WA 1:2021
(ICS 35.030)

WORKSHOP AGREEMENT

Cybersecurity self-evaluation checklist and guidelines for digitalisation in manufacturing

Singapore Standards Council

WA 1:2021
(ICS 35.030)

WORKSHOP AGREEMENT

Cybersecurity self-evaluation checklist and guidelines for digitalisation in manufacturing

Published by Enterprise Singapore

ISBN 978-981-5024-92-0

Contents

Foreword

This Workshop Agreement (WA) was developed from August to October 2021 under the purview of the Manufacturing Standards Committee, a committee under the Singapore Standards Council.

Experts met in a workshop setting on 1 October, 8 October and 15 October 2021 following the public call for participation made from 3 September to 4 October 2021 to discuss and reach general agreement on best practices for cybersecurity self-evaluation checklist and guidelines for digitalisation in manufacturing. The WA was finalised and endorsed by the Co-Chairmen of the workshop on 1 November 2021.

This WA is applicable to companies that have processes that are controlled by industrial automation and control systems (IACS) and hence will employ both information technology (IT) systems and operational technology (OT) systems.

This WA is a provisional standard made available for application over a period of two years. Users of the WA are invited to provide feedback on its technical content, clarity and ease of use. Feedback can be submitted using the form provided in the WA. At the end of the two years, the WA will be reviewed, taking into account any feedback or other considerations, to further its development as a Technical Reference or Singapore Standard, continue as a WA for further industry trials or be withdrawn.

In preparing this WA, reference was made to the following publications:

1. IEC 62443 series – Security for industrial automation and control systems
2. ISO/IEC 27000 family – Information technology

Permission has also been sought from the following organisations for the adaptation / reproduction of materials from their publications into this WA:

International Electrotechnical Commission (IEC)

- *Clause 5.9 was reproduced from Clause 5.3 of IEC TS 62443-1-1:2009, "Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models"*
- *Table 1 was adapted from Clause 3.3 of IEC 62443-3-3:2013, "Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels"*

International Organization for Standardization (ISO)

- *Clause 5.8, excluding items (c), (l) and (m), was reproduced from ISO/IEC 27001:2013 "Information technology – Security techniques – Information security management systems – Requirements".*

ISO and IEC standards can be purchased from Enterprise Singapore.

Attention is drawn to the possibility that some of the elements of this WA may be the subject of patent rights. Enterprise Singapore shall not be held responsible for identifying any or all of such patent rights.

NOTE

1. *A WA is voluntary in nature. Users are advised to assess and determine whether the WA is suitable for their intended use or purpose. If required, they should refer to the relevant professionals or experts for advice on the use of the document. The development of a WA does not necessarily include all relevant stakeholders and the WA does not undergo the 2-month public consultation carried out for Singapore Standards. Enterprise Singapore and the Singapore Standards Council shall not be liable for any damages whether directly or indirectly suffered by anyone or any organisation as a result of the use of the WA. Although care has been taken to draft this WA, users are also advised to ensure that they apply the information after due diligence.*

2. *Compliance with a WA does not exempt users from any legal obligations.*

Cybersecurity self-evaluation checklist and guidelines for digitalisation in manufacturing

0 Introduction

The first industrial revolution started in the 18th century and was powered by steam and coal and saw the development of the steam engine. The emergence of electricity, oil, and gas as sources of energy heralded the second industrial revolution at the end of the 19th century. The internal combustion engine was created during this stage. The emergence of nuclear energy in the second half of the 20th century started the third industrial revolution that saw the rise of electronics, telecommunications, computers and a high degree of automation.

We are now at the start of the fourth industrial revolution where cyber-physical systems, Internet of things (loT) and artificial intelligence drive automated and data driven processes that are highly flexible and enable a high degree of personalization. This is driven by vertical and horizontal integration of systems. Vertical integration brings together the systems in a traditional automation pyramid: the field level, the control level, the production level, the operations level and the enterprise planning level. The horizontal integration is the end-to-end integration from the supplier and the processes, information flows and IT systems in the product development and production stage to logistics, distribution and finally the customer.

These horizontal and vertical integrations bring about many benefits for companies such as increased efficiency and the ability to implement new business models and services. They also enable flexible customer-oriented production to delivery hyper-customised products, services and optimised logistics and supply chains.

However, this increased connectivity also increases the cybersecurity threat landscape and increases both the types of vulnerabilities as well as the kinds of threats faced by companies. We also see an increase in the number of cybersecurity attacks on SMEs. These attacks are also increasing in their sophistication and target both the IT systems as well as the OT systems.

To ensure safe and secure operations, it is imperative to protect digitalisation with appropriate cybersecurity measures and controls. This checklist is intended to be used by SMEs which have integrated IACS into their production workflows to evaluate their cybersecurity maturity and help them identify gaps so they can improve their cybersecurity controls and measures.

1 Scope

The self-evaluation cybersecurity checklist aims to help smart manufacturing companies identify their cybersecurity gaps and determine their cybersecurity readiness level. This will facilitate companies to implement and maintain a base level of cybersecurity hygiene.

This Workshop Agreement (WA) is applicable to companies that have processes that are controlled by IACS and hence will employ both IT systems and OT systems.

2 Normative references

There are no normative references in this document.