# Combating vulnerabilities with standards: new EU cybersecurity rules

Security vulnerabilities in product software often go undetected. New EU regulations are set to change that. The Cyber Resilience Act and the Machinery Regulation set out clear requirements for the protection of control systems against accidental or intentional corruption. Standards bodies are now called upon to create a basis for secure and trustworthy technology in the European market, with consideration for the planned guidance document for the Machinery Regulation.

Every year, security researchers report thousands of IT vulnerabilities in products, ranging from backdoors in industrial control systems to radio controls that unquestioningly trust each and every transmitting party. Many users are not even aware of these security vulnerabilities, and to date, manufacturers have also had very little incentive to devote more resources to eliminating them. Following the market's failure to solve this problem, the European Commission responded with a comprehensive legislative package:

The Cyber Security Act sets out the mandate for the European Union Agency for Cybersecurity (ENISA). ENISA is intended to improve communication of vulnerabilities between reporting parties, manufacturers, operators and public authorities in Europe, and has set up a European database for this purpose.

The NIS-2 Directive defines obligations upon essential and important entities (organizations and companies) to make their network and information systems (NISs) secure, together with binding requirements for the reporting of security incidents. At present, several Member States are behind schedule with transposition of this directive into national law.

The Cyber Resilience Act (CRA) sets out manufacturers' obligations to avoid and deal with vulnerabilities. For example, the manufacturers' availability must be ensured by way of a facility for contact in an emergency. Several freely available specifications have been established for this communication channel. These define, for example, standardized provisions for describing the criticality of security vulnerabilities, and data formats for their description:

The RFC 9116 specification of the Internet Engineering Task Force (IETF) describes how companies can use a simple text file to store information available worldwide on who is to be informed of a vulnerability in an emergency. The CRA does not require a specific format for the list of software contained in the product (software

© DGUV/https://dguv.de/securitytxt_de

bill of materials, SBOM) that is to be generated by the manufacturer. The CycloneDX format and the open ISO/IEC 5692 standard, System Package Data Exchange, in particular, are currently meeting with wide acceptance. The SBOM can be used for automatic reporting of products containing software in which a security vulnerability has been detected. The ISO/IEC 20153 Common Security Advisory Framework (CSAF) has been established for the machine-readable recommendations required in the CRA. The significance of the CRA is also reflected in new work items. In the course of 2025 alone, around 40 proposals are to be voted on for new standards that are to be harmonized under the CRA.

### EU guidance document supports the safety requirements of the Machinery Regulation

The Machinery Regulation, which is addressed to manufacturers, requires in Annex III, Sections 1.1.9 and 1.2.1 that adequate protection against accidental or intentional corruption be assured from the design stage onwards. In addition, evidence of legitimate or illegitimate intervention must be collected.

The European Commission plans to publish, by January 2027 at the latest, a guide providing a practical explanation of the concepts and clarifying the obligations. One of the five working groups developing the guide is to deal with the sections on protection against corruption. The guide constitutes the interpretation of the Regulation and will therefore also provide important support for standardization activity.

### First components for protection against corruption now in place

Standardization work on prEN 50742 has been launched at CENELEC. This standard is to support the requirements of the Machinery Regulation for protection against corruption. It is intended to be compatible as far as possible with other security standards such as ISO/IEC 15408 (Common Criteria), EN 17640 (fixed-time cybersecurity evaluation methodology for ICT products) and IEC 62443 (security for industrial automation and control systems). It should also be suitable for application to an extremely wide product spectrum, from cordless screwdrivers to machine tools, lifting platforms and safety components. A committee draft (CD) of prEN 50742 is expected in the summer of 2025. Ideally, the standard should be completed in time for it to be harmonized before the Machinery Regulation becomes applicable on 20 January 2027.

The trend for IT security issues to be considered as well as safety issues is also evident from the revision of ISO 12100 on the safety of machinery. It is becoming apparent that the most effective approach is for all possible hazards first to be identified in a conventional risk analysis. This involves analysis of the hazards presented by the machine in the absence of protective measures. The measures are implemented in the next step. The protective measures themselves must be protected against corruption, to ensure that they are able to function reliably. The guiding principle is that accidental or intentional corruption must not give rise to new hazards. Reliable evaluation of signals, such as an emergency stop request, must also be taken into account. The Institute for Occupational Safety and Health of the DGUV (IFA) has analysed a range of machine control systems and determined that in many cases, the emergency stop function can be corrupted remotely with surprising ease.

Standardization must also address simultaneous corruption of a large number of machines. For example, failure of a single lift or petrol pump is relatively uncritical. By contrast, a comprehensive attack on all systems equipped with the same control system may have catastrophic consequences. Whereas simultaneous failure of systems due to wear and tear is highly unlikely, comprehensive corruption of all systems of a particular type constitutes a serious security scenario.

Companies are advised to implement the emergency contact facility described in RFC 9116 immediately as the first step. Research has also been documenting the key elements of future IT security standards for decades. The current challenge lies in finding a consensus on the socially acceptable risk and developing practical test specifications.

*Jonas Stein*
*Institute for Occupational Safety*
*and Health of the DGUV (IFA)*
*jonas.stein@dguv.de*

*Arne Sonnenburg*
*Federal Institute of Occupational*
*Safety and Health (BAuA)*
*sonnenburg.arne@baua.bund.de*