



**UNIMORE**  
UNIVERSITÀ DEGLI STUDI DI  
MODENA E REGGIO EMILIA

Security, Edge and  
Cloud **Lab**



---

# Cybersecurity, Businesses, Institutions: a Holistic Approach

**Prof. Mirco Marchetti**

*Department of Engineering «Enzo Ferrari»  
University of Modena and Reggio Emilia*

# Mirco Marchetti

- Associate Professor at the Department of Engineering “Enzo Ferrari”
- Director of the Interdepartmental Research Center on Security and Risk Prevention (CRIS)
- Co-Founder of the “Security, Edge and Cloud” (SECLoud <https://secloud.ing.unimore.it/>) lab, leader of cybersecurity activities for IT and Cyber-Physical systems (ACES)
- Co-director of the Cyber Academy
- Lecturer of “Sicurezza Informatica” and “Automotive Cyber Security”



**UNIMORE**  
UNIVERSITÀ DEGLI STUDI DI  
MODENA E REGGIO EMILIA

Security, Edge  
and Cloud **Lab**







**CYBER  
ACADEMY**







**UNIMORE**  
UNIVERSITÀ DEGLI STUDI DI  
MODENA E REGGIO EMILIA

Centro di Ricerca Interdipartimentale sulla  
Sicurezza e Prevenzione dei Rischi - CRIS

# Components of an information system

Communication technologies		People
		Data
		Software
		Hardware

# Components of an information system

Communication technologies		People
		Data
		Software
		Hardware

All these components are vulnerable!

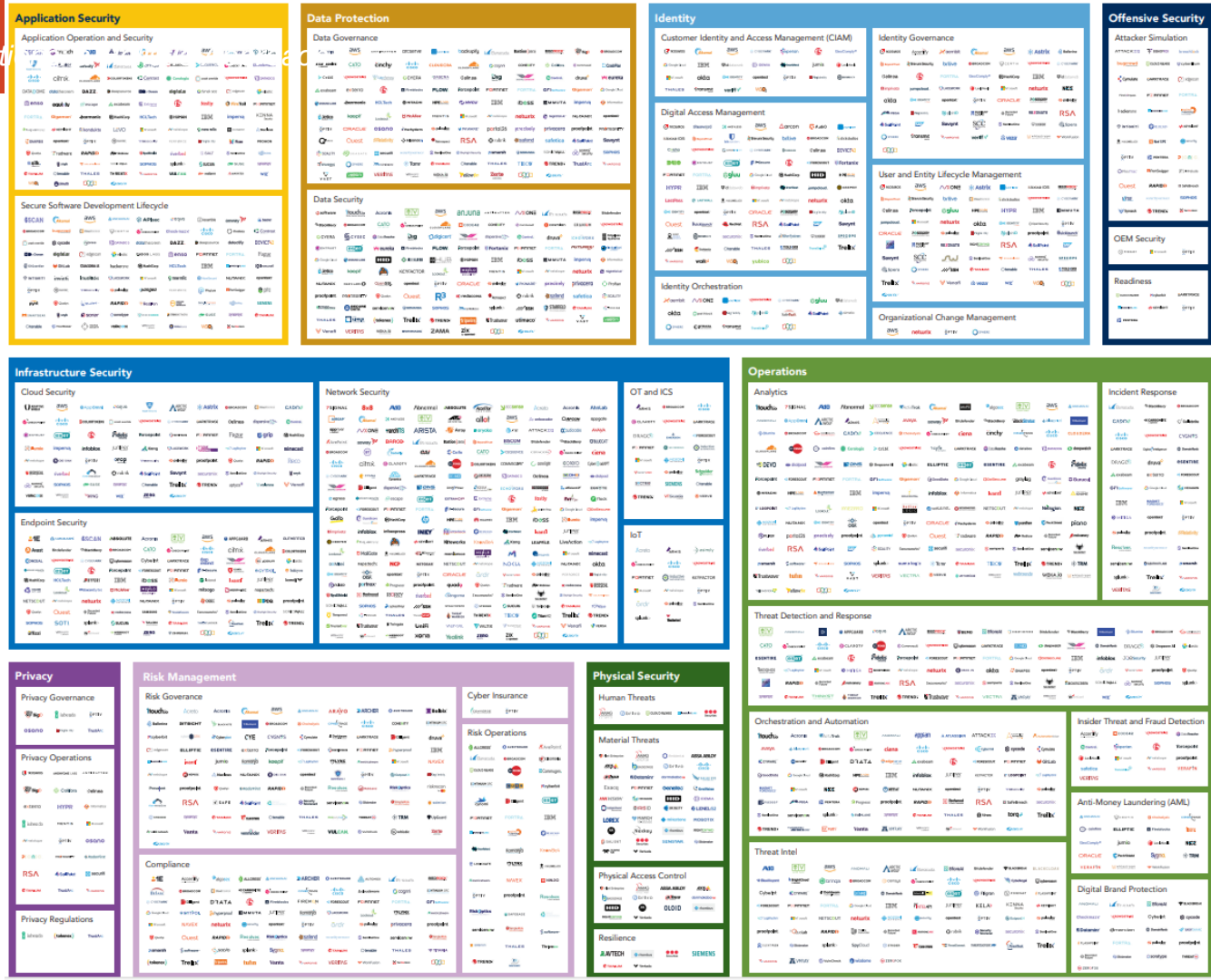
# Cybersecurity: a technology issue?

