

UNIVERSITY OF VERONA

Department of COMPUTER SCIENCE

Master's Degree in
COMPUTER SCIENCE AND ENGINEERING

Master Thesis

**Towards Process Comprehension of Industrial
Control Systems: a Framework for Analyzing
Industrial Systems**

Candidate:

Marco OLIANI
VR457249

Supervisor:

Prof. **Massimo MERRO**

Co-supervisor:

Prof. **Ruggero LANOTTE**
University of Insubria

Academic Year 2022/2023

*“If you spend more on coffee than on IT security, you
will be hacked. What’s more, you deserve to be hacked”*
(Richard Clarke)

Abstract

Bla bla bla

Contents

1	Introduction	1
1.1	Contribution	1
1.2	Outline	1
2	Background	3
2.1	Industrial Control Systems in a nutshell	3
2.2	ICS components	4
2.2.1	SCADA systems	4
2.2.1.1	SCADA architecture	5
2.2.2	Field devices	7
2.2.3	Programmable Logic Controllers	7
2.2.3.1	PLC Architecture	8
2.2.3.2	PLC Programming	9
2.2.3.3	PLC Security	10
2.2.4	Remote Terminal Units	11
2.2.5	Human-Machine Interface	12
2.2.6	Cybersecurity components	12
2.3	Communication Networks	13
2.3.1	ICS Communication Protocols	13
2.3.1.1	Modbus	13
2.3.1.2	EtherNet/IP	17
2.3.1.3	Common Industrial Protocol (CIP)	19
2.3.1.4	Other Protocols	20

3	State of the Art	21
3.1	Literature on Process Comprehension	22
3.2	Ceccato et al.'s methodology for analyzing water-tank systems	24
3.2.1	Testbed	26
3.2.2	Scanning of the System and Data Pre-processing . . .	28
3.2.3	Graphs and Statistical Analysis	30
3.2.4	Invariants Inference and Analysis	32
3.2.5	Business Process Mining and Analysis	33
3.2.6	Application	34
3.2.7	Limitations	41
4	A Framework to Improve Ceccato et al.'s Work.	51
4.1	The novel Framework	52
4.1.1	Framework Structure	54
4.1.2	Python Libraries and External Tools	55
4.2	Analysis Phases	56
4.2.1	Phase 1: Data Pre-processing	56
4.2.1.1	Subsystem Selection	58
4.2.1.2	Dataset Enrichment	60
4.2.1.3	Datasets Merging	67
4.2.1.4	Brief Analysis of the Obtained Subsystem .	68
4.2.2	Phase 2: Graphs and Statistical Analysis	71
4.2.3	Phase 3: Invariant Inference and Analysis	76
4.2.3.1	Revised Daikon Output	77
4.2.3.2	Types of Analysis	81
4.2.4	Phase 4: Business Process Analysis	86
5	Case study: the iTrust SWaT System	87
5.1	Architecture	87
5.1.1	Physical Process	88
5.1.2	Control and Communication Network	90
5.2	Datasets	92

5.2.1	Our Case Study: the 2015 Dataset	93
6	Our framework at work: reverse engineering of the SWaT system	97
6.1	Pre-processing	97
6.2	Graph Analysis	97
6.2.1	Conjectures About the System	97
6.3	Invariants Analysis	97
6.3.1	Actuators Detection	97
6.3.2	Daikon Analysis and Results Comparing	97
6.4	Extra information on the Physics	97
6.5	Business Process Analysis	97
7	Conclusions	99
7.1	Discussions	99
7.2	Guidelines	99
7.3	Future work	99
	List of Figures	101
	List of Tables	103
	Listings	105
	References	107

Introduction

LOREM ipsum dolor bla bla bla. Ma dove metto l'abstract? Prova di interlinea che direi posso anche andare bene, ma bisogna poi vedere il tutto come si incastra alla fine, in modo da ottenere un bel risultato alla vista.

1.1 Contribution

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum.

1.2 Outline

The thesis is structured as follows:

Chapter 2: provides background on the topics covered in this thesis: Industrial Control Systems (ICSs), Supervisory Control And Data Acquisition (SCADA), Programmable Logic Controllers (PLCs) and other devices, industrial communication protocols.

Chapter 3:

Chapter 4:

Chapter 5:

Chapter 6:

Chapter 7:

Chapter 2

Background

2.1 Industrial Control Systems in a nutshell

1 INDUSTRIAL CONTROL SYSTEMS (ICSs) are information systems used to
2 control industrial processes such as manufacturing, product handling,
3 production, and distribution [1].

4 ICSs are often found in critical infrastructure facilities such as power
5 plants, oil and gas refineries, and chemical plants.

6 ICSs are different from traditional IT systems in several key ways. Firstly,
7 ICSs are designed to control physical processes, whereas IT systems are
8 designed to process and store data. This means that ICSs have different
9 requirements for availability, reliability, and performance. Secondly, ICSs
10 are typically deployed in environments that are harsh and have limited
11 resources, such as extreme temperatures and limited power. Thirdly, the
12 protocols and hardware used in ICSs are often proprietary and not widely
13 used outside of the industrial sector.

14 ICSs are becoming increasingly connected to the internet and other net-
15 works, which has led to increased concerns about their security. Industrial
16 systems were not originally designed with security in mind, and many of
17 them have known vulnerabilities that could be exploited by attackers. Ad-
18 ditionally, the use of legacy systems and equipment can make it difficult to

19 implement security measures. As a result, ICSs are increasingly seen as a
20 potential target for cyber attacks, which could have serious consequences
21 for the safe and reliable operation of critical infrastructure.

22 The increasing connectivity of ICSs and the associated security risks
23 have led to a growing interest in the field of ICS security. Researchers
24 and practitioners are working to develop new security technologies, stan-
25 dards, and best practices to protect ICSs from cyber attacks. This includes
26 efforts to improve the security of ICS networks and devices, as well as the
27 development of new monitoring and detection techniques to identify and
28 respond to cyber attacks.

29 **2.2 ICS components**

30 *Industrial control systems* (ICSs) are composed of several different com-
31 ponents that work together to monitor and control industrial processes.

32 **2.2.1 SCADA systems**

33 *Supervisory Control And Data Acquisition (SCADA)* is a system of soft-
34 ware and hardware elements that allows industrial organizations to [2]:

- 35 • Control industrial processes locally or at remote locations
- 36 • Monitor, gather, and process real-time data
- 37 • Directly interact with devices such as sensors, valves, pumps, mo-
38 tors, and more through human-machine interface (HMI) software
- 39 • Record events into a log file

40 The SCADA software processes, distributes, and displays the data,
41 helping operators and other employees analyze the data and make im-
42 portant decisions.

43 SCADA systems are known for their ability to monitor and control
44 large-scale industrial processes, and for their ability to operate over long

distances. This makes them well-suited for use in remote locations or for controlling processes that are spread out over a wide area. However, the same features that make SCADA systems so useful also make them vulnerable to cyber attacks.

SCADA systems were not originally designed with security in mind, and many of them have known vulnerabilities that could be exploited by attackers. Additionally, the use of legacy systems and equipment can make it difficult to implement security measures. As a result, SCADA systems are increasingly seen as a potential target for cyber attacks, which could have serious consequences for the safe and reliable operation of critical infrastructure.

To secure SCADA systems, it is important to implement security measures such as network segmentation, secure communication protocols, and access control. Additionally, it is important to monitor SCADA systems for unusual activity and to implement incident response procedures to quickly detect and respond to any security breaches.

2.2.1.1 SCADA architecture

According to the *Purdue Enterprise Reference Architecture* (PERA), or simply **Purdue Model**, SCADA architecture consists in **six levels** each representing a functionality [3], as shown in Figure 2.1:

- Level 0 (**Processes**): contains **field devices** (2.2.2), or *sensors*.
- Level 1 (**Intelligent Devices**): includes **local or remote controllers** that sense, monitor and control the physical process, such as **PLCs** (2.2.3) and **RTUs** (2.2.4). Controllers interface directly to the field devices reading data from sensors and sending commands to actuators.
- Level 2 (**Control Systems**): contains computer systems used to supervising and monitoring the physical process: they provide a **Human-Machine Interface** (HMI, 2.2.5) and *Engineering Workstations* (EW) for operator control.



Figure 2.1: SCADA architecture schema

- Level 3 (**Manufacturing/Site Operations**): comprises systems used to manage the production workflow for plant-wide control: they collate informations from the previous levels and store them in Data Historian servers.
- Industrial Demilitarized Zone (DMZ)**: intermediate level that connects the *Operational Technology* (OT) part (levels 0-3) with the *Information Technology* (IT) part of the system (levels 4 and 5). Communication takes place indirectly through services such as *proxy servers* and *remote access servers*, which act as intermediaries between the two environments.
- Level 4 (**Business Logistics Systems**): collect and aggregates data from the Manufacturing/Site Operations level overseeing the IT-related activities to generate **reporting** to the Enterprise System layer. At

this layer we can find application and e-mail servers, and *Enterprise Resource Planning* (ERP) systems.

- Level 5 (**Enterprise Systems**): represents the enterprise network, used for the business-to-business activities and for business-to-client purpose services. At Enterprise Systems level are typical IT services such as mail servers, web servers and all the systems used to manage the ongoing process.

2.2.2 Field devices

Field devices are the **sensors** and **actuators** that are used to collect data from the process and control it. Examples of field devices include temperature sensors, pressure sensors, valves and pumps.

2.2.3 Programmable Logic Controllers

A *Programmable Logic Controller* (PLC) is a **small and specialized industrial computer** having the capability of controlling complex industrial and manufacturing processes [4].

Compared to relay systems and personal computers, PLCs are optimized for control tasks and industrial environments: they are rugged and designed to withdraw harsh conditions such as dust, vibrations, humidity and temperature: they have more reliability than personal computers, which are more prone to crash, and they are more compact and require less maintenance than a relay system. Furthermore, I/O interfaces are already on the controller, so PLCs are easier to expand with additional I/O modules (if in a rack format) to manage more inputs and outputs, without reconfiguring hardware as in relay systems when a reconfiguration occurs.

PLCs are more *user-friendly*: they are not intended (only) for computer programmers, but designed for engineers with a limited knowledge in programming languages: control program can be entered with a simple

and intuitive language based on logic and switching operations instead of a general-purpose programming language (*i.e.* C, C++, ...).

2.2.3.1 PLC Architecture

The basic hardware architecture of a PLC consists of these elements [5]:

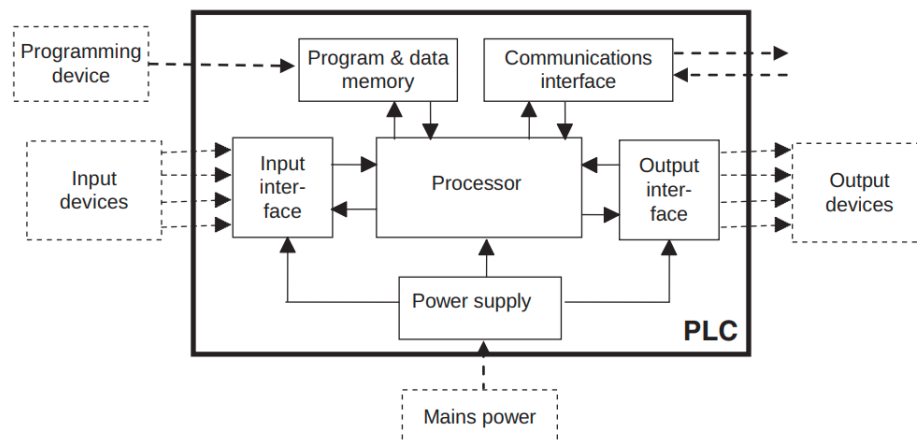


Figure 2.2: PLC architecture

- **Processor unit (CPU):** contains the microprocessor. This unit interpretes the input signals from I/O modules, executes the control program stored in the Memory Unit and sends the output signals to the I/O Modules. The processor unit also sends data to the Communication interface, for the communication with additional devices.
- **Power supply unit:** converts AC voltage to low DC voltage.
- **Programming device:** is used to store the required program into the memory unit.
- **Memory Unit:** consists in RAM memory and ROM memory. RAM memory is used for storing data from inputs, ROM memory for storing operating system, firmware and user program to be executed by the CPU.

- 130 • **I/O modules:** provide interface between sensors and final control
131 elements (actuators).
- 132 • **Communications interface:** used to send and receive data on a net-
133 work from/to other PLCs.



Figure 2.3: PLC communication schema

134 2.2.3.2 PLC Programming

135 Two different programs are executed in a PLC: the **operating system**
136 and the **user program**.

137 The operating system tasks include executing the user program, man-
138 aging memory areas and the *process image table* (memory registers where
139 inputs from sensors and outputs for actuators are stored).

140 The user program needs to be uploaded on the PLC via the program-
141 ming device and runs on the process image table in *scan cycles*: each scan
142 is made up of three phases [6]:

- 143 1. reading inputs from the process images table
- 144 2. execution of the control code and computing the physical process
145 evolution

146 3. writing output to the process image table to have an effect on the
147 physical process. At the end of the cycle, the process image table is
148 refreshed by the CPU

149 Standard PLCs **programming languages** are basically of two types:
150 **textuals** and **graphicals**. Textual languages include languages such as
151 *Instruction List (IL)* and *Structured Text (ST)*, while *Ladder Diagrams (LD)*,
152 *Function Block Diagram (FBD)* and *Sequential Function Chart (SFC)* belong
153 to the graphical languages.

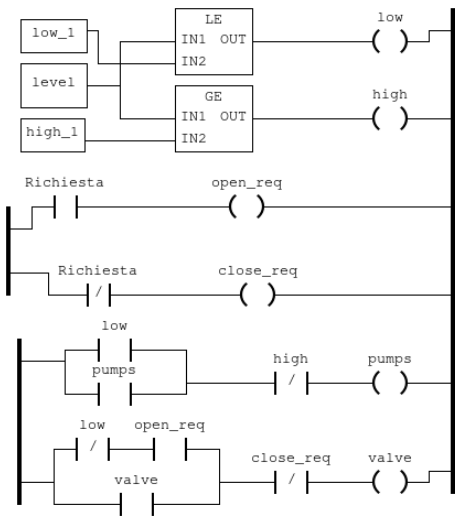
154 Graphical languages are more simple and immediate comparing to the
155 textual ones and are preferred by programmers because of their features
156 and simplicity, in particular the **Ladder Logic programming** (see Figure
157 2.4 for a comparison).

```
PROGRAM PLC1
VAR
    level AT %IW0 : INT;
    Richiesta AT %QX0.2 : BOOL;
    request AT %IW1 : INT;
    pumps AT %QX0.0 : BOOL;
    valve AT %QX0.1 : BOOL;
    low AT %MX0.0 : BOOL;
    high AT %MX0.1 : BOOL;
    open_req AT %MX0.3 : BOOL;
    close_req AT %MX0.4 : BOOL;
    low_1 AT %MW0 : INT := 40;
    high_1 AT %MW1 : INT := 80;
END_VAR
VAR
    LE3_OUT : BOOL;
    GE7_OUT : BOOL;
END_VAR

LE3_OUT := LE(level, low_1);
low := LE3_OUT;
GE7_OUT := GE(level, high_1);
high := GE7_OUT;
open_req := Richiesta;
close_req := NOT(Richiasta);
pumps := NOT(high) AND (low OR pumps);
valve := NOT(close_req) AND (open_req AND NOT(low) OR valve);
END_PROGRAM

CONFIGURATION Config0
RESOURCE Res0 ON PLC
TASK task0(INTERVAL := T#20ms,PRIORITY := 0);
PROGRAM instance0 WITH task0 : PLC1;
END_RESOURCE
END_CONFIGURATION
```

(a) Example of ST programming



(b) Example of Ladder Logic

Figure 2.4: Comparison between ST language and Ladder Logic

158 2.2.3.3 PLC Security

159 PLCs were originally designed to operate as closed systems, not con-
160 nected and exposed to the outside world via communication networks:

the question of the safety of these systems, therefore, was not a primary aspect. The advent of Internet has brought undoubted advantages, but has introduced problems relating to the safety and protection of PLCs from external attacks and vulnerabilities.

Indeed, a variety of different communication protocols used in ICSs are designed to be efficient in communications, but do not provide any security measure i.e. confidentiality, authentication and data integrity, which makes these protocols vulnerable against many of the IT classic attacks such as *Replay Attack* or *Man in the Middle Attack*.

Countermeasures to enhance security in PLC systems may include [7]:

- protocol modifications implementing **data integrity**, **authentication** and **protection** against *Replay Attacks*
- use of *Intrusion Detection and Prevention Systems* (IDP)
- creation of *Demilitarized Zones* (DMZ) on the network

In addition to this, keeping the process network and Internet separated, limiting the use of USB devices among users to reduce the risks of infections, and using strong account management and maintenance policies are best practices to prevent attacks and threats and to avoid potential damages.

2.2.4 Remote Terminal Units

Remote Terminal Units (RTUs) are computers with radio interfacing similar to PLCs: they transmit telemetry data to the control center or to the PLCs and use messages from the master supervisory system to control connected objects [8].

The purpose of RTUs is to operate efficiently in remote and isolated locations by utilizing wireless connections. In contrast, PLCs are designed for local use and rely on high-speed wired connections. This key difference

allows RTUs to conserve energy by operating in low-power mode for extended periods using batteries or solar panels. As a result, RTUs consume less energy than PLCs, making them a more sustainable and cost-effective option for remote operations.

Industries that require RTUs often operate in areas without reliable access to the power grid or require monitoring and control substations in remote locations. These include telecommunications, railways, and utilities that manage critical infrastructure such as power grids, pipelines, and water treatment facilities. The advanced technology of RTUs allows these industries to maintain essential services, even in challenging environments or under adverse weather conditions.

2.2.5 Human-Machine Interface

The *Human-Machine Interface* (HMI) is the hardware and software interface that operators use to monitor the processes and interact with the ICS.

An HMI shows the operator and authorized users information about system status and history; it also allows them to configure parameters on the ICS such as set points and, send commands and make control decisions [9].

The HMI can be in the form of a physical panel, with buttons and indicator lights, or PC software.

2.2.6 Cybersecurity components

Cybersecurity components, as seen in section 2.2.3.3 about PLCs security, are used to protect ICSs from cyber threats and vulnerabilities. They can include firewalls, *Intrusion Detection and Prevention systems* (IDP), and *Security Information and Event Management* (SIEM) systems.

2.3 Communication Networks

Communication Networks are the networks that are used to connect the different components of the ICS and allow them to communicate with each other. Communication networks can include wired and wireless networks, such as Ethernet/IP, Modbus, DNP3 and others.

2.3.1 ICS Communication Protocols

As mentioned in Section 2.1, industrial systems differ from classical IT systems in the purpose for which they are designed: controlling physical processes the former, processing and storing data the latter. For this reason, ICSs require different communication protocols than traditional IT systems for real time communications and data transfer.

A wide variety of industrial protocols exists: this is because originally each vendor developed and used its own proprietary protocol. However, these protocols were often incompatible with each other, resulting in devices from different vendors being unable to communicate with each other.

To solve this problem, standards were defined with a view to allowing these otherwise incompatible device to intercommunicates.

Among all the various protocols, some have risen to prominence as widely accepted standards. These *de facto* protocols are commonly utilized in industrial systems due to their proven reliability and effectiveness. In the following sections, we will provide a brief overview of some of the most prevalent and widely used protocols in the industry.

2.3.1.1 Modbus

Modbus is a serial communication protocol developed by Modicon (now Schneider Electric) in 1979 for use with its PLCs [10] and designed expressly for industrial use: it facilitates interoperability of different devices

connected to the same network (sensors, PLCs, HMIs, ...) and it is also often used to connect RTUs to SCADA acquisition systems.

Modbus is the most widely used communication protocol among industrial systems because it has several advantages:

- simplicity of implementation and debugging
- it moves raw bits and words, letting the individual vendor to represent the data as it prefers
- it is, nowadays, an **open** and *royalty-free* protocol: there is no need to sustain licensing costs for implementation and use by industrial device vendors

Modbus is a **request/response** (or *master/slave*) protocol: this makes it independent of the transport layer used.

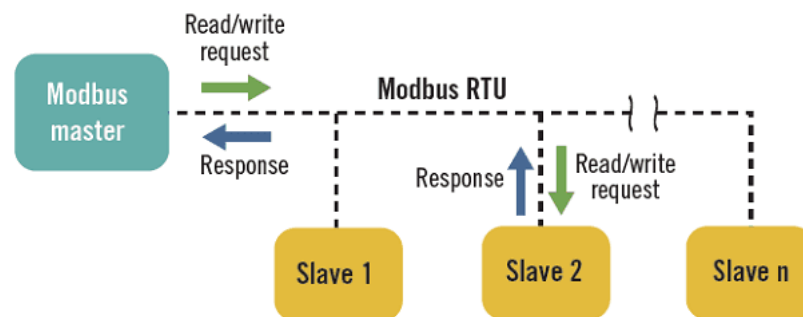


Figure 2.5: Modbus Request/Response schema

In this kind of architecture, a single device (master) can send requests to other devices (slaves), either individually or in broadcast: these slave devices (usually peripherals such as actuators) will respond to the master by providing data or performing the action requested by the master using the Modbus protocol. Slave devices cannot generate requests to the master [11].

259 There are several variants of Modbus, of which the most popular and
260 widely used are Modbus RTU (used in serial port connections) and Mod-
261 bus TCP (which instead uses TCP/IP as the transport layer). Modbus TCP
262 embeds a standard Modbus frame in a TCP frame (see Figure 2.6): both
263 masters and slaves listen and receive data via TCP port 502.

