A Simulated Steam Turbine Generator Subsystem for Research and Training

R. Altschaffel[1]
M. Hildebrandt[1]
J. Dittmann[1]

[1]Otto-von-Guericke University, Magdeburg, Germany

Outline

- Introduction
- Why to simulate a Steam Turbine in the first place?
- Steam Turbine
  - Components
  - Control Narrative
- Design of an IC Simulator
- Use-Cases
  - Training
  - Security Evaluation

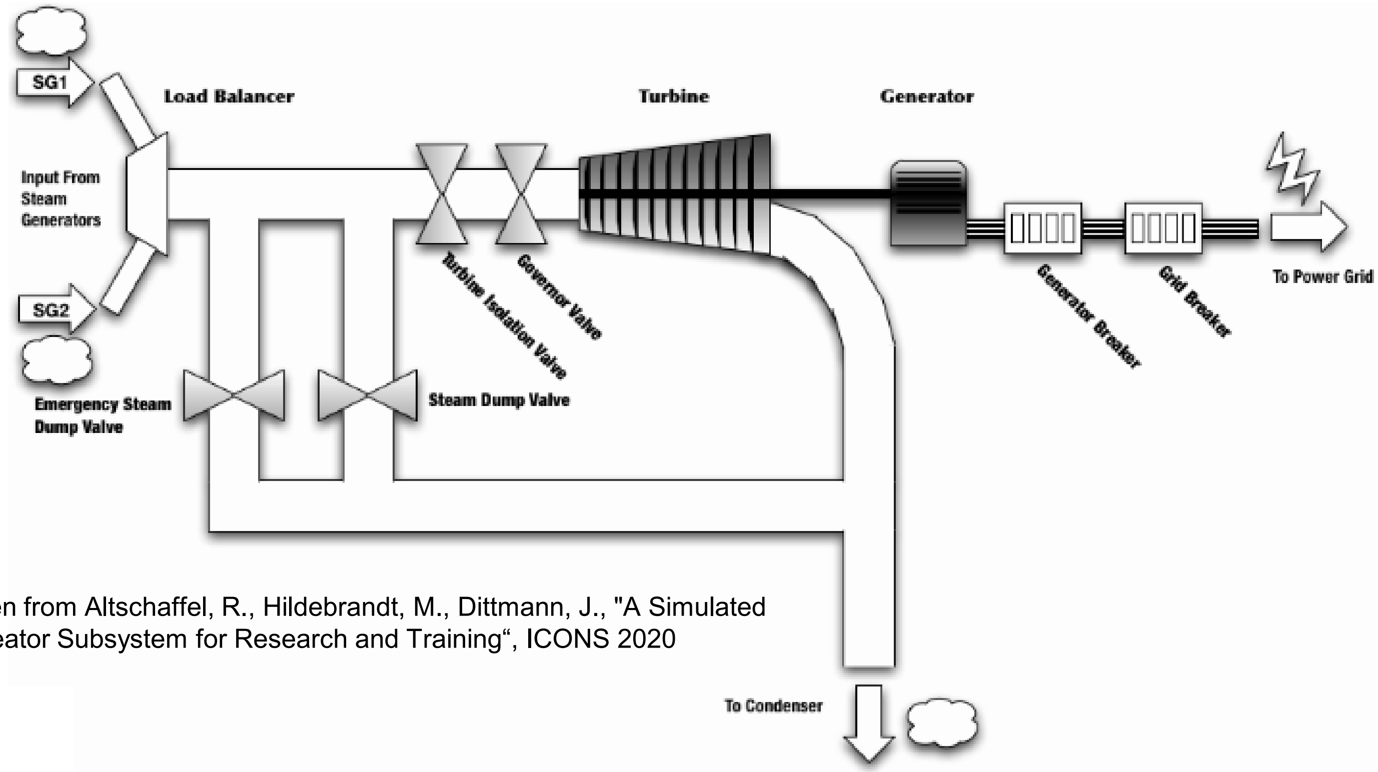
Why to simulate an NPP in the first place?

- A NPP is highly complex
  - Operators require training to increase safety
  - Research into better safety measures might also increase safety
- NPP have also become targets of cyber-attackers (=attacks performed by using the computing technology inside NPPs)
  - Cyber-Security training is also required
  - Research into better protection against cyber-attacks might also increase security, and therefore safety

- Training is performed using Mockups or simulators
  - Mockups are expensive
  - Simulators are geared towards showing the physical process, not the computing units (and are hence bad to train against cyber-attacks)
- Need for a simulator which includes realistic behavior of the computing technology
  - Easy to deploy, easy to alter, easy to scale …

Steam Turbines - Components

- Steam Turbines
  - Generate electric power by using the steam flow
  - Consists of a rotating shaft and a number of blades
  - Contain various sensors and actors



Steam Turbine Model, taken from Altschaffel, R., Hildebrandt, M., Dittmann, J., "A Simulated Steam Turbine Geneator Subsystem for Research and Training“, ICONS 2020

Steam Turbines – Control Narrative 1/2

- Normal Operation
  - Turbine Isolation Valve open
  - Emergency Steam Dump Valve and Steam Dump Valve closed
  - steam passes unaltered to the turbine, generating energy in the generator
  - steam is directed to the condenser.
- Start-up Procedure
  - turbine speed up slowly to setpoint by feeding a small amount of steam into the turbine
  - Emergency Steam Dump closed
  - Turbine Isolation Valve open.