We already have plenty of  
cybersecurity technologies...

... are we okay then?

Source: Optive Cybersecurity  
Landscape Map

<https://www.optiv.com/sites/default/files/2024-07/Cybersecurity-Landscape-Map-2024.pdf>



# IT vs «the real world»: clash of cultures

These license terms are an agreement between you and [REDACTED] (or one of its affiliates). They apply to the software named above and any [REDACTED] services or software updates [...] IF YOU COMPLY WITH THESE LICENSE TERMS, YOU HAVE THE RIGHTS BELOW. BY USING THE SOFTWARE, YOU ACCEPT THESE TERMS.

DISCLAIMER OF WARRANTY. THE SOFTWARE IS LICENSED “AS IS.” YOU BEAR THE RISK OF USING IT. [REDACTED] GIVES NO EXPRESS WARRANTIES, GUARANTEES, OR CONDITIONS. TO THE EXTENT PERMITTED UNDER APPLICABLE LAWS, [REDACTED] EXCLUDES ALL IMPLIED WARRANTIES, INCLUDING MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.

LIMITATION ON AND EXCLUSION OF DAMAGES. IF YOU HAVE ANY BASIS FOR RECOVERING DAMAGES DESPITE THE PRECEDING DISCLAIMER OF WARRANTY, YOU CAN RECOVER FROM [REDACTED] AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO U.S. \$5.00. YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT, OR INCIDENTAL DAMAGES.

# IT vs «the real world»: clash of cultures

These license terms are an agreement between you and **Microsoft Corporation** (or one of its affiliates). They apply to the software named above and any **Microsoft** services or software updates [...] IF YOU COMPLY WITH THESE LICENSE TERMS, YOU HAVE THE RIGHTS BELOW. BY USING THE SOFTWARE, YOU ACCEPT THESE TERMS.

DISCLAIMER OF WARRANTY. THE SOFTWARE IS LICENSED “AS IS.” YOU BEAR THE RISK OF USING IT. **MICROSOFT** GIVES NO EXPRESS WARRANTIES, GUARANTEES, OR CONDITIONS. TO THE EXTENT PERMITTED UNDER APPLICABLE LAWS, **MICROSOFT** EXCLUDES ALL IMPLIED WARRANTIES, INCLUDING MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.

LIMITATION ON AND EXCLUSION OF DAMAGES. IF YOU HAVE ANY BASIS FOR RECOVERING DAMAGES DESPITE THE PRECEDING DISCLAIMER OF WARRANTY, YOU CAN RECOVER FROM **MICROSOFT** AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO U.S. \$5.00. YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT, OR INCIDENTAL DAMAGES.