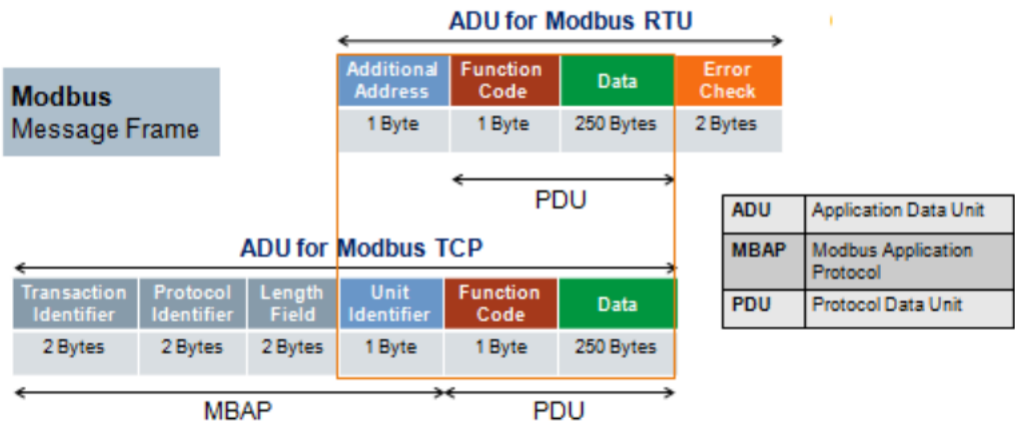


Figure 2.6: Modbus RTU frame and Modbus TCP frame

264 **Modbus registers** Modbus provides four object types, which map the
265 data accessed by master and slave to the PLC memory:

- 266 • *Coil*: binary type, read/write accessible by both masters and slaves
- 267 • *Discrete Input*: binary type, accessible in read-only mode by masters
268 and in read/write mode by slaves
- 269 • *Analog Input*: 16 bits in size (word), are accessible in read-only mode
270 by masters and in read/write mode by slaves
- 271 • *Holding Register*: 16 bits in size (word), accessible in read/write mode
272 by both masters and slaves. Holding Registers are the most com-
273 monly used registers for output and as general memory registers.

274 **Modbus Function Codes** *Modbus Function Codes* are specific codes used
275 by the Modbus master within a request frame (see Figure 2.6) to tell the

276 Modbus slave device which register type to access and which action to
277 perform on it.

278 Two types of Function Codes exists: for data access and for diagnostic
279 Function Codes list for data access are listed in Table 2.1:

Function Code	Description
FC01	Read Coils
FC02	Read Discrete Input
FC03	Read Holding Registers
FC04	Read Analog Input Registers
FC05	Write/Force Single Coil
FC06	Write/Force Single Holding Register
FC15	Write/Force Multiple Coils
FC16	Write/Force Multiple Holding Registers

Table 2.1: Modbus Function Codes list

280 **Modbus Security Issues** Despite its simplicity and widespread use, the
281 Modbus protocol does not have any security feature, which exposes it to
282 vulnerabilities and attacks.

283 Data in Modbus are transmitted unencrypted (*lack of confidentiality*),
284 with no data integrity controls (*lack of integrity*) and authentication checks
285 (*lack of authentication*), in addition to the *lack of session*. Hence, the protocol
286 is vulnerable to a variety of attacks, such as Denial of Services (DoS), buffer
287 overflows and reconnaissance activities.

288 The easiest attack to bring to the Modbus protocol, however, is **packet**
289 **sniffing**: since, as mentioned earlier, network traffic is unencrypted and
290 the data transmitted is in cleartext, it is sufficient to use a packet sniffer to
291 capture the network traffic, read the packets and thus gather informations
292 about the system such as ip addresses, function codes of requests and to
293 modify the operation of the devices.



Figure 2.7: Example of packet sniffing on the Modbus protocol

To make the Modbus protocol more secure, an encapsulated version was developed within the *Transport Security Layer* (TLS) cryptographic protocol, also using mutual authentication. This version of the Modbus protocol is called **Secure Modbus** or **Modbus TLS**. In addition to this, Secure Modbus also includes X.509-type certificates to define permissions and authorisations [12].

2.3.1.2 EtherNet/IP

EtherNet/IP (where IP stands for *Industrial Protocol*) is an open industrial protocol that allows the *Common Industrial Protocol* (CIP) to run on a typical Ethernet network [13]. It is supported by ODVA [14].

EtherNet/IP uses the major Ethernet standards, such as IEEE 802.3 and the TCP/IP suite, and implements the CIP protocol stack at the upper layers of the OSI stack (see Figure 2.8). It is furthermore compatible with the main Internet standard protocols, such as SNMP, HTTP, FTP and DHCP, and other industrial protocols for data access and exchange such as *Open Platform Communication* (OPC).



Figure 2.8: OSI model for EtherNet/IP stack

Physical and Data Link layer The use of the IEEE 802.3 standard allows EtherNet/IP to flexibly adopt different network topologies (star, linear, ring, etc.) over different connections (copper, fibre optic, wireless, etc.), as well as the possibility to choose the speed of network devices. IEEE 802.3 in addition defines at Data Link layer the *Carrier Sense Multiple Access - Collision Detection* (CSMA/CD) protocol, which controls access to the communication channel and prevents collisions.

Transport layer At the transport level, EtherNet/IP encapsulates messages from the CIP stack into an Ethernet message, so that messages can be transmitted from one node to another on the network using the TCP/IP protocol. EtherNet/IP uses two forms of messaging, as defined by CIP standard [13][15]:

- **unconnected messaging:** used during the connection establishment phase and for infrequent, low priority, explicit messages. Unconnected messaging uses TCP/IP to transmit messages across the network asking for connection resource each time from the *Unconnected*

Message Manager (UCMM).

- **connected messaging:** used for frequent message transactions or for real-time I/O data transfers. Connection resources are reserved and configured using communications services available via the UCMM.

EtherNet/IP has two types of message connection [13]:

- **explicit messaging:** *point-to-point* connections to facilitate *request-response* transactions between two nodes. These connections use TCP/IP service on port 44818 to transmit messages over Ethernet.
- **implicit messaging:** this kind of connection moves application-specific **real-time I/O data** at regular intervals. It uses multicast *producer-consumer* model in contrast to the traditional *source-destination* model and UDP/IP service (which has lower protocol overhead and smaller packet size than TCP/IP) on port 2222 to transfer data over Ethernet.

Session, Presentation and Application layer At the upper layers, Ethernet/IP implements the CIP protocol stack. We will discuss this protocol more in detail in Section 2.3.1.3.

2.3.1.3 Common Industrial Protocol (CIP)

The *Common Industrial Protocol* (CIP) is an open industrial automation protocol supported by ODVA. It is a **media independent** (or *transport independent*) protocol using a *producer-consumer* communication model and providing a **unified architecture** throughout the manufacturing enterprise [16][17].

CIP has been adapted in different types of network:

- **EtherNet/IP**, adaptation to *Transmission Control Protocol* (TCP) technologies

- 353 • **ControlNet**, adaptation to *Concurrent Time Domain Multiple Access*
354 (CTDMA) technologies
- 355 • **DeviceNet**, adaptation to *Controller Area Network* (CAN) technolo-
356 gies
- 357 • **CompoNet**, adaptation to *Time Division Multiple Access* (TDMA) tech-
358 nologies

359 **CIP objects** CIP is a *strictly object oriented* protocol at the upper layers:
360 each object of CIP has **attributes** (data), **services** (commands), **connec-**
361 **tions**, and **behaviors** (relationship between values and services of attributes)
362 which are defined in the **CIP object library**. The object library supports
363 many common automation devices and functions, such as analog and dig-
364 ital I/O, valves, motion systems, sensors, and actuators. So if the same
365 object is implemented in two or more devices, it will behave the same way
366 in each device [18].

367 **Security** [19] In EtherNet/IP implementation, security issues are the same
368 as in traditional Ethernet, such as network traffic sniffing and spoofing.
369 The use of the UDP protocol also exposes CIP to transmission route ma-
370 nipulation attacks using the *Internet Group Management Protocol* (IGMP)
371 and malicious traffic injection.

372 Regardless of the implementation used, it is recommended that certain
373 basic measures be implemented on the CIP network to ensure a high level
374 of security, such as *integrity*, *authentication* and *authorization*.

375 2.3.1.4 Other Protocols

Chapter 3

State of the Art

IN CONVENTIONAL IT, the objective of an attacker is to comprehend the behavior of a program using diverse techniques in order to launch attacks that alter its execution flow, functionalities, or bypass limitations imposed by software licensing. These attack techniques involve an initial examination of the program, consisting of *static analysis* (i.e., analyzing the software without running it) and *dynamic analysis* (i.e., analyzing the program while it is running).

The outcome of these two investigative techniques is the reverse engineering of the software, which serves the purpose of identifying vulnerabilities or bugs and subsequently strategizing an attack.

In the context of OT, the notion of *reverse engineering* is not limited to its conventional definition, but also includes the concept of **process comprehension**. This term, introduced by Green et al. [20], refers to gaining a comprehensive understanding of the system's characteristics and the physical components responsible for its proper functioning.

There is limited literature available concerning the gathering and analysis of information related to the comprehension and operation of an Industrial Control System (ICS). In Section 3.1, we will provide a brief overview of the existing literature on this topic, and in the subsequent sections, we will specifically focus on one of the presented papers.

3.1 Literature on Process Comprehension

Keliris and Maniatikos The first approach presented in this section is by Keliris and Maniatikos [21]: they present a methodology for automating the reverse engineering of ICS binaries based on a *modular framework* (called ICSREF) that can reverse binaries compiled with CODESYS, one of the most popular and widely used PLC compilers, irrespective of the language used.

Yuan et al. Yuan et al. [22] propose a *data-driven* approach to discovering cyber-physical systems from data directly: to achieve this goal, they have implemented a framework whose purpose is to identify physical systems and transition logic inference, and to seek to understand the mechanisms underlying these cyber-physical systems, making furthermore predictions concerning their state trajectories based on the discovered models.

Feng et al. Feng et al. [23] developed a framework that can generate system *invariant rules* based on machine learning and data mining techniques from ICS operational data log. These invariants are then selected by systems engineers to derive IDS systems from them.

The experiment results on two different testbeds, the *Water Distribution system* (WaDi) and the *Secure Water Treatment system* (SWaT), both located at the iTrust - Center for Research in Cyber Security at the University of Singapore [24], show that under the same false positive rate invariant-based IDSs have a higher efficiency in detecting anomalies than IDS systems based on a residual error-based model.

Pal et al. Pal et al. [25] work is somewhat related to Feng et al.'s: this paper describes a data-driven approach to identifying invariants automatically using *association rules mining* [26] with the aim of generate invariants sometimes hidden from the design layout. The study has the same objective of Feng et al.'s and uses too the iTrust SwaT System as testbed.

Currently this technique is limited to only pair wise sensors and actuators: for more accurate invariants generation, the technique adopted must be capable of deriving valid constraints across multiple sensors and actuators.

Winnicki et al. Winnicki et al. [27] instead propose a different approach to process comprehension based on the **attacker's perspective** and not limited to mere *Denial of Service* (DoS): their approach is to discover the dynamic behavior of the system, in a semi-automated and process-aware way, through *probing*, that is, slightly perturbing the cyber physical system and observing how it reacts to changes and how it returns to its original state. The difficulty and challenge for the attacker is to perturb the system in such a way as to achieve an observable change, but at the same time avoid this change being seen as a system anomaly by the IDSs.

Green et al. Green et al. [20] also adopt an approach based on the attacker's perspective: this approach consists of two practical examples in a *Man in the Middle* (MitM) scenario to obtain, correlate, and understand all the types of information an attacker might need to plan an attack to alter the process while avoiding detection.

The paper shows *step-by-step* how to perform a ICS **reconnaissance**, which is fundamental to process comprehension and thus to the execution of MitM attacks.

Ceccato et al. Ceccato et al. [6] propose a methodology based on a *black box dynamic analysis* of an ICS using a reverse engineering tool to derive from the scans performed on the memory registers of the exposed PLCs and network scans an approximate model of the physical process. This model is obtained by inferring statistical properties, business process and system invariants from data logs.

The proposed methodology was tested on a non-trivial case study, using a testbed inspired by an industrial water treatment plant.

456 In the next section I will examine this latest work in more detail,
457 which will be the basis for my work and thus the subsequent chap-
458 ters of this thesis.

459 3.2 Ceccato et al.'s methodology for analyzing water- 460 tank systems

461 As previously mentioned, the paper introduces a methodology that re-
462 lies on black box dynamic analysis of an Industrial Control System (ICS).
463 This methodology involves identifying potential Programmable Logic Con-
464 trollers (PLCs) within the network and scanning the memory registers of
465 these identified controllers. The purpose of this process is to obtain an
466 approximate model of the controlled physical process.

467 The primary goal of this black box analysis is to establish a correlation
468 between the different memory registers of the targeted PLCs and funda-
469 mental concepts of an ICS such as sensors (i.e., measurements), actuators,
470 setpoints (i.e., range of values of a physical variable), network communi-
471 cations, among others.

472 To accomplish this, the various types of memory registers associated with
473 the Modbus protocol are analyzed, and attempts are made to determine
474 the nature of the data they might contain.

475 The second goal is to establish a relationship between the dynamic evolu-
476 tion of these fundamental concepts.

477 To accomplish this, Ceccato et al. have developed a prototype tool [28]
478 that facilitates the reverse engineering of the physical system. This tool
479 goes through four distinct phases:

- 480 1. **scanning of the system and data pre-processing:** this phase involves
481 gathering data to generate data logs for the registers of PLCs.
- 482 2. **graphs and statistical analysis:** The collected data is utilized to pro-
483 vide insights into the memory registers by leveraging graphs and

statistical data. This analysis approach offers valuable information about the characteristics and patterns of the memory registers.

3. **invariants inference and analysis:** generates system invariants, which are used to identify specific patterns and regularities within the system. Additionally, this phase provides users with the capability to view invariants related to a particular sensor or actuator.
4. **business process mining and analysis:** Using event logs, this phase involves reconstructing the business process that depicts how a process is executed. This step enables a thorough understanding of the sequence of events that occur in the system and how they are interrelated, ultimately leading to a comprehensive overview of the business process.

Figure 3.1 presents a schematic representation of the workflow associated with this work. In the subsequent sections of this chapter, we will provide a detailed exploration of each of these phases, offering a comprehensive understanding of the entire process.

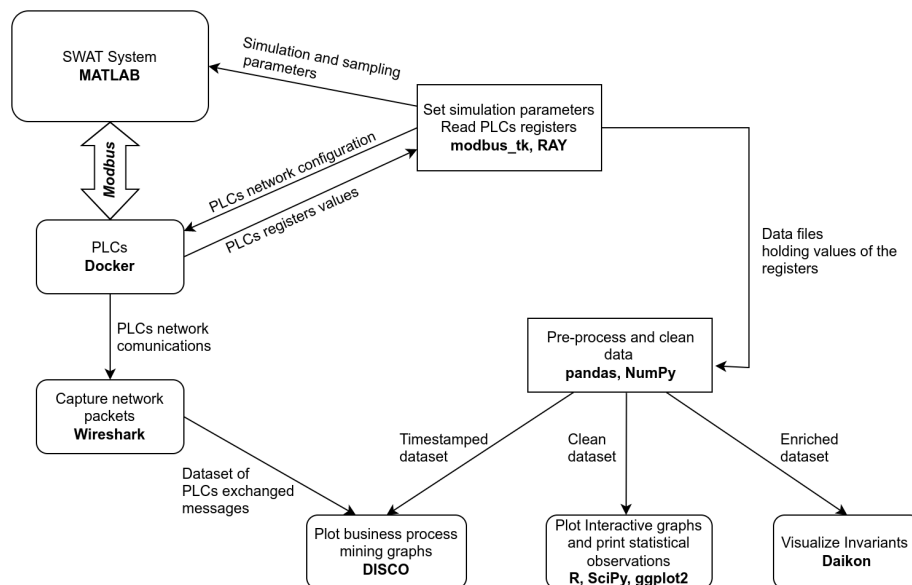


Figure 3.1: Overview

3.2.1 Testbed

Before delving into the description of the methodology's different phases, let's first examine the testbed utilized to evaluate this approach. The testbed employed for testing purposes is a (very) simplified rendition of the iTrust SWaT system [29], as implemented by Lanotte et al. [30]. Figure 3.2 provides a graphical representation of the testbed. This simplified version comprises three stages, each governed by a dedicated PLC.

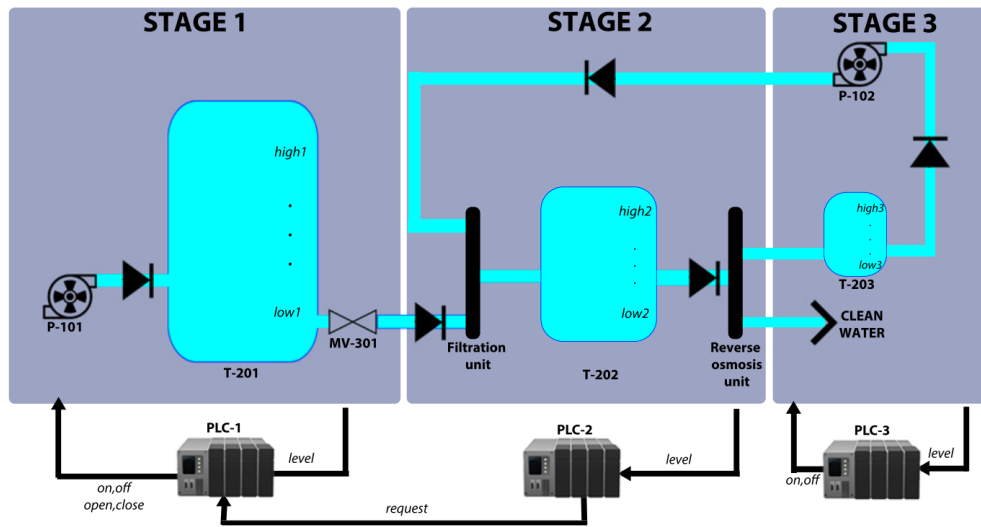


Figure 3.2: The simplified SWaT system used for running Ceccato et al. methodology

Stage 1 During the initial stage, a **tank** referred to as T-201 with a capacity of 80 gallons is filled with raw water using the P-101 pump. Connected to the T-201 tank, the MV-301 motorized valve flushes out the accumulated water from the tank, directing it to the next stage. Initially, the water flows from the T-201 tank to the *filtration unit* (which is not specifically identified by any sensor), and subsequently to a **second tank** denoted as T-202, with a capacity of 20 gallons.

Stage 2 At the second stage, the water stored in tank T-202 flows into the *reverse osmosis unit* (RO), which serves as both a valve and a continuous water extractor. The purpose of the RO unit is to reduce organic

impurities present in the water. Subsequently, the water flows from the *RO unit* to the third and final stage of the system.

Stage 3 At the third stage, the water coming from the *RO unit* undergoes division based on whether it meets the required standards. If the water is deemed clean and meets the standards, it is directed into the distribution system. However, if the water fails to meet the standards, it is redirected to a *backwash tank* identified as T-203, which has a capacity of one gallon. The water stored in this tank is then pumped back to the stage 2 *filtration unit* using pump P-102.

As previously mentioned, each stage of the system corresponds to a dedicated PLC, namely PLC1, PLC2, and PLC3, which are responsible for controlling their respective stages. Let's briefly explore the behavior of each PLC:

PLC1 PLC1 monitors the level of tank T-201 and distinguishes three different cases based on the level readings:

1. when the level of tank T-201 reaches the defined *low setpoint low1* (which is hardcoded in the memory registers), PLC1 **opens pump P-101** and **closes valve MV-301**. This configuration allows the tank to be filled with water.
2. if the level of T-201 reaches the *high setpoint high1* (which is also hardcoded in the memory registers), then the pump **P-101 is closed**.
3. in cases where the level of T-201 is between the *low setpoint low1* and the *high setpoint high1*, PLC1 waits for a request from PLC2 to open or close the valve MV-301. If a request to open the valve MV-301 is received, water will flow from T-201 to T-202. However, if no request is received, the valve remains closed. In both situations, the pump P-101 remains closed.

545 **PLC2** PLC2 monitors the level of tank T-202 and adjusts its behavior based
546 on the water level. There are three cases to consider:

- 547 1. when the water level in tank T-202 reaches *low setpoint low2* (also
548 hardcoded in the memory registers), PLC2 sends a request to
549 PLC1 through a Modbus channel to **open valve MV-301**. This
550 request is made in order to allow the water to flow from tank T-
551 201 to tank T-202. The transmission channel between the PLCs
552 is established by copying a boolean value from a memory reg-
553 ister of PLC2 to a corresponding register of PLC1.
- 554 2. when the water level in tank T-202 reaches the *high setpoint high2*
555 value (also hardcoded in the memory registers), PLC2 sends a
556 **close request to PLC1 for valve MV-301**. This request prompts
557 PLC1 to close the valve, stopping the flow of water from tank
558 T-201 to tank T-202.
- 559 3. In cases where the water level in tank T-202 is between the low
560 and high setpoints, the valve MV-301 remains in its current state
561 (open or closed) while the tank is either filling or emptying.

562 **PLC3** PLC3 monitors the level of the T-203 backwash tank and adjusts its
563 behavior accordingly. There are two cases to consider:

- 564 1. If the water level in the backwash tank reaches the *low setpoint*
565 *low3*, **PLC3 sets pump P103 to off**. This allows the backwash
566 tank to be filled.
- 567 2. If the water level in the backwash tank reaches the *high setpoint*
568 *high3*, **PLC3 opens pump P103**. This action triggers the pump-
569 ing of the entire content of the backwash tank back to the filter
570 unit of T-202.

571 3.2.2 Scanning of the System and Data Pre-processing

572 **Scanning tool** The Ceccato et al. scanning tool is closely derived from
573 a project I did [31] for the "Network Security" and "Cyber Security for IoT"

courses taught by Professors Massimo Merro and Mariano Ceccato, respectively, in the 2020/21 academic year. The original project involved, in its first part, the recognition within a network of potential PLCs listening on the standard Modbus TCP port 502 using the Nmap module for Python, obtaining the corresponding IP addresses: then a (sequential) scan of a given range of the memory registers of the found PLCs was performed to collect the register data. The data thus collected were saved to a file in *JavaScript Object Notation* (JSON) format for later use in the second part of my project.

The scanning tool by Ceccato et. al works in a similar way, but extends what I originally did by trying to discover other ports on which the Modbus protocol might be listening (since in many realities Modbus runs on different ports than the standard one, according to the concept of *security by obscurity*) and, most importantly, by **parallelizing and distributing the scan** of PLC memory registers through the Ray module [32], specifying moreover the desired granularity of the capture. An example of raw data capture can be seen at Listing 3.1:

```
"127.0.0.1/8502/2022-05-03 12_10_00.591": {  
  "DiscreteInputRegisters": {"%IX0.0": "0"},  
  "InputRegisters": {"%IW0": "53"},  
  "HoldingOutputRegisters": {"%QW0": "0"},  
  "MemoryRegisters": {"%MW0": "40", "%MW1": "80"},  
  "Coils": {"%QX0.0": "0"}}
```

Listing 3.1: Example of registers capture

The captured data includes PLC's IP address, Modbus port and timestamp (first line), type and name of registers with their values read from the scan (subsequent lines).

