



DPC: 25/30486280 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 09 December 2025

Origin: International

Latest date for receipt of comments: 01 February 2026

Project No. 2024/00171

Responsible committee: AGE/6 Agricultural tractors and forestry machinery

Interested committees:

Title: Draft BS EN ISO 24882 Agricultural machinery, tractors, and earth-moving machinery – Product cybersecurity.

Please notify admin.start@bsigroup.com if you are aware of any keywords that might assist in clarifying or identifying the standard or of the content of this standard:

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 01 February 2026

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

E-mail: admin.start@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



DRAFT International Standard

ISO/DIS 24882

Agricultural machinery, tractors, and earth-moving machinery – Product cybersecurity

ICS: 53.100; 65.060.01

ISO/TC 23/SC 19

Secretariat: **DIN**

Voting begins on:
2025-12-09

Voting terminates on:
2026-03-03

Member bodies are requested to consult relevant national interests in ISO/TC 127/SC 3 before casting their ballot to the e-Balloting application.

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/DIS 24882:2025(en)

Full document details: 25/30486280 DC

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

© ISO 2025



Documents

Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO 2025

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	viii
Introduction	ix
1 Scope	1
2 Normative references	1
3 Terms and Definitions and Abbreviated Terms	1
3.1 Terms and Definitions	1
3.2 Abbreviated Terms	4
4 General considerations	4
5 Risk assessment for the system of interest	8
5.1 Risk assessment introduction	8
5.2 System of interest identification	9
5.2.1 General	9
5.2.2 Prerequisites	9
5.2.3 Requirements	9
5.2.4 Work products	10
5.3 Assets, damage scenario identification	10
5.3.1 General	10
5.3.2 Prerequisites	10
5.3.3 Requirements	10
5.3.4 Work products	11
5.4 Threat identification	11
5.4.1 General	11
5.4.2 Prerequisites	11
5.4.3 Requirements	11
5.4.4 Work products	12
5.5 Impact rating determination	12
5.5.1 General	12
5.5.2 Prerequisites	12
5.5.3 Requirements	12
5.5.4 Work products	13
5.6 Likelihood rating determination	13
5.6.1 General	13
5.6.2 Prerequisites	14
5.6.3 Requirements	14
5.6.4 Work products	17
5.7 Risk rating determination	17
5.7.1 General	17
5.7.2 Prerequisites	17
5.7.3 Requirements	17
5.7.4 Work products	17
5.8 Risk treatment decision	18
5.8.1 General	18
5.8.2 Prerequisites	18
5.8.3 Requirements	18
5.8.4 Work products	18
5.9 Cybersecurity requirements determination	18
5.9.1 General	18
5.9.2 Prerequisites	19
5.9.3 Requirements	19
5.9.4 Work products	19
6 Cybersecurity technical requirements for risk mitigation	19
6.1 Technical requirements introduction	19
6.2 Secure software - update	19

6.2.1	Applicability	19
6.2.2	Requirement	19
6.2.3	Rationale	20
6.2.4	Guidance	20
6.2.5	Verification criteria	20
6.3	Secure software - update notification	20
6.3.1	Applicability	20
6.3.2	Requirement	21
6.3.3	Rationale	21
6.3.4	Guidance	21
6.3.5	Verification criteria	21
6.4	Secure software - integrity and authenticity check	21
6.4.1	Applicability	21
6.4.2	Requirement	21
6.4.3	Rationale	21
6.4.4	Guidance	21
6.4.5	Verification criteria	22
6.5	Hardening - secure configuration	22
6.5.1	Applicability	22
6.5.2	Requirement	22
6.5.3	Rationale	22
6.5.4	Guidance	22
6.5.5	Verification criteria	22
6.6	Hardening - production mode	22
6.6.1	Applicability	22
6.6.2	Requirement	23
6.6.3	Rationale	23
6.6.4	Guidance	23
6.6.5	Verification criteria	23
6.7	Secure logging and reporting - access control monitoring (authorized and unauthorized)	23
6.7.1	Applicability	23
6.7.2	Requirement	23
6.7.3	Rationale	23
6.7.4	Guidance	23
6.7.5	Verification criteria	24
6.8	Secure logging and reporting - anomaly detection	24
6.8.1	Applicability	24
6.8.2	Requirement	24
6.8.3	Rationale	24
6.8.4	Guidance	24
6.8.5	Verification criteria	24
6.9	Secure logging and reporting - detection of integrity violations	25
6.9.1	Applicability	25
6.9.2	Requirement	25
6.9.3	Rationale	25
6.9.4	Guidance	25
6.9.5	Verification criteria	25
6.10	Secure logging and reporting - secure logging mechanisms	25
6.10.1	Applicability	25
6.10.2	Requirement	25
6.10.3	Rationale	25
6.10.4	Guidance	25
6.10.5	Verification criteria	26
6.11	Secure logging and reporting - report logs & events	26
6.11.1	Applicability	26
6.11.2	Requirement	26
6.11.3	Rationale	26
6.11.4	Guidance	26
6.11.5	Verification criteria	26