# IT vs «the real world»: clash of cultures

These license terms are an agreement between you and **Microsoft Corporation** (or one of its affiliates). They apply to the software named above and any **Microsoft** services or software updates [...] IF YOU COMPLY WITH THESE LICENSE TERMS, YOU HAVE THE RIGHTS BELOW. BY USING THE SOFTWARE, YOU ACCEPT THESE TERMS. Source: **MICROSOFT SOFTWARE LICENSE TERMS**

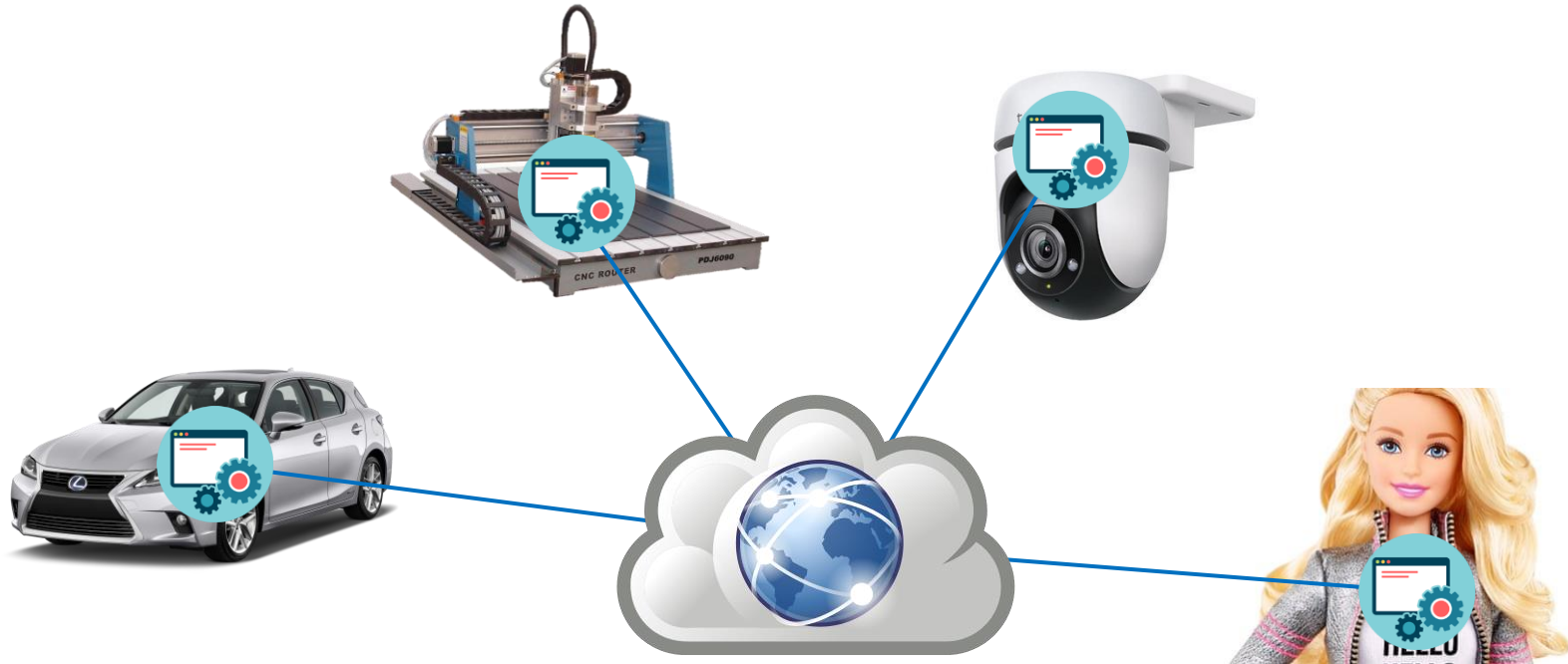
**License conditions applied to Microsoft Windows Server 2022**  
**MICROSOFT** GIVES NO EXPRESS WARRANTIES, GUARANTEES, OR CONDITIONS. TO THE EXTENT PERMITTED UNDER APPLICABLE [Microsoft software license terms for MICROSOFT.WINDOWSSERVER.SYSTEMINSIGHTS](#) | [Microsoft Learn](#) INCLUDING IMPLICIT WARRANTIES, INCLUDING MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.

LIMITATION <https://learn.microsoft.com/en-us/legal/windows-server/system-insights-eula> REGARDING DAMAGES  
DESPITE THE PRECEDING DISCLAIMER OF WARRANTY, YOU CAN RECOVER FROM **MICROSOFT** AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO U.S. \$5.00. YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT, OR INCIDENTAL DAMAGES.