The tool furthermore offers the possibility, in parallel to the memory registers scan, of **sniffing network traffic** related to the Modbus protocol using the *Man in the Middle* (MitM) technique on the supervisory control network using a Python wrapper for tshark/Wireshark [33] [34]. An example of raw data obtained with this sniffing can be seen in Listing 3.2:

```

605 Time,Source,Destination,Protocol,Length,Function Code,
606     ↳ Destination Port,Source Port,Data,Frame length on the
607     ↳ wire,Bit Value,Request Frame,Reference Number,Info
608 2022-05-03 11:43:58.158,IP_PLC1,IP_PLC2,Modbus/TCP,76,Read
609     ↳ Coils,46106,502,,76,TRUE,25,,,"Response: Trans: 62;
610     ↳ Unit: 1, Func: 1: Read Coils"

```

Listing 3.2: Example of raw network capture

Data Pre-processing The data collected by scanning the memory registers of the PLCs are then reprocessed by a Python script and converted in order to create a distinct raw dataset in *Comma Separated Value* format (CSV) for each PLC, containing the memory register values associated with the corresponding controller registers. These datasets are reprocessed again through the Python modules for **pandas** [35] and **NumPy** [36] by another script to first perform a **data cleanup**, removing all those memory registers that do not take values and are therefore useless within the system, **merged** into a single dataset, and finally **enriched** with additional data¹.

This process leads to the creation of two copies of the full dataset: one enriched with the additional data, but not timestamped, which will be used for the invariant analysis; the other unenriched, but timestamped, which will be used for business process mining.

3.2.3 Graphs and Statistical Analysis

The paper mentions the presence of a *mild graph analysis*, performed with **R** [37] at the time of data gathering to find any uncovered patterns, trends and identify measurements and/or actuator commands through the analysis of registers holding mutable values.

There is actually no trace of this within the tool: *graph analysis* and *statistical analysis* of the data contained in the PLC memory registers are in-

¹Not all additional data are calculated and entered automatically by the tool: some are manually inserted.

stead performed using the **matplotlib** libraries and statistical algorithms made available by the **SciPy** libraries [38], through two separate Python scripts (see Figure 3.3).

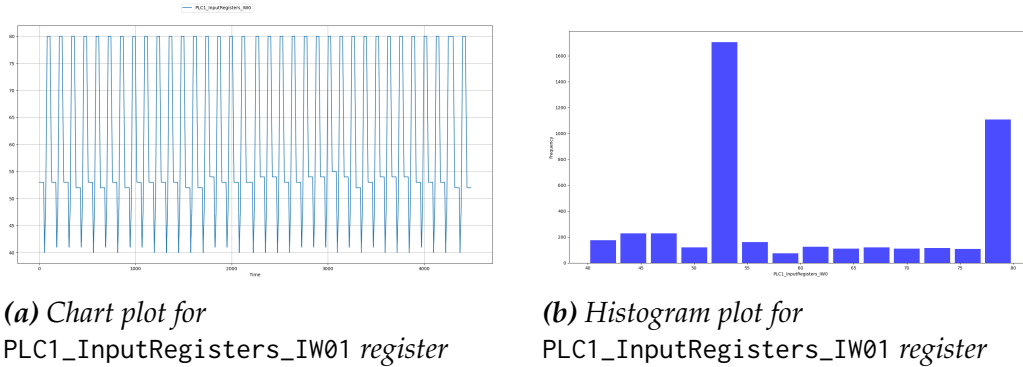


Figure 3.3: Output graphs from graph analysis

The first script plots the charts, one at the time, of certain registers entered by the user from the command line, plots in which one can see the trend of the data and get a first basic idea of what that particular register contains (a measurement, an actuation, a hardcoded setpoint, ...) and possibly the trend; the second script, instead, shows **a histogram and statistical informations** about the register entered as command-line input. These informations include:

- the mean, median, standard deviation, maximum value and minimum value
- two tests for the statistical distribution: *Chi-squared* test for uniformity and *Shapiro-Wilk* test for normality, as shown in Listing 3.3:

```
Chi-squared test for uniformity
Distance      pvalue      Uniform?
12488.340     0.00000000     NO

Shapiro-Wilk test for normality
Test statistic pvalue      Normal?
0.844         0.00000000     NO
```

```

654 Stats of PLC1_InputRegisters_IW0
655 Sample mean = 60.8881; Stddev = 13.0164; max = 80; min =
656 ↪ 40 for 4488 values

```

Listing 3.3: Statistical data for PLC1_InputRegisters_IW0 register

657 3.2.4 Invariants Inference and Analysis

658 For invariant analysis Ceccato et al. rely on **Daikon** [39], a framework
 659 to **dynamically detect likely invariants** within a program. An *invariant*
 660 is a property that holds at one or more points in a program, properties
 661 that are not normally made explicit in the code, but within assert state-
 662 ments, documentation and formal specifications: invariants are useful in
 663 understanding the behavior of a program (in our case, of the cyber physi-
 664 cal system).

665 Daikon uses *machine learning* techniques applied to arbitrary data with
 666 the possibility of setting custom conditions for analysis by using a spe-
 667 cific file [40] with a *.spinfo* extension (see Listing 3.4). The framework is
 668 designed to find the invariants of a program, with various supported pro-
 669 gramming languages, starting from the direct execution of the program
 670 itself or passing as input the execution run (typically a file in CSV format):
 671 the authors of the paper tried to apply it by analogy also to the execution
 672 runs of a cyber physical system, to extract the invariants of this system.

```

673 PPT_NAME aprogram.point:::POINT
674 VAR1 > VAR2
675 VAR1 == VAR3 && VAR1 != VAR4

```

Listing 3.4: Generic example of a .spinfo file for customizing rules in Daikon

676 Therefore, Daikon is fed with the no-timestamp enriched dataset ob-
 677 tained in the pre-processing phase (in the paper, the timestamped dataset
 678 is erroneously mentioned as input): a simple bash script launches Daikon
 679 (optionally specifying the desired condition for analysis in the *.spinfo* file),
 680 which output is simply redirected to a text file containing the general in-
 681 variants of the system (i.e., valid regardless of any custom condition speci-

fied), those generated based on the custom condition in the *.spinfo* file, and those generated based on the negation of the condition. When the analysis is finished, the user is asked to enter the name of a registry to view its related invariants.

Some examples of invariants derived from the enriched dataset may be:

- measurements bounded by some setpoint
- Actuators state changes occurred in the proximity of setpoints or, vice versa, proximity of setpoints upon the occurrence of a regular actuator state change
- state invariants of some actuator correspond to a specific trend in the evolution of the measurement (ascending, descending, or stable) or, vice versa, the measurement trend corresponds to a specific state invariant of some actuator

3.2.5 Business Process Mining and Analysis

Process mining is the analysis of operational processes based on the event log [41]: the aim of this analysis is to **extract useful informations** from the event data to **reconstruct and understand the behavior** of the business process and how it was actually performed.

Process mining for the system under consideration starts from the event logs obtained from scanning the memory registers of the PLCs and sniffing the network communications related to the Modbus protocol, described in Subsection 3.2.2 and representing the *execution trace* of the system: through a Java program, information is extracted and combined from these event logs, and the result saved in a CSV format file.

This file is fed to **Disco** [42], a commercial process mining tool, which generates an *activity diagram* similar to UML Activity Diagram and whose nodes represent the activities while the edges represent the relations be-

710 tween these activities: in Figure 3.4 we can see an example of this diagram
 711 referred to PLC2 of the testbed.

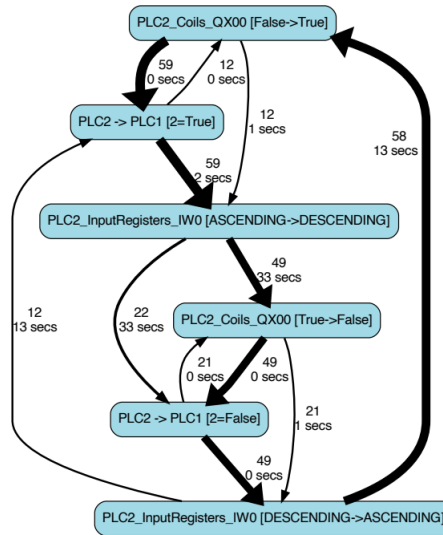


Figure 3.4: An example of Disco generated activity diagram for PLC2

712 The *business process* obtained in this way provides an **overview of the**
 713 **system** and makes it possible to **make conjectures** about its behavior, par-
 714 ticularly between changes in actuator state and measurement trends (i.e.,
 715 a given change in state of some actuators corresponds to a specific mea-
 716 surement trend and vice versa), and with the possibility of **establishing**
 717 **causality** between Modbus communications and state changes within the
 718 physical system.

719 3.2.6 Application

720 In this section we will see how the black box analysis presented above
 721 in its various phases is applied in practice, using the testbed described in
 722 Subsection 3.2.1. The methodology supports a **top-down approach**: that
 723 is, we start with an overview of the industrial process and then gradually
 724 refine our understanding of the process by descending to a higher and
 725 higher level of detail based on the results of the previous analyses and

focusing on the most interesting parts of the system for further in-depth analysis.

Data Collection and Pre-processing According to what is described in the paper, the data gathering process lasted six hours, with a granularity of one data point per second (a full system cycle takes approximately 30 minutes). Each datapoint consists of 168 attributes (55 registers plus a special register concerning the tank slope of each PLC) after the enrichment. In addition, IP addresses are automatically replaced by an abstract name identified by the prefix PLC followed by a progressive integer (PLC1, PLC2, PLC3), in order to make reading easier.

Graphs and Statistical Analysis It is unclear from the paper where exactly the information that follows was derived (graph analysis? Statistical analysis? Human reading of the dataset?), however, three properties about the contents of the registers were discovered:

Property 1: PLC1_MemoryRegisters_MW0, PLC1_MemoryRegisters_MW1, PLC2_MemoryRegisters_MW0, PLC2_MemoryRegisters_MW1, PLC3_MemoryRegisters_MW0 and PLC3_MemoryRegisters_MW1

registers contain constant integer values (40, 80, 10, 20, 0, 10 respectively)². We may speculate that they may be (relative) hardcoded **setpoints**.

Property 2: PLC1_Coils_QX01, PLC1_Coils_QX02, PLC2_Coils_QX01, PLC2_Coils_QX02, PLC3_Coils_QX01 and PLC3_Coils_QX03 contain mutable binary (Boolean) values. We can assume that these registers can be associated with the **actuators** of the system.

Property 3: PLC1_InputRegisters_IW0, PLC2_InputRegisters_IW0 and PLC3_InputRegisters_IW0 registers contain mutable values.

²From my tests on the original tool and dataset, the PLC3_MemoryRegisters_MW0 register is deleted during the *pre-processing* phase, as it is recognized as an unused register because of the constant value "0" it takes on. This leads me to assume that the properties are derived from a human read of the dataset prior to the *pre-processing* phase.

Property 3 suggests that those registers might contain **values related to measurements**: it is therefore necessary to investigate further to see if the conjecture (referred to as *Conjecture 1* in the paper) is correct.

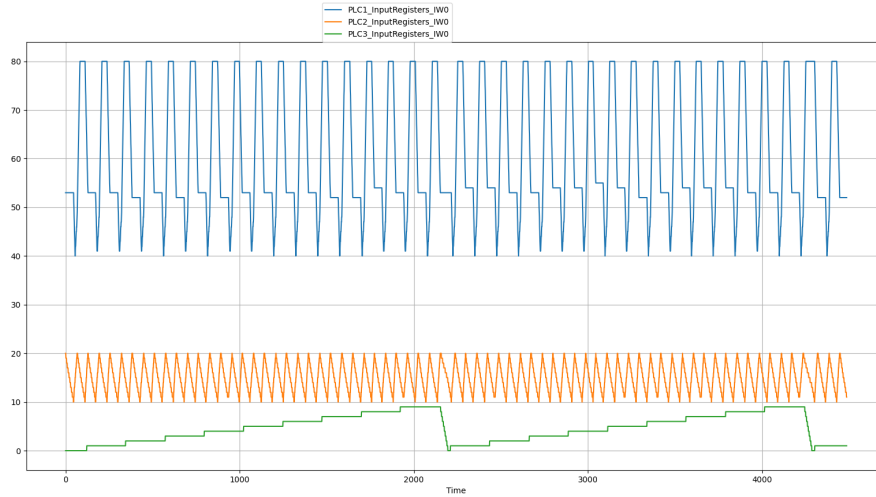


Figure 3.5: Execution traces of InputRegisters_IW0 on the three PLCs

The graph analysis of the InputRegisters_IW0 registers of the three PLCs (summarized in Figure 3.5 with a single plot) not only seems to confirm the conjecture, but also allows the measurements to be correlated with the contents of the MemoryRegisters_MW0 and MemoryRegisters_MW1 registers to the measurements, which represent the **relative setpoints of the measurements**.

Hence, we have *Conjecture 2* described in the paper referring to the relative setpoints:

Conjecture 2:

- 40 and 80 are the relative setpoints for PLC1_InputRegisters_IW0
- 10 and 20 are the relative setpoints for PLC2_InputRegisters_IW0
- 0 and 9 are the relative setpoints for PLC3_InputRegisters_IW0

Further confirmation of this conjecture may come from statistical analysis. Indeed, in the example in Listing 3.1, some statistical data are given for the register PLC1_InputRegisters_IW0, including the maximum value

and the minimum value: these values are, in fact, 80 and 40 respectively.

Business Process Mining and Analysis With Business Process Mining, the authors aim to **visualize and highlight relevant system behaviors** by relating PLC states and Modbus commands.

Through analysis of the activity diagrams shown in Figure 3.6, drawn through Disco, we derive the following properties and conjectures:

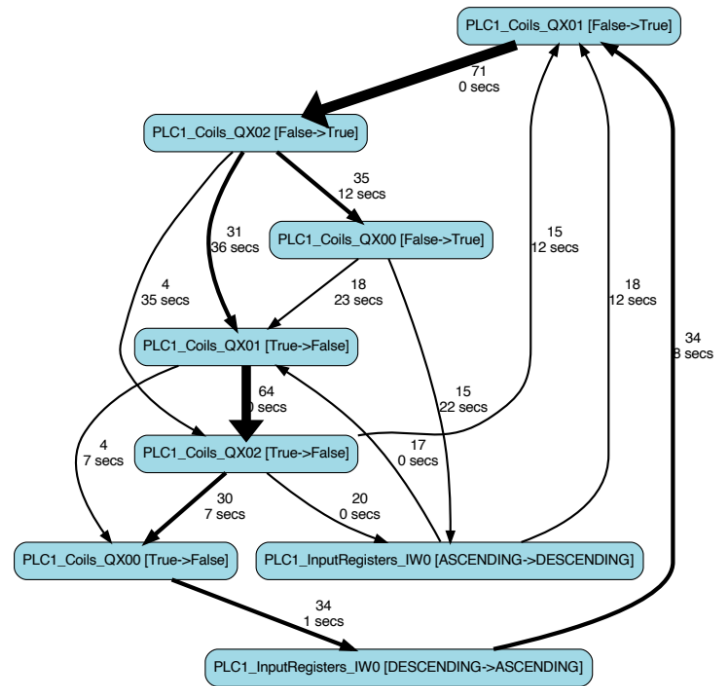
Property 4: PLC2 sends messages to PLC1 (see Figure 3.6b) which are recorded to PLC1_Coils_QX02.

Conjecture 3: PLC2_Coils_QX00 determines the trend in tank T-202 (Figure 3.6b).

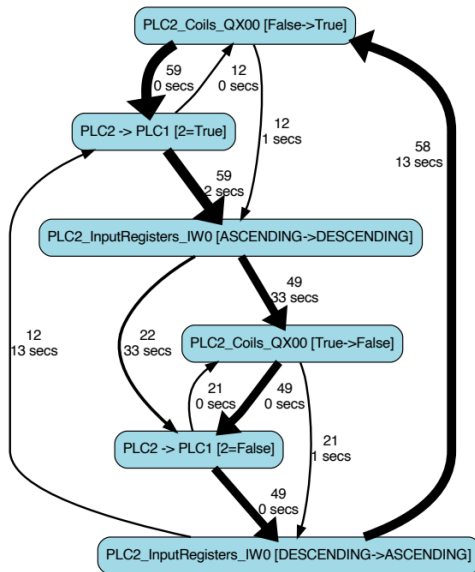
When this register is set to *True*, the input register PLC2_InputRegisters_IW0 related to the tank controlled by PLC2 starts an **ascending trend**; vice versa, when the coil register is set to *False*, the input register starts a **descending trend**.

Conjecture 4: If PLC1_Coils_QX00 change his value to True, trend in tank T-201, related to PLC1_InputRegisters_IW0 and controlled by PLC1, become **ascending** (see Figure 3.6a)

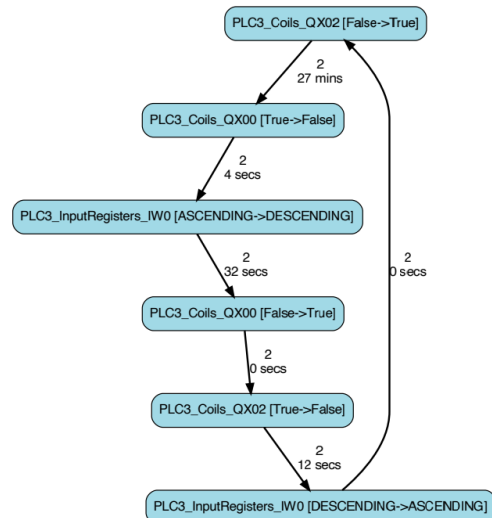
Conjecture 5: PLC3_Coils_QX00 starts a **decreasing trend** in tank T-203, related to PLC3_InputRegisters_IW0 and controlled by PLC3, whereas PLC3_Coils_QX02 starts an **increasing trend** on the tank (see Figure 3.6c)



(a) States in PLC1



(b) States and Modbus command in PLC2



(c) States in PLC3

Figure 3.6: Business process with states and Modbus commands for the three PLCs

Invariants Inference and Analysis The last phase of the analysis of the example industrial system is invariant analysis, performed through Daikon framework. At this stage, an attempt will be made to confirm what has been seen previously and to derive new properties of the system based on the results of the Daikon analysis.

To get gradually more and more accurate results, the authors presumably performed more than one analysis with Daikon, including certain rules within the *splitter information file* (see Section 3.2.4 and Listing 3.4) based on specific conditions placed on the measurements, for example, the level of water contained in a tank. Given moreover the massive amount of invariants generated by Daikon's output, it is not easy to identify and correlate those that are actually useful for analysis: this must be done manually.

However, it was possible to have confirmation of the conjectures made in the previous stages of the analysis: starting with the setpoints, analyzing the output of the invariants returned by Daikon³ reveals that

```

PLC1_InputRegisters_IW0 >= PLC1_MemoryRegisters_MW0 == 40.0
PLC1_InputRegisters_IW0 <= PLC1_MemoryRegisters_MW1 == 80.0
PLC2_InputRegisters_IW0 >= PLC2_MemoryRegisters_MW0 == 10.0
PLC2_InputRegisters_IW0 <= PLC2_MemoryRegisters_MW1 == 20.0
PLC3_InputRegisters_IW0 >= PLC3_MemoryRegisters_MW0 == 0.0
PLC3_InputRegisters_IW0 <= PLC3_MemoryRegisters_MW1 == 9.0

```

i.e., that the MemoryRegisters_MW0 and MemoryRegisters_MW1 registers of each PLC contain the **absolute minimum and maximum setpoints**, respectively (*Property 5*).

There is also a confirmation regarding *Property 4*: from the computed invariants it can be seen that

³The invariants shown here are a manual summary and derivation of those actually returned in output by Daikon. I will discuss this more in Section 3.2.7

821

822 `PLC1_Coils_QX01 == PLC1_Coils_QX02 == PLC2_Coils_QX00`

823

824 and from this derive that there is a **communication channel between PLC2**
 825 **and PLC1**, where the value of `PLC2_Coils_QX00` is copied to `PLC1_Coils_QX01`
 826 and `PLC1_Coils_QX02` (*Property 6*).

827 Regarding the **relationships between actuator state changes and mea-**
 828 **surement trends**, invariant analysis yields the results summarized in the
 829 following rules:

830 *Property 7:* Tank T-202 level *increases* iif `PLC1_Coils_QX01 == True`. Oth-
 831 erwise, if `PLC1_Coils_QX01 == False` will be *non-increasing*.

832 This is because if the coil is *True* the condition

833 `PLC2_InputRegisters_IW0 == PLC2_MemoryRegisters_MW0 == 20.0 && PLC2_slope > 0`

834 is verified. On the opposite hand, if the coil is *False*, the condition

835 `PLC2_InputRegisters_IW0 == PLC2_MemoryRegisters_MW0 == 20.0 && PLC2_slope <= 0` is verified. The
 836 *slope* is an auxiliary attribute indicating the trend of the measurement: in-
 837 creasing if > 0 , decreasing if < 0 , stable otherwise.

838 *Property 8:* Tank T-201 level *increases* iif `PLC1_Coils_QX00 == True`. On the
 839 other hand, if `PLC1_Coils_QX00 == False` and if `PLC1_Coils_QX01 ==`
 840 `True` the level will be *non-decreasing*.

841 *Property 9:* Tank T-203 level *decreases* iif `PLC3_Coils_QX00 == True`. It will
 842 be *non-decreasing* if `PLC1_Coils_QX00 == False`.

843 The last two properties concern the **relationship between actuator state**
 844 **changes and the setpoints**: it is intended to check what happens to the
 845 actuators when the water level reaches one of these setpoints. From the
 846 analysis of the relevant invariants, the following properties are derived:

847 *Property 10:* Tank T-201 reaches the upper absolute setpoint when
 848 `PLC1_Coils_QX00` changes its state from *True* to *False*. If the coil changes
 849 from *False* to *True*, the tank reaches its absolute lower setpoint.

Property 11: Tank T-203 reaches the upper absolute setpoint when PLC3_Coils_QX00 changes its state from *True* to *False*. If the coil changes from *False* to *True*, the tank reaches its absolute lower setpoint.

3.2.7 Limitations

The methodology proposed by Ceccato et al. is certainly valid and offers a good starting point for approaching the reverse engineering of an industrial control system from the attacker's perspective, while also providing a tool to perform this task.

The limitations of this approach, however, all lie in the tool mentioned above and also in the testbed described in Section 3.2.1. In this section I will explain which are the criticisms of each phase, while in Chapter 4 I will formulate proposals to improve and make this methodology more efficient.

General Criticism The general critical aspects of the application of this approach are many: the primary one concerns the fact that the proposed tool seems to be built specifically for the testbed used and that it is not applicable to other contexts, even to the same type of industrial control system (water treatment systems, in this case).

What severely limits the analysis performed with the tool implemented by Ceccato et al. is the use of *ad hoc* solutions and *a posteriori* interventions done manually on the datasets after the data gathering process: I will discuss this last aspect in more detail later.

