

Analysis of and Mitigation Strategies for Real World OT Security Incidents

Nico Fechtner

Technical University of Munich, Arcisstraße 21, 80333 Munich, Germany

nico.fechtner@tum.de

<https://www.tum.de/en/>

Abstract. The abstract should briefly summarize the contents of the paper in 150–200 words. The goal is to communicate: Background/motivation/context, Aim/objective(s)/problem statement, Approach/method(s)/procedure(s), Results, Conclusion(s)/implications.

Keywords: OT Security · Security Incident · Triton.

1 Introduction

2 Related Work

3 Comparative Overview of OT incidents

3.1 Targets

3.2 Techniques

3.3 Time of Discovery, Reaction and Impact

3.4 Threat Actors

4 Detailed Analysis of the Triton Attack

4.1 Stage 1

4.2 Stage 2

4.3 Possible Mitigation Strategies

5 Conclusion

References