# Under these terms, would you buy...



# Under these terms, would you buy...



# Unforeseen consequences of cyber attacks

## Hackers can hijack Wi-Fi Hello Barbie to spy on your children

Security researcher warns hackers could steal personal information and turn the microphone of the doll into a surveillance device



Hello Barbie listens to children and uses cloud-based voice recognition technology to understand them and talk back. Photograph: Mattel

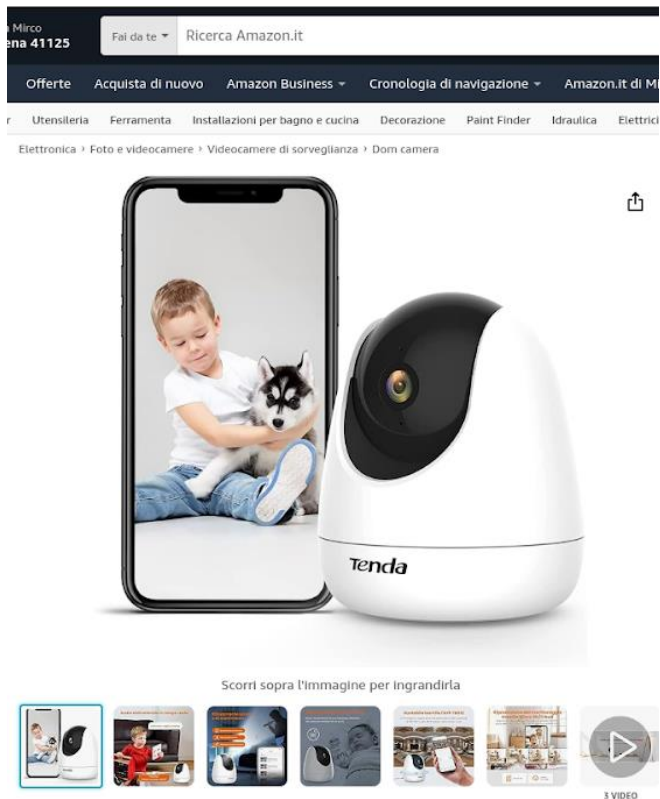
Mattel's latest Wi-Fi enabled Barbie doll can easily be hacked to turn it into a surveillance device for spying on children and listening into conversations without the owner's knowledge.



<https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children>

The  
Guardian

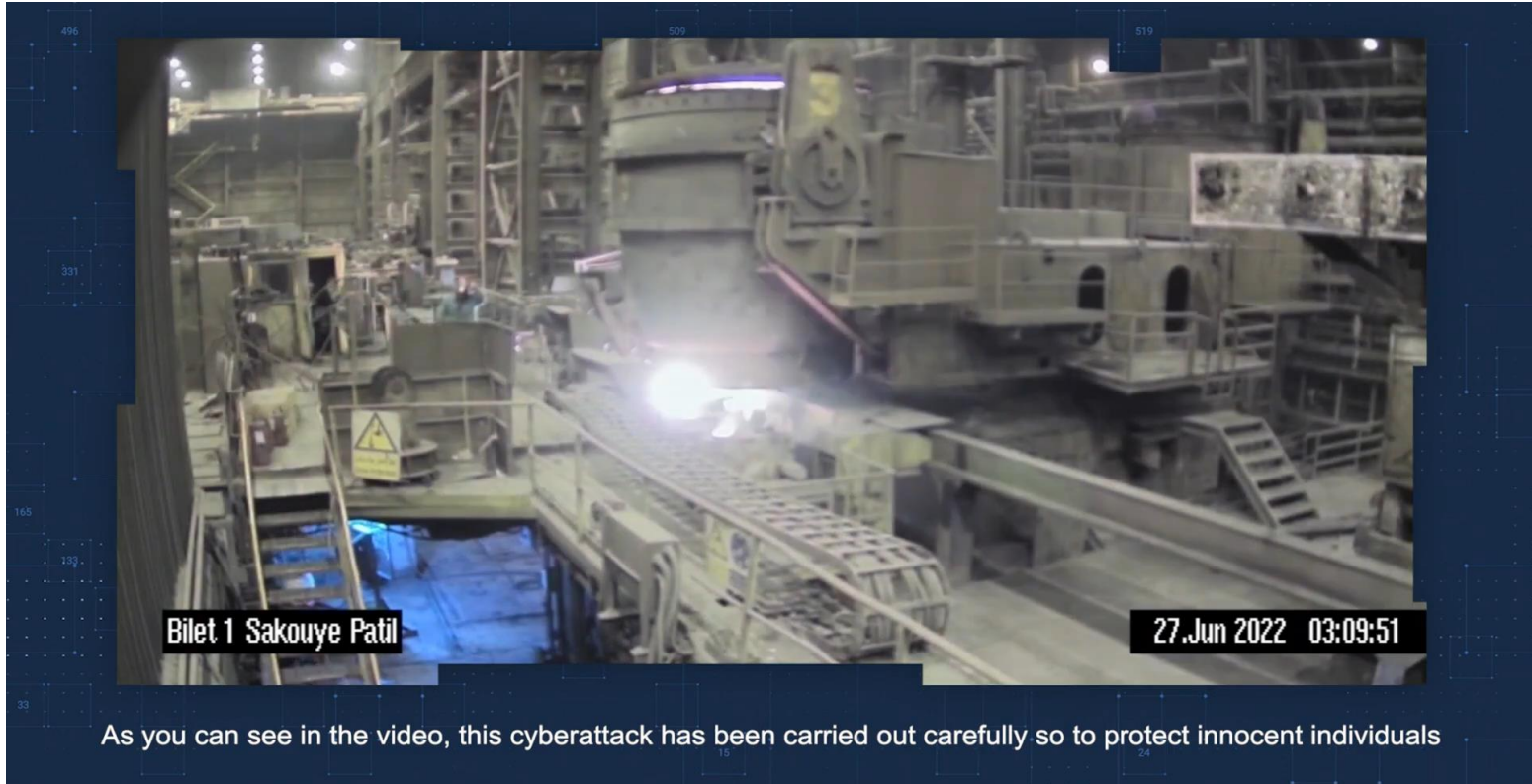
# Unforeseen consequences of cyber attacks