Moreover, there is the presence of many *hardcoded* variables and conditions within the scripts: this makes the system unconfigurable and unable to properly perform the various stages of the analysis as errors can occur due to incorrect data and mismatches with the system under analysis.

Having considered, furthermore, only the Modbus protocol for network communications between the PLCs is another major limiting factor and does not help the methodology to be adaptable to different systems

879 communicating with different protocols (sometimes even multiple ones
880 on the same system).

881 Let us now look at the limitations and critical aspects of each phase.

882 **Testbed** The testbed environment used by Ceccato et. al is entirely simu-
883 lated, from the physical system to the control system. The PLCs were built
884 with **OpenPLC** [43] in a Docker environment [44], while the physics part
885 was built through **Simulink** [45].

886 OpenPLC is an open source cross-platform software that simulates the
887 hardware and software functionality of a physical PLC and also offers a
888 complete editor for PLC program development with support for all stan-
889 dard languages: *Ladder Logic* (LD), *Function Block Diagram* (FBD), *Instruc-*
890 *tion List* (IL), *Structured Text* (ST), and *Sequential Function Chart* (SFC).

891 It is for sure an excellent choice for creating a zero-cost industrial or home
892 automation and *Internet of Things* (IoT) system that is easy to manage via a
893 dedicated, comprehensive and functional web interface. In spite of these
894 undoubted merits, however, there are (at the moment) **very few supported**
895 **protocols**: the main one and also referred to in the official documentation
896 is **Modbus**, while the other protocol is DNP3.

897 The biggest problem with the testbed, however, is not with the con-
898 troller part, but with the **physical part**: first of all, it must be said that
899 although this is something purely demonstrative even though it is fully
900 functional, the implemented Simulink model is really **oversimplified** com-
901 pared to the iTrust SWaT system, which itself is a scaled-down version of a
902 real water treatment plant. In fact, in the entire system there are only three
903 actuators, two of which are connected to the same tank and controlled by
904 the same PLC, and sensors related only to the water level in the system's
905 tanks: in a real system there are many more *field devices*, which can mon-
906 itor and control other aspects of the system beyond the mere contents of
907 the tanks. Consider, for example, measuring and controlling the chemicals
908 in the water, the pressure of the liquid in the filter unit, or more simply the

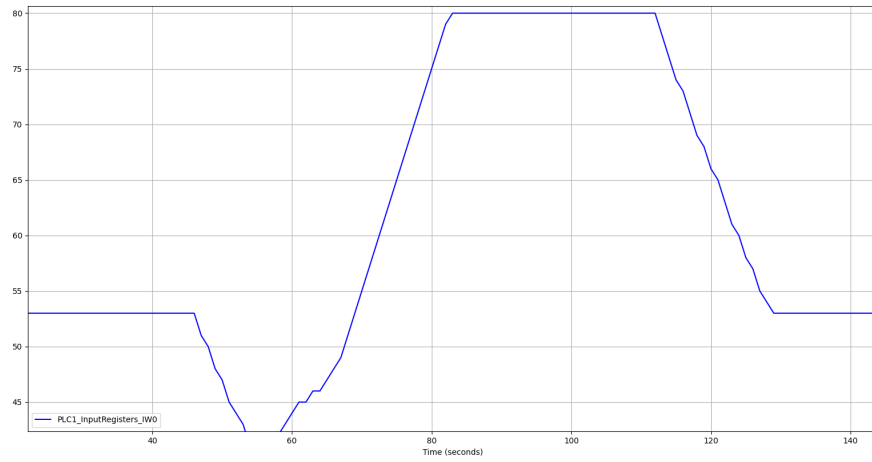
amount of water flow at a given point or time.

All these must be considered and represent a number of additional variables that makes analysis and consequently reverse engineering of the system more difficult.

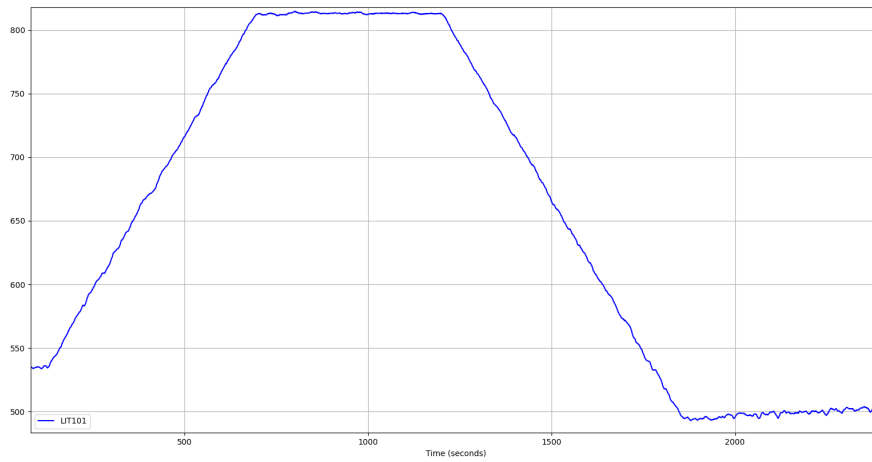
The second critical aspect concerns the **simulation of the physics of the liquid** inside the tanks: Simulink does not consider the fact that inside a tank that is filling (emptying) the liquid in it undergoes **fluctuations** which cause the level sensor not to see the water level constantly increasing (decreasing) or at most being stable at each point of detection. Figure 3.7 exemplifies more clearly with an example the concept just expressed: these oscillations cause a **perturbation** in the data.

This issue leads to the difficulty, on a real physical system, of **correctly calculating the trend of a measurement** by using the slope attribute: if this was obtained with a too low granularity, the trend will be oscillating between increasing and decreasing even when in reality this would be in general increasing (decreasing) or stable; on the other hand, if the slope was obtained with a too high granularity there is a loss of information and the trend may be "flattened" with respect to reality.

In the present case, the slope in the Simulink model was calculated statically *point-to-point*, thus with a granularity of one second: an averagely careful reader will have already guessed that this granularity is inapplicable to the real system in Figure 3.7b. As we will later see, we need to **operate on the data perturbations** to be able to obtain a suitable granularity and a correct calculation of the slope and consequently of the measurement trend.



(a)



(b)

Figure 3.7: Water physics compared: simulated physics in the Simulink model (a) and physics in a real system (iTrust SWaT) (b). Fluctuations in the tank level in (b), almost completely absent in (a), can be appreciated.

934 **Pre-processing** In the pre-processing phase, the authors make use of a
 935 Python script to merge all the datasets of the individual PLCs into a single
 936 dataset, remove the (supposedly) unused registers, and finally enrich the
 937 obtained dataset with additional attributes. These attributes are:

- 938 • the previous value of all registers

- some additional relative setpoints named `PLCx_Max_safety` and `PLCx_Min_safety` (where x is the PLC number), which represent a kind of alert on reaching the maximum and minimum water levels of the tanks
- the measurement slope, that is, the trend of the water level in the system tanks along the system cycles.

Merging the datasets of all individual PLCs into a single dataset representing the entire system can be a sound practice if the system to be analyzed is (very) small as is the testbed analyzed here, consisting of a few PLCs and especially a few registers. If, however, the complexity of the system increases, this type of merging can become counterproductive and make it difficult to analyze and understand the data obtained in subsequent steps.

In short, there is no possibility to analyze only a subsystem and thus make the analysis faster and more understandable. Moreover, a data gathering can take up to days, and the analyst/attacker may need to make an analysis of the system isolating a precise time range, ignoring everything that happens before and/or after: all of this, with the tool we have seen, cannot be done.

Regarding the additional attributes, looking at the code of the script that performs the enrichment, I observed that **some attributes were manually inserted** after the merging phase: I am referring in particular to the attributes `PLCx_Max_safety` and `PLCx_Min_safety`, whose references were moreover hardcoded into the script, and the *slope* whose calculation method I mentioned in the previous paragraph about the testbed limitations.

In the end, only the attribute *prev* related to the value at the previous point of the detection is inserted automatically for all registers, moreover without the possibility to choose whether this attribute should be extended to all registers or only to a part.

969 **Graphs and Statistical Analysis** Describing the behavior of graphical
970 analysis in Section 3.2.3 I had already mentioned that only one register plot
971 at a time was shown and not, for example, a single window containing the
972 charts of all registers entered by the user as input from the command line,
973 such as in Figure 3.5.

974 While displaying charts for individual registers still provides useful in-
975 formation about the system such as the distinction between actuators and
976 measurements and the general trend of the latter, single display does not
977 allow one to catch, or at least makes it difficult, the relationship that exists
978 between actuators and measurements, where it exists, because a view of
979 the system as a whole is missing.

980 In this way, the risk is to make conjectures about the behavior of the system
981 that may prove to be at least imprecises, if not inaccurates.

982 On the other hand, regarding the statistical analysis, two observations
983 need to be made: the first is that for the given system, I personally was
984 unable to appreciate the usefulness of the generated histogram, as it does
985 not provide any particular new information that has not already been ob-
986 tained from the graphical analysis (except maybe something marginal);
987 the second observation is that precisely the plot of the histogram "hides"
988 the statistical informations obtained: these are in fact shown on the ter-
989 minal from which the script is launched, but to an uncared eye or one
990 unfamiliar with the script's behavior they can easily be interpreted as sim-
991 ple debugging output, since at the same time the window containing the
992 histogram plot is shown. In general, however, little statistical information
993 is provided.

994 **Business Process Mining and Analysis** Concerning the data mining,
995 this is a purely *ad hoc solution*, designed to work under special conditions:
996 first, the timestamped dataset of the physical process and the one obtained
997 after the packet sniffing operation of Modbus traffic on the network need
998 to be synchronized and have the same granularity, in this case one event
999 per second.

It is relatively easy, therefore, to find correspondences between Modbus commands sent over the network and events occurring on the physical system, such as state changes in actuations, due in part to the fact that the number of communications over the network is really small (see Section 3.2.1). In a real system, network communications are much more numerous and involve many more devices even in the same second: finding the exact correspondence with what is happening in the cyber physical system becomes much more difficult.

Since this is, as mentioned, an *ad hoc* solution, only the Modbus protocol is being considered: as widely used as this industrial protocol is, other protocols that are widely used such as EtherNet/IP (see Section 2.3.1.2) should be considered in order to extend the analysis to other industrial systems that use a different communication network.

The other limiting aspect of the business process mining phase is the **process mining software** used to generate the activity diagram. As mentioned in Section 3.2.5, the process mining software used by Ceccato et al. is **Disco**: this is commercial software, with an academic license lasting only 30 days (although free of charge), released for Windows and MacOS operating systems only, which makes its use under Linux systems impossible except by using emulation environments such as Wine. For what is my vision and training as a computer scientist, it would have been preferable to use a *cross-platform, freely licensed open source* software alternative to Disco: one such software could have been **ProM Tools** [46], a framework for process mining very similar to Disco in functionality, but fitting the criteria just described, or use Python libraries such as **PM4PY** [47], which offer ready-to-use algorithms suitable for various process mining needs.

Invariants Inference and Analysis The limitation in this case is principally Daikon: this software is designed to compute the invariants of a software from its live execution or from a file containing its execution flow, not to find the invariants of a cyber physical system. Since there are currently

no better consolidated alternatives for inferring invariants, however, an attempt was still made to use Daikon as best as possible.

```

daikon version 5.8.14, released October 6, 2022; http://plse.cs.washington.edu/daikon.
Reading splitter info files
(read 1 spinfo file, 1 splitter)
Reading declaration files .aprogram.point::POINT: 1 of 1 splitters successful

(read 1 decls file)
Processing trace data; reading 1 dtrace file:

Warning: No non-obvious non-suppressed exclusive invariants found in
aprogram.point::POINT
Warning: No non-obvious non-suppressed exclusive invariants found in
aprogram.point::POINT
=====
aprogram.point::POINT
PLC2_MemoryRegisters_MW1 == PLC3_MemoryRegisters_MW1
PLC1_MemoryRegisters_MW0 == 40.0
PLC1_MemoryRegisters_MW1 == 80.0
PLC1_Coils_QX00 one of { 0.0, 1.0 }
PLC1_Coils_QX01 one of { 0.0, 1.0 }
PLC1_Coils_QX02 one of { 0.0, 1.0 }
PLC2_MemoryRegisters_MW1 == 10.0
PLC2_MemoryRegisters_MW2 == 20.0
PLC2_Coils_QX00 one of { 0.0, 1.0 }
PLC3_InputRegisters_IW0 >= 0.0
PLC3_Coils_QX00 one of { 0.0, 1.0 }
PLC3_Coils_QX02 one of { 0.0, 1.0 }
prev_PLC1_Coils_QX00 one of { 0.0, 1.0 }
prev_PLC1_Coils_QX01 one of { 0.0, 1.0 }
prev_PLC2_Coils_QX00 one of { 0.0, 1.0 }
prev_PLC3_InputRegisters_IW0 >= 0.0
prev_PLC3_Coils_QX00 one of { 0.0, 1.0 }
prev_PLC3_Coils_QX02 one of { 0.0, 1.0 }
PLC1_Max_safety == 77.0

```

Figure 3.8: Example of Daikon's output

The biggest problem with Daikon applied to the computation of invariants of an industrial system is the difficult reading of the resulting output: the software in fact returns a very long list of invariants, one invariant per line, many of no use and without correlating invariants that may have common features or deriving additional information from them. The process of screening and recognizing the significant invariants, as well as the correlation between them, must be done by a human: certainly not an easy task given the volume of invariants one could theoretically be faced with (hundreds and hundreds of invariants). An example of Daikon's output

1042 can be seen in Figure 3.8.

1043 The bash script used in this phase of the analysis does not help at all
1044 in deriving significant invariants more easily: it merely launches Daikon
1045 and saves its output to a text file by simply redirecting the stdout to file.
1046 No data reprocessing is done during this step. In addition, if a condition
1047 is to be specified to Daikon before performing the analysis, it is necessary
1048 each time to edit the .spinfo file by manually entering the desired rule, an
1049 inconvenient operation when multiple analyses are to be performed with
1050 different conditions each time.

Chapter 4

A Framework to Improve Ceccato et al.'s Work.

1051 **I**N CHAPTER 3, I presented the state of the art of *process comprehension* of
1052 an Industrial Control System (ICS) focusing later on the methodology
1053 proposed by Ceccato et al. [6][Section 3.2], explaining what it consists of,
1054 its practical application on a testbed, and most importantly highlighting
1055 its limitations and critical issues (see Section 3.2.7).

1056 In this chapter I will present **my proposals to improve the methodol-**
1057 **ogy** presented in the previous chapter, overcoming (or at least trying to do
1058 so) the criticalities mentioned above by almost completely rewriting the
1059 original framework, enhancing its functionalities and inserting new ones
1060 where possible, while keeping its general structure and approach: the sys-
1061 tem analysis will in fact consist of the same four steps as in the original
1062 methodology (Data Pre-processing, Graph and Statistical Analysis, Busi-
1063 ness Process Mining and Invariants Inference), but each of them will be
1064 deeply revised in order to provide a richer, clearer and more complete
1065 process comprehension of the industrial system to be analyzed and its be-
1066 havior.

1067 As it may have already been noted, my proposals do not involve im-
1068 proving the data gathering phase: this is due simply to the fact that the
1069 novel framework will not be tested on the same case study used by Cec-

1070 cato et, al. (Section 3.2.1), but on a different case study, the ITrust SWaT
1071 system [29], of which (some) datasets containing the execution trace of
1072 the physical system and the network traffic scan are already provided by
1073 iTrust itself. For more details about this case study, see Chapter 5.

1074 4.1 The novel Framework

1075 The implementation of the novel framework for ICSs analysis starts
1076 from several assumptions:

- 1077 1. it must be implemented in a **single programming language**
- 1078 2. it must be **independent of the system** to be analyzed
- 1079 3. It must provide greater **flexibility and ease of use** for the user at
1080 every stage

1081 In the following, these three points will be discussed in more detail.

1082 **Single Programming Language** The original tool was implemented us-
1083 ing various programming languages in each of the different phases:
1084 from Python up to Java, passing through Bash scripting.
1085 In my opinion, this heterogeneity makes it more difficult and less
1086 intuitive for the user to operate on the tool: moreover, the use of
1087 multiple technologies makes it more difficult to maintain the code
1088 and add new features, particularly if only a single person is manag-
1089 ing the code (he/she might be proficient in one language, but little
1090 of the others).

1091 For these reasons, I decided to use a single programming language,
1092 to ensure homogeneity to the framework and ease of use and main-
1093 tenance of the code for anyone who wants to manage it in the future:
1094 I chose to use Python, because of its simplicity and easy readability
1095 combined with its versatility and powerfulness: moreover, Python
1096 can count on a massive number of available libraries and packages
1097 that meet all kinds of needs.

System Independence One of the biggest limitations of Ceccato et al.'s tool that I highlighted in Section 3.2.7 is the fact that it is **highly dependent on the testbed used**: that is, it is *not* possible to configure any of the tool's parameters to analyze different industrial systems. To overcome this issue and make my framework independent of the system to be analyzed, also eliminating all references to hardcoded variables and values present in the previous tool, I decided to use a **general configuration file**, named *config.ini*, in which the user can, at will, customize all the parameters necessary to perform the analysis of the targeted system.

Flexibility and Ease on Use The lack of flexibility and ease of use in a tool can be a significant disadvantage, limiting its effectiveness and making it challenging for the user to get the desired outcomes. The original tool suffered from these limitations, with users having to run scripts from the command line, with little to no options or parameters available to customize the analysis. As a result, the tool was not user-friendly and lacked the flexibility to adapt to specific user needs.

To settle these issues, I enhanced the command-line interface in the novel framework by adding new options and parameters. These new features provide the user with greater flexibility, enabling to specify parameters and options that allow for more in-depth analysis and focused results analyzing data more effectively and efficiently. With these enhancements, the framework has become more user-friendly, reducing the learning curve and making it more accessible to a wider range of users.

This, in turn, makes the framework more valuable and useful, increasing its adoption and effectiveness across a range of industries and applications.

Moreover, with new options and parameters users no longer have to rely solely on the command line interface, which can be challenging and intimidating for those with limited technical expertise. Instead,

1130 users can now access a range of customizable options and paramete-
1131 ters, making the tool more intuitive and user-friendly.

1132 Overall, the enhancements made to the framework represent a significant
1133 step forward in making it more effective, efficient, and user-friendly.

1134 4.1.1 Framework Structure

1135 The structure of the novel framework mostly follows the structure of
1136 the original tool: it is divided into four main directories each representing
1137 the different phases of the analysis (data pre-processing, graphs and sta-
1138 tistical analysis, process mining, and invariant analysis), and containing
1139 the relevant Python scripts that perform the analysis, as well as subdirec-
1140 tories and any input/output files necessary for the proper behavior of the
1141 framework.

```
1142 .  
1143 |-- config.ini  
1144 |-- daikon  
1145 |   |-- Daikon_Invariants  
1146 |   |-- daikonAnalysis.py  
1147 |   |-- runDaikon.py  
1148 |-- network-analysis  
1149 |   |-- data  
1150 |   |-- export_pcap_data.py  
1151 |   |-- swat_csv_extractor.py  
1152 |-- pre-processing  
1153 |   |-- mergeDatasets.py  
1154 |   |-- system_info.py  
1155 |-- process-mining  
1156 |   |-- data  
1157 |   |-- process_mining.py  
1158 |-- statistical-graphs  
1159 |   |-- histPlots_Stats.py  
1160 |   |-- runChartSubPlots.py
```

Listing 4.1: Novel Framework structure and Python scripts

Ahead of these directories there is the most important part, that allows the framework to be independent of the industrial control system being analyzed: the *config.ini* file. Here the user can configure general parameters and options, such as paths to read from or write files to, or related to individual analysis phases.

The file is divided into sections, each covering a different aspect of the configuration: each section contains user-customizable parameters that will then be called within the Python scripts that constitute the framework. Sections of *config.ini* are:

- **[PATHS]**: defines general paths such as the project root directory and some source directories for datasets
- **[PREPROC]**: contains some parameters needed for the pre-processing phase
- **[DAIKON]**: defines parameters needed for invariant analysis with Daikon
- **[DATASET]**: defines settings and parameters used during the dataset enrichment stage and possibly in further phases
- **[MINING]**: contains parameters used during the process mining phase
- **[NETWORK]**: Contains specific settings for extracting the data obtained from the packet sniffing phase on the ICS network and converting it to CSV format. It also defines the network protocols that are to be analyzed

4.1.2 Python Libraries and External Tools

Since the framework has been entirely developed in Python, I have tried to make use of external tools as little as possible, with the idea of integrating all the various functionalities within the framework and making it independent of further software: the only external tool remaining from the old Ceccato et al. tool is Daikon, precisely because there is currently

no better alternative or Python packages that performs the same functionalities.

Instead, large use of Python libraries is made for handling functionality and input data: the fundamental libraries upon which the framework is based are:

- **Pandas**, also used in the previous tool for dataset management, but whose use here has been deepened and extended
- **NumPy**, often used together with Pandas to perform some operations to support it
- **Matplotlib**, for managing and plotting graphical analysis
- other scientific libraries such as **SciPy**, **StatsModel** [48] and **NetworkX** [49], for mathematical, statistical and analysis operations on the data
- **GraphViz**, for the creation of activity diagrams in the process mining phase

Having now seen the structure of the framework, in the next sections we will go into more detail describing my proposals and what I have done to improve the various stages of the analysis.

4.2 Analysis Phases

4.2.1 Phase 1: Data Pre-processing

Data Pre-processing phase is probably the most delicate and significant one: depending on how large the industrial system to be analyzed is, the data collected, and how it is enriched using the additional attributes, the subsequent system analysis will provide more or less accurate outcomes.

The previous tool has many limitations, especially at this stage: it is not possible to isolate a subsystem (either on a temporal basis or on the number of PLCs to be analyzed - the system is considered in its whole), and many of the additional attributes were actually added manually: moreover, for those automatically entered, there is no way to specify which register type to associate the additional attribute with.

All this, combined with the fact that in the tool code many references to attributes and registers are hardcoded, makes the analysis of the system much more difficult and the obtained results less accurate in terms of quantity and quality.

In the novel framework these problems have been overcome by introducing the possibility, starting from the datasets of individual PLCs obtained from data gathering process, to select a subsystem from the command line both on a temporal basis and of the PLCs to be considered; I have also redesigned the whole process of enrichment of the resulting dataset, eliminating the manual entry of additional attributes and giving the user the possibility to be able to decide which type of additional attribute to associate with a given register. In addition to this, at the end of the pre-processing operation, it is possible to perform a brief preliminary analysis of the obtained dataset in order to estimate which registers are connected to actuators, which to measurements, and which represent hardcoded relative setpoints or constants: this operation also makes it possible to be able to refine the enrichment step by setting the relevant parameters in the *config.ini* file

In the next sections we will look in more detail at what has been accomplished.

