



# Safety & Security

**Giovanni B. Lucido**

Member CEI Technical Committee CT 321 „Smart Manufacturing-Industria 4.0“

General Manager Schmersal Italia Srl

General Manager Schmersal Schweiz AG



- 7 Produktionsstandorte
- 20 Tochtergesellschaften
- Mehr als 50 Handelsvertretungen



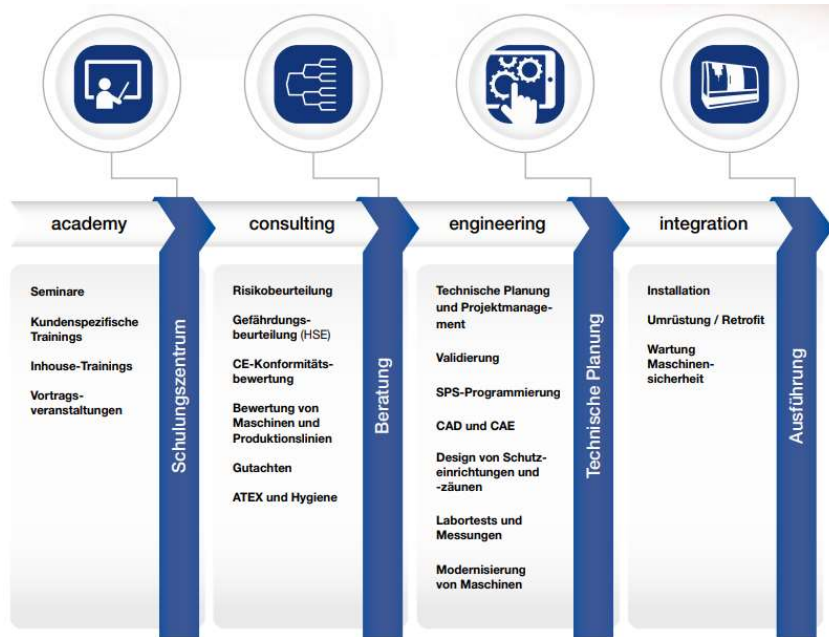


Technologies for our future



# Safety & Security

**tec.nicum**  
excellence in safety





## Regulations

A "Regulation" is a binding legislative act. It must be applied in its entirety across the E.U.

## Directives

A "Directive" is a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to devise their own laws on how to reach these goals.

1.1.2. **Principles of safety integration**

- (a) Machinery must be designed and constructed so that it is fitted for its function, and can be operated, adjusted and maintained without putting persons at risk when these operations are carried out under the conditions foreseen but also taking into account any reasonably foreseeable misuse thereof.

The aim of measures taken must be to eliminate any risk throughout the foreseeable lifetime of the machinery including the phases of transport, assembly, dismantling, disabling and scrapping.

- (b) In selecting the most appropriate methods, the manufacturer or his authorised representative must apply the following principles, in the order given:

- eliminate or reduce risks as far as possible (inherently safe machinery design and construction),
- take the necessary protective measures in relation to risks that cannot be eliminated,
- inform users of the residual risks due to any shortcomings of the protective measures adopted, indicate whether any particular training is required and specify any need to provide personal protective equipment.

- (c) When designing and constructing machinery and when drafting the instructions, the manufacturer or his authorised representative must envisage not only the intended use of the machinery but also any reasonably foreseeable misuse thereof.

The machinery must be designed and constructed in such a way as to prevent abnormal use if such use would engender a risk. Where appropriate, the instructions must draw the user's attention to ways — which experience has shown might occur — in which the machinery should not be used.

- (d) Machinery must be designed and constructed to take account of the constraints to which the operator is subject as a result of the necessary or foreseeable use of personal protective equipment.

- (e) Machinery must be supplied with all the special equipment and accessories essential to enable it to be adjusted, maintained and used safely.

The safety result, during the use of work equipment, depends on a combination of factors that are  
**CLEARLY EXPRESSED ABOVE**



## Machinery Directive **2006/42/CE**

Bullet point: Essential Health and Safety Requirements (E.H.S.R.)  
**(mandatory)**

### Objectives:

- Free circulation of goods
- The same Safety requirements for machinery in all Member States
- A high level of safety



## **For CE marking:**

- **Declaration of Conformity**
- **Technical File**
- **Instruction Manual**

**Guide to application of the Machinery Directive 2006/42/EC - Edition 2.2**

<https://ec.europa.eu/docsroom/documents/38022>

- **Electromagnetic Compatibility Directive (EMC): 2014/30/EU**  
Guide available: <https://ec.europa.eu/docsroom/documents/33601>
- **Radio Equipment Directive (RED): 2014/53/EU**  
Guide available: <http://ec.europa.eu/docsroom/documents/23321>
- **Low Voltage Directive (LVD) : 2014/35/EU**  
Ensures that electrical equipment within certain voltage limits provides a high level of protection for European citizens
- **ATEX Directive 2014/34/EU:** for explosive atmospheres

and more...



