Charter of Trust

Partner Use Case

Mitsubishi Heavy Industries

Principle 2 “Responsibility throughout the digital supply chain”

1. Starting point

It was agreed among MHI, Siemens, and TÜV SÜD to check a joint approach to verify adherence to the Charter of Trust’s baseline requirements for supply chain security and gain best practices and challenges to reduce future efforts amongst parties. For this purpose, the partners launched a verification pilot project.

2. Objectives

The objectives of the pilot were (1) to design a verification methodology, (2) to report verification results and analyze the effectiveness of this approach, and (3) to plan for next steps based on the results.

3. Description

MHI followed the three steps below having close contact with the relevant parties (Siemens, TÜV SÜD, Primetals Technologies) through bi-weekly or monthly meetings.

(1) Design a verification methodology: In this step, MHI carefully designed the methodology for verification, and if needed, revised the methodology based on the results of pilot project.

(2) Report verification result and analysis of effectiveness: Besides reporting the verification results, MHI also focused on the analysis of the effectiveness regarding needed efforts/costs/willingness of the supplier.

(3) Plan for next steps based on the result: Based on the results of the pilot, MHI defined further actions and points to redefine the approach.

4. Lessons learned/results

In general, MHI found that the results of this project will serve as a good ground in establishing cybersecurity assessment practices not only within MHI and Siemens, but also among CoT partners.