6.12	User access management - authentication authorization	26
6.12.1	Applicability	26
6.12.2	Requirement	27
6.12.3	Rationale	27
6.12.4	Guidance	27
6.12.5	Verification criteria	27
6.13	User access management - role-based access control (RBAC)	27
6.13.1	Applicability	27
6.13.2	Requirement	27
6.13.3	Rationale	27
6.13.4	Guidance	28
6.13.5	Verification criteria	28
6.14	Diagnostics access management - authentication authorization	28
6.14.1	Applicability	28
6.14.2	Requirement	28
6.14.3	Rationale	28
6.14.4	Guidance	28
6.14.5	Verification criteria	29
6.15	Diagnostics access management - role-based access control	29
6.15.1	Applicability	29
6.15.2	Requirement	29
6.15.3	Rationale	29
6.15.4	Guidance	29
6.15.5	Verification criteria	29
6.16	Data confidentiality - secure data at rest	30
6.16.1	Applicability	30
6.16.2	Requirement	30
6.16.3	Rationale	30
6.16.4	Guidance	30
6.16.5	Verification criteria	30
6.17	Data confidentiality - secure data in transit	30
6.17.1	Applicability	30
6.17.2	Requirement	30
6.17.3	Rationale	30
6.17.4	Guidance	31
6.17.5	Verification criteria	31
6.18	Data integrity - secure data at rest	31
6.18.1	Applicability	31
6.18.2	Requirement	31
6.18.3	Rationale	31
6.18.4	Guidance	31
6.18.5	Verification criteria	31
6.19	Data integrity - secure data in transit	32
6.19.1	Applicability	32
6.19.2	Requirement	32
6.19.3	Rationale	32
6.19.4	Guidance	32
6.19.5	Verification criteria	32
6.20	Data minimisation	32
6.20.1	Applicability	32
6.20.2	Requirement	32
6.20.3	Rationale	32
6.20.4	Guidance	33
6.20.5	Verification criteria	33
6.21	Cybersecurity resilience - availability	33
6.21.1	Applicability	33
6.21.2	Requirement	33
6.21.3	Rationale	33
6.21.4	Guidance	33

6.21.5	Verification criteria.....	33
6.22	Cybersecurity resilience - denial of service protection.....	34
6.22.1	Applicability.....	34
6.22.2	Requirement.....	34
6.22.3	Rationale.....	34
6.22.4	Guidance.....	34
6.22.5	Verification criteria.....	34
6.23	Network protection.....	34
6.23.1	Applicability.....	34
6.23.2	Requirement.....	34
6.23.3	Rationale.....	34
6.23.4	Guidance.....	34
6.23.5	Verification criteria.....	35
6.24	Secure by design.....	35
6.24.1	Applicability.....	35
6.24.2	Requirement.....	35
6.24.3	Rationale.....	35
6.24.4	Guidance.....	35
6.24.5	Verification criteria.....	35
6.25	Defence in depth.....	36
6.25.1	Applicability.....	36
6.25.2	Requirement.....	36
6.25.3	Rationale.....	36
6.25.4	Guidance.....	36
6.25.5	Verification criteria.....	36
6.26	Cryptography.....	36
6.26.1	Applicability.....	36
6.26.2	Requirement.....	36
6.26.3	Rationale.....	36
6.26.4	Guidance.....	37
6.26.5	Verification criteria.....	37
7	Product Lifecycle.....	37
7.1	Rational.....	37
7.2	Development phase.....	37
7.2.1	Design phase.....	37
7.2.2	Implementation phase.....	37
7.2.3	Verification phase.....	37
7.2.4	Validation phase.....	38
7.2.5	Conformity assessment phase.....	38
7.3	Production phase.....	38
7.4	Operation phase.....	39
7.5	Decommissioning phase.....	39
7.6	Work products.....	39
8	Vulnerability requirements.....	40
8.1	Objectives.....	40
8.2	Prerequisites.....	40
8.3	Vulnerability monitoring requirements.....	40
8.4	Vulnerability analysis requirements.....	41
8.5	Vulnerability handling requirements.....	41
8.6	Vulnerability disclosure requirements.....	42
8.7	Work products.....	42
9	Supplier handling (or third-party development).....	42
9.1	Objectives.....	42
9.2	Prerequisites.....	43
9.3	Requirements for the integration of off-the-shelf components.....	43
9.4	Requirements for the integration of open-source components.....	43
9.5	Requirements for component developed by supplier.....	44

9.6	Work products	44
10	Documentation	45
10.1	General.....	45
10.2	Product design documentation.....	45
10.3	Production documentation.....	45
10.4	Vulnerability handling documentation	45
10.5	Release documentation.....	46
Annex A (informative) Role definitions		47
Annex B (informative) Example of damage scenarios and mitigations with impact rating types.....		49
Annex C (informative) Example of cybersecurity goals and requirements		52
Annex D (informative) Mapping of ISO/SAE 21434 work products to ISO 24882 work products.....		54
Annex ZA (informative) Relationship between this European Standard and the essential requirements of Regulation 2023/1230/EU aimed to be covered.....		56
Bibliography		60

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity, or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement except for the ones mentioned in this Foreword.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Joint Working Group JWG 12, *Cybersecurity Engineering* which includes: ISO/TC 23/SC 19 - ISO/TC 127/SC 3 - ISO/TC 82 WG: *Cybersecurity engineering* in collaboration with Technical Committee CEN/TC 144, *Tractors and machinery for agriculture and forestry* in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement), both of which have DIN as their secretariat.