CVE ID	Nome	CVSS
CVE-2023-30351	Remote access via hard-coded credentials	7.5 HIGH
CVE-2023-30352	RTSP feed access via hard-coded credentials	9.8 CRITICAL
CVE-2023-30353	Unauthenticated RCE	9.8 CRITICAL
CVE-2023-30354	Physical access and WiFi credentials disclosure	9.8 CRITICAL
CVE-2023-30356	Missing support for Integrity Check	7.5 HIGH



# Unforeseen consequences of cyber attacks



As you can see in the video, this cyberattack has been carried out carefully so to protect innocent individuals

# Unforeseen consequences of cyber attacks



VS



Jeep Cherokee (2014)

**Remote to local** vulnerable software running on the Infotainment system and reachable from the Internet

**Lateral movement** from the infotainment system it is possible to inject spoofed data that is used by other Electronic Control Units to perform many functions (including ADAS)

**Reversing** black box analysis of communications among all Electronic Control Units to identify ways to interfere with ADAS

**Remote control** fake data sent to safety-relevant Electronic Control Units from a laptop connected to the Internet, hundred of km away from the target

**Impact** ... engine shutdown, partial control of the steering wheel, disengaging the brakes, ...

<https://www.youtube.com/watch?v=MK0SrxBC1xs>



# Cybersecurity → Safety

You don't mess around with safety:

- it's not something you “patch” onto a product
- nor something to be ignored during design

... otherwise, you will not be able to sell your product!

- type-approval regulations
- CE marking
- legal obligations

Spedit. abb. post. - art. 1, comma 1  
Legge 27-02-2004, n. 46 - Filiale di Roma

Anno 159° - Numero 231



IL PRESIDENTE DELLA REPUBBLICA

Vista la direttiva 2006/42/CE del Parlamento europeo e del Consiglio, del 17 maggio 2006, relativa alle macchine [...]

E M A N A  
il seguente decreto legislativo:

