Cybersecurity to Protect and Allow Exchange of Manufacturing Data

Executive Summary Report

Deliverable: ESR

Submitted to:
EUROPEAN SPACE AGENCY (ESA) -
Keplerlaan 1,
2201 AZ Noordwijk,
The Netherlands
Technical Officer:
Jose Pizarro
jose.pizarro@esa.int

Submitted by:
Nexova Cyber S.A.
Avenue Einstein 8
1300 Wavre,
Belgium
Project Manager:
Peter Hagstrom
p.hagstrom@nexovagroup.eu

ESA Contract Number: 4000138573/22/NL/MGu
Date Submitted: 22/04/2024
Nexova File No.: WO301190

Work Package	WP6	Deliverable	PAEMD-ESR-TEC-TN Executive Summary Report
Due Date	03/05/2024	Date Submitted	03/05/2024
Issue	1.1	Status	Final
Keywords	Assessment, Security Guidelines, MAIT		

Prepared by:

Anders Hagström (Signature)

Digitally signed by Anders Hagström (Signature)
Date: 2024.05.06 10:11:47 +02'00'

Peter Hagstrom
Project Manager, Nexova Cyber

Date

Reviewed and approved by:

Jose Pizarro
Technical Officer

Date

ESA Unclassified - For ESA Official Use Only
© Copyright European Space Agency 2022-2024

DOCUMENT CHANGE CONTROL

This document is under configuration control. Latest changes to the document are listed last.

Issue	Date	Name	Comment
1.0	19/03/2024	Peter Hagstrom	Initial version of document
1.0	21/04/2024	Peter Hagstrom	Document reviewed and closed
1.1	03/05/2024	Peter Hagstrom	Rebranding because of RHEA Group demerger

© Copyright European Space Agency 2022-2024

TABLE OF CONTENTS

© Copyright European Space Agency 2022-2024

TABLE OF FIGURES

© Copyright European Space Agency 2022-2024

LIST OF TABLES

NO TABLE OF FIGURES ENTRIES FOUND.

© Copyright European Space Agency 2022-2024

1 INTRODUCTION

1.1 Context

Modern manufacturing, assembly and testing (MAIT) for spacecraft manufacturing is increasingly more reliant on digitalization. This digital transformation is frequently referred to as Industry 4.0, benefitting the industry by reducing cost and time to produce. However, at the same time, it significantly elevates cybersecurity risks since sensitive data is being exchanged over greater distances, within and across national and organizational boundaries. This is especially true in distributed and cloud manufacturing, with potentially severe implications for the protection of IPRs (intellectual properties rights) and trade secrets. Furthermore, an increased exposure is faced due to the large number of sensors and various Internet-of-Things devices being used across the MAIT processes. This new and evolving threat landscape is posing new operational risks to product integrity, intellectual property and the safekeeping of operations. Why this is a growing concern for MAIT security, especially in the space sector.

The PAEMD project aim to analyse the threat landscape for modern MAIT within the spacecraft manufacturing and provide best practices on how to secure the exchange of data.

1.2 Purpose

This deliverable is part of the final reports of the PAEMD project, the purpose is to provide a concise summary of the findings within the scope of the contract.

1.3 Scope

The scope of the deliverable is to:

- Provide background information about the PAEMD project
- Summarize the main findings and key results
- Analyse the impact and application of the PAEMD project

© Copyright European Space Agency 2022-2024

2 PAEMD OVERVIEW

Manufacturing, Assembly, Integration, and Testing (MAIT) are four fundamental processes on which production of aerospace components and systems are built on. These processes encompass everything from the initial manufacturing to the final testing of assembled systems.

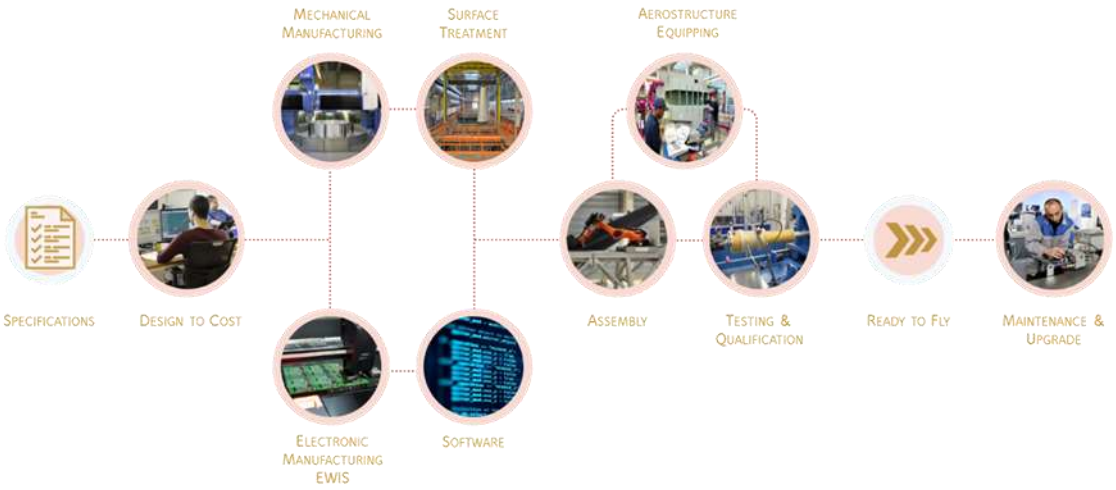

Figure 1: Example of MAIT processes

The aerospace industry is a critical sector in modern societies, enabling everything from everyday services, such as safe navigation, internet and telecommunications, to defence and research. This is placing the aerospace sector in the focal point of threat actors wanting gain commercial advantages/lucrative purposes, destabilize or steal data for spying purposes. This means that you find state sponsored threat actors, specialist outfits, and competitors targeting your MAIT processes if not properly secured.