This document was prepared under a mandate given to CEN and CENELEC by the European Commission and the European Free Trade Association and supports essential requirements of EU Regulations.

For relationship with EU Regulations, see the informative [Annex ZA](#), which is an integral part of this document.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and Switzerland.

Introduction

In today's increasingly interconnected world, the agricultural machinery, tractors, and earth-moving machinery sector is becoming more reliant on technology and automation to improve efficiency, productivity, and sustainability. Agricultural machinery, tractors, and earth-moving machinery have evolved to incorporate advanced electronic systems, software, and communication technologies. These advancements have brought about significant benefits, but they have also introduced new vulnerabilities and risks associated with cybersecurity.

This document addresses the cybersecurity aspects in engineering of agricultural machinery, tractors, and earth-moving machinery. By ensuring appropriate consideration of cybersecurity, this document aims to enable the engineering of agricultural machinery, tractors, and earth-moving machinery to keep up with state-of-the-art technology and evolving attack methods specific to the agricultural industry.

This document provides vocabulary, objectives, requirements, and guidelines related to cybersecurity engineering.

ISO/IEC Guide 51 has been considered as far as practicable at the time of drafting of this document.

This standard is a Type C standard.

Agricultural machinery, tractors, and earth-moving machinery – Product cybersecurity

1 Scope

This document defines process requirements for cybersecurity risk identification, risk handling, and vulnerability handling for risks to the user. It addresses risks arising from cybersecurity threats, including intentional malicious actions by external parties, while taking into account the operational environment and assets requiring protection. These process requirements apply to the programmable electronic system for a product (machine or component).

These process requirements apply during the product lifecycle (product development, production, operations, and decommissioning phases).

These process requirements apply to remote data processing solutions only when they are essential to the product's functionality (e.g. remote precision farming). However, back-end services are beyond the scope of this standard. For guidelines regarding back-end services, refer to enterprise solution standards.

This document additionally defines common language for communications about cybersecurity risks.

This document includes examples of cybersecurity damage scenarios, risk mitigation, and possible technical solutions that are typical for the agricultural machinery, tractor, and earth-moving machinery industry.

This document includes activities that also apply to suppliers or third-party companies that are providing the product or components for the end product.

This document applies to agricultural machinery, tractors, earth-moving machinery, construction machinery, mining machinery, and forestry machinery.

NOTE This document can also be used to assess the cybersecurity engineering requirements for other off-road mobile machinery.

2 Normative references

There are no normative references in this document.

3 Terms and Definitions and Abbreviated Terms

3.1 Terms and Definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1.1

asset

valuable attributes of the system of interest reviewed in cybersecurity risk assessment

3.1.2

component

part that is a logically and technically separable entity, which provides resources in a product

3.1.3

controller area network (CAN)

serial communication technology covering the data link layer and the physical coding sublayer

Note 1 to entry: Definition derived from [\[1\]](#) ISO 11898-1:2024

3.1.4

cybersecurity control

procedural or technical measure that modifies the cybersecurity risk

EXAMPLE Access control or data encryption

3.1.5

cybersecurity development interface agreement (CDIA)

Cybersecurity agreement between customer and supplier in which the responsibilities for cybersecurity activities to be performed, evidence to be reviewed, or work products to be exchanged by each party related to the cybersecurity development of items or elements are specified

3.1.6

cybersecurity event

cybersecurity change that may have an impact on operation

3.1.7

cybersecurity goal

higher-level intention for what to do to secure the system

Note 1 to entry: Throughout this document, when the term "goal" is used alone, it refers to a cybersecurity goal.

3.1.8

cybersecurity incident

event that has an impact on the cybersecurity properties of an asset and is being exploited

Note 1 to entry: Throughout this document, when the term "incident" is used alone, it refers to a cybersecurity incident.

3.1.9

cybersecurity support period

time period during which the manufacturer will monitor and handle cybersecurity vulnerabilities

3.1.10

damage scenario

adverse consequence involving a machine or function that affects a user

3.1.11

impact

magnitude of harm that can result from the exploitation of a vulnerability

3.1.12

impact rating

assigned value for a comparative assessment of the impact

3.1.13

likelihood

measure of the probability or frequency of a specific threat or event

3.1.14

likelihood rating

assigned value for a comparative assessment of the likelihood

3.1.15

off-the-shelf

product or system already developed and available

3.1.16

product

machine, system, sub-system, or component

Note 1 to entry: A product comprises all electronic equipment and software realizing a specific function. Several systems can interact with each other in a product to fulfil its overall function.

