Raimo Rahkonen

Engineering a digitalized plant

Abstract: Modern industrial plants rely heavily on numerous software and firmware applications for their operational systems. However, engineering activities are often distributed among various suppliers and other parties without clear implementation requirements or context.

This document discusses of how design engineering and task coordination should be structured to enable plant owners and stakeholders to effectively manage the information about applications and the data they generate. This approach ensures compliance with cybersecurity asset documentation requirements and aligns with European NIS2 [1] and CRA [2] directives.

Keywords: plant engineering, applications context, CRA, NIS2, cyber physical systems, CVEs, CSAF, AI

***Corresponding Author: Raimo Rahkonen**, E-mail: raimo.rahkonen@remuscon.fi

1 Background

In the digital plants managing numerous software and firmware applications is crucial. Two key European directives, NIS2 (Directive (EU) 2022/2555, for a high common level of cybersecurity) and CRA (Cyber Resilience Act), address digitalization and cyber assets management. Proper organization of applications within the plant context is essential for effective risk assessment and management.

This document outlines how to structure applications engineering to empower plant owners and stakeholders. By creating a comprehensive cyber model of the plant, the owner and other stakeholders can sustainably leverage Artificial Intelligence (AI) and related advanced algorithms, to efficiently handle issues related to plant documentation and compliance.

2 Methods

To ensure successful outcomes for various engineering personnel, a systematic and easily understood method is essential. The following chapters outline the key aspects of this approach.

Physical Assets structure

A digital plant consists of several cyber physical systems which may contain other systems [3]. The physical assets are typically organized into an asset tree. In the tree the assets are shown as parents and children, indicating where they belong to in the plant functional structure.

As part of cyber engineering, some physical and functional characteristics may be recorded for information enrichment. Such information contains the purpose of the asset and generic or detailed function. Additional information may be included, especially if the cyber engineering system is not connected to physical engineering. Physical engineering typically provides information on 3D models, mechanical structures' physical connectivity, fluid flows, and power and data networking.

Application requirements

A good practice of defining the functionality of the controls with industrial control systems has been implemented for decades. Functional descriptions or control narratives are useful in providing clear and consistent description of the control logic and operational procedures, to be achieved with the software.

With the software and firmware distributed from field devices, OT systems to cloud instances, it has become necessary to extend this practice to concern all applications, wherever they are executed. In this document we call them application requirements.

The computing platforms where the applications shall be run can be:

- embedded into the asset (sensors, actuators,

IIOT equipment etc.) itself,
- a drive for an electrical motor, lighting fixture, electrical power distribution IED
- PLC or ICS controller, building automation controller
- platform in virtual environment at the
    - edge,
    - at plant level or
    - cloud

The application requirements are connected to the exact asset (at any level of the asset tree) which the required application shall serve. This method is useful to contextualize the data provided by the actual implemented application. It is also useful to know the context in case of known or foreseen vulnerability to define the risk it may cause.

Implemented Applications

Applications to be run in systems of any plant are effectively composed by manufacturers with methods including previous versions of the same, and relating applications and open-source components. A list of SW components is typically given as Software Bill of Material (SBOM) [4].

The implemented applications themselves are based on selected typical solutions, called for the assets as required by the application requirements. The typical solutions are further developed for the exact asset of the plant, or to a computing platform of a plant system.

It is essential to record the exact version of the typical application to trace the possible bugs and vulnerabilities, CVEs [5] (Common Vulnerabilities and Exposures). There are public sources where known vulnerabilities are published. Some are by governmental authorities and researchers, some by private specialist vendors and applications and systems providers.

A further development to enable a plant owner to disclose information about CVEs are the security advisories.

The security advisories contain not only information about vulnerability, but also advise what to do if you happen to have the application concerned. Some suppliers provide advisories in a machine-readable format according to Common Security Advisory Framework [6] (CSAF). These facilitate automation and reduce the time required to understand impact to plant applications and drive timely remediation.

By creating an inventory database of applications as given in this document, and using the CSAF advisories, companies can maintain overview and secure the plant systems in an efficient manner.

Summary

Engineering the cyber part of a cyber physical plant as part of the implementation engineering gives the plant owner several advantages compared to finding out the cyber part afterwards.

Allowing plant engineering designers, suppliers and OEM manufacturers to work collaboratively within the plant context with their knowledge on cyber physical systems gives better results both technically and financially.

Additionally, developing contextual information of applications and data enhances the effectiveness of Artificial Intelligence (AI) in case the plant owner decides to use such advanced tools.

3 Bibliography

Attached sources of information cited in the text.

[1] NIS2 directive: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555
[2] Cyber Resilience Act (CRA): https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
[3] Framework for Cyber-Physical Systems: Volume 2, Working Group Reports https://doi.org/10.6028/NIST.SP.1500-202
[4] Software Bill of Materials (CISA): Software Bill of Materials (SBOM) | CISA
[5] Overview of CVE program: Overview | CVE
[6] Common Security Advisory Framework (by BSI): BSI - Common Security Advisory Framework (CSAF)