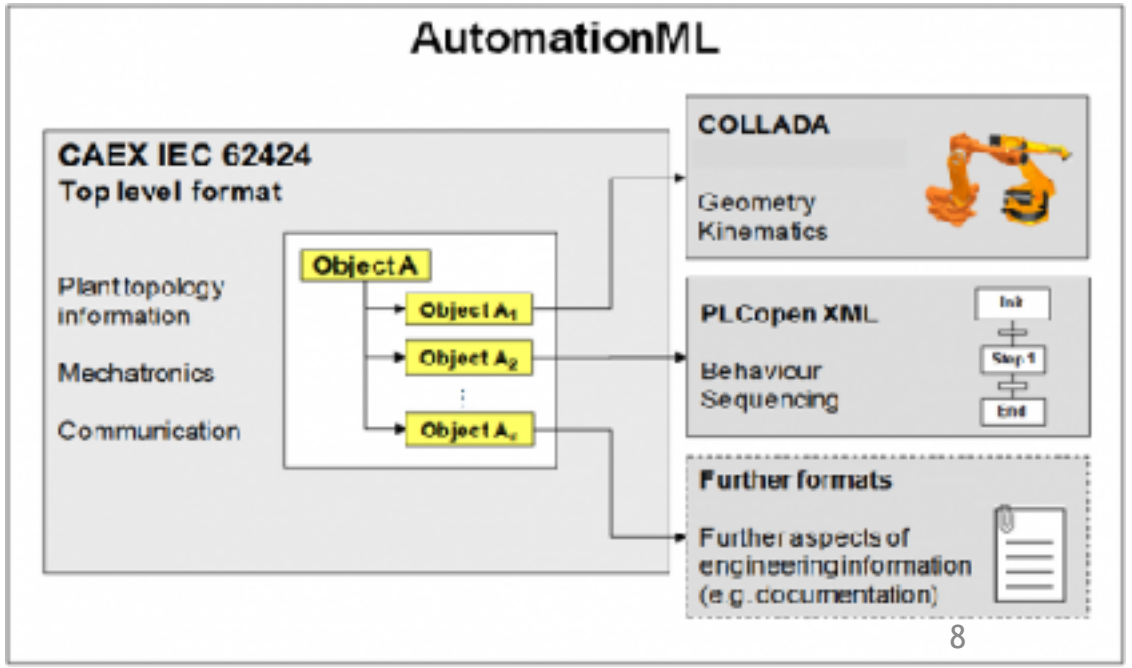
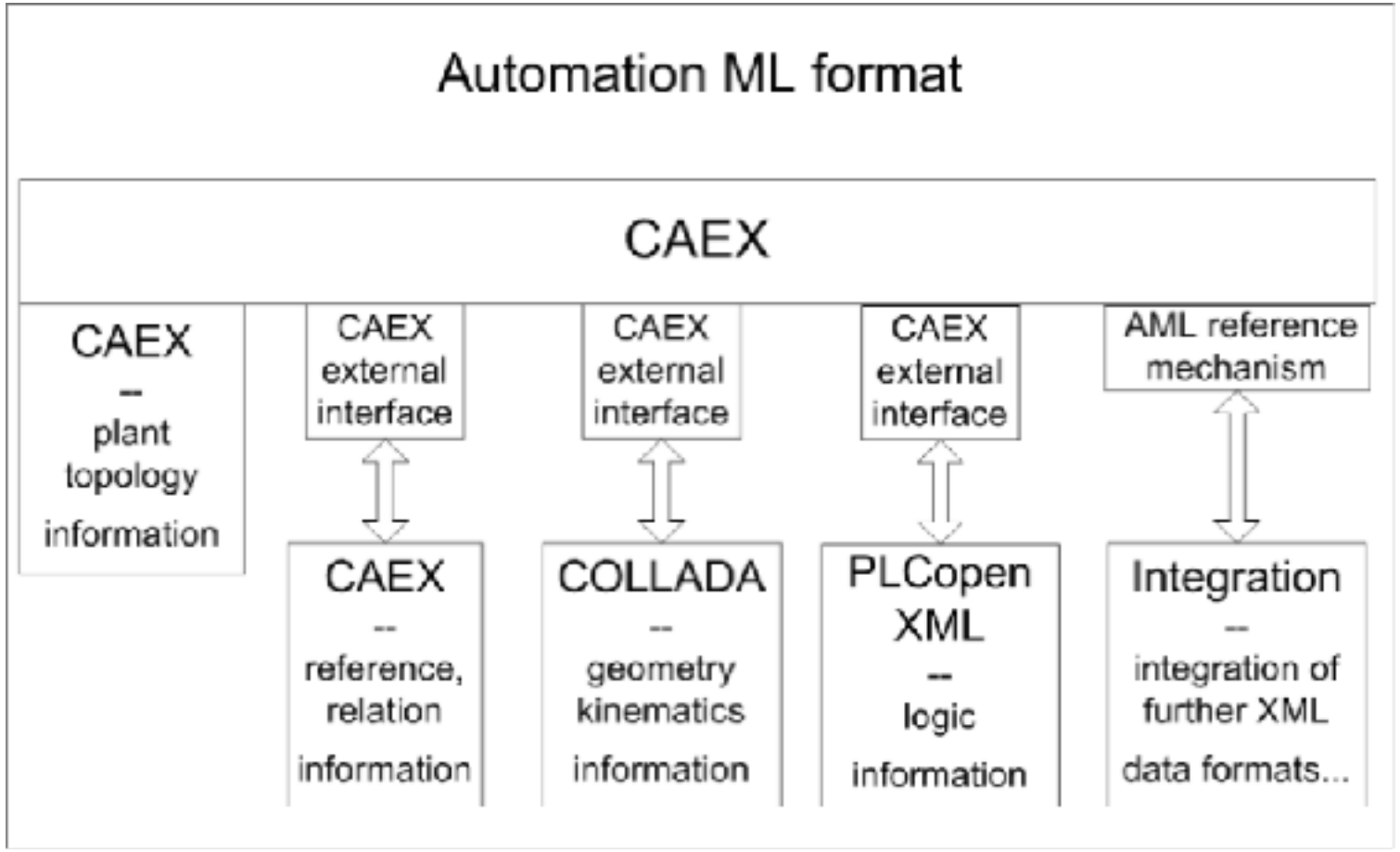