3.1.17

product lifecycle

description of all stages of the product throughout its life starting from the expression of its need until the disposal

3.1.18

remote data processing

data processing at a distance the absence of which prevents the product from performing one of its functions

Note 1 to entry: The data processing on the product is not remote data processing.

3.1.19

risk

potential for damage caused by a cybersecurity event on a system of interest expressed as a combination of the impact and the likelihood of that event to occur

Note 1 to entry: Throughout this document, when the term "risk" is used alone, it refers to a cybersecurity risk.

3.1.20

risk assessment

process of identifying, analysing, and evaluating risks for a system of interest

3.1.21

risk mitigation

process of selecting and implementing control measures to modify risks to be within tolerable levels

3.1.22

risk rating

assigned value for a comparative assessment of the risk

Note 1 to entry: Risk rating is based on the potential for the impact of an event (impact rating) and the probability of that event to occur (likelihood rating).

3.1.23

risk treatment

process of deciding to reduce a risk, avoid a risk, share a risk, or retain a risk

3.1.24

system of interest

portion of the product that is being analysed in a cybersecurity risk assessment

EXAMPLE Transmission system or hitch system

Note 1 to entry: In^[2] ISO/SAE 21434:2021 this is analogous to "Item" definition, in^[3] EN ISO 25119-1:2023 & A1:2023 this is analogous to "Unit of Observation" definition, and in^[4] EN ISO 19014-1:2018 this is analogous to "machine control system" definition.

3.1.25

threat

cybersecurity event that has the potential to cause harm to an asset

3.1.26

threat scenario

potential cause of compromising the confidentiality, integrity, or availability in order to realize a damage scenario

3.1.27

vulnerability

weakness in a system of interest that can be exploited by a threat

3.2 Abbreviated Terms

API	application programming interface
CAN	controller area network
CMAC	cipher-based message authentication code
CPU	central processing unit
CVE	common vulnerabilities and exposures
DOS	denial of service
ECU	electronic control unit
ENISA	European Union agency for cybersecurity
HMAC	hashed-based message authentication code
HSM	hardware security module
IDS	intrusion detection system
PIN	product identification number
OEM	original equipment manufacturer
SAE	Society of Automotive Engineers
SSH	secure shell
TLS	transport layer security
TPM	trusted platform module
UDS	unified diagnostic services
XCP	universal measurement and calibration protocol

4 General considerations

The cybersecurity process described in this document is from the perspective of a product during all phases of the product's lifecycle to ensure an appropriate level of security.

A product consists of various components (e.g. the engine, wheels, and ECUs). Together all components are used to fulfil the functions of a product (e.g. Driving and Remote Data Processing). In [Figure 1](#), the product (e.g. a tractor) consists of two functions (Function: Driving and Function: Remote Data Processing). The Function: Driving contains the components wheel, engine, gearbox, Engine Control Unit and Transmission Control Unit. The Function: Remote Data Processing contains the Telemetry Unit. The manufacturer (OEM) defines the system of interest as shown in [Figure 1](#) including the Engine Control Unit, Transmission Control Unit, Telemetry Unit and messages between the ECUs.

