Exploring the Possibility of Forensic Investigations on Steam Turbine Governing Systems

Robert Altschaffel
Mario Hildebrandt
Stefan Kiltz
Jana Dittmann

Otto-von-Guericke-University
Magdeburg, Germany

Outline

- Introduction
- Fundamentals
  - Steam Turbine Governing Systems
  - Computer Forensic Investigation
- Generalized Steam Turbine Governing System
  - Data Streams
  - Possibilities for Forensic Investigation
- Simulation Model of a STG System
- Conclusion & Future Work

Introduction

- Industrial automation is a central aspect of modern power plants
  - Controls different functions
  - Relies on electronic control systems
  - Might be interconnected
- Like any computer system, an industrial control system might fail
  - By attack or by accident
- How can the events that led to such an incident be reconstructed?

Steam Turbine Governing Systems

- Steam Turbine Governing (STG) Systems are used as a starting point
- Steam Turbine [Dic15]
  - Generates electric power by using steam pressure generated by the steam generator
  - Consists of a shaft connected to a number of blades
  - Steam turbine needs a stream with specific temperature and pressure
  - STG is used to ensure these characteristics
- Steam Turbine Governing Systems
  - Have a range of sensors for temperature and pressure
  - Have valves as actuators
  - ➢ Classical control system

Forensics

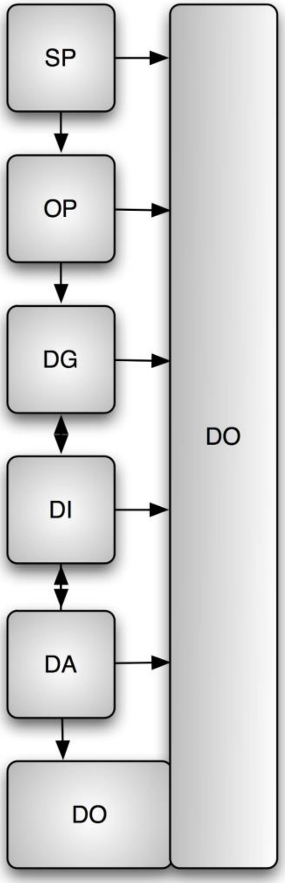
- Forensics = the reconstruction of events by using scientific methods
  - Events might be attacks or failures
- Validation of a forensic examination depends on …
  - Integrity / Authenticity of the traces
  - Trustworthiness of the forensic method
- Forensic Investigation on computer systems is a well-researched domain
  - Interest in specialized/connected domains (e.g. automotive, ICS) rises

Computer Forensic Investigations 1/2

- Three principal sources of data (‘data streams’) [ALK17]
  - Communication
    - Data exchanged between components using physical network connections
    - Can only be gathered at the moment of transmission
  - Volatile data
    - Data stored in volatile memory which is lost after voltage loss and/or deactivation of a system
    - Can be gathered by querying the respective system for this data
  - Persistent data
    - Data stored in persistent memory
    - Can be gathered by querying the respective system for this data or by extracting the data directly from the component