## Institutes for Technical Standards (voluntary)

International



Electrical



All others



Europe



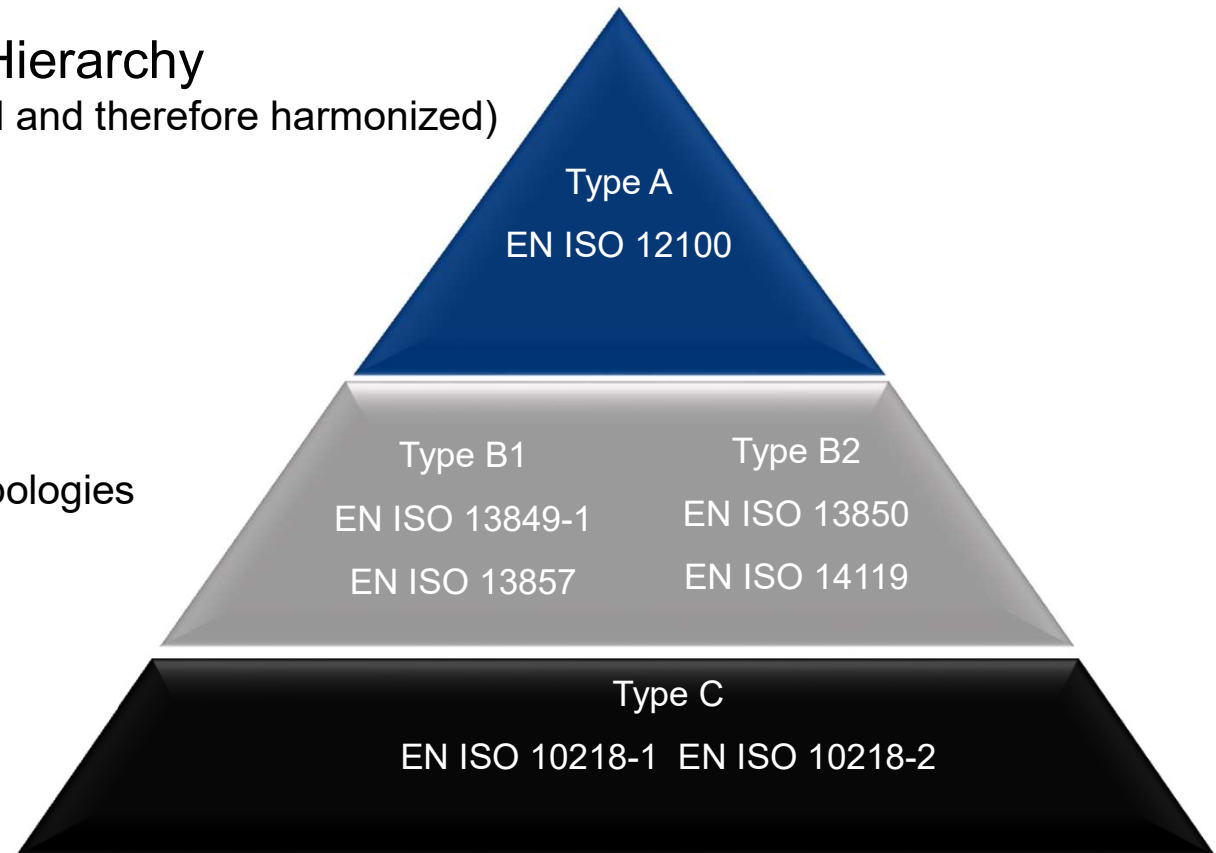
Italy




## Standards Hierarchy

(most published on official EU Journal and therefore harmonized)

- Type A: basic standards
- Type B: safety standards
  - B1 safety aspects
  - B2 protective devices
- Type C: standards for machine typologies



EUROPEAN STANDARD		<b>EN ISO 12100</b>
NORME EUROPÉENNE		
EUROPÄISCHE NORM		November 2010
ICS 13.110	Supersedes EN ISO 12100-1:2003, EN ISO 12100-2:2003, EN ISO 14121-1:2007	
English version		
<b>Safety of machinery - General principles for design - Risk assessment and risk reduction (ISO 12100:2010)</b>		
Sécurité des machines - Principes généraux de conception - Appréciation du risque et réduction du risque (ISO 12100:2010)		Sicherheit von Maschinen - Allgemeine Gestaltungsgrundsätze - Risikobeurteilung und Risikominderung (ISO 12100:2010)
This European Standard was approved by CEN on 9 October 2010.		
CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.		
This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.		
CEN members are the national standards bodies of 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, Switzerland and United Kingdom.		
		