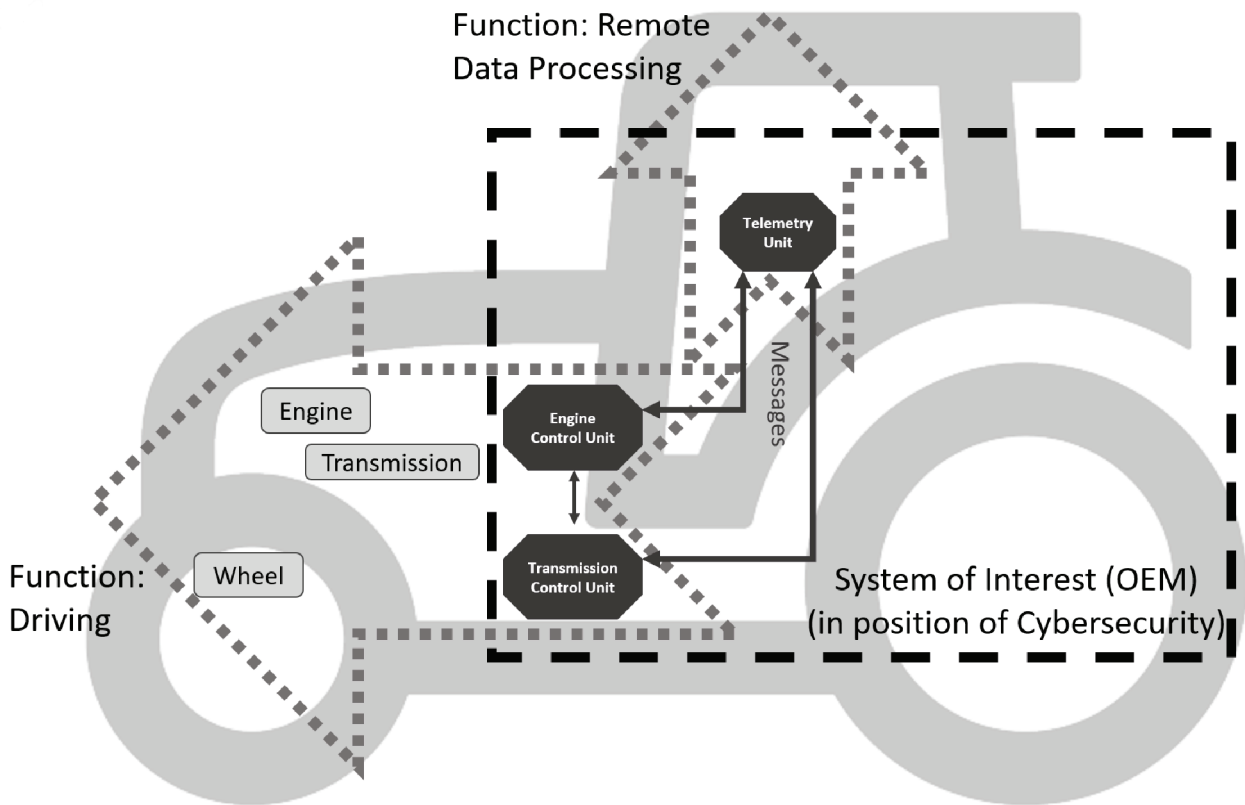


Figure 1 — Product with OEM system of interest identification

The product and the corresponding system of interest may vary between the OEM and a supplier. For a supplier, the product may be a single ECU which will be part of an overall OEM product function (e.g. Function: Driving) as shown in [Figure 2](#). The supplier defines the system of interest as shown in [Figure 2](#) including only the Telematics Unit and messages between the ECUs.

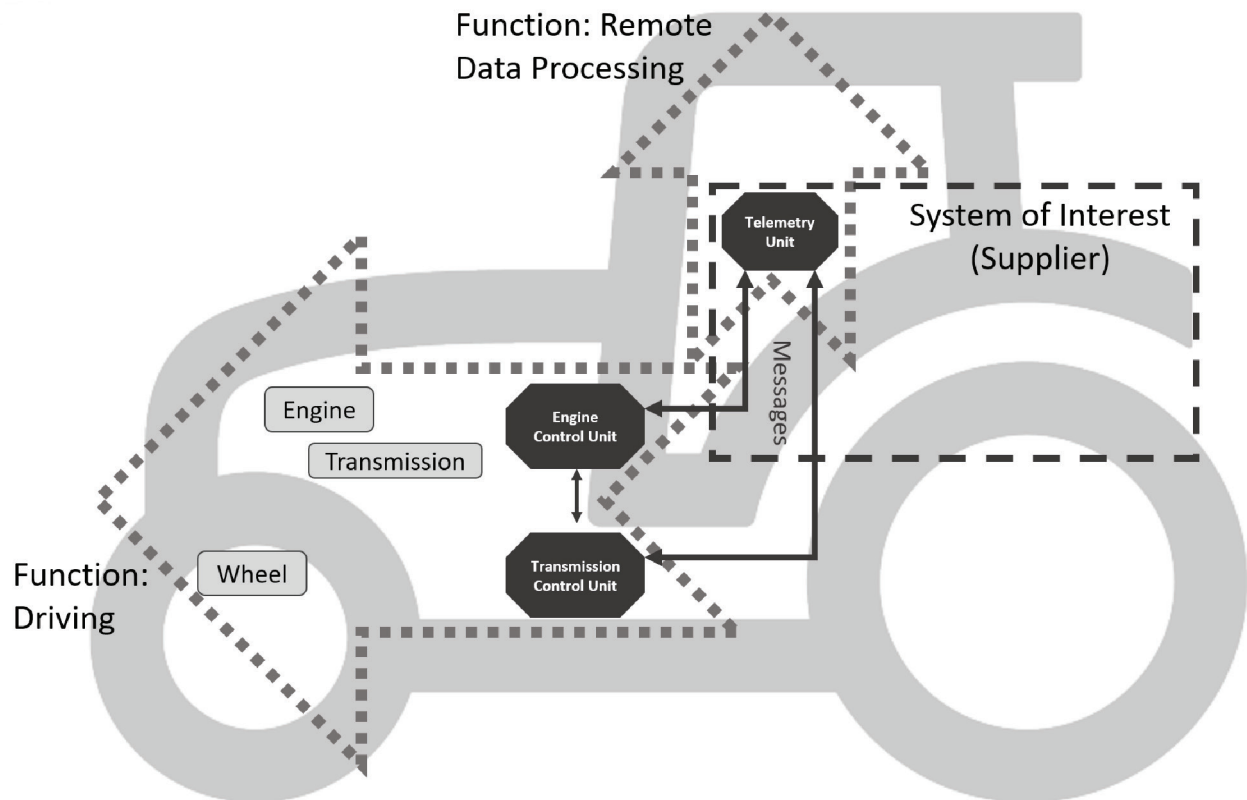


Figure 2 — Product with supplier system of interest identification

To determine if a system of interest is cybersecurity relevant, an initial assessment can be performed using the decision diagram shown in [Figure 3](#). If the candidate system of interest is determined to be cybersecurity relevant, then the risk assessment process defined in [clause 5](#) shall be applied. [Clause 5](#) describes the risk assessment process in detail and covers the requirements and work packages for asset identification, impact rating, threat scenario identification, risk rating and risk treatment decision.