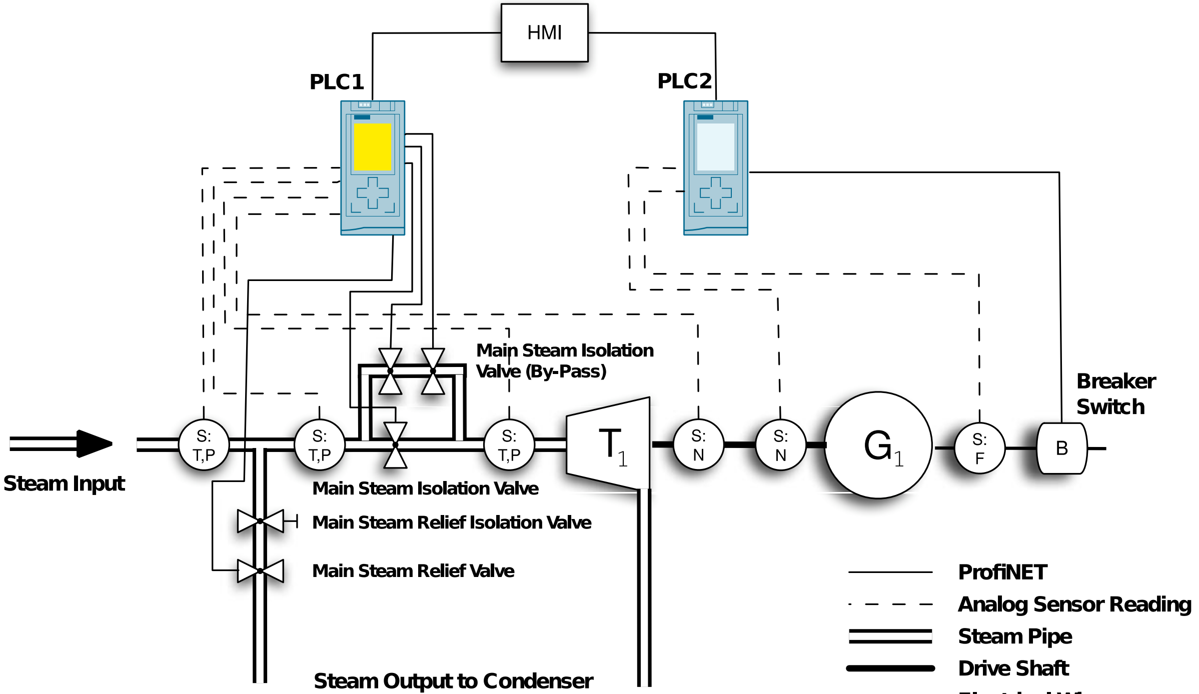
Computer Forensic Investigations 2/2

- Forensic model according to [KVD15]
  - **Strategic preparation** (*SP*) measures taken by the operator n prior to an incident.
  - **Operational preparation** (*OP*) measures of preparation after a suspected incident.
  - **Data gathering** (*DG*) measures to acquire and secure digital evidence.
  - **Data investigation** (*DI*) measures to evaluate and extract data for further investigation.
  - **Data analysis** (*DA*) measures for detailed analysis and correlation between digital evidence from various sources.
  - **Documentation** (*DO*) measures for the detailed documentation of the proceedings



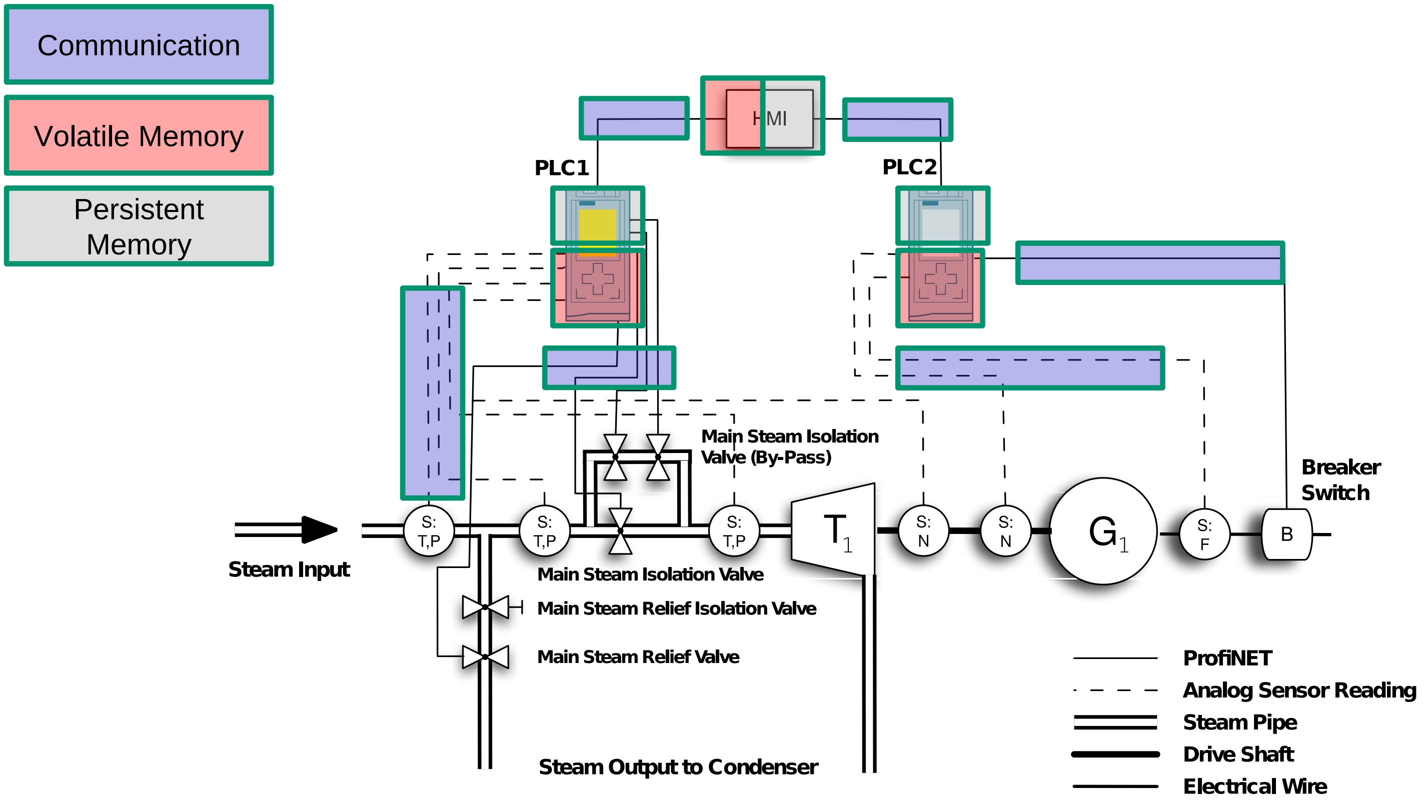
Generalized Steam Turbine Governing System