EUROPEAN COMMITTEE FOR STANDARDIZATION COMITÉ EUROPÉEN DE NORMALISATION EUROPÄISCHES KOMITEE FÜR NORMUNG		
Management Centre: Avenue Marnix 17, B-1000 Brussels		
© 2010 CEN	All rights of exploitation in any form and by any means reserved worldwide. Ref. No. EN ISO 12100:2010 E for CEN national Members.	



## Safety & Security

---

- **ISO/TR 22100-1:2021** Safety of machinery - Relationship with ISO 12100 - Part 1: How ISO 12100 relates to type-B and type-C standards

**Provides assistance to the designer/manufacture of machinery and related components** as to how the system of existing type-A, type-B and type-C machinery safety standards should be applied in order to design a machine to achieve a level of tolerable risk by adequate risk reduction.

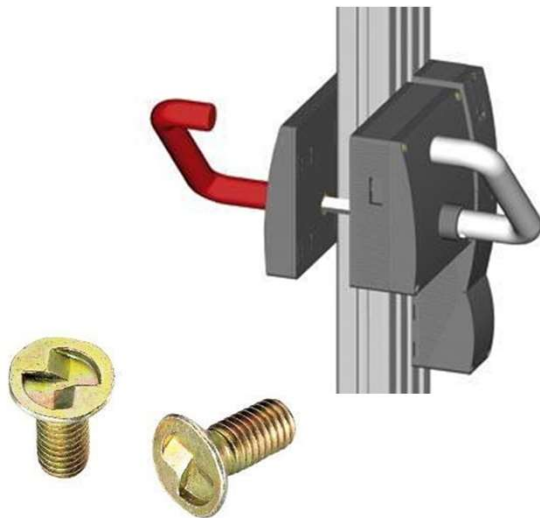
TR are important documents, but are no standards and are no harmonized, contain examples

No Presumption of Conformity

## More on the topic “Information for use”

- **EN ISO 20607:2019** Safety of machinery - Instruction handbook - General drafting principles
- **IEC/IEEE 82079-1:2019** Preparation of information for use (instructions for use) of products - Part 1: Principles and general requirements
- **UNI 10653:2003** Technical documentation - Quality Of Product Technical Documentation
- **UNI 11083:2003** Technical documentation – Guidelines for the preparation of useful documents for instruction and training in the use of goods
- **UNI/TS 11192:2006** Product Technical Documentation - Guidelines for classification
- **UNI ISO 15226:2007** Technical product documentation - Life cycle model and allocation of documents

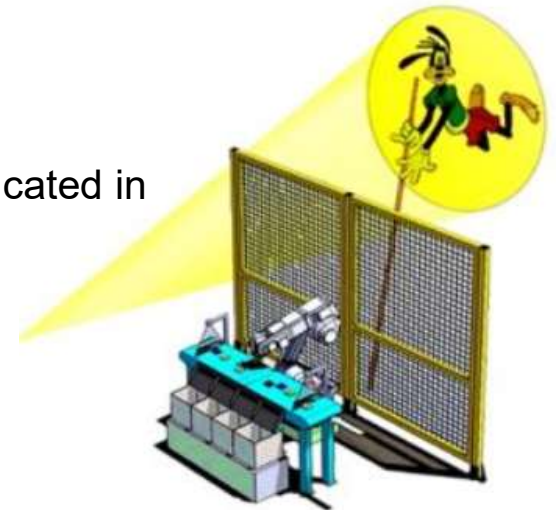
- **EN ISO 14119:** Safety of machinery - Interlocking devices associated with guards - Principles for design and selection  
Type B2 Standard



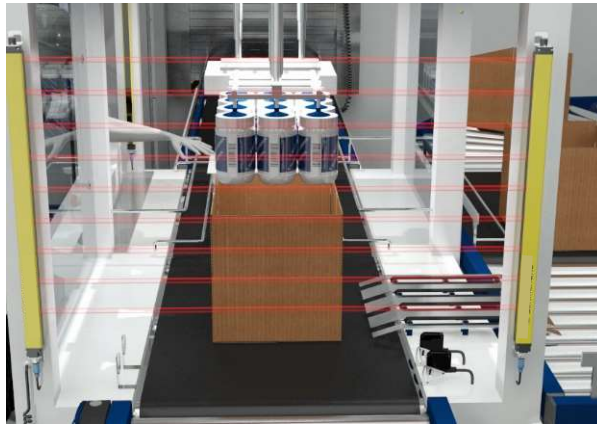
Focus on measures required to **minimize defeat possibilities**  
It is addressed to devices and machinery manufacturers