## ART. 1

1. Le norme del presente decreto legislativo si applicano ai seguenti prodotti [...]:

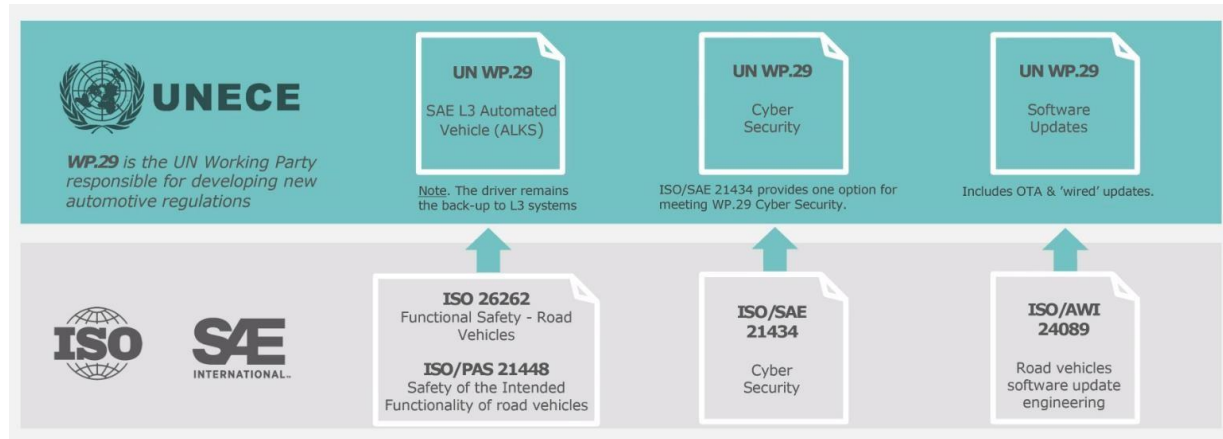
- a) macchine;
- b) attrezzature intercambiabili;
- c) componenti di sicurezza;
- d) accessori di sollevamento;
- e) catene, funi e cinghie;
- f) dispositivi amovibili di trasmissione meccanica;
- g) quasi-macchine.

