Guide to application of the Machinery Regulation (EU) 2023/1230

Annex III, 1.1.9 and 1.2.1(a) & (f)- protection against corruption

Final version – 18 October 2026

Note that references to other paragraphs (§xx) are references to the paragraph numbers in the current guide for the Machinery Directive Edition 2.3 – April 2024.

1.1.9. Protection against corruption

The machinery or related product shall be designed and constructed so that the connection to it of another device, via any feature of the connected device itself or via any remote device that communicates with the machinery or related product does not lead to a hazardous situation.

A hardware component transmitting signal or data, relevant for connection or access to software that is critical for the compliance of the machinery or related product with the relevant essential health and safety requirements shall be designed so that it is adequately protected against accidental or intentional corruption. The machinery or related product shall collect evidence of a legitimate or illegitimate intervention in that hardware component, when relevant for connection or access to software that is critical for the compliance of the machinery or related product.

Software and data that are critical for the compliance of the machinery or related product with the relevant essential health and safety requirements shall be identified as such and shall be adequately protected against accidental or intentional corruption.

The machinery or related product shall identify the software installed on it that is necessary for it to operate safely, and shall be able to provide that information at all times in an easily accessible form.

The machinery or related product shall collect evidence of a legitimate or illegitimate intervention in the software or a modification of the software installed on the machinery or related product or its configuration.

Prefix for complete section 1.1.9

Section 1.1.9. specifies requirements for the protection of machinery against unauthorised or harmful modification of the integrity or authenticity ("corruption" / “manipulation”) of all signals or data that are safety-relevant within the meaning of the Machinery Regulation.

This requires an assessment of the risks arising from the accidental or intentional corruption of the machinery.

The assessment involves analysing the machinery’s exposure and vulnerabilities, as well as the relevant threats, to identify measures that will prevent hazardous situations throughout its lifecycle.

DRAFT

Examples of typical exposures include remote access, cloud connectivity and unprotected interfaces.

In general, the section covers safety related aspects. It does not cover the confidentiality of data or intellectual property.

This guide does not include any further general guidance related to cyber security requirements or business continuity.

§1: *The machinery or related product shall be designed and constructed so that the connection to it of another device, via any feature of the connected device itself or via any remote device that communicates with the machinery or related product does not lead to a hazardous situation*

Section 1.1.9 Paragraph 1 requires that the direct or indirect connection of the machinery or related product to another device must not lead to a hazardous situation.

- "*connection*" means both a physical connection (e.g. the insertion of a plug) and a logical connection (e.g. the establishment of a network connection) and wireless as well as wired connections. This includes both temporary and permanent connections.
- "*another device*" means both stand-alone devices (e.g. another machine or a network switch) and devices that are external to the machinery or related product (e.g. a remote control, a programming device or a portable HMI).
- "*indirect*" means that the connection is not made directly, but via one or more other devices, e.g. via a network.
- "*not leading to a hazardous situation*" means that the residual security risk to be considered, in particular for harm, must be reduced by security measures (inherent and if not possible technical measures) to an acceptable level comparable to the accepted residual safety risk. This means that the health and safety requirements can be expected to be met throughout the entire lifecycle of the machinery or related product, considering reasonably foreseeable (malicious) attempts by third parties to corrupt signals or data (see Annex III, 1.2.1, a)). Appropriate measures have to be applied to reduce security risk(s) to an acceptable level.

Intentional modifications (e.g. by cyber-attacks) must therefore be considered. This means that connections that are not accessible or only accessible to a limited extent in the context of intended use (and reasonably foreseeable misuse), e.g. debug connections on a circuit board in a housing, may also have to be considered. This is particularly relevant if it is expected that someone will use them, e.g. on a publicly accessible machine.

As a guideline, additional information security methods and measures, as well as specific assumptions (e.g. regarding the threat situation), are required for risk assessment and reduction based on data corruption: All data flows and their communication paths that could lead to a hazardous situation must be identified.

Interfaces that can be accessed over public networks during the intended use or foreseeable misuse, e.g. network sockets require special attention.

DRAFT

The machinery or related product is not required to maintain normal operation in the event of an accidental or intentional corruption. It can also switch to a safe state, e.g. "stopped".

§2, first sentence: *A hardware component transmitting signals or data, relevant for connection or access to software that is critical for the compliance of the machinery or related product with the relevant essential health and safety requirements shall be designed so that it is adequately protected against accidental or intentional corruption.*

Paragraph 2 specifies requirements for safety-relevant hardware components that transmit signals or data and provide the connection to other devices (see paragraph 1) or access to safety-relevant software.

The transmission includes the routing of data to the targeted software application and authorization to access data (e.g., programming, configuring, writing, changing, reading passwords). The hardware components identified are, for example, remote controllers, safety controllers, remote maintenance devices for safety controllers and wireless sensors. There are also hardware components whose function is realised without software, but whose communication is nevertheless vulnerable, e.g. remote controls with discrete electronics.

"Safety-relevant" means that the component or software is of critical importance for compliance with the essential health and safety requirements.