- **EN ISO 14120:** Safety of machinery - Guards - General requirements for the design and construction of fixed and movable guards  
Type B2 Standard
- **EN ISO 13857:** Safety of machinery - Safety distances to prevent hazard zones being reached by upper and lower limbs  
Type B1 Standard

Machine protective structures must be positioned with safety distances as indicated in  
**EN ISO 13857**



- **EN IEC 62046:2018** Application of protective equipment to detect the presence of persons  
This standard covers the application of electro-sensitive protective equipment (ESPE) specified in IEC 61496 (all parts) and pressure sensitive mats and floors specified in ISO 13856-1



- **IEC 61496-3:2018** Safety of machinery - Electro-sensitive protective equipment - Part 3: Particular requirements for Active Opto-electronic Protective Devices responsive to Diffuse Reflection(AOPDDR)



- **IEC 60204-1:2018** Safety of machinery - Electrical equipment of machines - Part 1: General requirements

Applies to electrical, electronic and programmable electronic equipment and systems to machines not portable by hand while working, including a group of machines working together in a co-ordinated manner.

- **IEC 61439-1:2020** Low-voltage switchgear and controlgear assemblies - Part 1: General rules
- **IEC 61439-2:2020** Low-voltage switchgear and controlgear assemblies - Part 2: Power switchgear and controlgear assemblies
- **ATTENTION: PARTIAL OVERLAP**



## MAIN STANDARDS ON MACHINERY SAFETY CONTROL SYSTEM

- **IEC 61511-1:2016+AMD1:2017 CSV** Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and application programming requirements
- **IEC 61508 (Parts 1 to 7)** Functional safety of electrical/electronic/programmable electronic safety-related systems
- **IEC 62061:2021** Safety of machinery - Functional safety of safety-related electrical, electronic and programmable control systems



Technologies for our future



## MAIN STANDARDS ON MACHINERY SAFETY CONTROL SYSTEM

- **ISO 13849-1:2015** Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design
- **ISO 13849-2:2012** Safety of machinery - Safety-related parts of control systems - Part 2: Validation
- **ISO 12100:2010** Safety of machinery - General principles for design - Risk assessment and risk reduction

Note: **Project ISO/IEC 17305 ED1** Safety of machinery - Safety functions of control systems  
has been discontinued



Technologies for our future



# Safety & Security

---

## MAIN STANDARDS ON MACHINERY SAFETY CONTROL SYSTEM

- **IEC TS 62988-1:2019** Safety of machinery - Safety-related sensors used for the protection of persons
- **IEC 61496 (series)** Safety of machinery - Electro-sensitive protective equipment
- **IEC 62745:2017** Safety of machinery - Requirements for cableless control systems of machinery



## Safety & Security

---

see also D.lgs. 81/2008 and INAIL if you are operating  
in Italy

see also SUVA if you are operating in Switzerland



- > Covid-19: misure adottate dall'Istituto
- > Covid-19: prodotti informativi
- > Avvisi e scadenze
- > News ed eventi
- > Sala Stampa
- > Campagne
- > Pubblicazioni
  - > **Catalogo Generale**
  - > Come acquisire una pubblicazione
  - > Dossier e Speciali
  - > Prodotti interattivi
  - > Rapporti e relazioni Inail
  - > Quaderni di ricerca
  - > Pubblicazioni del CIV
  - > Dati Inail
  - > Rivista Infortuni
  - > Bollettino trimestrale
  - > Superabile
  - > Multimedia

## Il defeating di un dispositivo di interblocco associato ai ripari

*Le linee di indirizzo contenute nella pubblicazione, edita nelle due lingue italiano e tedesco, sono state elaborate - dal gruppo di lavoro formato dal Laboratorio macchine ed attrezzature di lavoro del Dit dell'Inail insieme a Ministero del Lavoro, Gruppo Interregionale macchine e impianti, Federmacchine, UNI, UCIMA, Schmersal Italia S.p.A. - con l'intento di approfondire un argomento di grande rilevanza sociale e prevenzionale quale il defeating ovvero la neutralizzazione di un dispositivo con funzioni di sicurezza per macchine ed attrezzature di lavoro.*

Si configurano quindi come valido aiuto ai fabbricanti, datori di lavoro e progettisti che si confrontano con la necessità di utilizzare le prescrizioni contenute nella nuova edizione della norma entrata in vigore dal 1 maggio 2015.