# In the automotive domain...

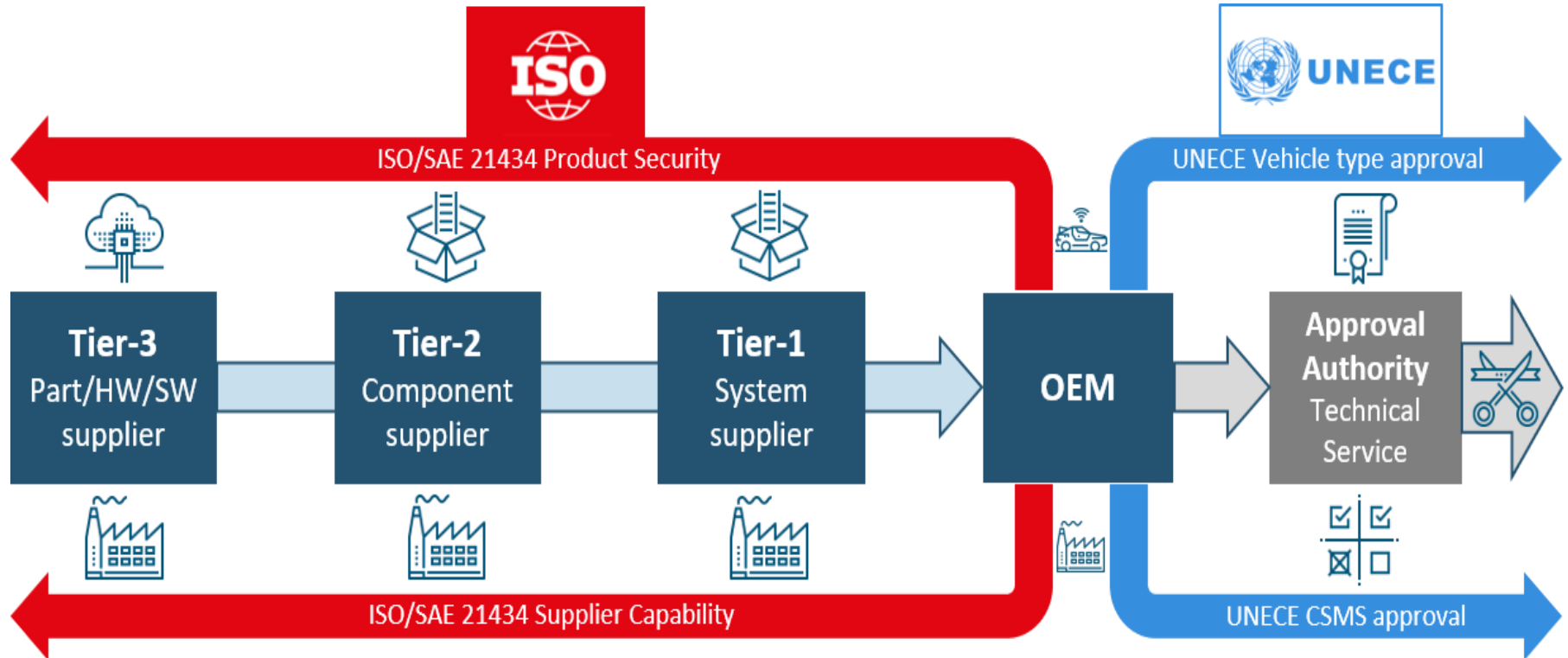


**UN Regulation No. 155 - Cyber security and cyber security management system**

**UN Regulation No. 156 - Software update and software update management system**



# Cybersecurity trickles down the whole supply chain



Security Management on organizational level

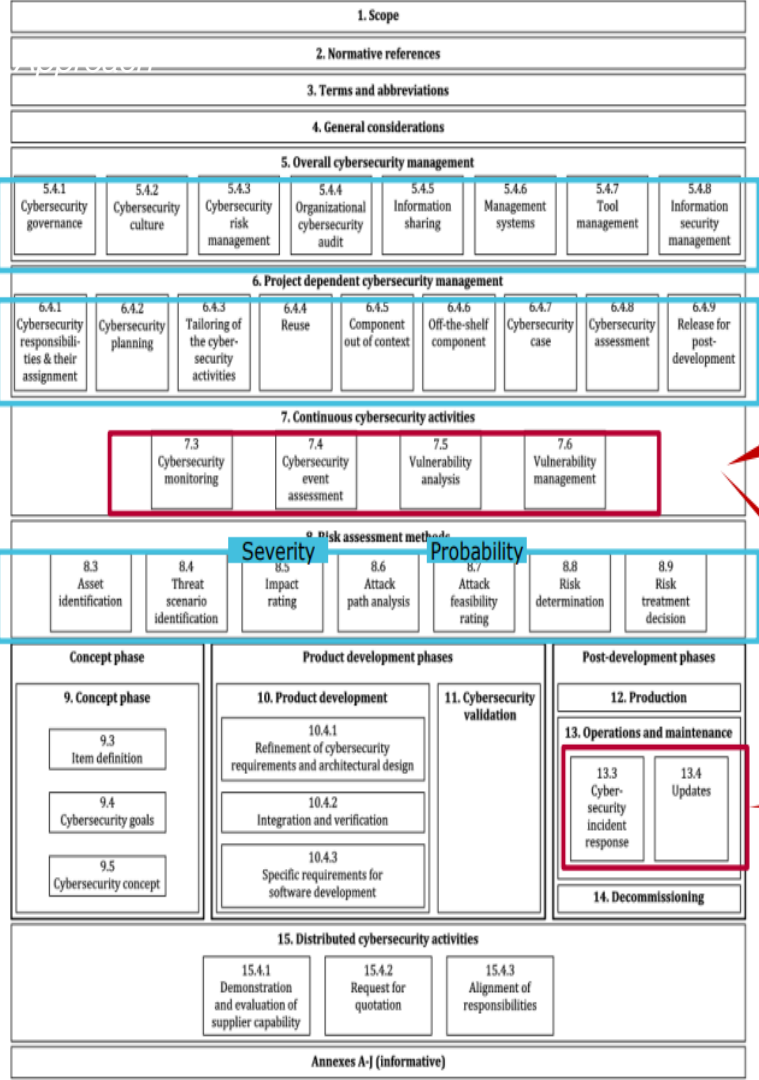
Classic Security Management

TARA (Risk Assessment)

**Cybersecurity Information:**  
*Information* derived from data collected by the monitoring process for which relevance to an item or component has not been determined.

**Cybersecurity Event:**  
*Cybersecurity information*, that has been confirmed as potentially relevant to an item or component.

ISO SAE 21434 (Draft DIS)



Can be applied even outside a project (Cybersecurity Information/Event)

Significant addition to safety approach

## Shaping Europe's digital future

[Home](#) | [Policies](#) | [Activities](#) | [News](#) | [Library](#) | [Funding](#) | [Calendar](#) | [Consultations](#) | [AI Office](#)

[Home](#) > [Policies](#) > [EU Cyber Resilience Act](#)

### EU Cyber Resilience Act

New EU cybersecurity rules ensure safer hardware and software.

From baby-monitors to smart-watches, products and software that contain a digital component are omnipresent in our daily lives. Less apparent to many users is the security risk such products and software may present.