Figure source: IEC 62714

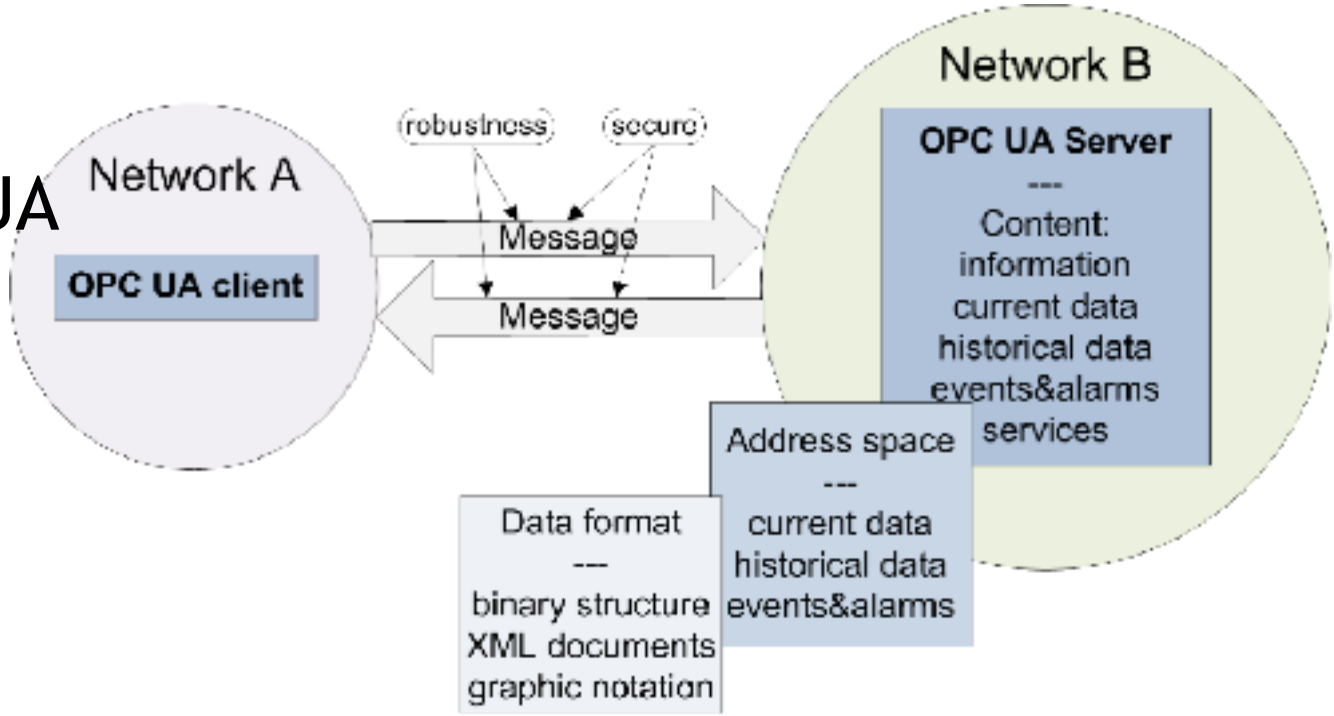
2. Background - Automation ML

- Main parts of AML



2. Background – OPC UA

- The OPC Unified Architecture (OPC UA)—IEC 62541
- Using C/S architecture to realize the communication
  - Secure
- Advantages of using OPC UA
  - Interoperability
  - Platform independence
  - Secure channels