Prodotto: Volume  
Edizioni: Inail - 2016  
Disponibilità: Sì - Consultabile anche in rete  
Info: [dcplanificazione-comunicazione@inail.it](mailto:dcplanificazione-comunicazione@inail.it)



> [Il defeating di un dispositivo di interblocco associato ai ripari](#)  
(.pdf - 14,4 mb)

Ultimo aggiornamento: 15/12/2016



## CH - SPECIFIC CONTENT

**suva**



**Avviamento inatteso di macchine e impianti**  
Lista di controllo

La vostra azienda ha adottato misure adeguate per evitare l'avviamento inatteso di macchine e impianti?

**Sono i pericoli principali:**

- rimessa in moto accidentale della macchina o dell'impianto
- accesso alla zona di pericolo della macchina senza aver prima disatteso ogni funzione particolare
- impossibilità di smaltire una funzione particolare
- disturbi avvertibili soprattutto durante l'installazione dei gasi, la riparazione, la pulizia o la manutenzione di una macchina.

Con la presente lista di controllo potete individuare meglio queste fonti di pericolo.



**Otto regole vitali per i manutentori**  
di macchine e impianti

**suva**

## CH - SPECIFIC CONTENT

### Allgemein Standardisierung (2), Wichtige Links

SNV (ISO/CEN Normen): [www.snv.ch](http://www.snv.ch)

SNV (Shop, ISO/CEN Normen): <https://shop.snv.ch>

Electrosuisse (IEC/CENELEC Normen): [www.electrosuisse.ch](http://www.electrosuisse.ch)

Electrosuisse (Shop, IEC/CENELEC Normen): [www.electrosuisse.ch/de/shop](http://www.electrosuisse.ch/de/shop)

ISO Normen (Stand der Normen):

<https://www.iso.org/standards-catalogue/browse-by-tc.html>

IEC Normen (Stand der Normen):

<https://www.iec.ch/technical-committees-and-subcommittees#tclist>

CEN Normen (Stand der Normen): <https://standards.cen.eu/dyn/www/f?p=CENWEB:6:::NO>

Switec Liste: [Neue harmonisierte Normen / SWITEC](#)





# Safety & Security

---

## SOME HINTS ON CYBERSECURITY



# Safety & Security

---

**Industrie**  
**:: 2025**



<https://www.industrie2025.ch/angebote/workshops/cybersecurity>



## Draft new machine regulation

### CONFORMITY OF THE MACHINERY

#### Article 17

1. .... Presumption of conformity of machinery products

.....

5. Machinery products that have been certified or for which a statement of conformity has been issued under a cybersecurity scheme adopted in accordance with Regulation (EU) 2019/881 and the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the essential health and safety requirements set out in Annex III, sections 1.1.9 and 1.2.1, as regards protection against corruption and safety and reliability of control systems in so far as those requirements are covered by the cybersecurity certificate or statement of conformity or parts thereof.

## Draft

### REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on machinery products

#### E.H.S.R. 1.1.9 - Protection against corruption

- The machinery 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 product does not lead to a hazardous situation.
- A hardware component for connection that is critical for the compliance of the machinery product with the relevant health and safety requirements shall be designed so that it is adequately protected against accidental or intentional corruption. The machinery product shall collect evidence of a legitimate or illegitimate intervention in the hardware component.

## Draft

### REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on machinery products

#### E.H.S.R. 1.1.9 - Protection against corruption

- Software and data that are critical for the compliance of the machinery product with the relevant health and safety requirements shall be identified as such and shall be adequately protected against accidental or intentional corruption.
- The machinery 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 product shall collect evidence of a legitimate or illegitimate intervention in the software or a modification of the software installed on the machinery product or its configuration.

## Draft

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on machinery products

E.H.S.R. 1.2.1 - Protection against corruption

### Changes to the requirement

- Control systems shall be designed and constructed in such a way that:  
they can withstand, where appropriate to the circumstances and the risks, the intended operating stresses and intended and unintended external influences, including malicious attempts from third parties to create a hazardous situation;
- The safety functions cannot be changed beyond the limits defined by the manufacturer in the machinery product risk assessment.