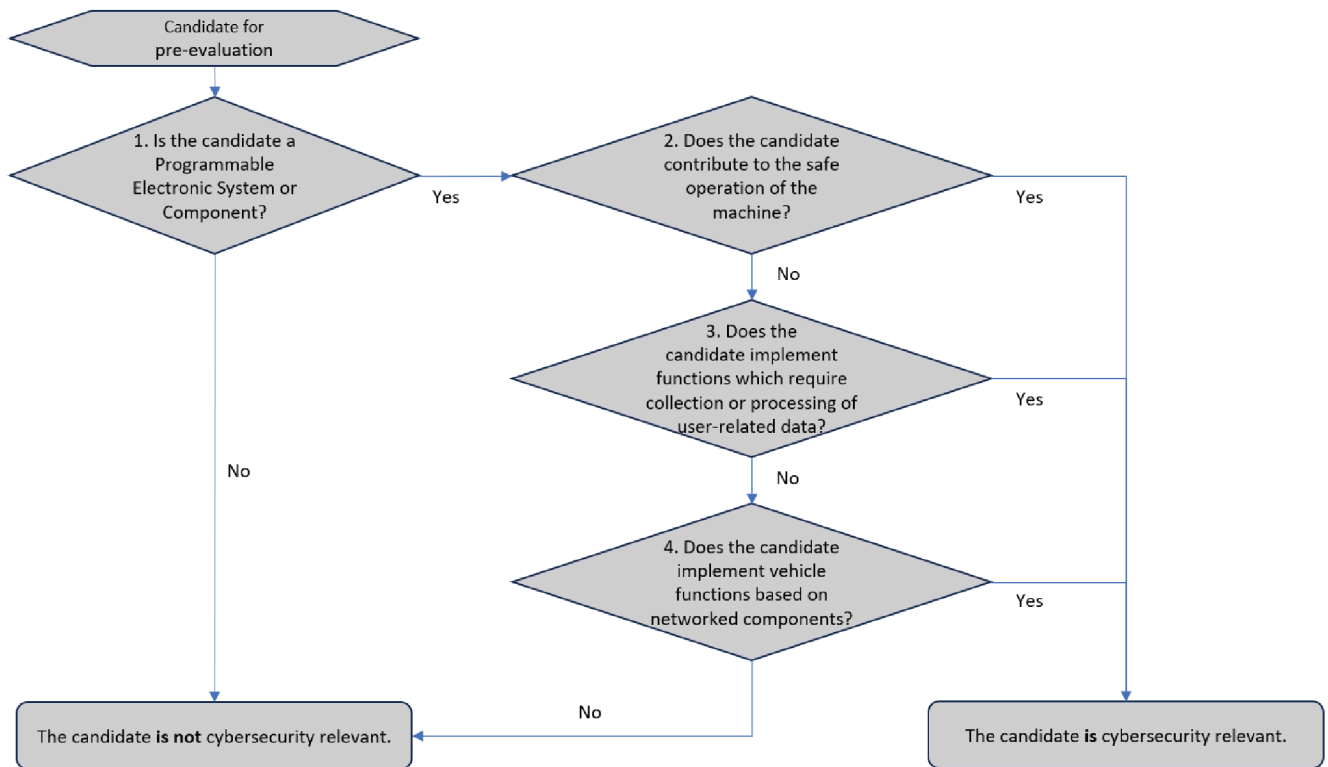


Figure 3 — Cybersecurity relevancy decision diagram

Examples of cybersecurity relevant system of interest candidates:

- Safety related parts of a control system for use on agricultural and earth-moving machinery (e.g. [3] EN ISO 25119-1:2023 & A1:2023 or [4] EN ISO 19014-1:2018);
- Data related to operators or personnel, or to potentially sensitive information such as geolocation of machinery, field boundaries, or construction site layouts;
- Internal connections -- CAN (Controller Area Network), Ethernet, serial communication (e.g. RS-485), or TCP/IP for machine-to-machine communication;
- Interface to fleet management or telematics server; cellular or satellite telecommunications network, diagnostic interface;
- Wireless connected sensors or actuators – remote start/stop systems, RFID for operator authentication, or soil moisture sensors and load monitoring systems.

The cybersecurity process shall be applied throughout the supply chain to support the security engineering. The security activities can be tailored to accommodate the needs of a specific situation. Manufacturer / supplier for a specific system of interest agree on the responsibility-split for the applicable security activities.

The manufacturer may define roles that are accountable and responsible for the activities and work products defined by the standard and to allocate those roles accordingly with sufficient resources and responsibility. [Annex A](#) includes examples of roles that can exist in an organisation.

NOTE 1 Involving individuals from different disciplines often provides valuable input.

The vulnerability and incident handling processes specified in [Clause 8](#) shall be applied as a means to define the appropriate activities in case a weakness is identified in a system of interest.