Steam Turbines – Control Narrative 2/2

- Excess Steam
  - steam pressure exceeds a given limit
  - Steam Dump Valve opens (partly)
  - Excess steam is directed towards the condenser
  - Reduced steam passes on to the turbine, generating electrical energy in the generator
  - Steam that reached the turbine is directed to the condenser
- Trip:
  - Turbine Isolation Valve closes
  - Emergency Steam Dump Valve and the Steam Dump Valve opens
  - All steam passes directly to the condenser
  - Turbine will not be powered by steam and hence no energy will be produced in the generator
  - Notification is triggered

Design of an IC Simulator 1/2

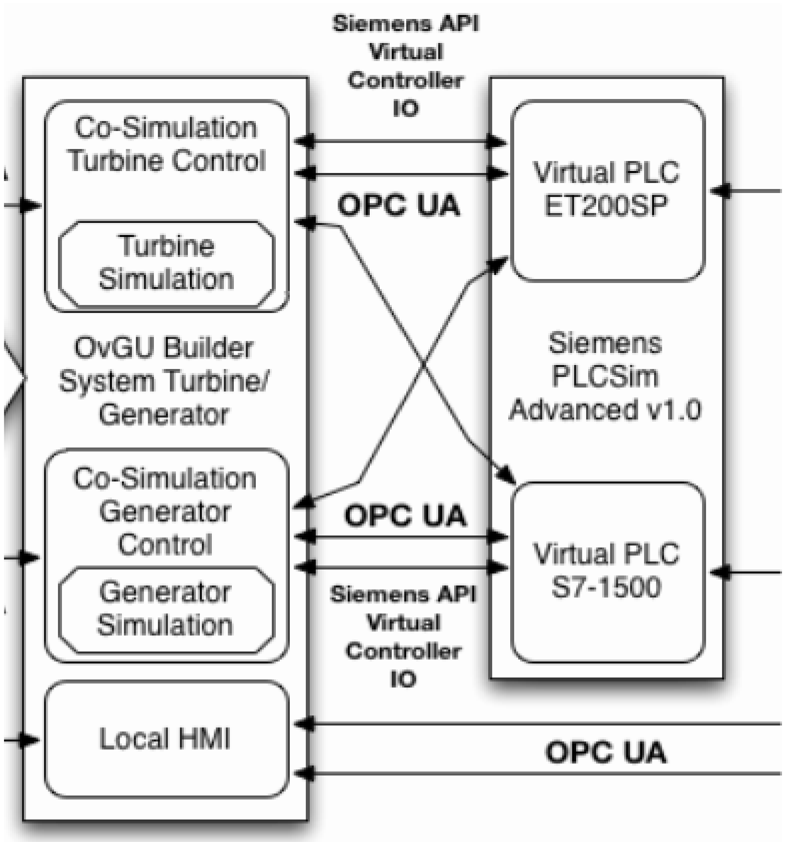
- From an automation point of view, we have various components
  - Sensors (collecting data about physical process)
  - Computing units (computing this data)
  - Actors (influence this process based on this computation)

- Actors & Sensors can be done either by …
  - Physical Mock-Up (implementing the physical process)
    - Hard to transport
    - Expensive
    - Can be physically destroyed
  - Software Simulation (simulating the physical process)
    - Requires a good underlying model
    - Easy to transport / deploy / clone / reset