1240 4.2.1.1 Subsystem Selection

1241 In the previous tool, the datasets in CSV format referring to each single
1242 PLC are placed in a fixed directory (hardcoded in the script) from which
1243 the dedicated script later perform merge and enrichment of them all, re-
1244 sulting in a single dataset representing the entire process trace of the in-
1245 dustrial system as an output. As mentioned, the script makes no provision
1246 to choose the individual PLCs to be analyzed, nor to decide on a temporal
1247 range over which to perform the analysis: in fact, it may happen that dur-
1248 ing the period of scanning and data gathering there is a so-called *transient*,
1249 i.e., a general state in which the industrial system is still initializing before
1250 actually reaching full operation; or, more simply, there is the need to ana-
1251 lyze the process of only a specific part of the industrial system in a certain
1252 period of interest: whatever the motivation, the lack of elasticity and op-
1253 tions to provide to the user makes the analysis much more complex than
1254 it might be, affecting even the later phases, as the number of variables to
1255 be analyzed becomes enormously higher.

1256 In addition, it is not possible to specify an output CSV file where to save
1257 the resulting dataset: at each dataset creation and enrichment operation,
1258 therefore, the resultant file will be overwritten. This is very awkward
1259 when making comparisons between two different execution traces, for ex-
1260 ample, unless the files are renamed manually.

1261 Let's see how all these issues were solved in the novel framework I
1262 developed: first of all, in the general *config.ini* file there are some general
1263 default settings about paths, and among them the one concerning the di-
1264 rectory where to place the datasets of the individual PLCs to be processed.
1265 In addition to this option, there are other ones that define further aspects
1266 related to the operations performed in this phase. Listing 4.2 shows the
1267 settings in question:

```
1268 [PATHS]  
1269 root_dir = /home/marcuzzo/Univr/Tesi  
1270 project_dir = %(root_dir)s/PLC-RE  
1271 input_dataset_directory = %(root_dir)s/datasets_SWaT/2015
```

```

1272     net_csv_path = %(root_dir)s/datasets_SWaT/2015/Network_CSV
1273
1274     [DEFAULTS]
1275     dataset_file = PLC_SWaT_Dataset.csv # Default output
1276     ↪ dataset
1277     granularity = 10 # slope granularity
1278     number_of_rows = 20000 # Seconds to consider
1279     skip_rows = 100000 # Skip seconds from beginning

```

Listing 4.2: Paths and parameters for the Pre-processing phase in config.ini file

Concurrently, the same options can be specified by the user via the command line of the new Python script (named `mergeDatasets.py` and contained in the directory `pre-processing` of the project) and will override the default ones found in `config.ini`. These options are:

- **-s or --skiprows:** seconds to jump from the beginning of the file. This option is useful in case the system has an initial transient or to start the analysis from a certain point in the dataset
- **-n or --nrows:** reference temporal period in seconds (rows) for the analysis from the beginning of the dataset or from the point specified in the `-s` option or in the corresponding setting in `config.ini`. This option makes a **selection** on the data of the dataset.
- **-p or --plcs:** PLCs to be merged and enriched. The user can specify the desired PLCs by indicating the CSV file names of the associated datasets with no limitations on number. This option makes a **projection** on the data of the dataset.
- **-d or --directory:** performs the merge and enrichment of all CSV files contained in the directory specified by user, overriding the default setting in `config.ini`. It is in fact the old functionality of the previous tool, maintained here to give the user more flexibility and convenience in case he wants to perform the analysis on the whole system. This is also the default behavior in case the `-p` option is not specified.

- 1301 • **-o** or **--output**: specifies the name of the file in which the obtained
1302 dataset will be saved. It must necessarily be a file in CSV format.
- 1303 • **-g** or **--granularity**: specifies a granularity that will be used to cal-
1304 culate the measurement slope during the dataset enrichment phase.
1305 We will discuss this later in Section 4.2.1.2.

1306 4.2.1.2 Dataset Enrichment

1307 After a step in which a function is applied to each PLC-related dataset
1308 that eliminates its registers that have not been used within the system (this
1309 is especially true if the Modbus register scan has been performed, in which
1310 ranges of registers are scanned: it is assumed that unused registers have
1311 constant value zero), the **dataset enrichment operation** is performed.

1312 This operation differs from the previous version not only in the fact that
1313 it is performed on each individual dataset and not on the resulting dataset,
1314 but also in the additional attributes: not only are they greater in number,
1315 but they are automatically calculated and inserted by the `mergeDatasets.py`
1316 script into the dataset and, most importantly, it is possible to decide through
1317 the parameters in the `config.ini` configuration file under the [DATASET] sec-
1318 tion to which registers these attributes should be assigned.
1319 In Listing 4.3 we can see the list of additional attributes and how they
1320 should be associated with the registers of the dataset:

```
1321 [DATASET]
1322 timestamp_col = Timestamp
1323 max_prefix = max_
1324 min_prefix = min_
1325 max_min_cols_list = lit|ait|dpit
1326 prev_cols_prefix = prev_
1327 prev_cols_list = mv[0-9]{3}|p[0-9]{3}
1328 trend_cols_prefix = trend_
1329 trend_cols_list = lit
1330 trend_period = 150
1331 slope_cols_prefix = slope_
```

```
slope_cols_list = lit
```

Listing 4.3: config.ini parameters for dataset enriching

Following is a brief explanation of the parameters just seen:

timestap_col indicates the name of the column that contains the data timestamps. This parameter is used not only in this phase, but is also referred to in the Process Mining phase. In the previous work, this parameter was hardcoded and not configurable (and thus causing errors if the system being analyzed changed)

max_prefix, min_prefix, max_min_cols_list refer to any relative maximum or minimum values (*relative setpoints*) of one or more measures and that can be found and inserted as new columns within the dataset. The first two parameters indicate the prefix to be used in the column names affected by this additional attribute, while the third specifies of which type of registers we want to know the maximum and/or minimum value reached (several options can be specified using the logical operator | - or).

If, for example, we want to know the maximum value of the registers associated with the tanks, indicated in the iTrust SWaT system by the prefix LIT, we only need to specify the necessary parameter in the *config.ini* file, so `max_min_cols_list = lit`.

The result will be to have in the dataset thus enriched a new column named `max_P1_LIT101`.

prev_cols_prefix, prev_cols_list refer to the values at the previous step of the registers specified in `prev_cols_list`. It is possible to specify registers using *regex*, as in the example shown. It may be useful in some cases to have this value available to check, for example, when a change of state of a single given actuator occurs. The behavior of these parameters is the same as described in the point above.

slope_cols_prefix, slope_cols_list are related to the calculation of the slope of a specific register (usually a measure), that is, its trend. The

slope can be ascending (if its value is greater than zero), descending (if less than zero) or stable (if approximately equal to zero). I will discuss the slope calculation in more detail in the next paragraph, as it is related to the attributes `trend_cols_prefix`, `trend_cols_list` and `trend_period`

Initially, the parameters for registers to be associated with each additional attribute may be left blank, assuming that we do not know the system at all and therefore do not know which registers may be actuators, which measures, and which further. This information can be obtained from the **brief analysis** following the datasets merging operation: this analysis, performed at the user's choice, indicates which may be likely sensors, which actuators, and further information of various kinds: these indications allow the user to be able to set the desired values in `config.ini` file and hence refine the enrichment process by re-launching the `mergeDatasets.py` script again.

Slope Calculation The *slope* is an attribute that indicates the trend of the measurement we are considering and is useful, in our context, during the inference and invariant analysis phase in order to derive information about this trend given specific conditions: this trend can be, in general, increasing (slope > 0), decreasing (slope < 0) or stable (slope = 0). Normally, the slope is calculated through a simple mathematical formula: given an interval a, b relative to the measurement l , the slope is given by the difference of these two values divided by the amount of time t that the measurement takes to reach b from a :

$$slope = \frac{l(b) - l(a)}{t(b) - t(a)}$$

In the novel framework as in the old tool, this time interval (also called **granularity**) can be either long or short, depending on the accuracy desired on the slope: the lower the granularity, the more the slope will reflect the actual measurement trend; the higher the granularity, on the other hand, the more the slope data will be flattened. Each time interval into

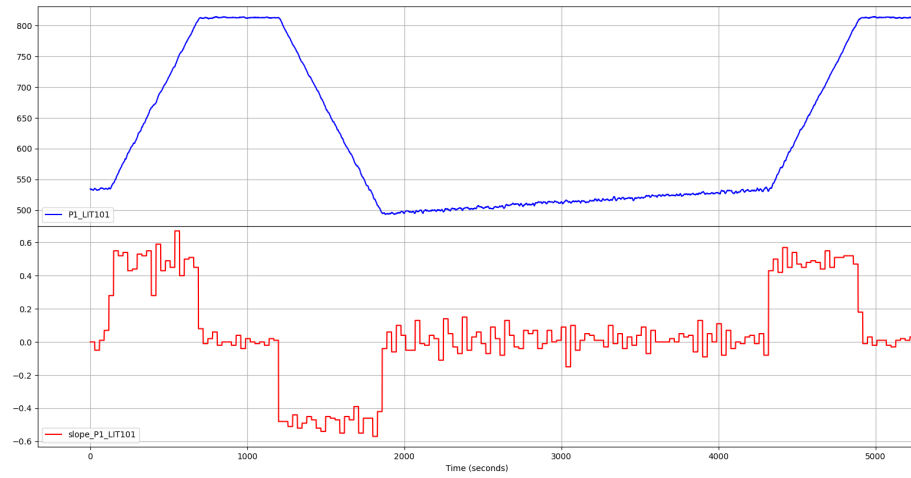
which the measure is divided corresponds to a slope, the set of which inserted as an additional attribute in the dataset will later be used to define the trend of the measure itself in specific situations.

Calculating the slope directly from the raw measurement data may be an acceptable solution for those systems whose measurements are not significantly affected by **perturbations** (such as the oscillations of the liquid inside a tank during the filling and emptying phases, leading to fluctuating level readings): in this case, granularity can be kept low and thus obtain a very accurate overall trend calculation close to the actual measurement trend. This is the case, for example, with the tanks of the testbed used by Ceccato et al.

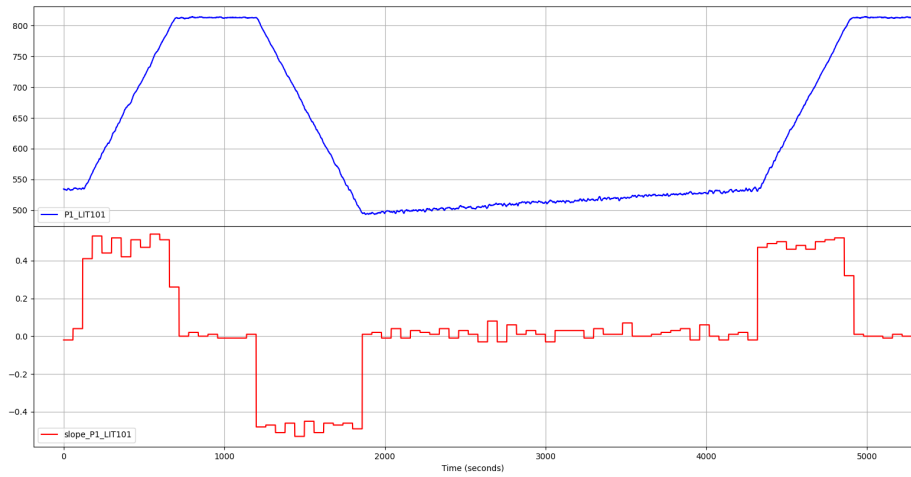
However, in the case where these perturbations significantly afflict the detections on the measurement, the slope calculation on the individual time intervals of the measurement may lead to an erroneous result in trend definition, regardless of the granularity used.

Figure 4.1 demonstrates this assertion: the measurement, in blue, refers to the LIT101 tank of the iTrust SWaT system; in red, the slope calculation related to the measurement with three different granularities: 30 (Figure 4.1a), 60 (Figure 4.1b) and 120 seconds (Figure 4.1c). It can be seen that in addition to the flattening of slope values as the granularity increases, in the time interval between seconds 1800 and 4200 the level of LIT101 has a generally increasing trend, but the slope values vary from positive to negative: the result is that in the invariant analysis the general increasing trend will not be detected thus losing the information.

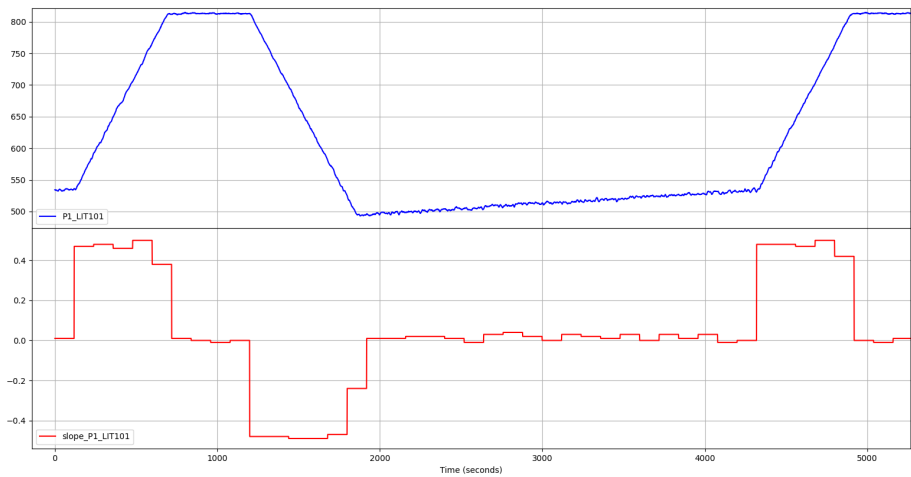
The possibility of a having (strongly) perturbed data was not considered in the previous tool, so I was faced with this issue to solve.



(a)



(b)



(c)

Figure 4.1: Slope comparison with granularity 30 (a), 60 (b) and 120 seconds (c)

The solution to this problem is trying to remove as much "noise" as possible from the data, in order to get a more linear trend in the curve representing the measurement and consequently be able to calculate slopes more accurately.

There are several ways to smooth out the noise, but two of them seemed to me to be the most suitable and that I considered and evaluated: using **polynomial regression**, thus creating a filter on the noise, or a **seasonal decomposition**, and more specifically the part concerning the **trending**. With regard to polynomial regression, I evaluated the *Savitzky-Golay* algorithm [50], and with regard to seasonal decomposition, I evaluated *Seasonal-Trend decomposition using LOESS* (STL) [51].

For reasons of the length of this paper I cannot describe these two solutions in detail (for this, I refer to the bibliographical notes): Figure 4.2, however, shows a quick graphical comparison of them compared with the original data. The solution chosen is the STL decomposition, which is more effective in attenuating noise than the Savitzky-Golay filter although at the cost of more delay (still present in all algorithms of this kind) in some parts.

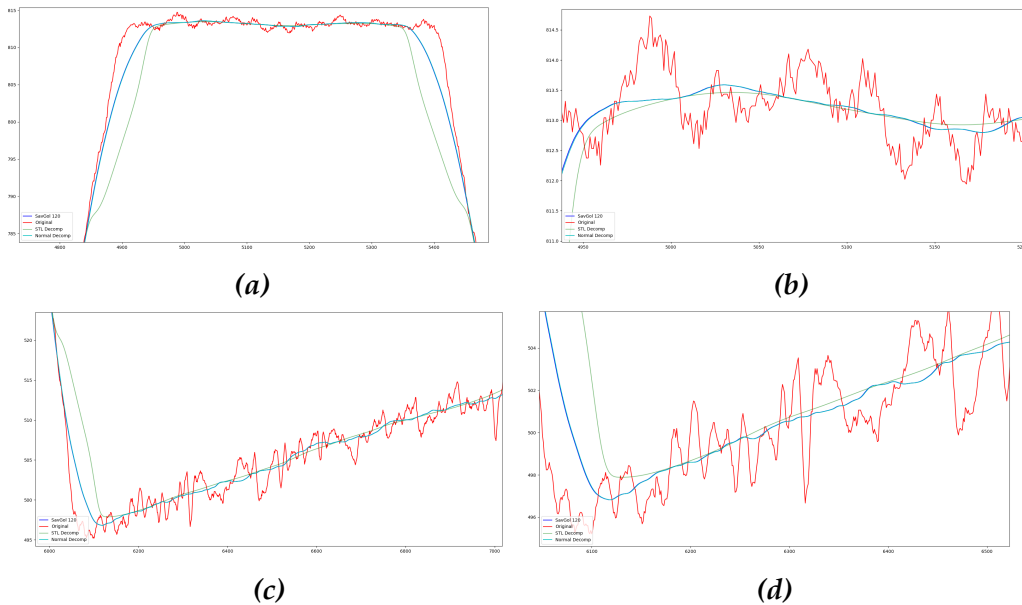


Figure 4.2: Savitzky-Golay filter (blue line) and STL decomposition (green) comparison

1433 The application of the STL decomposition results in a significant im-
 1434 provement in slope calculation even when using low granularity: in Fig-
 1435 ure 4.3 it can be seen that, with the same granularity used for the example
 1436 in Figure 4.1a, the slope values, although with unavoidable fluctuations,
 1437 remain within the same trend, corresponding to the trend of the data curve
 1438 net of the introduced lag caused by the periodicity set for the decomposi-
 1439 tion.

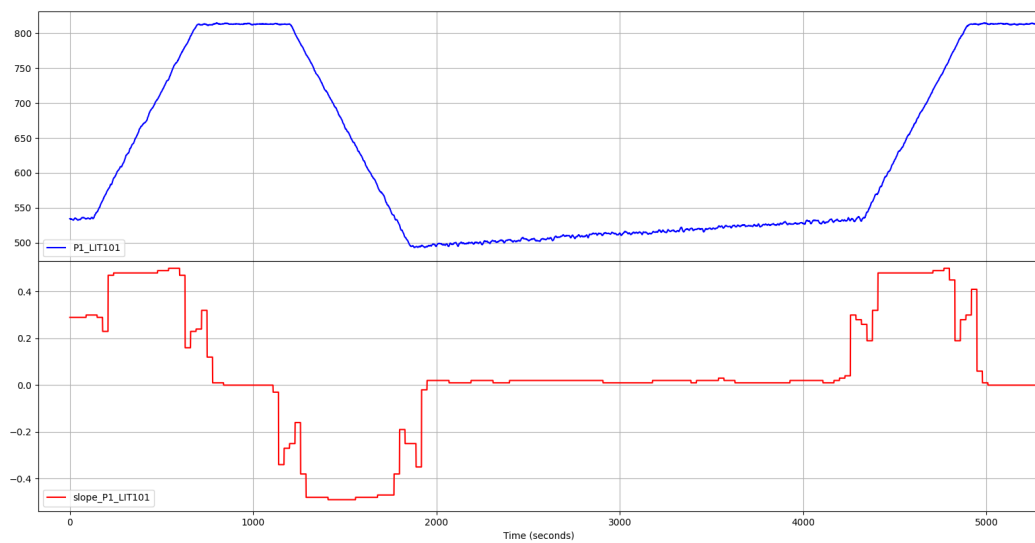


Figure 4.3: Slope after the application of the STL decomposition

1440 This periodicity, which indicates the sampling time window for de-
 1441 composition and thus the level of noise smoothing, can be set in the *con-*
 1442 *fig.ini* configuration file in the *trend_period* directive.

1443 The slope calculation will then be performed on the data from the addi-
 1444 tional measurement trend attributes specified in the *trend_cols_list* di-
 1445 rective in the configuration file, and no longer on the original unfiltered
 1446 data.

1447 Finally, to enable Daikon to correctly interpret the slope data, the deci-
 1448 mal values corresponding to each calculated slope are converted into three
 1449 numerical values -1, 0, and 1, which correspond to the decreasing (if the
 1450 slope is less than zero), stable (if it is equal to zero), and increasing (if it is

greater than zero) trends, respectively. In Figure 4.4, the new slope can be seen, along with the curve obtained from the STL decomposition:

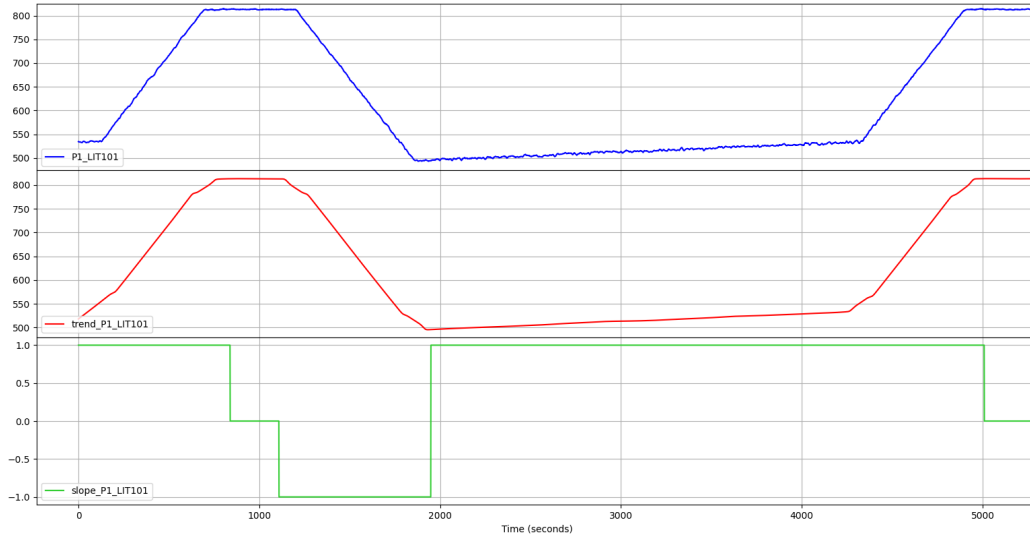


Figure 4.4: The new slope representation (green line) and the smoothed measurement data obtained with the STL decomposition (red)

4.2.1.3 Datasets Merging

In this step the individual datasets are merged, obtaining two new distinct datasets: one without the enrichment and that will be use in the process mining phase, and the other, containing the additional attributes but with the timestamp column removed, intended for inference and invariant analysis.

The first of the two datasets obtained will be saved in CSV format by default in the $\$(\text{project-dir})/\text{process-mining}/\text{data}$ directory while the second one in the $\$(\text{project-dir})/\text{daikon}/\text{Daikon_Invariants}$ directory (both paths are however configurable via *config.ini*).