Draft

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on machinery products

E.H.S.R. 1.2.1 - Protection against corruption

Changes to the requirement

- **The tracing log of the data generated** in relation to an intervention and of the versions **of safety software** uploaded after the machinery 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 product with this Annex **further to a reasoned request from a competent national authority**;

## Draft

### REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on machinery products E.H.S.R. 1.2.1 - Protection against corruption

#### Changes to the requirement

- Particular attention shall be given to the following points:

.....

(c) modifications to the settings or rules, generated by the machinery product or by operators covering also the learning phase, shall be prevented, where such modifications may lead to hazardous situations;

.....

For autonomous mobile machinery products, the control system shall be designed to perform the safety functions by itself as set out in this section, even when actions are ordered by using a remote supervisory function.



## Human & Machine: Safety & Security

EN ISO 13849-1

EN IEC 62061

EN ISO 11161

EN ISO 12100



Safety: protects human from the machine



Security: protects machine from the human

IEC 62443  
(all parts)

ISO TR 22100-4

IEC TR 63074

ISO TR 22053

## MAIN STANDARDS ON IACS (INDUSTRIAL AUTOMATION CONTROL SYSTEM)

- **IEC 62443-3-2:2020** Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design
- **IEC 62443-3-2:2013** Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels
- **IEC TR 63074:2019** Safety of machinery - Security aspects related to functional safety of safety-related control systems
- **IEC TR 22100-4:2018** Safety of machinery - Relationship with ISO 12100 - Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects

Primary aspect: Human's Safety

**Machinery Directive  
2006/42/CE**



Secondary aspect: Data's Security

**WARNING:  
a compromised parameter  
could become a SAFETY  
related problem**

IEC 62443-2-4:2015 Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers

## ISO/TR 22053: Safety of machinery - Safeguarding supportive system

### Safeguarding supportive system (SSS)

Complementary risk reduction/protective measure to enable mode selection by the use of authentication means

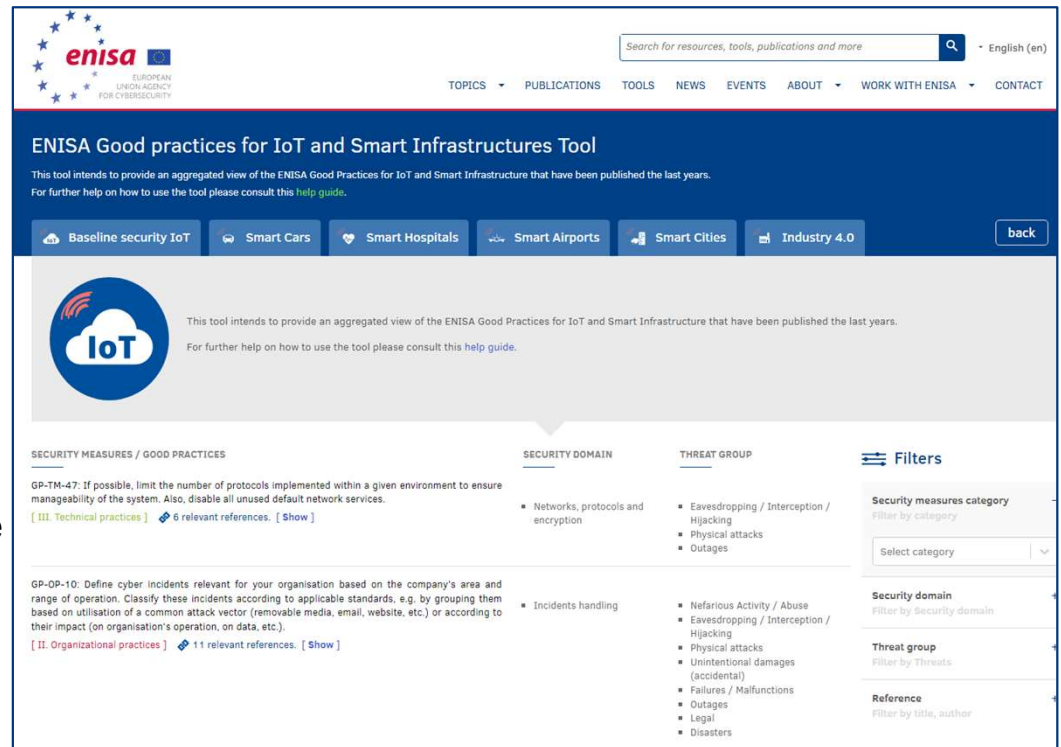
Technical measure to minimize the probability of dangerous human errors occurring



## European Union Agency for Cybersecurity

### ENISA (europa.eu)

As part of the EU Cybersecurity strategy the European Commission proposed the EU Network and Information Security directive. The NIS Directive (see EU 2016/1148) is the first piece of EU-wide cybersecurity legislation. The goal is to enhance cybersecurity across the EU.