- Understanding of components is essential to identify possible traces
  - Creation of a generalized and simplified model for a STG system



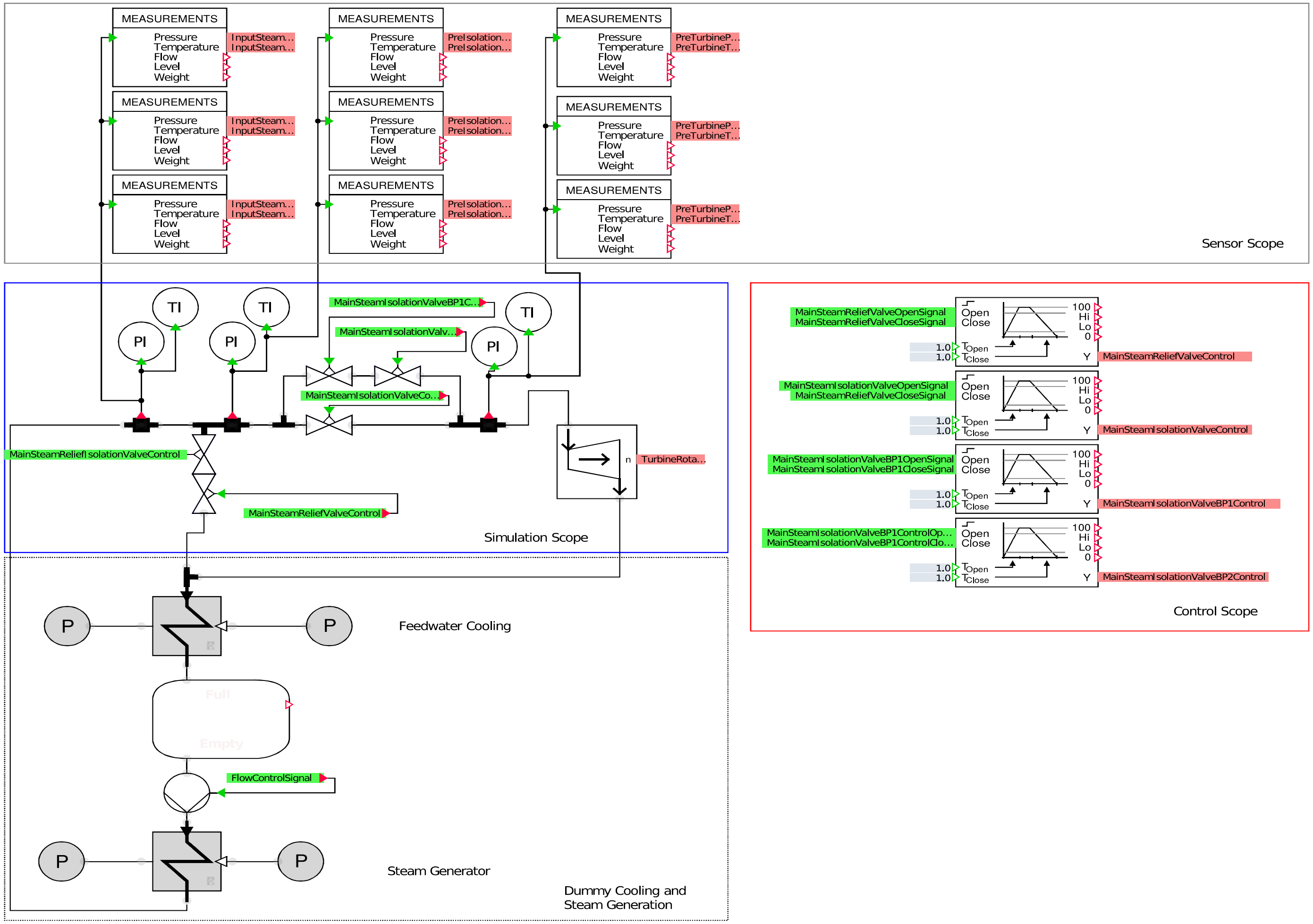
Generalized Steam Turbine Governing System – Data Streams