The hardware component must be designed in such a way that it is adequately protected against unintentional or intentional violation of the integrity or authenticity ("corruption") of the transmitted signals and data.

Necessary countermeasures must be determined based on a threat assessment. As a rule, additional information security methods/measures and special assumptions, e.g. about the threat situation, are required to assess and reduce risks based on the corruption of data.

Countermeasures must comply with the order of priority for risk reduction set out in section 1.1.2 (b). If connection of another device to the machinery or related product or access via a remote access device is not required, access may be blocked as an inherent security measure.

One technical measure could be the use of a data diode, which only allows data to pass in one direction.

These measures are not limited to electronic means; e.g., the risk of intentional corruption can be mitigated by restriction of the accessibility of interfaces to authorized persons in the physical proximity of the machinery or related product. The countermeasures guarding a particular component against corruption may be provided by another component (security appliance, e.g. a firewall) of the machinery or related product.

If a connection or remote access is required, the machinery or related product should be delivered by the manufacturer in such a way that this is in a secure state (e.g. deactivated) in the delivery status (“security by default”), and the user manual describes which measures must be taken by the user to ensure secure access.

DRAFT

§2, second sentence: *The machinery or related product shall collect evidence of a legitimate or illegitimate intervention in that hardware component, when relevant for connection or access to software that is critical for the compliance of the machinery or related product.*

The machinery or related product must be designed in such a way that any legitimate or illegitimate intervention in the above-mentioned safety-relevant hardware (see first sentence) can be subsequently traced. To this end, appropriate state-of-the-art measures must be used to ensure that the intervention (e.g. tampering) can be traced. If the measures are based on logging, the storage period of the evidence must be designed to be reasonably long. In principle, the measures must be effective over the entire product life cycle.

The potential impact of a particular intervention must be assessed during the security risk assessment, to determine if it is critical for the compliance and thus covered by this requirement.

If supplemental safeguarding mechanisms are included in the communication protocol itself (e.g. black channel communication), then a corruption of the hardware component in the communication path may not impair the compliance of the machinery or related product. In this case, logging of evidence of legitimate or illegitimate intervention in that component is not required.

Measures can be based:

- on physical effects, e.g. security paint for screws, sealing stickers on housings or glued housings,
- on data processing, e.g. intrusion detection,
- on monitoring, e.g. continuous, independent camera monitoring with recording.

When the evidence of an intervention is collected through data processing or monitoring and is realised by external devices (for storage or monitoring) it must be ensured that the machinery or related product can only operate when the external data processing or monitoring is fully operational.

§3: *Software and data that are critical for the compliance of the machinery or related product with the relevant essential health and safety requirements shall be identified as such and shall be adequately protected against accidental or intentional corruption.*

Paragraphs 3 to 5 define requirements for software, paragraph 3 additionally for safety-relevant data:

Paragraph 3 requires that:

- safety-relevant software, e.g. the software of a safety controller or the firmware of a safety laser scanner, the operating system of a computer on which safety-relevant software is executed, and
- safety-relevant data, e.g. pressure sensor values or parameterised maximum speeds,

must be identified and indicated as such by the manufacturer and must be adequately protected against unintentional or intentional changes to integrity or authenticity (“corruption”).

"Safety-relevant" means that the software/data is critical for compliance with the relevant essential health and safety requirements.

DRAFT

"Adequate" in this context is to be understood to reduce the risk, based on foreseeable intentional or unintentional corruption, to an acceptable level.

Note: This may be achieved through state-of-the-art measures.

Necessary countermeasures must be based on the security risk assessment. As a rule, additional information security methods/measures and special assumptions, e.g. about the threats, are required to assess and reduce risks based on the corruption of data.

Countermeasures must comply with the order of priority for risk reduction set out in section 1.1.2 (b).

Examples of potential countermeasures for protection against accidental or intentional corruption are:

- protecting of service interfaces,
- signature verification upon software updating,
- cryptographic message authentication code,
- hashes,
- checksums (only protection against accidental corruption),
- organizational measures (special procedural instructions).

If the machinery or related product can be connected to public networks (within the scope of its intended use, through foreseeable misuse or accidentally) and safety-related systems can be affected as a result, the requirements for security protective measures are particularly high.

Manufacturers should pay particular care to the selection of security protective measures (e.g., state-of-the-art cryptographic measures) and validation of selected measures (e.g., penetration testing).

Critical software configuration files should not be accessible to the user or third parties through other means than those explicitly intended by the manufacturer (e.g., having proper access management/level) and be protected as determined in the risk assessment and according to the state of art.

§4: *The machinery or related product shall identify the software installed on it that is necessary for it to operate safely, and shall be able to provide that information at all times in an easily accessible form.*

The information about the installed safety-relevant software and, if available, integrity/authenticity checks, must be provided in an easily accessible form according to the state-of-the-art, e.g., on the machine's display or as an exportable file.

It should be ensured that the information provided is maintained at correct version and/or revision level.

