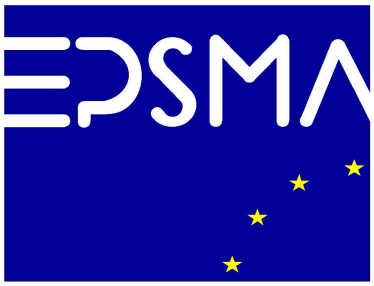

EUROPEAN POWER SUPPLIES MANUFACTURERS' ASSOCIATION
(Visit the EPSMA website at www.epsma.org)

Embedded Software Verification and Validation in Power Supplies

First edition 17th September 2020
Full text available to EPSMA Members only

ABSTRACT

Paper prepared by the EPSMA Technical Committee. Special thanks and acknowledgements to the report champion Pasi Lauronen (Efore), Andrej Rakar (SIQ, Ljubjana), and Benjamin Stoll (Inpotron), the technical reviewers Mathias Emsermann (Phoenix Contact), Rami Abraham (Vicor), Wolfgang Paul (Siemens), and the facilitator, Vlad Grigore (Efore) for their contribution to this document.

The European Power Supplies Manufacturers' Association was established in 1995, to represent the European power supply industry.

Index

1 Scope

The objective of this document is to review the current use of embedded software in power supply units and explain the need for verification of its correct functionality and validation for the application. It lists many existing standards and guidelines and describes a selection of techniques and methods that are relevant to software verification and validation. However, it does not prescribe comprehensive methods.

2 Background

2.1 Definitions of terms

The terms ‘Embedded software’, ‘Verification’, ‘Validation’ and ‘PSU, Power Supply Unit’ are defined.

3 Existing guidelines and standards

This chapter refers to some of the common standards, for quality management and their guidelines, covering a wide range of industrial areas. If there are no specific standards applicable for a PSU application, then generic standards are suggested. In this document, guidelines and standards are divided in to two tables, generic and application-specific.

Table 1. Generic guidelines and standards

Table 2. Application specific guidelines and standards

4 Use of embedded software in power supply units

This chapter discusses the general implications of digital control of power supplies compared with traditional analogue types. The extra performance and functionality possible with digital control with embedded software is highlighted, along with options for external connectivity and accessibility, either intentional or illicit.
Typical embedded software functionality in power supply units is itemised.

5 Verification of correct functionality and validation for the application

This chapter discusses the implication of ‘failure’ of embedded software in power supplies. Loss of function, reputational damage and unsafe operation are considered including the possibility of personal injury.
To counter these outcomes, the processes of embedded software verification and validation are considered across all operational conditions, integrated into the life-cycle of product design. Possible

published standards for verification and validation are suggested, where target application standards are not available.

5.1 Key elements of a typical verification and validation process

This chapter describes key elements that are needed, starting with a customer requirement demanding the use of embedded software, to the implementation of software in a power supply application in the field. This listing describes important areas that must be considered for verification and validation. The workflow can be altered to meet common development models such as waterfall, V-shaped, scrum or other iterative or agile models. Typical stages are itemised.

6 Cyber security

6.1 Cyber security risks associated with power supplies

Power supplies with embedded software and external communication capability can be susceptible to malicious cyber-attack or at least IP theft. The different communication channel possibilities are itemised. It is noted that cyber-security is a shared responsibility between power supply manufacturer and end user who has control over password and physical access.

Most common cyber security risks are itemised and described, as identified by 'OWASP IoT Top 10' list, with references to risks specific to power supplies.

- **Weak, Guessable, or Hardcoded Passwords**
- **Insecure Network Services**
- **Insecure Ecosystem Interfaces**
- **Lack of Secure Update Mechanism**
- **Use of Insecure or Outdated Components**
- **Insufficient Privacy Protection**
- **Insecure Data Transfer and Storage**
- **Lack of Device Management**
- **Insecure Default Settings**
- **Lack of Physical Hardening**

6.2 IEC 62443 Overview

An overview is given of IEC 62443 'Security for industrial automation and control systems series of standards' which specifies requirements for security capabilities. These capabilities may be technical capabilities (security mechanisms) or process capabilities (human procedures).

Figure 1: IEC 62443 Overview

From IEC 62443, the following security practices are itemised, with descriptions.

- **Security management**
- **Specification of security requirements**
- **Secure by design**
- **Secure implementation**
- **Security verification and validation testing**
- **Management of security-related Issues**
- **Security update management**
- **Security guidelines**

6.3 Certification types and conformity assessment procedure

Various certification types in IEC 62443 are defined based on products and services being certified:

- **Product Supplier**
- **Maintenance Provider**
- **Integrator Certificate**
- **Solution Certificate**

6.4 Different levels of cyber security requirements

In the document, different levels of cyber security requirements are defined, in line with REGULATION (EU) 2019/881

- **Basic**
- **Substantial**
- **High**

7 Conclusions

A summary of the issues discussed and overall recommendations

8 References & Bibliography

A list of references to standards, guidelines and other references to the subject.