Part of the OPC UA concept

2. Background—Functional specification

- The Functional Specification (FS) and the Refueling Machine(RM)
  - Describe what are the functions of a system
  - Using Hoare Logic
  - A refuelling machine in Nuclear Power Plant is described in our example

$$\begin{aligned} &Precon(Lift\_FA\_Cell) \\ &\Leftrightarrow \\ &Inside(FA,Cell) \wedge Empty(RM) \wedge Above(RM,Cell) \\ &\wedge Along(RM,Setdown\text{-}Axis) \wedge \neg Movement(RM,X\text{-}Axis) \\ &\wedge \neg Movement(RM,Y\text{-}Axis) \wedge \neg Movement(RM,Z\text{-}Axis) \\ &\wedge RotationLocked(FAGripper) \wedge In(FAGripper,FAGripperLowerLevel) \end{aligned}$$

$$\begin{aligned} &Postcon(Lift\_FA\_Cell) \\ &\Leftrightarrow \\ &\neg Inside(FA,Cell) \wedge Full(RM) \wedge Above(RM,Cell) \\ &\wedge Along(RM,Setdown\text{-}Axis) \wedge \neg Movement(RM,X\text{-}Axis) \\ &\wedge \neg Movement(RM,Y\text{-}Axis) \wedge \neg Movement(RM,Z\text{-}Axis) \\ &\wedge RotationLocked(FAGripper) \wedge In(FAGripper,FAGripperHighLevel) \end{aligned}$$

- The correctness and the consistency of FS have been checked in previous work [2].

[2] Xinxin Lou et.al. “Combining AI planning advantages to assist preliminary formal analysis on ICS cybersecurity vulnerabilities,” in IEEE ECAI2018, Iasi, Romania, 2018.

3. Building a DT (Digital Twin)

- Functional Specification (FS)
  - FS of a refuelling machine: already existing description of system
  - → using AML +OPC UA
- AML
  - Physical components + processes
  - Using CAEX and COLLADA (in AML standards)
  - e.g. the field site, the context structures, the physical components of a system, mechanical relations
  - Environment static and dynamic data containing in Refueling Machine
- OPC UA
  - Communication
  - Realize secure communication, interoperability access among various layer
    - from office to field
  - Sensor, actuator variables → in OPC UA address space

4. Idea of performing analysis based on a DT

- Safety aspect
  - Real time data+ history data + algorithm
    - →Analysis +predicate failures/faults
  - According to the data value in the DT,
    - e.g. process variables like thresholds, relevant with safety to evaluate the countermeasures of system failures/components are sufficient as a basic towards a specific SIL (Safety Integrity Levels) evaluation.
  - Interaction with a physical control system via HMI while in operation is usually not feasible and during the operation the process data (state, variables) is missing

4. Idea of performing analysis based on a DT

- Security aspect
  - Security configuration details can be read from the OPC UA configuration XML
  - Evaluate the physical protection measures
    - e.g. access control
  - Evaluate the security of communication networks and network equipment
- Security and Safety
  - Integrated formal/semi-formal modelling and analysis

5. Advantages of doing analysis based on a DT

- The advantages of using DT to do the safety and cybersecurity analysis
  - The effect of any changes in system can be seen immediately
    - E.g. countermeasures setup
  - Safety analysists, can consider what kind of measures can be used to improve the safety with direct links to the involved processes and objects

5. Advantages of doing analysis based on a DT

- Security by design can be represented:
  - AML: the role-based control can be utilized to realize the Role Based Access Control (RBAC)
  - OPC UA: secure channel
  - not only current communication content, also the history data, the events etc. can also be accessed by the client, based on the history data and the current status, predication can be made
  - Attribute based access control (ABAC) provides support for restricting access down to the object level
  - Before the real implementation of a system, based on the DT, evaluate security measures to see the effectiveness of these measures, e.g. assign roles, rights of staff and restrict access to assets

6. Conclusion

- Twinning a system
  - Functional Specification
  - AML
  - OPC UA
- Analysis based on the Digital Twin
  - Safety
    - Redundancy, diversity, Safety Defense-in-Depth(DiD), ...
  - Security
    - Security by design, Security DiD, Security Controls, …
  - Integrated Safety & Security
    - Formal/Semi-formal Modelling
    - Digital Twin

Tanks Again!

- Xinxin Lou
- Ph.D. Candidate
- Kassel/Germany, 2019-09-24