"*At all times*" means that, whenever the information is required by a relevant user in connection with the intended use of the machinery or related product (e.g. an operator, service technician, manufacturer, or market surveillance authority), the machinery or related product is capable of providing it e.g., when it is powered on. This does not mean that the information needs to be visible at all times, but it means that the information can be provided e.g., on a screen, after an action by a relevant user such

as selecting a menu item or pressing an operating button. For example: the software identification feature should not disappear after placement on the market, should remain available throughout the service life of the machinery or related product, and should be retrievable during normal operation or maintenance activities.

"*Easily accessible*" means that access to the information does not require disproportionate effort. For example, the information should be obtainable through the means normally provided with the machinery or related product and for machinery it should not require special engineering tools, or complex multi-step procedures.

§5: *The machinery or related product shall collect evidence of a legitimate or illegitimate intervention in the software or a modification of the software installed on the machinery or related product or its configuration.*

Machinery (or related product) must maintain evidence of an intervention e.g.,

- intervention in the software that could have an impact on the safety and its related security (e.g. changes to safety program sequences or algorithms)
- change to this software (e.g. update of the firmware of the safety controller)
- change of its hardware or software configuration (e.g. process parameters, minimum and maximum values).

For example, the configuration which could have an impact on safety and security which is performed using hardware such as DIP switches or a potentiometer, can be traced either by the controller's software, or the integrity of the software can be confirmed by the hash or, alternatively, by a mechanical hardware seal that provides evidence of an intervention.

To this end, appropriate state-of-the-art measures should be used to ensure that all changes and safety-related interventions (authorised or unauthorised) can be traced and recorded.

"Appropriate" means that the procedure corresponds to the state of the art (see Guide to application of the Machinery Directive 2006/42/EC Edition 2.3, §161 and §162) and the recording of evidence should be designed to ensure that an attack or a data corruption can be traced retrospectively.

Dependent on the type of machinery or related product and the associated technical feasibility it might be necessary that supplementary information such as timestamps, counters, or details of the type of intervention (e.g. firmware update or configuration change) is collected and stored appropriately within or externally to, the machinery or related product.

Evidence of an intervention must be stored appropriately. If external devices are used for storage or monitoring, it must be ensured that the machinery or related product can only be operational when the external data processing or monitoring has stored all necessary evidence of an intervention successfully.

DRAFT

Prefix for section 1.2.1 (a) and (f)

Section 1.2.1(a) is closely linked to section 1.1.9 (Protection against corruption) and should be read together with it. In some cases, the same security countermeasures might be appropriate for compliance with both sections 1.1.9 and 1.2.1(a). Article 20(9) further provides for a presumption of conformity with sections 1.1.9 and 1.2.1 where the machinery or related product is covered by a cybersecurity certificate or statement of conformity issued under Regulation (EU) 2019/881.

1.2.1. Safety and reliability of control systems

Control systems shall be designed and constructed in such a way as to prevent hazardous situations from arising.

Control systems shall be designed and constructed in such a way that:

(a) they can withstand, where appropriate to the circumstances and the risks, the intended operating stresses and intended and unintended external influences, including reasonably foreseeable malicious attempts from third parties leading to a hazardous situation

Control systems must withstand malicious attempts, where these may affect the control system and lead to a hazardous situation. This is particularly relevant for control systems that can be connected directly or indirectly with external devices, networks or systems

Examples of such malicious attempts include but are not limited to unauthorised remote access to a safety-related part of the control system, unauthorised modification of software or configuration parameters, manipulation or corruption of safety-related data transmission, or the unauthorised use of a local interface, such as a maintenance port or removable media, to interfere with a safety function. Such attempts may exploit a networking capability but are not limited to it; they may also be carried out through other means e.g., supply chain, accessible service interfaces.

Influences and actions originating beyond previously identified limits to fulfil the health and safety requirements, for example, a third party with malicious intent that has no physical access to the machinery or related product, must nonetheless be taken into account where it could be reasonably foreseeable that those influences and actions could lead to a hazardous situation.

It is likely that for some circumstances and risks, security risk reduction measures should be applied. Common examples of security countermeasures to mitigate these risks are protection against unauthorised access, ensuring the authenticity and integrity of software updates, integrity protection of safety-related software, configuration and data, secure configuration management, and physical or logical protection of local service interfaces.

(f) the tracing log of the data generated in relation to an intervention and of the versions of safety software uploaded after the machinery or related product has been placed on the market or put into service is enabled for five years after such upload, exclusively to demonstrate the conformity of the machinery or related product with this Annex further to a reasoned request from a competent national authority.

DRAFT

As required in Annex III, Section 1.1.9, interventions and version changes to safety-related software (see 1.1.9, fifth paragraph) must be stored in a traceable manner.

1.2.1(f) states that the tracing log that is created during this process must be designed in such a way that, upon reasoned request (e.g. after an incident has occurred), the competent national authorities can verify the conformity of the machinery or related product with Annex III.

Each specific event must be stored for at least five years after a change in the safety software.

This requirement applies if there is a possibility of making changes to the safety software after it has been placed on the market or put into service. It is irrelevant who made the change and if this is intended or not. It must be ensured that the tracing log reflects the actual status of the safety-related software.

The tracing log should be stored in a reliable storage location.

DRAFT