UNIVERSITÀ DEGLI STUDI DI VERONA
DEPARTMENT OF COMPUTER SCIENCE

MASTER'S DEGREE IN
COMPUTER SCIENCE AND ENGINEERING

Master Thesis

DECONSTRUCTING THE UNKNOWN: A BLACK BOX APPROACH TO REVERSE ENGINEERING ICS USING GRAPHS AND INVARIANTS

Supervisor:
Prof. **Massimo MERRO**

Co-supervisors:
Prof. **Ruggero LANOTTE**
Marco LUCCHESE

Candidate:
Marco OLIANI
Matr. VR457249

Academic Year 2022/2023

"Gallina vecchia fa buon brodo"
(Valentino Rossi)

Abstract

Bla bla bla

Contents

Chapter 1

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 Contibution

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

Why do we use it? It is a long established fact that a reader will be distracted by the readable content of a page when looking at its layout.

The point of using Lorem Ipsum is that it has a more-or-less normal distribution of letters, as opposed to using 'Content here, content here', making it look like readable English. Many desktop publishing packages and web page editors now use Lorem Ipsum as their default model text, and a search for 'lorem ipsum' will uncover many web sites still in their infancy. Various versions have evolved over the years, sometimes by accident, sometimes on purpose (injected humour and the like).

Where does it come from? Contrary to popular belief, Lorem Ipsum is not simply random text. It has roots in a piece of classical Latin literature from 45 BC, making it over 2000 years old. Richard McClintock, a Latin professor at Hampden-Sydney College in Virginia, looked up one of the more obscure Latin words, consectetur, from a Lorem Ipsum passage, and going through the cites of the word in classical literature, discovered the undoubtable source. Lorem Ipsum comes from sections 1.10.32 and 1.10.33 of "de Finibus Bonorum et Malorum" (The Extremes of Good and Evil) by Cicero, written in 45 BC. This book is a treatise on the theory of ethics, very popular during the Renaissance. The first line of Lorem Ipsum, "Lorem ipsum dolor sit amet..", comes from a line in section 1.10.32.

The standard chunk of Lorem Ipsum used since the 1500s is reproduced below for those interested. Sections 1.10.32 and 1.10.33 from "de Finibus Bonorum et Malorum" by Cicero are also reproduced in their exact original form, accompanied by English versions from the 1914 translation by H. Rackham.

Chapter 2

Background

2.1 What ICSs are

2.2 ICS components

2.2.1 RTU

2.2.2 PLC

2.2.3 IED

2.2.4 HMI

2.3 ICS Communication Protocols

2.3.1 Modbus

2.3.2 Ethernet/IP

Test cite [1]
test cite 2 [2]
test cite 3 [3]
test cite 3 [4]

Col1	Col2	Col2	Col3
1	6	87837	787
2	7	78	5415
3	545	778	7507
4	545	18744	7560
5	88	788	6344

Table 2.1: This is the caption for the first table.

Figure 1: SWaT's six-stage processes

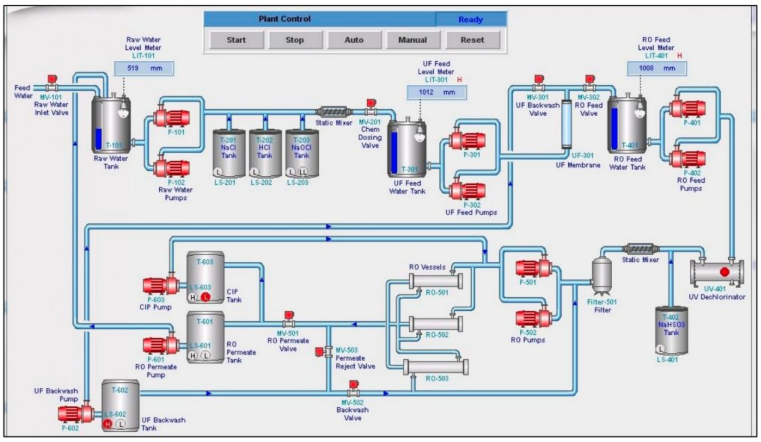

Figure 2.1: SWaT schema

Chapter 3

Related work

Chapter 4

State of the Art: Presentation of Ceccato et al. Work [1]

4.1 Paper's Goal

4.2 Process Analysis Steps

4.2.1 Scanning of the System and Graph Analysis

4.2.2 Businness Process Analysis

4.2.3 Invariants Analysis

4.3 Application to a Simulated Testbed

4.4 Limitations

Chapter 5

Proposal to Improve Ceccato et al. Work

5.1 Improving Pre-processing

5.2 Improving Graph Analysis

5.3 Improving Invariants Analysis

5.3.1 Automatic Detection of Actuators and Sensors

5.3.2 Invariants Generation

5.4 Obtaining Extra Information on the Runtime Evolution of the Physical Process

5.5 Improving Businness Process Analysis

Chapter 6

Case study: the iTrust SWaT System

Chapter 7

Application to the iTrust SWaT System

7.1 Pre-processing

7.2 Graph Analysis

7.2.1 Conjectures About the System

7.3 Invariants Analysis

7.3.1 Actuators Detection

7.3.2 Daikon Analysis and Results Comparing

7.4 Obtaining extra information on the runtime evolution of the physical system

7.5 Businness Process Analysis

Chapter 8

Conclusions

8.1 Discussions

8.2 Guidelines

8.3 Future work

List of Figures

List of Tables

References

[1] 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.

[2] 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.

[3] Singapore University of Technology and Design. *iTrust - Center for Research in Cyber Security*. URL: https://itrust.sutd.edu.sg/ (visited on 12/08/2022).

[4] C. Feng, V.R. Palleti, A. Mathur, and D. Chana. "A Sysematic 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.