The dataset name is specified in *config.ini* or via the *-o* command-line option: in the case of the dataset intended for process mining, the script will automatically add a *_TS* suffix to the filename, indicating the fact that the dataset includes the timestamp.

1467 The opportunity for the user to specify a different filename for the output
1468 each time allows the user to save the execution trace of the selected sub-
1469 system without overwriting the previous ones and thus to use all of them
1470 in the subsequent phases of the analysis.

1471 4.2.1.4 Brief Analysis of the Obtained Subsystem

1472 At the end of the datasets merging and saving step, the user is asked
1473 whether to perform a brief optional analysis of the final resulting dataset
1474 to extract preliminary data, with the purpose of obtaining basic informa-
1475 tion about the (sub)system and possibly refining the enrichment.
1476 If the user responds affirmatively to the request, `mergeDatasets.py` launches
1477 within it a further Python script located in the same
1478 `$(project-dir)/pre-processing` directory, called `system_info.py`. This
1479 script, using a combination of Daikon and Pandas analysis, performs a
1480 quick analysis of the dataset contents trying to **recognize**, however roughly,
1481 **the register types**, with possible maximum and minimum values and hard-
1482 coded setpoints. In addition, using the additional attribute `prev_`, it is ca-
1483 pable of deriving measurement values in correspondence with state changes
1484 of individual actuators.
1485 Listing 4.4 shows an example of this brief analysis elated to PLC1 of the
1486 iTrust SWaT system (for brevity, only one measurement is reported in the
1487 analysis of actuator state changes):

```
1488 Do you want to perform a brief analysis of the dataset? [y  
1489 ↪ /n]: y  
1490  
1491 Actuators:  
1492 P1_MV101 [0.0, 1.0, 2.0]  
1493 P1_P101 [1.0, 2.0]  
1494  
1495 Sensors:  
1496 P1_FIT101 {'max_lvl': 2.7, 'min_lvl': 0.0}  
1497 P1_LIT101 {'max_lvl': 815.1, 'min_lvl': 489.6}  
1498  
1499 Hardcoded setpoints or spare actuators:
```

```

1500   P1_P102 [1.0]
1501
1502   Actuator state changes:
1503           P1_LIT101  P1_MV101  prev_P1_MV101
1504   669      800.7170      0          2
1505   1850     499.0203      0          1
1506   4876     800.5992      0          2
1507   6052     498.9026      0          1
1508   9071     800.7170      0          2
1509   10260    499.1381      0          1
1510   13268    801.3058      0          2
1511   14435    498.4315      0          1
1512   17423    801.4628      0          2
1513   18603    498.1567      0          1
1514
1515   P1_LIT101  P1_MV101  prev_P1_MV101
1516   677      805.0741      1          0
1517   4885     805.7414      1          0
1518   9079     805.7806      1          0
1519   13276     805.1133      1          0
1520   17432     804.4068      1          0
1521
1522   P1_LIT101  P1_MV101  prev_P1_MV101
1523   1858     495.4483      2          0
1524   6060     497.9998      2          0
1525   10269     495.9586      2          0
1526   14443     495.8016      2          0
1527   18611     494.5847      2          0
1528
1529           P1_LIT101  P1_P101  prev_P1_P101
1530   118      536.0356      1          2
1531   4322     533.3272      1          2
1532   8537     542.1591      1          2
1533   12721     534.8581      1          2
1534   16883     540.5890      1          2
1535
1536   P1_LIT101  P1_P101  prev_P1_P101
1537   1190     813.0031      2          1
1538   5395     813.0031      2          1

```

```

1539      9597      811.8256      2      1
1540      13776     812.7283      2      1
1541      17938     813.3171      2      1
1542
1543      Actuator state durations:
1544      P1_MV101 == 0.0
1545      9  9  10  9  9  10  9  9  10  9
1546
1547      P1_MV101 == 1.0
1548      1174  1168  1182  1160  1172
1549
1550      P1_MV101 == 2.0
1551      669  3019  3012  3000  2981
1552
1553      P1_P101 == 1.0
1554      1073  1074  1061  1056  1056
1555
1556      P1_P101 == 2.0
1557      118  3133  3143  3125  3108

```

Listing 4.4: Example of preliminar system analysis

From these results we can see that:

- the probable actuators are P1_MV101, which assumes three states identified by the values 0, 1 and 2, and P1_P101, which instead assumes two states identified by the values 1 and 2
- there are two probable measures: P1_FIT101 whose values range from 2.7 to 0.0, and P1_LIT101 whose values range from 815.1 to 489.6. One conjecture could already be made about the topology of the system: P1_LIT101 represents a tank
- apparently there are no related *hardcoded setpoints*, but a probable spare actuator, P1_P102, whose value is always 1. From this data, another conjecture can be made: the value 1 is the close state for that particular type of actuators, while 2 represents the open state
- from the analysis of state changes, in summary, we derive some *relative setpoints*: for example, we know that P1_P101 changes state from

value 1 to value 2 when the level of P1_LIT101 is about 813, while it changes from value 2 to 1 when the level of P1_LIT101 is about 535. We can deduce that P1_P101 is responsible for emptying the tank

- as the last information we have duration of actuator states for each cycle of the system: this information can be useful for making assumptions and conjectures about the behavior of an actuator in a specific state or, by observing the duration values of each cycle, highlighting anomalies in the system.
- In the specific case, the very short duration of P1_MV101 in state 0 is observable: since we are unable, at this preliminary stage, to make assumptions about this, we will try to understand the behavior of the system in this actuator state in the next stages of the analysis

The information obtained here can be used, as mentioned above, to refine the enrichment of the dataset by setting directives in the [DATASET] section of the *config.ini* file, should this be empty or only partially set, or to make the first conjectures about the system, as we have just seen.

The *system_info.py* file can also run in standalone mode if needed: it takes as command-line arguments the dataset to be analyzed, a list of actuators, and a list of sensors. For analysis related to state changes, the dataset must mandatorily be of the enriched type.

4.2.2 Phase 2: Graphs and Statistical Analysis

The new *graph analysis* arises from the need to give the user an overview of the (sub)system obtained in the previous pre-processing phase, identifying more easily the typology of the registers and grasping more effectively the relationships and the dynamics that may exist between the registers controlled by one or more PLCs, confirming the initial conjectures if the brief analysis described in the previous section has been performed, or making new ones thanks to the visual graph support.

In the previous tool, as already pointed out in Section 3.2.7, it is possible to view the chart of one only register at a time: this certainly makes it possible to identify, or at least to hypothesize, the type of that register, but it makes it very complicated to be able to relate it to the other components of the system and thus to derive conjectures about the behavior of the latter, conjectures to be possibly confirmed in the later phases. Hence the need to create a tool that was better than the previous one and that provided more information in an easier way.

The first thing I thought was that an approach similar to Figure 3.5, with all the graphs contained within a single plot, might be the most suitable one: unfortunately, I quickly realized that this solution presented several issues, which are highlighted in figure 4.5.

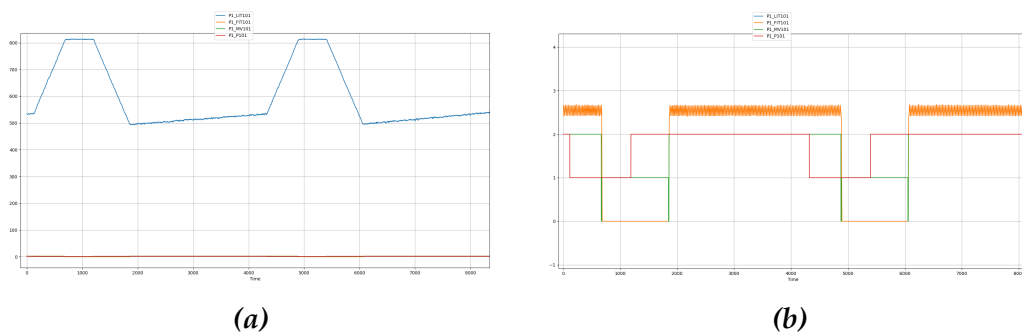
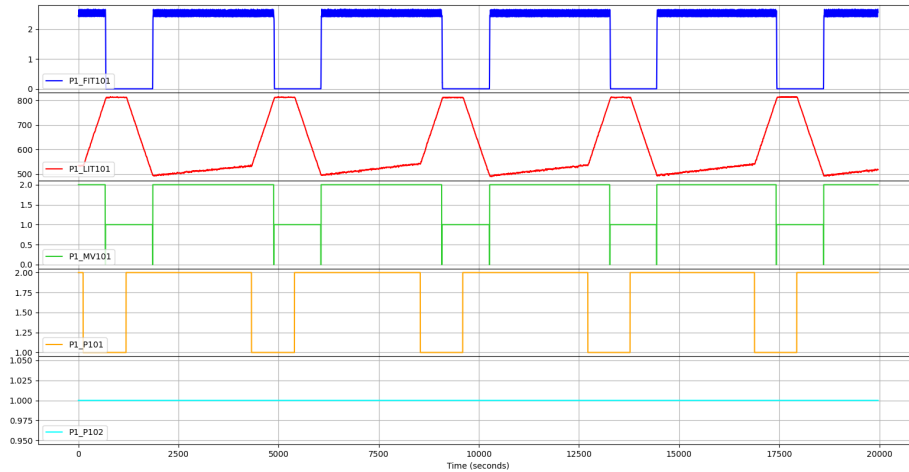


Figure 4.5: Plotting registers on the same y-axis

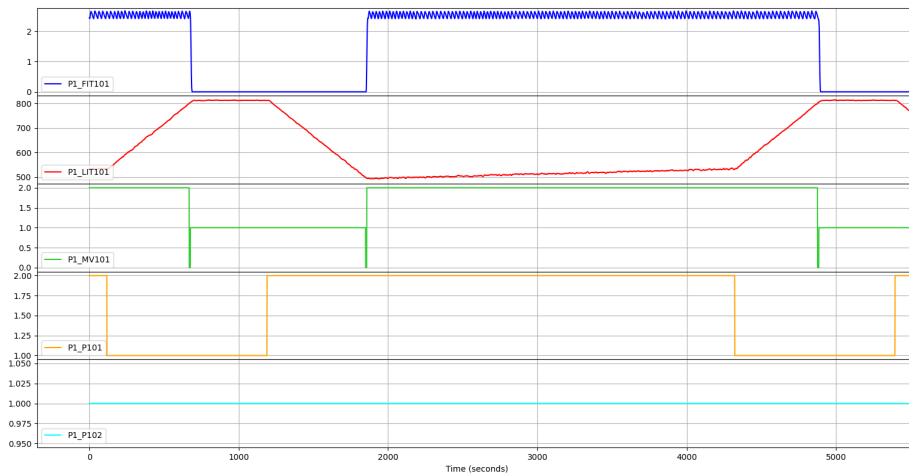
In figure 4.5a it can be seen that the biggest issue is the use of the same y-axis, related to the values of the individual registers, for all charts: if the range between register values is wide, the risk of some charts resembling a single flat line, or at any rate being in fact indistinguishable and very difficult to read immediately; furthermore, as shown in Figure 4.5b, if registers have similar values to each other, the respective graphs may be confusing to each other, making them more difficult to understand.

The solution to this issue is simple and effective: the use of **subplots**. Basically, each register corresponds to a subplot of the graph that shares the time axis (the x-axis) with the other subplots, but keeps the y-axis of

the values of each register independent. This maintains the readability and comprehensibility of the charts, while simultaneously being able to immediately grasp the relationships between them. In addition, by sharing the time axis, it is possible to zoom in on a particular area of one of the charts and automatically the other ones will be zoomed in as well, thus not losing any information and no connection between registers. Figure 4.6 illustrates more clearly what has just been explained: the charts refer to the PLC1 registers of the iTrust SWaT system.



(a) Example of plotting charts of a PLC registers using subplots



(b) Zooming on a particular zone of the charts

Figure 4.6: Example of the new graph analysis

1630 To demonstrate the behavior and effectiveness of the new graph anal-
1631 ysis process, we observe in particular, Figure 4.6b: we can already have
1632 some validation on the conjectures made in the brief analysis from the
1633 previous step:

- 1634 • the chart of P1_FIT101 seems to confirm that this register can be as-
1635 sociated with a **measurement**; moreover, we can see that the trend
1636 of this register is closely related to the periods in which P1_LIT101
1637 has an increasing trend and to the evolution of P1_MV101. Its values,
1638 between about 0 and 2.5, are too narrow to say that this register rep-
1639 represents the tank, and the general trend also leads in that direction:
1640 we can therefore assume that it is a **pressure or flow sensor**
- 1641 • P1_LIT101, because of the above, would therefore seem to **represent**
1642 **a tank**, as already assumed in the brief analysis
- 1643 • P1_MV101 assumes value 2 at the beginning of the ascending trend of
1644 P1_LIT101, while it has value 1 in correspondence with the *plateau*
1645 that is seen when the measurement is about 800 and when the trend
1646 of it is descending. Thus, we can have a confirmation of the ini-
1647 tial conjecture: 1 represents the OFF state of the sensor, 2 the ON
1648 state, and P1_MV101 is the **actuator responsible for the rising level**
1649 of P1_LIT101
- 1650 • in the brief analysis we observed the short duration of P1_MV101 in
1651 state 0, but we were not able to speculate on the reason for this.
1652 Graph analysis shows that P1_MV101 switches and stays in the 0
1653 state acting as a kind of "transient" between states 1 and 2. It can
1654 be assumed that that is the period of time it actually takes for the
1655 actuator to change state
- 1656 • P1_P101 assumes value 2 at the beginning of the descending trend of
1657 P1_LIT101, after the *plateau*, and returns to value 1 at the change of
1658 slope of the (likely) tank increase: taken by itself this fact is not very
1659 clear, so it needs to be compared with P1_LIT101 and P1_MV101 to un-
1660 derstand its behavior: it can be seen that when P1_101 and P1_MV101

are in state 1 the water level remains stable, whereas, when P1_P101 changes to state 2 the level of the measurement drops rapidly; when P1_MV101 then also returns to state 2, the level of the measurement slowly starts rising again and then has a sudden rise at the change of state of P1_P101 from 2 to 1. We can therefore infer that P1_P101 is the **actuator responsible for emptying** the (presumed) tank: state 1 represents the OFF state, while state 2 represents the ON state

- P1_P102 seems to play no role in the system, since its state remains at 1 all the time. It seems improbable that it could be a relative setpoint, so it can be assumed, according to the brief analysis, that it may be a **spare actuator**

As you have probably already noticed, the vast majority of the graphs shown in the previous sections and chapters were generated precisely using the new graph analysis script.

The script that performs the new graph analysis is `runChartsSubPlots.py`, located in the `$(project-dir)/statistical-graphs` directory, which is written in Python and makes use, like the previous one, of the *matplotlib* libraries to generate the graph plots.

The script accepts the following command-line parameters:

- **-f** or **--filename**: specifies the dataset, in CSV format, from which to read the data. The dataset must be located within the directory containing the enriched datasets for the invariant analysis phase. If subsequent parameters are not specified, the script will show all registers in the dataset, except for additional attributes
- **-r** or **--registers**: specifies one or more specific registers to be displayed
- **-a** or **--addregisters**: adds one or more registers to the default visualization. This option is useful in case an additional attribute such as slope is to be analyzed

1690 • **-e** or **--excluderegisters**: excludes one or more specific registers from
1691 the default visualization. This option is useful to avoid displaying
1692 hardcoded setpoints or spare registers

1693 This script, like the previous ones, is designed to provide the maximum
1694 flexibility and ease of use for the user, combined with greater power and
1695 effectiveness in deriving useful information about the analyzed system.

1696 **Statistical Analysis** A quick mention of the statistical analysis part: after
1697 careful evaluation, I decided **not to include this aspect** of the previous
1698 tool within the framework, because I saw no real practical use for it. The
1699 actual statistical information can be easily integrated into the brief analysis
1700 immediately following the pre-processing phase, while the histogram has
1701 relative utility and, in my opinion, is outdated by the new graph analysis
1702 I implemented.

1703 However, the Python `histPlots_Stats.py` script remains in the directory,
1704 essentially unchanged from the one developed by Ceccato et al., in case
1705 future use is needed.

1706 4.2.3 Phase 3: Invariant Inference and Analysis

1707 The phase of invariant inference and analysis has undergone a redesign
1708 and improvement to offer the user a more comprehensive and effortless
1709 approach to identify invariants. This has been achieved through the ap-
1710 plication of new criteria to analyze and reorganize the Daikon analysis
1711 results. The outcome of this is a more compact presentation of informa-
1712 tion that highlights the possible relationships among invariants.

1713 The new design not only enables the identification of undiscovered aspects
1714 of the system behavior but also confirms the hypotheses made during the
1715 earlier stages of analysis. This step is now semi-automated, unlike before,
1716 and allows for the analysis of invariants on individual actuator states and
1717 their combinations.

4.2.3.1 Revised Daikon Output

To streamline the process of identifying invariants quickly and efficiently, it is necessary to revise the output generated by standard Daikon analysis. The goal is to create a more compact and readable format for the output.

The current Daikon results consist of three sections:

1. the first section containing generic invariants, i.e., valid regardless of whether a condition is specified for the analysis
2. the second section containing invariants obtained by specifying a condition for the analysis in the *.spinfo* file
3. a third section containing the invariants that are obtained from the negations of the condition possibly specified in the *.spinfo* file

In each section only a single invariant per row is shown, without relating it in any way to the others: this makes it difficult to identify significant invariants and any invariant chains that might provide much more information about the behavior of the system than the single invariant.

A brief example of the structure and format of this output related to PLC1 of the iTrust SWaT system is shown in Listing 4.5, where a condition was specified on the measurement P1_LIT101 and on actuator P1_MV101:

```

aprogram.point:::POINT
P1_P102 == prev_P1_P102
P1_FIT101 >= 0.0
P1_MV101 one of { 0.0, 1.0, 2.0 }
P1_P101 one of { 1.0, 2.0 }
P1_P102 == 1.0
max_P1_LIT101 == 816.0
min_P1_LIT101 == 489.0
slope_P1_LIT101 one of { -1.0, 0.0, 1.0 }
[...]
P1_LIT101 > P1_MV101
P1_LIT101 > P1_P101

```

```

1750     P1_LIT101 > P1_P102
1751     P1_LIT101 < max_P1_LIT101
1752     P1_LIT101 > min_P1_LIT101
1753     [...]
1754     P1_MV101 < min_P1_LIT101
1755     P1_MV101 < trend_P1_LIT101
1756     P1_P101 >= P1_P102
1757     P1_P101 < max_P1_LIT101
1758     [...]
1759     =====
1760     aprogram.point:::POINT;condition="P1_MV101 == 2.0 &&
1761     ↪ P1_LIT101 < max_P1_LIT101 - 16 && P1_LIT101 >
1762     ↪ min_P1_LIT101 + 15"
1763     P1_MV101 == prev_P1_MV101
1764     P1_P102 == slope_P1_LIT101
1765     P1_MV101 == 2.0
1766     P1_FIT101 > P1_MV101
1767     P1_FIT101 > P1_P101
1768     P1_FIT101 > P1_P102
1769     P1_FIT101 > prev_P1_P101
1770     P1_MV101 >= P1_P101
1771     P1_MV101 >= prev_P1_P101
1772     P1_P101 <= prev_P1_P101
1773     =====
1774     aprogram.point:::POINT;condition="not(P1_MV101 == 2.0 &&
1775     ↪ P1_LIT101 < max_P1_LIT101 - 16 && P1_LIT101 >
1776     ↪ min_P1_LIT101 + 15)"
1777     P1_P101 >= prev_P1_P101
1778     Exiting Daikon.

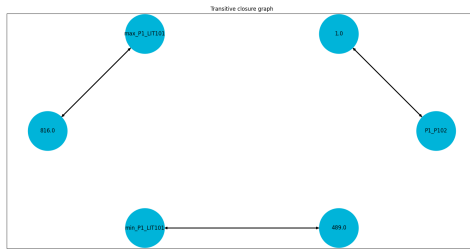
```

Listing 4.5: Standard Daikon output for PLC1 of the iTrust SWaT system

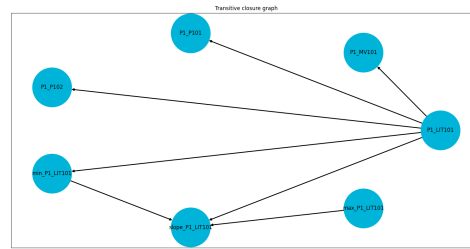
In the framework I am presenting, this output is reduced to two sections, the general one and the related to the user-specified condition, eliminating the one related to the negated condition because it is not useful in this context and a source of potential misinterpretation; moreover, the relationships between invariants will be highlighted instead by using **transitive closures**: transitive closure of a relation R is another relation, typically denoted R^+ that adds to R all those elements that, while not necessarily

related directly to each other, can be reached by a *chain* of elements related to each other. In other words, the transitive closure of R is the smallest (in set theory sense) transitive relation R such that $R \subset R^+$ [52].

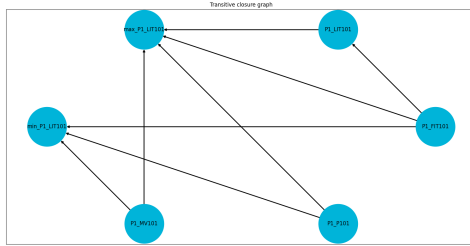
To implement the transitive closure of the invariants generated by Daikon, I first divided the invariants in each section by type according to their equivalence relation, not considering all those invariants that refer to additional attributes except for the slope, and for each of them I generated a **graph** using the NetworkX libraries, connecting with an arc the registers (represented by nodes) that have a common endpoint in the invariant through the transitive property. To reconstruct the individual invariant chains, then, I used a simple *Depth-first Search* (DFS) on each of the graphs, thus obtaining the desired outcome. Figure 4.7 shows some examples of these graphs:



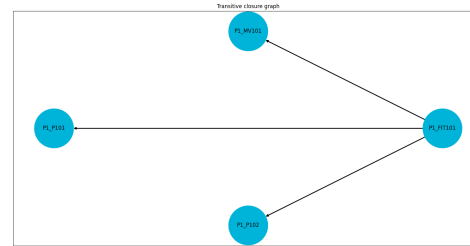
(a) Transitive closure graph for "="



(b) Transitive closure graph for ">"



(c) Transitive closure graph for "<"



(d) Transitive closure graph for ">" cond.