The screenshot shows the ENISA website interface for the 'ENISA Good practices for IoT and Smart Infrastructures Tool'. The page features a search bar, navigation menu, and a main content area with a table of security measures and good practices. The table is organized into columns for Security Measures / Good Practices, Security Domain, and Threat Group. A 'Filters' sidebar is visible on the right.

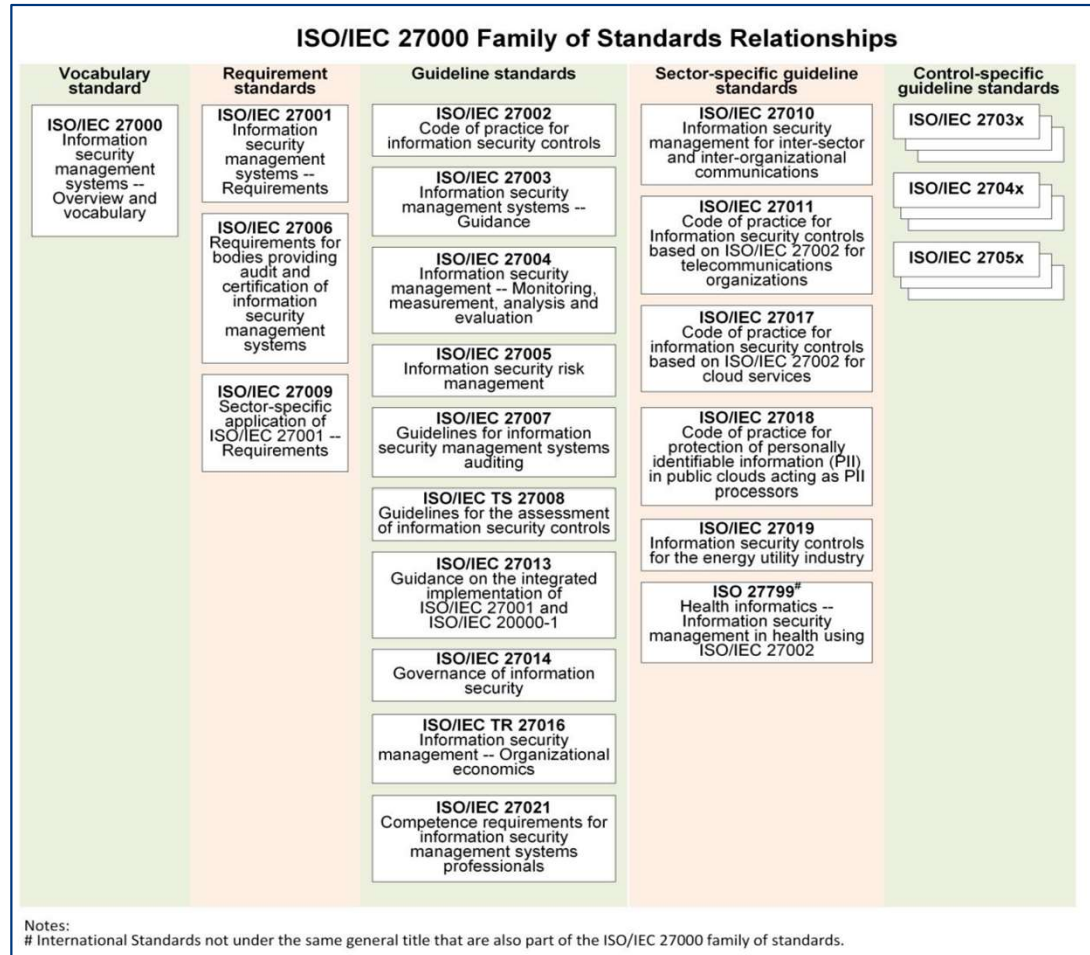
SECURITY MEASURES / GOOD PRACTICES	SECURITY DOMAIN	THREAT GROUP
<p>GP-TM-47: If possible, limit the number of protocols implemented within a given environment to ensure manageability of the system. Also, disable all unused default network services.</p> <p>[ III. Technical practices ] 6 relevant references. [ Show ]</p>	<ul style="list-style-type: none"> <li>Networks, protocols and encryption</li> </ul>	<ul style="list-style-type: none"> <li>Eavesdropping / Interception / Hijacking</li> <li>Physical attacks</li> <li>Outages</li> </ul>
<p>GP-OP-10: Define cyber incidents relevant for your organisation based on the company's area and range of operation. Classify these incidents according to applicable standards, e.g. by grouping them based on utilisation of a common attack vector (removable media, email, website, etc.) or according to their impact (on organisation's operation, on data, etc.).</p> <p>[ II. Organizational practices ] 11 relevant references. [ Show ]</p>	<ul style="list-style-type: none"> <li>Incidents handling</li> </ul>	<ul style="list-style-type: none"> <li>Nefarious Activity / Abuse</li> <li>Eavesdropping / Interception / Hijacking</li> <li>Physical attacks</li> <li>Unintentional damages (accidental)</li> <li>Failures / Malfunctions</li> <li>Outages</li> <li>Legal</li> <li>Disasters</li> </ul>