As modern MAIT is shifting to encompass modern and digital technologies, i.e. additive manufacturing, cloud and distributed manufacturing, the threat landscape is significantly shifting. The more interconnected processes and data flow, as well as many suppliers, cause a large threat surface, making MAIT security increasingly difficult to maintain.

The industry has been targeted by several high-profile attacks that have impacted both operational technology and regular IT. Many attacks on critical sectors go unnoticed by the public, as organisations are reluctant to share information due to reputational risks and the potential exposure of valuable information to adversaries. Despite this, several attacks have become known. One of the most infamous attacks is the Stuxnet attack, which caused substantial damage to the Iranian nuclear program by targeting their SCADA systems. Another adjacent case is the 2017 NotPetya ransomware attack that caused the radiation monitoring at Chernobyl nuclear power plant to go offline. This shows how vulnerable operational and ICT environments can be if specifically targeted.

© Copyright European Space Agency 2022-2024

Overall, there is an increased threat to MAIT business and process. According to the Dragos report “ICT/OT Cybersecurity year in review 2022” [ICT/OT] there has nearly been a doubled number of reported attacks on industrial infrastructure during 2022, and 70% of all ransomware attacks are focused on manufacturing.

The aim of PAEMD is to analyse the MAIT for space manufacturing threat landscape and provide the industry with guidance, technologies and best practices. This has been achieved through the following main activities:

- **Case Study Selection**: Selection of a case study for a modern digital-based MAIT processes.
- **High-level Threat and Risk Assessment:** Analysis of potential cyber threats and vulnerabilities associated with the selected processes
- **Development of Demonstrator:** By integrating MAIT processes, attacks and protective mechanisms, the PAEMD demonstrator aims to provide awareness about cyber impact and show how MAIT can be secured against various attacks.
- **Guidelines for MAIT Space Industry:** PAEMD project aims to provide guidance as to how organizations can bolster their security and assessment how these guidelines can be applied to various cyber-challenges within MAIT sector.
- **Analyse Applicability of Innovative Encryption:** The PAEMD project aims to analyse how zero-knowledge protocols, secure multiparty-computations and fully homomorphic encryption can be applied to cyber challenges within MAIT.

© Copyright European Space Agency 2022-2024

3 KEY FINDINGS AND RESULTS

The key findings of the PAEMD project are:

- **Increased Threat Landscape Knowledge:** The PAEMD project conducted a risk analysis of the chosen use case, which has contributed to the understanding of the risks faced by the MAIT industry. We have identified 16 operational attack scenarios that have reached a critical severity level. The identified threat actors at this level are related entities, specialist organizations, and competitors. These actors intend to destabilize, steal data for profitable purposes, gain commercial advantages, or spy on the industry.
- **Cybersecurity Demonstrator:** As part of the project a new demonstrator has been developed, capable of process, attack and control measure simulation. Enabling organisations and individuals to better understand security risks and cyber impacts.
- **Guidance Development:** The guidance provided to the industry spans hygienic measures such as applying a risk-based approach to security, information handling and classification, and provides practical guidance on implementation and responsibilities. The guidelines also provide valuable references to well-established security frameworks, such as EBIOS RM, NIST Cybersecurity Framework and control catalogues (i.e., NIST-800-53, Cyber Fundamentals Framework, IEC 62443 and CIS critical security controls) as well as highlighting documentation standards for security requirements specifications. In addition, a set of assessments was conducted yielding the result that guidelines and controls are largely available for the MAIT industry, and standard best practices and information security systems largely address the fundamental needs of the MAIT industry. However, in the case of distributed manufacturing, we identified that there was a lack of practical and readily available mitigations. For instance, against overhearing or side-channel attacks in the automatic request for quotation in distributed manufacturing.
- **Recommendations for ZKP, FHE and MPC:** The following use cases were identified: securing finite element calculations with FHE, the possibility of verifying document metadata with ZKP, and enhancing bidding processes. The resulting analysis shows that FHE is currently not viable for immediate application due to performance issues. ZKP shows promise for verifying document properties without compromising content privacy, particularly useful for internal data-sharing policy compliance. MPC and ZKP could theoretically support a secure marketplace for manufacturing services, though practical implementation would require substantial infrastructure development and industry support.

© Copyright European Space Agency 2022-2024

4 IMPACT AND APPLICATION

The PAEMD project has highlighted the critical need for robust cybersecurity measures and provides strategic focus, strengthening the overall security posture of the MAIT industry. The comprehensive guidelines provide actionable advice to cyber organizations, specifically to the organizations that are early in their security journey by recommending a continuous risk-based approach with strong pointers to the various standards and frameworks.

The demonstrator developed during the project serves as a training and simulation platform, allowing hands-on experience in managing and mitigating security attacks. This provides an improved capability to provide awareness training and visualise impacts of cyber-attacks.

By analysing the advancements made in recent cryptographic research, the project opens new possibilities for securing sensitive operations within MAIT processes. Although some technologies are not ready for immediate application, the project provides a potential future direction as these technologies mature.

By improving cybersecurity practices the PAEMD project contributes to the overall resilience of the aerospace industry against cyber threats, which is crucial for national security and economic development.

© Copyright European Space Agency 2022-2024

5 CONCLUSIONS

The PAEMD project has significantly contributed to the understanding and mitigation of cybersecurity risks in the spacecraft manufacturing industry. By developing targeted guidelines and a dynamic demonstrator, the project not only enhances immediate cybersecurity practices but also lays the groundwork for future research and development in the field. Continued exploration and adaptation of innovative security measures, alongside industry-wide dissemination and training, are recommended to sustain and build upon the achievements of this initiative.

© Copyright European Space Agency 2022-2024