Figure 4.7: Example of transitive closure graphs for invariants in PLC1 of iTrust SWaT system

At the end of this process, still applied to PLC1 of the iTrust SWaT system and with the same analysis condition, we get the following complete output:

```

1802 1  =====
1803 2  Generic
1804 3  =====
1805 4  P1_MV101 one of { 0.0, 1.0, 2.0 }
1806 5  P1_P101 one of { 1.0, 2.0 }
1807 6  slope_P1_LIT101 one of { -1.0, 0.0, 1.0 }
1808 7  P1_FIT101 != P1_P101, P1_P102
1809 8  P1_P102 == 1.0
1810 9  max_P1_LIT101 == 816.0
1811 10 min_P1_LIT101 == 489.0
1812 11 P1_LIT101 > P1_MV101
1813 12 P1_LIT101 > P1_P101
1814 13 P1_LIT101 > P1_P102
1815 14 P1_LIT101 > min_P1_LIT101 > slope_P1_LIT101
1816 15 P1_FIT101 >= 0.0
1817 16 P1_P101 >= P1_P102 >= slope_P1_LIT101
1818 17
1819 18 =====
1820 19 P1_MV101 == 2.0 && P1_LIT101 < max_P1_LIT101 - 16 &&
1821    ↪ P1_LIT101 > min_P1_LIT101 + 15
1822 20 =====
1823 21 slope_P1_LIT101 == P1_P102
1824 22 P1_MV101 == 2.0
1825 23 P1_FIT101 > P1_MV101
1826 24 P1_FIT101 > P1_P101
1827 25 P1_FIT101 > P1_P102
1828 26 P1_MV101 >= P1_P101

```

Listing 4.6: Revised Daikon output with transitive closures for PLC1 of the iTrust SWaT system

Transitive closures can be appreciated in lines 7, 14 and 16 of Listing 4.6. In general, the output has been reduced in the number of effective rows (19 versus the 61 in the output of Listing 4.5, making it certainly better to read and identify significant invariants) and the invariant chains make it more immediate to grasp the relationships between registers.

4.2.3.2 Types of Analysis

Compared to Ceccato et al.'s solution, in which individual analyses are performed manually, my proposal is to implement two types of semi-automated analysis: the first performs an analysis of all states for each individual register, while the second performs the analysis on the current system configuration based on the actual states of the actuators.

Both analyses refer to a specific measurement, selected by the user.

These two types of analysis will be handled by the Python script `daikonAnalysis.py`, contained in the default directory `$(project_dir)/daikon`. The script accepts the following command-line arguments:

- **-f** or **--filename**: specifies the enriched dataset, in CSV format, from which to read the data. The dataset must be located within the directory containing the enriched datasets specified in the `config.ini` file (by default `$(project_dir)/daikon/Daikon_Invariants`).
- **-s** or **--simpleanalysis**: performs the analysis on the states of individual actuators
- **-c** or **--customanalysis**: performs the analysis on combinations of actual states of the actuators
- **-u** or **--uppermargin**: defines a percentage margin on the maximum value of the measurement
- **-l** or **--lowermargin**: defines a percentage margin on the minimum value of the measurement

One or both types of analysis can be selected. The last two parameters set a condition on the value of the measurement that is meant to bypass the transient periods between the actuator state change and the actual trend change at the maximum and minimum values: this expedient is especially useful for the first type of analysis, allowing for generally more accurate data on measurement trends.

1862 **Analysis on single actuator states** Analysis on the states of individual
 1863 actuators is the simplest: after the user is prompted to input the measure-
 1864 ment, chosen from a list of likely available measurements, the script rec-
 1865 ognizes the likely actuators and the relative states of each, using the same
 1866 mixed Daikon/Pandas technique adopted in the brief analysis during the
 1867 pre-processing phase.
 1868 For each actuator and each state it assumes, a single Daikon analysis is
 1869 performed, eventually placing the condition on the maximum and mini-
 1870 mum level of the measurement.
 1871 The result of these analyses are saved in the form of text files in a directory
 1872 having the name corresponding to the analyzed actuator and contained in
 1873 the default parent directory $\$(project_dir)/daikon/Daikon_Invariants/results$:
 1874 each file generated by the analysis is identified by the name of the actuator,
 1875 the state and the condition, if any, on the measurement (see Figure 4.8).

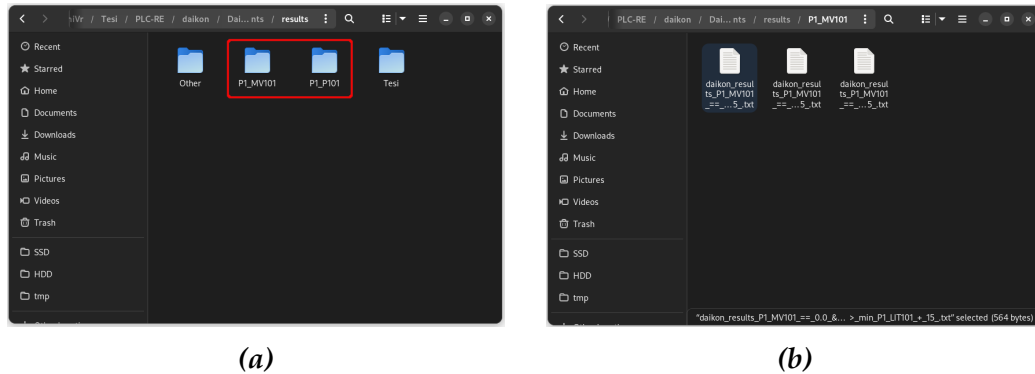


Figure 4.8: Directory (a) and outcome files (b) for the single actuator states analysis

1876 An example of the outcome of this analysis is Listing 4.6, where the
 1877 actuator analyzed is P1_MV101 in state 2: from the generic invariants we
 1878 can observe that P1_P101 is a likely actuator (line 5), assuming binary val-
 1879 ues; from line 8, however, we note that P1_P102 is permanently equal to 1,
 1880 so it can be confirmed that it is a spare actuator rather than a setpoint;
 1881 furthermore, lines 9 and 10 show the maximum and minimum values
 1882 reached by P1_LIT101, which we have assumed to be the register con-
 1883 nected to the tank. The most interesting information, however, comes

from the condition-generated invariants: at line 21 we notice that the slope of P1_LIT101 is 1 (thus increasing) when P1_MV101 is set to 2: this confirms what we assumed in the previous steps, namely, that P1_MV101 represents the ON state of the actuator and is responsible for filling the tank P1_LIT101; moreover, at line 23 we see that P1_FIT101 is greater than P1_MV101: this means that when the actuator assumes the value 2 the sensor P1_FIT101 detects data (in contrast, if P1_MV101 is 1 P1_FIT101 is 0, detecting nothing), confirming the original hypothesis made that this may be a pressure or flow sensor.

Analysis of the Current System Configuration The analysis of the current system configuration based on the actual states of the actuators is more complex, but at the same time offers more interesting outcomes as it provides better evidence of actuator behavior in relation to the selected measurement.

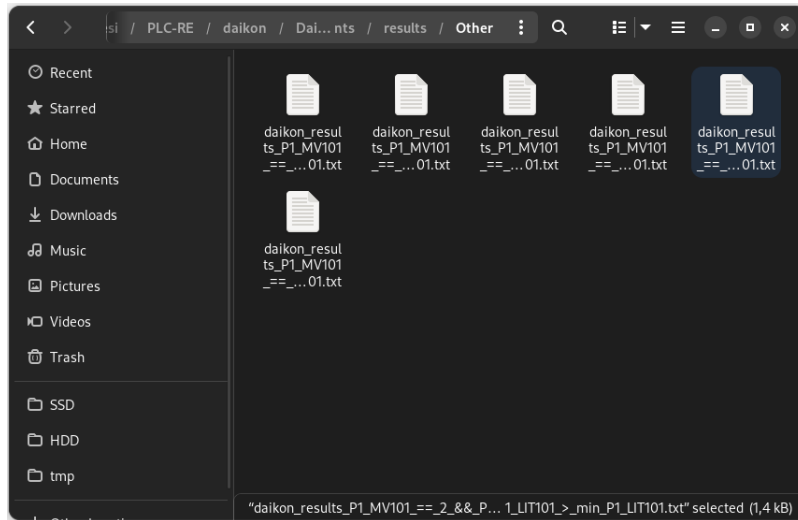


Figure 4.9: Daikon outcome files for system configuration analysis. Each file represents a single system state

For this analysis, the script automatically recognizes the actual configurations of the actuators (e.g., P1_MV101 == 2, P1_P101 == 1) that represent a system state, and for each of these configurations Daikon analysis is automatically run, after prompting the user for the measurement and

eventually the actuators whose configurations are to be studied (If the user does not select any actuators, all those previously detected by the Python script will be considered): the analysis outcomes are saved, still in the text format, within a specific directory under the same parent directory of the previous type of analysis and, as before, their name is characterized by the rule used for the analysis (see Figure 4.9).

1908

1909 An example of the obtained outcomes can be seen in Listing 4.7:

```

1910 1  =====
1911 2  Generic
1912 3  =====
1913 4  P1_MV101 <= P1_P101 ==> P1_FIT101 >= 0.0
1914 5  P1_MV101 <= P1_P101 ==> P1_MV101 one of { 0.0, 1.0, 2.0
1915 6  ↪ }
1916 7  P1_MV101 <= P1_P101 ==> P1_P101 one of { 1.0, 2.0 }
1917 8  P1_MV101 <= P1_P101 ==> slope_P1_LIT101 one of { -1.0,
1918 9  ↪ 0.0, 1.0 }
1919 10 P1_MV101 > P1_P101 ==> P1_FIT101 > P1_MV101
1920 11 P1_MV101 > P1_P101 ==> P1_FIT101 > P1_P101
1921 12 P1_MV101 > P1_P101 ==> P1_FIT101 > P1_P102
1922 13 P1_MV101 > P1_P101 ==> P1_FIT101 > slope_P1_LIT101
1923 14 P1_MV101 > P1_P101 ==> P1_MV101 == 2.0
1924 15 P1_MV101 > P1_P101 ==> P1_MV101 > P1_P102
1925 16 P1_MV101 > P1_P101 ==> P1_MV101 > slope_P1_LIT101
1926 17 P1_MV101 > P1_P101 ==> P1_P101 == 1.0
1927 18 P1_MV101 > P1_P101 ==> P1_P101 == P1_P102
1928 19 P1_MV101 > P1_P101 ==> P1_P101 == slope_P1_LIT101
1929 20 P1_MV101 > P1_P101 ==> slope_P1_LIT101 == 1.0
1930 21 [...]
1931 22
1932 23 =====
1933 24 P1_MV101 == 2 && P1_P101 == 1 && P1_LIT101 < max_P1_LIT101
1934 25 ↪ && P1_LIT101 > min_P1_LIT101
1935 26 =====
1936 27 slope_P1_LIT101 == P1_P102 == P1_P101 == 1.0
1937 28 P1_MV101 == 2.0
1938 29 P1_FIT101 > P1_MV101

```

```
1939 27 P1_FIT101 > P1_P101
```

Listing 4.7: Daikon outcomes for the system configuration $P1_MV101 == 2$, $P1_P101 == 1$ on $P1_LIT101$

1940 Compared to Listing 4.6, this time we can observe in the general invari-
 1941 ants section the presence of implications, which were previously absent
 1942 (the remaining generic invariants have been omitted for reasons of space).
 1943 Such implications can provide very useful information, as in this case: for
 1944 example, the invariant on line 18 tells us that if the value of $P1_MV101$ is
 1945 greater than that of $P1_P101$ then the value of the slope is 1, that is, the
 1946 tank level is increasing. Consequently, we have further confirmation that
 1947 the state $P1_MV101 == 2$ is the ON state for that actuator and that it is the
 1948 actuator responsible for filling the tank $P1_LIT101$. Comparing the other
 1949 analysis outcomes, we will discover that $P1_P101$ is instead responsible
 1950 for emptying the tank and that its ON and OFF states are 2 and 1, respec-
 1951 tively.

1952 In addition, the invariant at line 8 also indicates that when the actuator
 1953 $P1_MV101$ is in state 2 and $P1_P101$ is in state 1 then the value of $P1_FIT101$
 1954 is greater than 2: consequently, it follows that the corresponding sensor is
 1955 measuring something relative to the tank $P1_LIT101$.

1956 The above is confirmed by the invariants related to the analysis condition:
 1957 at line 24 we have that the slope is indeed equal to 1 (thus increasing) and
 1958 that $P1_FIT101$, at line 26, takes values greater than 2 when $P1_MV101$ is
 1959 equal to 2.

1960 **Refining the Analysis** In some cases, it may happen that the outcomes
 1961 provided by the semi-automated analyses are not satisfactory to the user
 1962 (e.g., the value of the slope may not emerge clearly) or simply the user
 1963 wants to investigate a particular aspect of the system in more detail by
 1964 trying to discover additional invariants that did not emerge previously: in
 1965 this case, it is possible to run a new and more specific invariant analysis
 1966 using the Python script `runDaikon.py`, which allows for more punctual
 1967 analyses of the system.

The script, also contained in the default directory `$(project_dir)/daikon`, accepts three command-line parameters:

- **-f** or **--filename**: specifies the enriched dataset, in CSV format, from which to read the data. Even in this case, the dataset must be located within the directory containing the enriched datasets
- **-c** or **--condition**: specifies the condition for the analysis, which will be automatically overwritten in the *.spinfo* file. It is possible to specify more than one condition, but it is recommended to use the logical operator `&&`
- **-r** or **--register**: specifies the directory where to save the text file with the outcomes

Performing this single analysis will produce a single output file containing the invariants discovered, file that will be saved in the directory specified by the user via the `-r` command-line option (by default the file will be saved in the directory `$(project_dir)/daikon/Daikon_Invariants/results`) to be examined later by the user.

In conclusion, the two types of analysis presented, along with the possibility of allowing for more refined analysis at a later date and Daikon's redefined output, make this stage much more complete, clear, and powerful than before

4.2.4 Phase 4: Business Process Analysis

Chapter 5

Case study: the iTrust SWaT System

HAVING introduced the innovative framework and highlighted its potential in the preceding chapter, we now turn our attention to the case study where we will apply this framework. As previously mentioned in Chapter 4 and demonstrated through various examples in the same chapter, our focus will be on the **iTrust SWaT system** [29], developed by the iTrust – Center for Research in Cyber Security of University of Singapore for Technology and Design [24]. The acronym SWaT represents *Secure Water Treatment*.

The iTrust SWaT system is a testbed that replicates on a small scale a real water treatment plant arises to support research in the area of cyber security of industrial control systems and has been operational since March 2015: it is still being used by students at the University of Singapore for educational and training purposes and is available to organizations to train their operators on cyber physical incidents.

5.1 Architecture

In contrast to the virtualized testbed discussed in Section 3.2.1 by Cecato et al., the iTrust SWaT system is composed entirely of physical hardware components. It encompasses various elements, starting from field

2007 devices and extending to PLCs, HMI, SCADA workstations, and the SCADA
2008 server (also referred to as the *historian*). The historian is responsible for
2009 recording data from field devices for further analysis. In the upcoming
2010 sections, we will delve deeper into the architecture of the physical process
2011 and the communication network.

2012 5.1.1 Physical Process

2013 The physical process of the SWaT consists of six stages, denoted P1
2014 through P6. These stages are [53][54]:

- 2015 1. **taking in raw water:** feeds unfiltered water into the system
- 2016 2. **chemical dosing:** adds chemicals to water useful for initial pretreat-
2017 ment
- 2018 3. **Ultra Filtration (UF) system:** the water is filtered through a semi-
2019 permeable membrane (ultrafiltration membrane) using the liquid pres-
2020 sure, effectively capturing impurities and suspended solids, as well
2021 as removing bacteria, viruses, and other pathogens present in the
2022 water.
- 2023 4. **dechlorination:** removes residual chlorine from disinfected water
2024 using ultraviolet lamps
- 2025 5. **Reverse Osmosis (RO):** performs further filtration of the water
- 2026 6. **backwash process:** cleans the membranes in UF using the water pro-
2027 duced by RO

2028 Figure 5.1 shows a graphical representation of the architecture and the six
2029 stages of the SWaT system.

2030 The SWaT system incorporates an array of sensors that play a crucial
2031 role in monitoring the system's operations and ensuring their safe. These
2032 sensors are responsible for continuously collecting data and providing
2033 valuable insights into the functioning of the system. These sensors are:

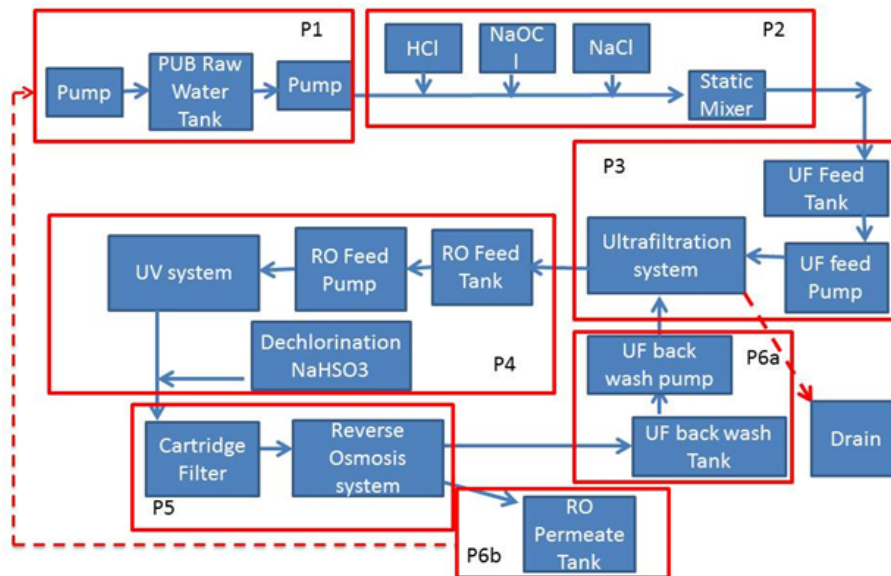


Figure 5.1: SWaT architecture

- Level Indication Transmitter (measured in mm)
- Flow Indication Transmitter (m³/hr)
- Analyser Indicator Transmitter
 - o Conductivity (μS/cm)
 - o pH
 - o Oxidation Reduction Potential (mV)
- Differential Pressure Indicator Transmitter (kPa)
- Pressure Indicator Transmitter (kPa)

The sensors and actuators associated with each PLC are shown in Figure 5.2.

Sensors and actuators are mapped to tags by the communication protocol used (see 5.1.2): a tag can be addressed via string descriptor defined by the system designer (e.g. MV101, to indicate motorized valve number 1 at stage 1) or by referring directly to the analog/digital pins of the PLC I/O unit [54].

Raw Water	Pre-Treatment	Ultra-Filtration	De-Chlorination	Reverse Osmosis	RO Product
P-101 Stopped	P-201 Stopped	P-301 Stopped	P-401 Stopped	P-501 Stopped	P-601 Stopped
P-102 Stopped	P-202 Stopped	P-302 Stopped	P-402 Stopped	P-502 Stopped	P-602 Stopped
MV-101 Closed	P-203 Stopped	MV-301 Closed	P-403 Stopped	MV-501 Closed	P-603 Stopped
LIT-101 520 mm	P-204 Stopped	MV-302 Closed	P-404 Stopped	MV-502 Closed	LS-601 Normal
FIT-101 0.00 m³/h LL	P-205 Stopped	MV-303 Closed	UV-401 Stopped	MV-503 Closed	LS-602 HIGH
FIT-201 0.00 m³/h LL	P-206 Stopped	MV-304 Closed	LS-401 Normal	MV-504 Closed	LS-603 LOW
	P-207 Stopped	PSH-301 Normal	LIT-401 1008 mm H	PSL-501 Normal	FIT-601 0.00 m³/h LL
	P-208 Stopped	DPSH-301 Normal	FIT-401 0.00 m³/h LL	PSH-501 Normal	
	MV-201 Closed	LIT-301 1012 mm H	AIT-401 0.17 ppm	AIT-501 6.89	
	LS-201 Normal	FIT-301 0.00 m³/h	AIT-402 275.70 mV	AIT-502 204.20 mV	
	LS-202 Normal	DPIT-301 0.95 kPa LL		AIT-503 264.23 µS/cm H	
	LS-203 Normal			AIT-504 14.27 µS/cm H	
	AIT-201 142.18 µS/cm L			FIT-501 0.00 m³/h L	
	AIT-202 7.20 H			FIT-502 0.00 m³/h HH	
	AIT-203 293.59 mV L			FIT-503 0.00 m³/h HH	
				FIT-504 0.00 m³/h LL	
				PIT-501 2.64 kPa LL	
				PIT-502 0.00 kPa H	
				PIT-503 0.00 kPa	

Figure 5.2: Sensors and actuators associated with each PLC

2049 5.1.2 Control and Communication Network

2050 The SWaT system’s network architecture follows the principles of lay-
2051 ering and zoning, which enable segmentation and control of traffic within
2052 the network.

2053

2054 Five layers are present starting from the highest to the lowest:

- 2055 • Layer 3.5 – Demilitarised Zone (DMZ)
- 2056 • Layer 3 – Operation Management (Historian)
- 2057 • Layer 2 – Supervisory Control (Touch Panel, Engineering Worksta-
2058 tion, HMI Control Clients)
- 2059 • Layer 1 – Plant Control Network (PLCs) (Star Network)
- 2060 • Layer 0 – Process (Actuator/Sensors and Input/output modules)
2061 (Ring Network)

2062 PLCs at Layer 1 communicate with their respective sensors and actuators
2063 at Layer 0 through a conventional ring network topology based on Eth-
2064 erNet/IP, to ensure that the system can tolerate the loss of a single link

without any adverse impact on data or control functionality.

PLCs between the different process stages at Layer 1 communicate with each other through a star network topology using the CIP protocol on Ethernet/IP, previously discussed in Section 2.3.1.3.

Regarding zoning, the SWaT system is divided into three zones, each containing one or more layers. These zones are, in descending order of security level:

- **Plant Control Network, or Control System:** includes layers from 0 to 2
- **DMZ:** includes Layer 3.5
- **Plant Network:** includes Layer 3

Figure 5.3 provides a clearer visualization of the zoning and layer division within the network architecture of the SWaT system. This diagram highlights the distinct zones and their corresponding layers, offering a comprehensive overview of the system's network structure.