- Allows Identification of the three forensic useable data streams

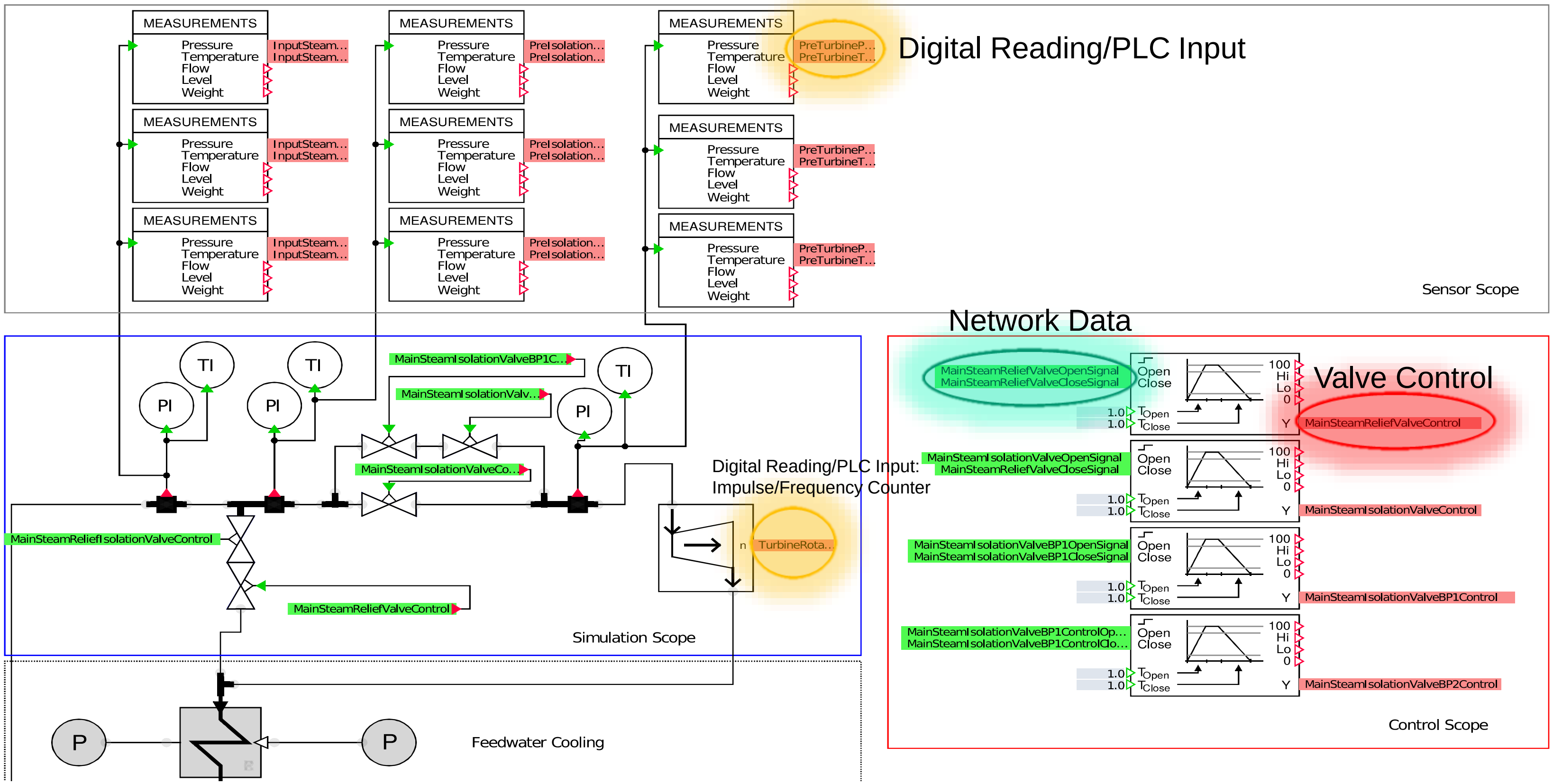


Simulation Model of a STG System 1/3

- Simulation environment to create data streams based on an abstract, simplified model
- Objective: customizable setup to analyze forensic traces for various attack patterns
- FlowNet-based model with simplified thermodynamics



Simulation Model of a STG System 2/3


MEASUREMENTS
Pressure
Temperature
Flow
Level
Weight
InputSteam...
InputSteam...
PreIsolation...
PreIsolation...
PreTurbineP...
PreTurbineT...
Sensor Scope
TI
PI
MainSteamIsolationValveBP1C...
MainSteamIsolationValv...
MainSteamIsolationValveCo...
MainSteamReliefIsolationValveControl
MainSteamReliefValveControl
n
TurbineRota...
Simulation Scope
P
Feedwater Cooling
MainSteamReliefValveOpenSignal
MainSteamReliefValveCloseSignal
Open
Close
100
Hi
Lo
0
1.0
TOpen
TClose
Y
MainSteamReliefValveControl
MainSteamIsolationValveOpenSignal
MainSteamReliefValveCloseSignal
MainSteamIsolationValveControl
MainSteamIsolationValveBP1OpenSignal
MainSteamIsolationValveBP1CloseSignal
MainSteamIsolationValveBP1Control
MainSteamIsolationValveBP1ControlOp...
MainSteamIsolationValveBP1ControlClo...
MainSteamIsolationValveBP2Control
Control Scope

Digital Reading/PLC Input

Network Data

Valve Control

Digital Reading/PLC Input: Impulse/Frequency Counter

Simulation Model of a STG System 3/3

- Simulation model has to cover all operational modes – power-up, operation, power-down
- Forensic investigation is not limited to attacks as a result of malicious intent – malfunctions are considered as well