[Figure 4](#) describes the relationship between the terminology used throughout this document.

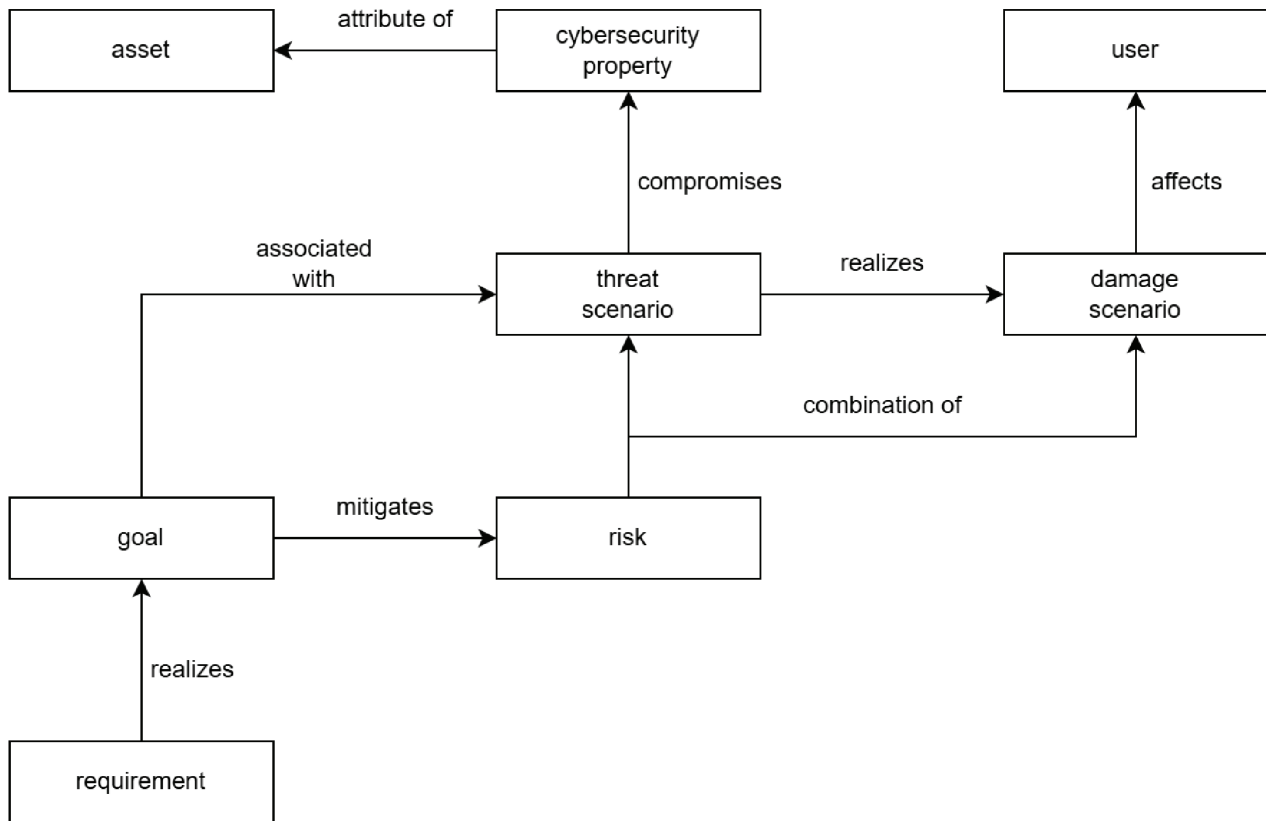


Figure 4 — Relationship between the document terminologies

NOTE 2 Some work products of [\[2\]](#) ISO/SAE 21434:2021 can be utilized to create work products for this document. See [Annex D](#).

5 Risk assessment for the system of interest

5.1 Risk assessment introduction

The system of interest shall have a risk assessment performed and risk treatments shall be identified per [clause 5](#). The risk assessment may be performed at different levels of a machine. For example, a risk assessment may be done at the highest level of the machine considering the whole machine and external interfaces. At a lower level, a risk assessment may be done on a sub-system of the machine such as steering system, power train system, functional component, etc. For a product, all cybersecurity relevant sub-systems shall be evaluated. Reference [Annex A](#) to understand the roles that should be included in a risk assessment.

The risk assessment typically includes the work products and sequence flow as shown in [Figure 5](#).

