Available online at www.sciencedirect.com

ScienceDirect

Procedia CIRP 00 (2021) 000–000

www.elsevier.com/locate/procedia

54th CIRP Conference on Manufacturing Systems

Machine Learning use case in manufacturing – an evaluation of the model's reliability from an IT security perspective

Beatriz Bretones Cassoli[a,*], Amina Ziegenbein[a], Joachim Metternich[a], Siniša Đukanović[b], Julien Hachenberger[b], Martin Laabs[b]

[a] *Institute of Production Management, Technology and Machine Tools (PTW), Otto-Berndt-Str. 2, 64287, Darmstadt, Germany*
[b] *Fraunhofer Institute for Secure Information Technology, Rheinstr. 75, 64295, Darmstadt, Germany*

* Corresponding author. Tel.: +49 6151 16-20048; fax: +49 6151 16-20087. E-mail address: b.cassoli@ptw.tu-darmstadt.de

Abstract

The use of Machine Learning (ML) solutions for decision automation in manufacturing environments is critical if operators trust ML-predictions without critically questioning them. The vulnerability of ML-applications to data manipulation, data-poisoning and adversarial examples raise concerns about its reliability and security. This paper evaluates an on-edge predictive maintenance solution through an IT security perspective, showing how the model's forecasting can be affected by intentional data manipulation and thus identifying the system's vulnerabilities for this particular use case. It concludes with suggestions on how to mitigate threats and manage risks.

Keywords: Artificial Intelligence; Predictive Maintenance; IT Security