- Extension of the model: generator control and communication with the steam turbine governing control, HMI integration

Conclusion & Future Work

- Identification of possible data traces usable for forensic investigation in ICS environment within a power plant
- A simplified generic model for STG systems is presented for supporting the forensic process by identifying data traces
- The possibility of acquiring these traces has been investigated using a simulated environment
- Future work requires practical confirmation on the results yielded in the simulated environment

References

Thank you for your Attention!

References:

- [Dic15] E. Dick, “Fundamentals of Turbomachines”, Springer, Dordrecht 2015
- [KDV15] S. Kiltz, J. Dittmann, C. Vielhauer, "Supporting Forensic Design - a Course Profile to Teach Forensics", IMF 2015
- [ALK17] R. Altschaffel, K. Lamshöft, S. Kiltz, J. Dittmann, “A Survey on Open Automotive Forensics”, SECUREWARE 2017

Contact information:

Robert Altschaffel
Department of Computer Science
Research Group Multimedia and Security
Institute of Technical and Business Information Systems
Otto-von-Guericke-University of Magdeburg

Universitaetsplatz 2
39106 Magdeburg, Germany
EMail: robert.altschaffel@iti.cs.uni-magdeburg.de
Phone: +49 (391) 67 58046

Mario Hildebrandt
Department of Computer Science
Research Group Multimedia and Security
Institute of Technical and Business Information Systems
Otto-von-Guericke-University of Magdeburg

Universitaetsplatz 2
39106 Magdeburg, Germany
EMail: mario.hildebrandt@iti.cs.uni-magdeburg.de
Phone: +49 (391) 67 51603