Design of an IC Simulator 2/2

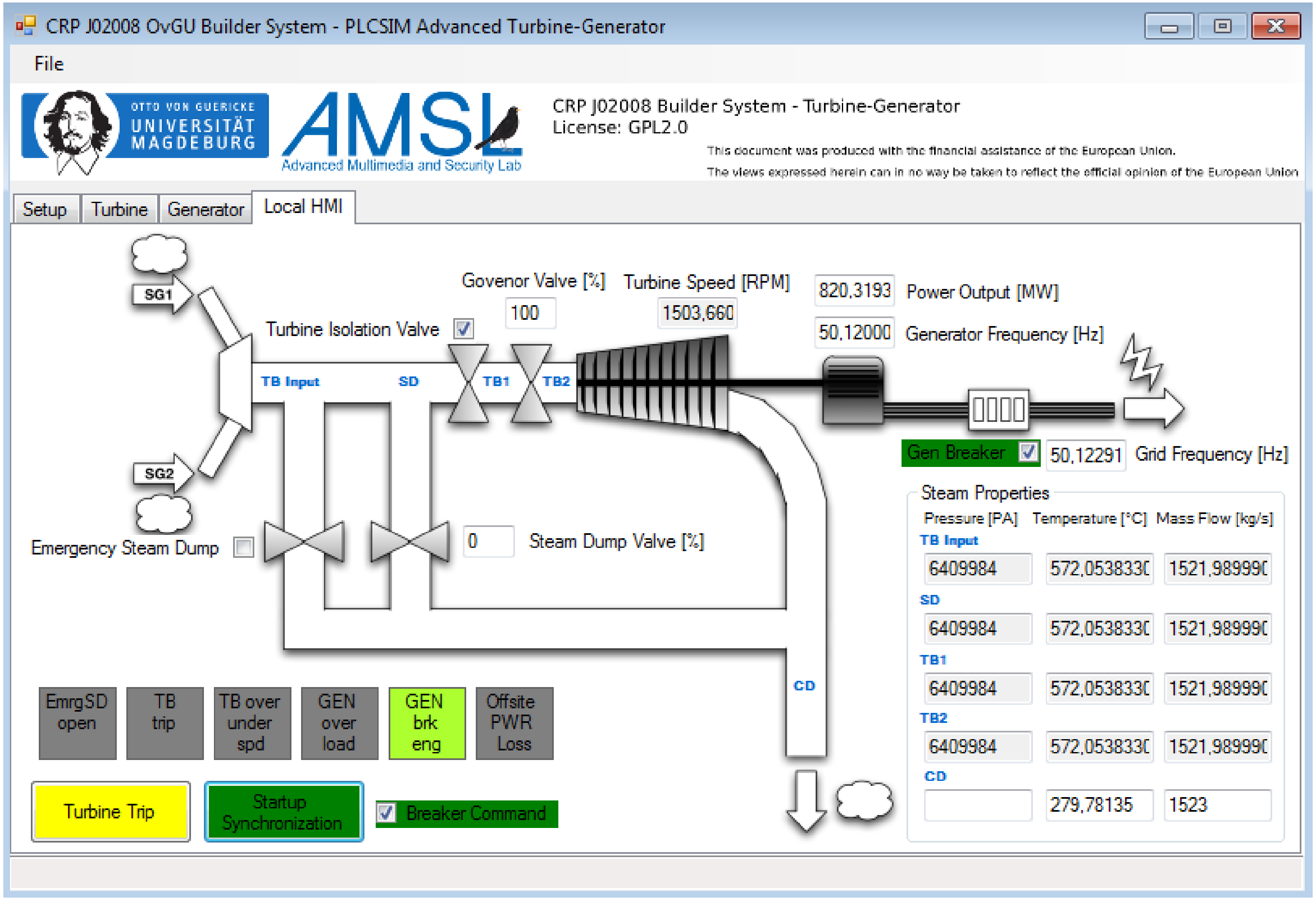
- Computing Units can be done either by …
  - Physical PLC
    - Harder to transport
    - Expensive
    - Can be physically destroyed
  - SoftPLC (PLC done in software)
    - Internal processes not realistic
    - Communication with actors and sensors realistic
  - Simulated PLC (Runtime environment is emulated, purpose-built implementation of real PLC specification)
    - Internal processes realistic
    - Does not use the same internal software (firmware) like the PLC which specification it implements. Hence, it might have other software bugs.
    - Communication with actors and sensors realistic
  - PLC Firmware in Emulator (the same firmware as in a PLC)
    - Same implementation - mostly same bugs are present in PLC
    - PLC behavior and communication with sensors, actors and other PLCs is realistic
    - However, some aspects of a physical PLC might be still missing