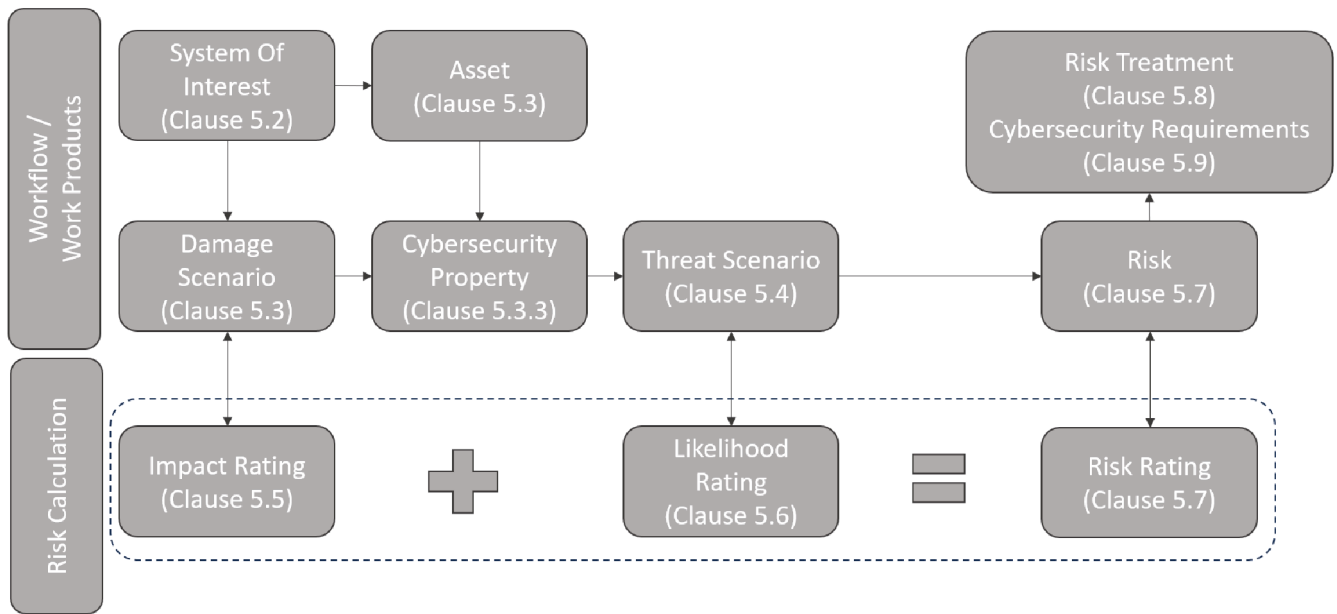


Figure 5 — Risk assessment sequence diagram

5.2 System of interest identification

5.2.1 General

For the risk assessment, identify and document the boundary of the system of interest, including the components, interfaces, functions, and architectures that are within the boundary.

5.2.2 Prerequisites

The prerequisites can include but are not limited to:

- Description of the system of interest (e.g. machine or sub-system), functions and use cases (e.g. tractor or steering system);
- Functional diagrams (e.g. system architecture diagram, function, data flow, interfaces);
- Safety related parts of control system (e.g. safety related modules, functions, interfaces);
- Diagnostic specifications (e.g. available services);
- Network architecture and message specifications.

5.2.3 Requirements

The following information shall be identified and documented for the system of interest:

- a) A boundary diagram or description to identify the interfaces/data and to clarify what elements are part of the system being analysed.
- b) A functional diagram or description to identify the intended purpose of the system of interest.
- c) A data flow diagram or description to identify the cybersecurity relevant data flow.

Items a) through c) above shall include the following details:

- List of diagnostic services that can be used to access/manipulate internal data (if exists);

- List of assets that include/embed/contribute to any functional safety control (if exists);
- List of assets that include/embed/contribute to any function the absence of which can have negative satisfaction to user (if exists).

5.2.4 Work products

The work products of [clause 5.2](#) shall include:

- **[WP-5.2-01]** Boundary diagram and/or description;
- **[WP-5.2-02]** Functional diagram and/or description;
- **[WP-5.2-03]** Data flow diagram and/or description.

NOTE The [5.2.4](#) items will include the diagnostics services and assets identified in [clause 5.2.3](#).

5.3 Assets, damage scenario identification

5.3.1 General

Identify the assets and damage scenarios within the system of interest that may require cybersecurity protection.

5.3.2 Prerequisites

The following work products shall be available:

- Boundary diagram and/or description **[WP-5.2-01]**;
- Functional diagram and/or description **[WP-5.2-02]**;
- Data flow diagram and/or description **[WP-5.2-03]**.

5.3.3 Requirements

The damage scenario shall be identified. The list of damage scenarios should include:

- items such as, but not limited to, interrupting core product functions or essential services, stealing, manipulating, depriving, or deleting personal or other data / software; and
- at least the impact categories safety, financial, privacy, and availability for the user.

The manufacturer shall identify the asset(s) that can be the target of an attack to realize any identified damage scenario.

Each identified asset shall be assigned one or more cybersecurity properties (e.g. confidentiality, integrity, availability). Additional specific properties can be used (e.g. authorization, authenticity, non-repudiation, freshness).

NOTE 1 A pre-defined list (e.g. damage scenarios, assets) can be created, maintained, and updated periodically by the manufacturer.

NOTE 2 Asset list can include items such as:

- Any data flow from an external connection interface that can be exploited to lead to a damage scenario;
- Any commands, calibration, settings, configuration data which rest in the system of interest or is in transit to or from the system of interest that, if manipulated, can lead to a damage scenario;
- Any personal data at rest or in transit to the system of interest;
- Any hardware or software components related to core product functionality and safety of the system of interest.