## Convergence IT and OT threats

7.6.2019	EN	Official Journal of the European Union	L 151/15
<p><b>REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL</b></p> <p>of 17 April 2019</p> <p><b>on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)</b></p> <p>(Text with EEA relevance)</p> <p>THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,</p> <p>Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,</p> <p>Having regard to the proposal from the European Commission,</p> <p>After transmission of the draft legislative act to the national parliaments,</p> <p>Having regard to the opinion of the European Economic and Social Committee <sup>(1)</sup>,</p> <p>Having regard to the opinion of the Committee of the Regions <sup>(2)</sup>,</p> <p>Acting in accordance with the ordinary legislative procedure <sup>(3)</sup>,</p> <p>Whereas:</p> <p>(1) Network and information systems and electronic communications networks and services play a vital role in society and have become the backbone of economic growth. Information and communications technology (ICT) underpins the complex systems which support everyday societal activities, keep our economies running in key sectors such as health, energy, finance and transport, and, in particular, support the functioning of the internal market.</p> <p>(2) The use of network and information systems by citizens, organisations and businesses across the Union is now pervasive. Digitisation and connectivity are becoming core features in an ever growing number of products and services and with the advent of the internet of Things (IoT) an extremely high number of connected digital devices are expected to be deployed across the Union during the next decade. While an increasing number of devices is connected to the internet, security and resilience are not sufficiently built in by design, leading to insufficient cybersecurity. In that context, the limited use of certification leads to individual, organisational and business users having insufficient information about the cybersecurity features of ICT products, ICT services and ICT processes, which undermines trust in digital solutions. Network and information systems are capable of supporting all aspects of our lives and drive the Union's economic growth. They are the cornerstone for achieving the digital single market.</p> <p>(3) Increased digitisation and connectivity increase cybersecurity risks, thus making society as a whole more vulnerable to cyber threats and exacerbating the dangers faced by individuals, including vulnerable persons such as children. In order to mitigate those risks, all necessary actions need to be taken to improve cybersecurity in the Union so that network and information systems, communications networks, digital products, services and devices used by citizens, organisations and businesses – ranging from small and medium-sized enterprises (SMEs), as defined in Commission Recommendation 2003/361/EC <sup>(4)</sup>, to operators of critical infrastructure – are better protected from cyber threats.</p> <p>(4) By making the relevant information available to the public, the European Union Agency for Network and Information Security (ENISA), as established by Regulation (EU) No 526/2013 of the European Parliament and of the Council <sup>(5)</sup> contributes to the development of the cybersecurity industry in the Union, in particular SMEs and start-ups. ENISA should strive for closer cooperation with universities and research entities in order to contribute to reducing dependence on cybersecurity products and services from outside the Union and to reinforce supply chains inside the Union.</p> <p>(5) Cyberattacks are on the increase and a connected economy and society that is more vulnerable to cyber threats and attacks requires stronger defences. However, while cyberattacks often take place across borders, the competence of, and policy responses by, cybersecurity and law enforcement authorities are predominantly national. Large-scale incidents could disrupt the provision of essential services across the Union. This necessitates effective and coordinated responses and crisis management at Union level, building on dedicated policies and wider instruments for European solidarity and mutual assistance. Moreover, a regular assessment of the state of cybersecurity and resilience in the Union, based on reliable Union data, as well as systematic forecasts of future developments, challenges and threats, at Union and global level, are important for policy-makers, industry and users.</p>			

## Other sources

IEC 62443 series for Industrial  
Automation and Control Systems (IACS)  
builds on established Standards  
e.g. ISO/IEC 27000 series  
ON SAFETY OF INFORMATIONS





## ISO/IEC 27001/2 key clauses



 = Unique Domains





# Safety & Security

---

## Cloud versions

- **ISO/IEC 27017:2015** Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services



---

# THANKS !

Giovanni B. Lucido