The IC Simulator



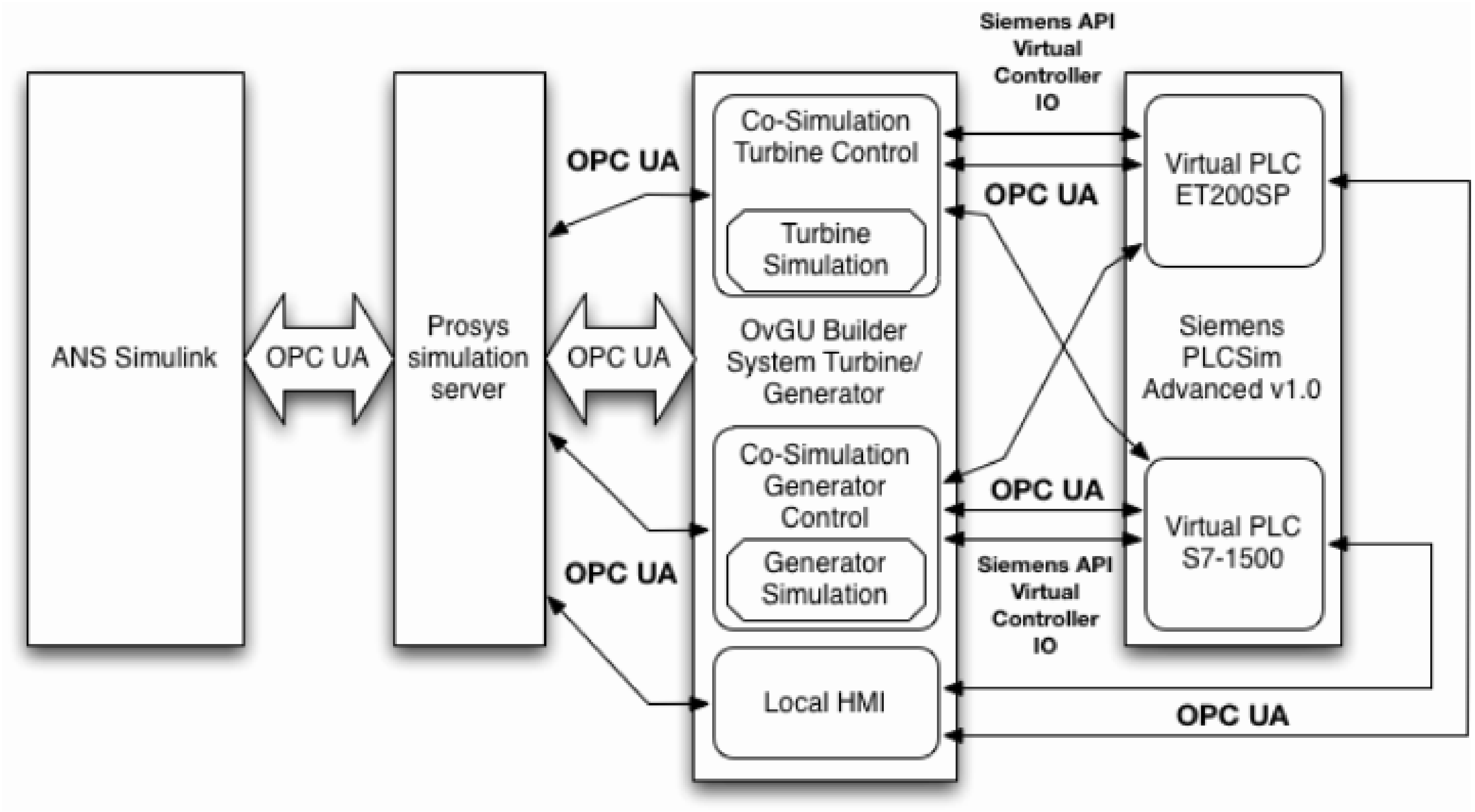
- (Co-)Simulation of physical process
- Virtual Sensors
- Real Computing Unit Firmware running in Virtual PLCs
- Virtual Actors
- Local HMI

Virtualized Subsystem, taken from Altschaffel, R., Hildebrandt, M., Dittmann, J., "A Simulated Steam Turbine Geneator Subsystem for Research and Training“, ICONS 2020



Virtualized Subsystem HMI, taken from Altschaffel, R., Hildebrandt, M., Dittmann, J., "A Simulated Steam Turbine Geneator Subsystem for Research and Training", ICONS 2020

The IC Simulator – Connection to ANS



Virtualized Subsystem, taken from Altschaffel, R., Hildebrandt, M., Dittmann, J., "A Simulated Steam Turbine Geneator Subsystem for Research and Training“, ICONS 2020

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
AMSL Advanced Multimedia and Security Lab

Usage

- Training in Turbine Operation
  - Including reaction to misbehavior of components
  - Including incident response to suspected cyber-attacks
  - Offers view at ‘model reality’, ‘PLC reality’ and ‘Operator reality’

- Security Evaluation
  - The realistic internal behavior allows for developing and/or evaluating security measures to prevent attacks
  - … or to at least detect and/or investigate these attacks

Summary and Outlook

- Easy to deploy simulator which focuses on a realistic behavior of an NPP subsystem (Steam Turbine), including
  - Physical process
  - Operational Technology
  - Local HMI
- Can be used for Research and Training concerning cyber attacks and normal attacks

- Open points:
  - Increase performance
  - Include more attack patters (or components faults)

Thank you for the attention

Robert.Altschaffel@iti.cs.uni-magdeburg.de
Mario.Hildebrandt@iti.cs.uni-magdeburg.de

This document was produced with the financial assistance of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union.