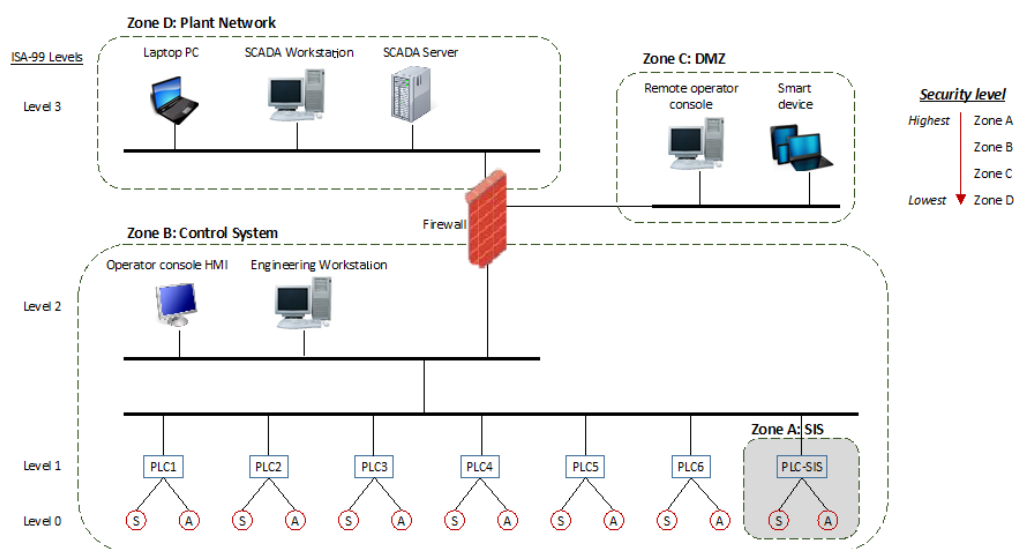


Figure 5.3: SWaT network architecture

A specific IP address is associated with each device: in Table 5.1 we report the addresses for the PLCs, historian, and Touch Panel in the *Plant Control Network* (PCN) zone:

IP Address	Device
192.168.1.10	PLC1
192.168.1.20	PLC2
192.168.1.30	PLC3
192.168.1.40	PLC4
192.168.1.50	PLC5
192.168.1.60	PLC6
192.168.1.100	Touch Panel (PCN)
192.168.1.200	Historian Server

Table 5.1: Main IP addresses of the six PLCs and SCADA in SWaT

5.2 Datasets

To facilitate the study and testing of technologies related to cyber security in Industrial Control Systems and critical infrastructure, iTrust offers researchers worldwide the opportunity to access a range of datasets [55]. These datasets consist of a collection of data obtained from the SWaT system, encompassing information on both the physical processes and network communications. The data is organized into different years, and researchers can request access to these datasets for their analysis and experimentation purposes.

Physical Process Datasets The datasets containing information about the physical processes are provided in CSV format files. These files encompass data collected during different time intervals, which can vary from a few hours to entire days. The granularity of the data is typically at a one-second interval, although there may be some exceptions. The collected data primarily consists of timestamped sensor measurements and

actuator status values for each PLC, describing the physical properties of the testbed in operational mode.

Network Communications Datasets Network communications are typically available in the form of *Packet Capture* format (PCAP) files. These files contain captures of communication network traffic, allowing researchers to analyze and examine the network interactions. In some instances, CSV files are provided instead of PCAP files, featuring different characteristics for the collected data.

5.2.1 Our Case Study: the 2015 Dataset

The dataset selected as a case study to apply the framework discussed in the previous chapter is specifically the dataset from the year 2015 [56]. The main reason for this choice is the unique characteristics found in the physical process dataset that are not present in datasets from subsequent years.

Physical Process Data The data collection process lasted 11 consecutive days, 24 hours per day. During the first 7 days, the system operated normally without any recorded attacks. However, attacks were observed during the remaining 4 days. The collected data reflects the impact of these attacks, leading to the creation of two separate CSV files: one containing the recorded data of SWaT during the system's regular operations, and the other containing data recorded during the days of the attacks. To ensure accurate information about the system, the dataset pertaining to the normal operations, which spans seven days, was chosen for analysis.

Data collection occurs at a frequency of one data point per second, with the assumption that significant attacks cannot occur within a shorter time frame. Additionally, the firmware of the PLCs remains unchanged throughout the data collection period.

At the beginning of data gathering the tanks are empty and the system must be initialized in order to then reach full operation: it typically takes

2127 around five hours for all tanks to be fully filled and for the system to sta-
2128 bilize and reach the appropriate operational state (see Figure 5.4).

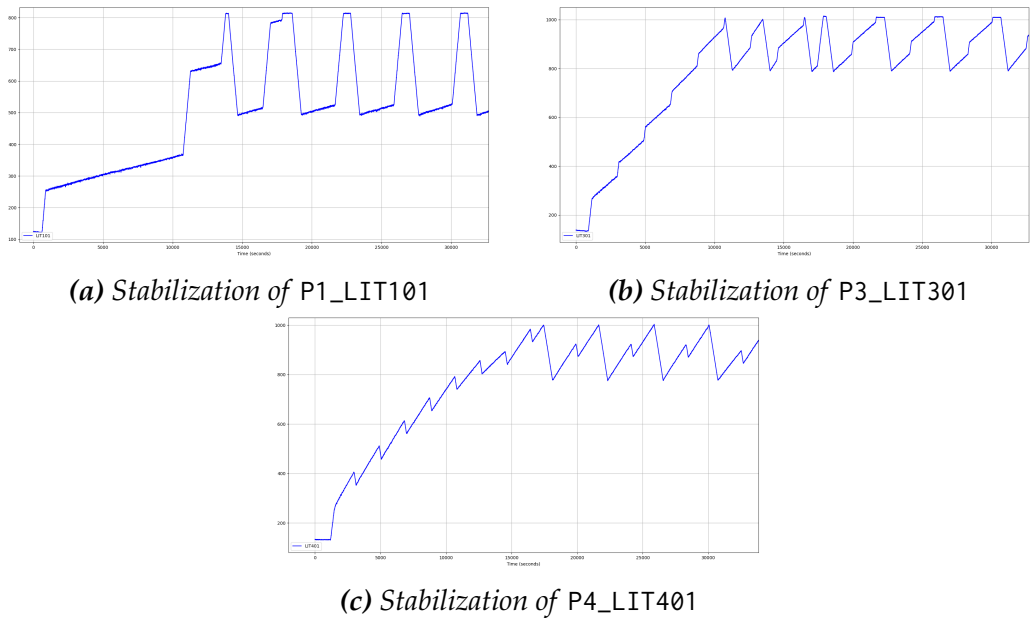


Figure 5.4: SWaT stabilization

2129 In total, the dataset consists of thousand and thousand of samples re-
2130 lated to 51 attributes.

2131 **Network Traffic** The network traffic was collected using an appliance
2132 from a well-known network hardware manufacturer and was made avail-
2133 able only in CSV format and not PCAP format. Table 5.2 shows some of
2134 the main data captured:

Category	Description
Date	Date of Log
Time	Time of Log
Origin	IP of server
Source IP	IP address of source
Destination IP	IP address of destination
Protocol	Network protocol

Application Name	Name of application
Modbus Function Code	Function Code
Modbus Function Description	Description of function
Modbus Transaction ID	Transaction ID
SCADA Tag	Sensor or actuator ID
Modbus Value	Value transmitted
Service / Destination Port	Port number of destination IP
Source Port	Port number of source IP

Table 5.2: SWaT network traffic data

Unfortunately, the data provided are partial as it only includes readings from sensors and does not include information on actuator status.

Do not mislead by the word *Modbus* in the captured data fields: this is most likely a feature of the sniffing appliance, which may have encapsulated EtherNet/IP-CIP protocol packets in Modbus frames, as described by T. A. Snide in [57].

To provide evidence that the protocol being used is CIP over EtherNet/IP, we can examine the "Source / Destination port" field in the captured data. The presence of TCP port 44818 as the destination port aligns with the TCP port used for transporting **explicit messages** in the EtherNet/IP protocol, as explained in Section 2.3.1.2. Additionally, the "Application name", "Modbus Function Code" and "Modbus Function Description" fields further support this conclusion. The "Application name" explicitly states "CIP_read_tag_service," while the "Modbus Function Code" field contains a decimal value of 76, which does not correspond to any known Modbus Function Calls. When converted to hexadecimal, this value is 4C, matching the CIP protocol read tag request code as indicated in the "Modbus Function Description" field.

In summary, the datasets for subsequent years were not selected due to certain limitations. In the case of the year 2017, the physical system

2156 data had a wide granularity, resulting in significant information loss. Ad-
2157 ditionally, in some cases, the datasets were considered "spurious" as there
2158 was no clear differentiation between data obtained during normal SWaT
2159 operations and data associated with attacks.

2160 Regarding network traffic data, there were instances where the data was
2161 either missing or fragmented into large PCAP files weighing several gi-
2162 gabytes (more than 6 GB each!), despite containing only a few minutes'
2163 worth of data. This made it impractical to manage such files given the
2164 available resources.

2165 Despite their large quantity, the CSV files associated with network traffic
2166 for the year 2015 are comparatively smaller in size, just slightly over 100
2167 MB each. These files cover a more extensive time period, which facilitates
2168 easier management and analysis. Prioritizing the physical process dataset
2169 as crucial, I have selected the year 2015 as a case study, even though the
2170 network data may be incomplete.

Chapter **6**

Our framework at work: reverse engineering of
the SWaT system

6.1 Pre-processing

6.2 Graph Analysis

6.2.1 Conjectures About the System

6.3 Invariants Analysis

6.3.1 Actuators Detection

6.3.2 Daikon Analysis and Results Comparing

6.4 Extra information on the Physics

6.5 Business Process Analysis

Chapter **7**

Conclusions

7.1 Discussions

7.2 Guidelines

7.3 Future work

List of Figures

2.1	SCADA architecture schema	6
2.2	PLC architecture	8
2.3	PLC communication schema	9
2.4	Comparison between ST language and Ladder Logic	10
2.5	Modbus Request/Response schema	14
2.6	Modbus RTU frame and Modbus TCP frame	15
2.7	Example of packet sniffing on the Modbus protocol	17
2.8	OSI model for EtherNet/IP stack	18
3.1	Overview	25
3.2	The simplified SWaT system used for running Ceccato et al. methodology	26
3.3	Output graphs from graph analysis	31
3.4	An example of Disco generated activity diagram for PLC2 .	34
3.5	Execution traces of InputRegisters_IW0 on the three PLCs .	36
3.6	Business process with states and Modbus commands for the three PLCs	38
3.7	Water physics compared: simulated physics in the Simulink model (a) and physics in a real system (iTrust SWaT) (b). Fluctuations in the tank level in (b), almost completely ab- sent in (a), can be appreciated.	44
3.8	Example of Daikon's output	48

4.1	Slope comparison with granularity 30 (a), 60 (b) and 120 seconds (c)	64
4.2	Savitzky-Golay filter (blue line) and STL decomposition (green) comparison	65
4.3	Slope after the application of the STL decomposition	66
4.4	The new slope representation (green line) and the smoothed measurement data obtained with the STL decomposition (red)	67
4.5	Plotting registers on the same y-axis	72
4.6	Example of the new graph analysis	73
4.7	Example of transitive closure graphs for invariants in PLC1 of iTrust SWaT system	79
4.8	Directory (a) and outcome files (b) for the single actuator states analysis	82
4.9	Daikon outcome files for system configuration analysis. Each file represents a single system state	83
5.1	SWaT architecture	89
5.2	Sensors and actuators associated with each PLC	90
5.3	SWaT network architecture	91
5.4	SWaT stabilization	94

List of Tables

2.1	Modbus Function Codes list	16
5.1	Main IP addresses of the six PLCs and SCADA in SWaT . . .	92
5.2	SWaT network traffic data	95

Listings

3.1	Example of registers capture	29
3.2	Example of raw network capture	30
3.3	Statistical data for PLC1_InputRegisters_IW0 register	31
3.4	Generic example of a .spinfo file for customizing rules in Daikon	32
4.1	Novel Framework structure and Python scripts	54
4.2	Paths and parameters for the Pre-processing phase in <i>con-</i> <i>fig.ini</i> file	58
4.3	<i>config.ini</i> parameters for dataset enriching	60
4.4	Example of preliminar system analysis	68
4.5	Standard Daikon output for PLC1 of the iTrust SWaT system	77
4.6	Revised Daikon output with transitive closures for PLC1 of the iTrust SWaT system	80
4.7	Daikon outcomes for the system configuration P1_MV101 == 2, P1_P101 == 1 on P1_LIT101	84

References

- [1] NIST. *ICS definition*. URL: https://csrc.nist.gov/glossary/term/industrial_control_system (visited on 2023-04-06).
- [2] *What is SCADA?* URL: <https://www.inductiveautomation.com/resources/article/what-is-scada> (visited on 2023-04-05).
- [3] G. M. Makrakis, C. Kolias, G. Kambourakis, C. Rieger, and J. Benjamin. "Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents". In: *IEEE Access* (2021-12-06). DOI: <https://dx.doi.org/10.1109/ACCESS.2021.3133348>.
- [4] NIST. *PLC definition*. URL: https://csrc.nist.gov/glossary/term/programmable_logic_controller (visited on 2023-04-06).
- [5] W. Bolton. *Programmable Logic Controllers, 6th edition*. Newnes, 2015, pp. 7–9.
- [6] M. Ceccato, Y. Driouich, R. Lanotte, M. Lucchese, and M. Merro. "Towards Reverse Engineering of Industrial Physical Processes". In: *CPS4CIP@ESORICSAt 2022* (Copenhagen, Denmark, Sept. 30, 2022). 2022, 273–290. DOI: https://doi.org/10.1007/978-3-031-25460-4_15.
- [7] H. S. G. Pussewalage, P. S. Ranaweera, and V. Oleshchuk. "PLC security and critical infrastructure protection". In: *2013 IEEE 8th International Conference on Industrial and Information Systems* (Dec. 2013). 2013. DOI: <https://dx.doi.org/10.1109/ICIIInfS.2013.6731959>.

- [8] Wikipedia. *Remote Terminal Unit*. URL: https://en.wikipedia.org/wiki/Remote_terminal_unit (visited on 2023-04-08).
- [9] NIST. *HMI definition*. URL: https://csrc.nist.gov/glossary/term/human_machine_interface (visited on 2023-04-11).
- [10] Schneider Electric. *What is Modbus and how does it work?* URL: <https://www.se.com/us/en/faqs/FA168406/> (visited on 2023-04-13).
- [11] O. Morando. *Hacking: Modbus - Cyber security OT/ICS*. URL: <https://blog.omarmorando.com/hacking/ot-ics-hacking/hacking-modbus> (visited on 2023-04-15).
- [12] Modbus.org. "MODBUS/TCP Security". In: pp. 7–8. URL: https://modbus.org/docs/MB-TCP-Security-v21_2018-07-24.pdf (visited on 2023-04-16).
- [13] ODVA Inc. "EtherNet/IP - CIP on Ethernet Technology". In: URL: https://www.odva.org/wp-content/uploads/2021/05/PUB00138R7_Tech-Series-EtherNetIP.pdf (visited on 2023-04-18).
- [14] *Odva, Inc.* URL: <https://www.odva.org> (visited on 2023-04-21).
- [15] *Introduction to EtherNet/IP Technology*. URL: https://scadahacker.com/library/Documents/ICS_Protocols/Intro%20to%20EthernetIP%20Technology.pdf (visited on 2023-04-19).
- [16] ODVA Inc. *Common Industrial Protocol*. URL: <https://www.odva.org/technology-standards/key-technologies/common-industrial-protocol-cip/> (visited on 2022-12-26).
- [17] Wikipedia. *Common Industrial Protocol*. URL: https://en.wikipedia.org/wiki/Common_Industrial_Protocol (visited on 2023-04-21).
- [18] *What is the Common Industrial Protocol (CIP)?* URL: <https://www.motioncontroltips.com/what-is-the-common-industrial-protocol-cip/> (visited on 2023-04-21).
- [19] *CIP (Common Industrial Protocol): CIP messages, device types, implementation and security in CIP*. URL: <https://resources.infosecinstitute.com/topic/cip/> (visited on 2023-04-21).

- [20] B. Green, M. Krotofil, and A. Abbasi. "On the Significance of Process Comprehension for Conducting Targeted ICS Attacks". In: Workshop on Cyber-Physical Systems Security and PrivaCy (Nov. 2017). ACM, 2017, pp. 57–67. DOI: <https://doi.org/10.1145/3140241.3140254>.
- [21] A. Keliris and M. Maniatakos. "ICSREF: A Framework for Automated Reverse Engineering of Industrial Control Systems Binaries". In: 26th Annual Network and Distributed System Security Symposium (NDSS) (Feb. 2019). 2019. DOI: <https://doi.org/10.48550/arXiv.1812.03478>.
- [22] Y. Yuan, X. Tang, W. Zhou, W. Pan, X. Li, H. T. Zhang, H. Ding, and J. Goncalves. "Data driven discovery of cyber physical systems". In: *Nature Communications* 10 (2019-10-25). URL: <https://www.nature.com/articles/s41467-019-12490-1> (visited on 2023-04-20).
- [23] C. Feng, V.R. Palleti, A. Mathur, and D. Chana. "A Sysemantic Framework to Generate Invariants for Anomaly Detection in Industrial Control Systems". In: NDSS Symposium 2019 (San Diego, CA, USA, Feb. 24–27, 2019). 2019. DOI: <https://dx.doi.org/10.14722/ndss.2019.23265>.
- [24] Singapore University of Technology and Design. *iTrust - Center for Research in Cyber Security*. URL: <https://itrust.sutd.edu.sg/> (visited on 2023-05-15).
- [25] K. Pal, A. Adepur, and J. Goh. "Effectiveness of Association Rules Mining for Invariants Generation in Cyber-Physical Systems". In: 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE) (Jan. 2017). 2017. DOI: <https://doi.org/10.1109/HASE.2017.21>.
- [26] *Association rules mining*. URL: https://en.wikipedia.org/wiki/Association_rule_learning (visited on 2023-04-21).

- [27] K. Pal, A. Adepu, and J. Goh. “Cyber-Physical System Discovery: Reverse Engineering Physical Processes”. In: 3rd ACM Workshop on Cyber-Physical System Security (Apr. 2017). 2017, pp. 3–14. DOI: <https://doi.org/10.1145/3055186.3055195>.
- [28] Ceccato et al. *reverse engineering prototype tool*. URL: <https://github.com/SeUniVr/PLC-RE> (visited on 2023-04-23).
- [29] iTrust Singapore University of Technology and Design. *Secure Water Treatment*. URL: <https://itrust.sutd.edu.sg/testbeds/secure-water-treatment-swat/> (visited on 2023-05-15).
- [30] R. Lanotte, M. Merro, and A. Munteanu. “Industrial Control Systems Security via Runtime Enforcement”. In: *ACM Transactions on Privacy and Security* 26.4 (2023-02), pp. 1–41. DOI: <https://doi.org/10.1145/3546579>.
- [31] M. Oliani. *AttackPLC - Project for Network Security teaching*. URL: <https://github.com/marcooliani/AttackPLC> (visited on 2023-04-23).
- [32] Ray - *Productionizing and scaling Python ML workloads simply*. URL: <https://www.ray.io/> (visited on 2023-04-25).
- [33] Tshark. URL: <https://tshark.dev/> (visited on 2023-04-25).
- [34] Wireshark. URL: <https://www.wireshark.org/> (visited on 2023-04-25).
- [35] pandas - *Python Data Analysis library*. URL: <https://pandas.pydata.org/> (visited on 2023-04-25).
- [36] NumPy - *The fundamental package for scientific computing with Python*. URL: <https://numpy.org/> (visited on 2023-04-25).
- [37] R project for statistical computing. URL: <https://www.r-project.org/> (visited on 2023-04-25).
- [38] SciPy - *Fundamental algorithms for scientific computing with Python*. URL: <https://scipy.org/> (visited on 2023-04-25).
- [39] *The Daikon dynamic invariant detector*. URL: <http://plse.cs.washington.edu/daikon/> (visited on 2023-04-25).

-
- [40] *Enhancing Daikon output*. URL: <https://plse.cs.washington.edu/daikon/download/doc/daikon/Enhancing-Daikon-output.html#Splitter-info-file-format> (visited on 2023-04-25).
 - [41] *Process mining*. URL: https://en.wikipedia.org/wiki/Process_mining (visited on 2023-04-26).
 - [42] *Fluxicon Disco*. URL: <https://fluxicon.com/disco/> (visited on 2023-04-26).
 - [43] *OpenPLC - Open source PLC software*. URL: <https://openplcproject.com/> (visited on 2023-04-23).
 - [44] *Docker*. URL: <https://www.docker.com/> (visited on 2023-04-26).
 - [45] MathWorks. *Simulink*. URL: <https://it.mathworks.com/products/simulink.html> (visited on 2023-04-26).
 - [46] *ProM Tools - The Process Mining Framework*. URL: <https://promtools.org/> (visited on 2023-04-26).
 - [47] Fraunhofer Institute for Applied Information Technology. *pm4py - Process Mining for Python*. URL: <https://promtools.org/> (visited on 2023-04-26).
 - [48] statsmodels. *statsmodels - statistical models, hypothesis tests, and data exploration*. URL: <https://www.statsmodels.org/stable/index.html> (visited on 2023-05-05).
 - [49] NetworkX. *NetworkX - Network Analysis in Python*. URL: <https://networkx.org/> (visited on 2023-05-05).
 - [50] Wikipedia. *Savitzky-Golay filter*. URL: https://en.wikipedia.org/wiki/Savitzky%E2%80%93Golay_filter (visited on 2023-05-06).
 - [51] Otext. *STL decomposition*. URL: <https://otexts.com/fpp2/stl.html> (visited on 2023-05-06).
 - [52] Wikipedia. *Transitive closures*. URL: https://en.wikipedia.org/wiki/Transitive_closure (visited on 2023-05-11).

- [53] iTrust Singapore University of Technology and Design. *Secure Water Treatment (SWaT) Testbed*. URL: https://itrust.sutd.edu.sg/wp-content/uploads/2021/07/SWaT_technical_details-160720-v4.4.pdf (visited on 2023-05-15).
- [54] A. Mathur and N. O. Tippenhauer. "SWaT: a water treatment testbed for research and training on ICS security". In: 2016 International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater) (Apr. 2016). 2016. DOI: <http://dx.doi.org/10.1109/CySWater.2016.7469060>.
- [55] iTrust Singapore University of Technology and Design. *Datasets*. URL: https://itrust.sutd.edu.sg/itrust-labs_datasets/ (visited on 2023-05-15).
- [56] S. Adepu, J. Goh, K.N. Junejo, and A. Mathur. "A Dataset to Support Research in the Design of Secure Water Treatment Systems". In: The 11th International Conference on Critical Information Infrastructures Security (France, Oct. 2016). 2016.
- [57] T. A. Snide. *CIP-Modbus Integration*. 2008. URL: https://www.modbus.org/docs/CIP%20Modbus%20Integration%20Hanover%20Fair_0408.pdf (visited on 2023-05-17).