The [Cyber Resilience Act \(CRA\)](#) aims to safeguard consumers and businesses buying or using products or software with a digital component. The Act would see inadequate security features become a thing of the past with the introduction of mandatory cybersecurity requirements for manufacturers and retailers of such products, with this protection extending throughout the product lifecycle.

And the  
automotive  
domain is not an  
exception...

# Radio Equipment Devices

- Cybersecurity requirements for any device that connects to a computer network via radio frequency communications (any form)
- It comes into force in Italy in August 2025!





**DECRETO LEGISLATIVO 4 settembre 2024, n. 138**

Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148. (24G00155)

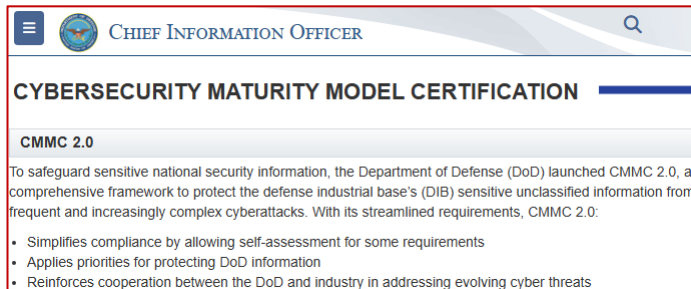
*(GU n.230 del 1-10-2024)*

# ... standards, directives, regulations ...

## **DIRETTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO**

**del 14 dicembre 2022**

**relativa a misure per un livello comune elevato di cibersecurity nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2)**



The screenshot shows the header of a Chief Information Officer's page with a search icon. Below the header is the title "CYBERSECURITY MATURITY MODEL CERTIFICATION" followed by a blue progress bar. Underneath is the section "CMMC 2.0". The main text describes the purpose of CMMC 2.0: "To safeguard sensitive national security information, the Department of Defense (DoD) launched CMMC 2.0, a comprehensive framework to protect the defense industrial base's (DIB) sensitive unclassified information from frequent and increasingly complex cyberattacks. With its streamlined requirements, CMMC 2.0:". A bulleted list follows, detailing the benefits: "Simplifies compliance by allowing self-assessment for some requirements", "Applies priorities for protecting DoD information", and "Reinforces cooperation between the DoD and industry in addressing evolving cyber threats".

**CHIEF INFORMATION OFFICER**

### **CYBERSECURITY MATURITY MODEL CERTIFICATION**

#### **CMMC 2.0**

To safeguard sensitive national security information, the Department of Defense (DoD) launched CMMC 2.0, a comprehensive framework to protect the defense industrial base's (DIB) sensitive unclassified information from frequent and increasingly complex cyberattacks. With its streamlined requirements, CMMC 2.0:

- Simplifies compliance by allowing self-assessment for some requirements
- Applies priorities for protecting DoD information
- Reinforces cooperation between the DoD and industry in addressing evolving cyber threats

## **REGOLAMENTO (UE) 2023/1230 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO**

**del 14 giugno 2023**

**relativo alle macchine e che abroga la direttiva 2006/42/CE del Parlamento europeo e del Consiglio e la direttiva 73/361/CEE del Consiglio**

## **REGOLAMENTO (UE) 2022/2554 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO**

**del 14 dicembre 2022**

**relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011**

# ... standards, directives, regulations ...



## Healthcare

IEC SC 62A

ISO/IEC 80001

(via Joint Working Group with ISO)

risk management for IT-networks incorporating medical devices



## Industry

IEC TC 65

IEC 62443

series of publications that specify security requirements for industrial automation and control systems (IACS)



## Shipping

IEC TC 80

IEC 63154

maritime navigation and radiocommunication equipment and systems



## Nuclear power plants (NPPs)

IEC SC 45A

IEC 62645

protection of microprocessor-based information and control systems in nuclear power plants

IEC 62859

framework for managing the interactions between safety and cyber security.



## Electric power utilities

IEC TC 57

IEC 61850

series of publications for communication networks and systems for power utility automation

IEC 60870

series for telecontrol equipment and systems

IEC 62351

series on power systems management and associated information exchange

# The roles of institutions

**Force** a cybersecurity-by-design approach

- Change people's perception of cybersecurity

**Force** a cybersecurity management approach

- Change people's perception of the impact of cyber attacks

**Force** cybersecurity improvements for whole industrial sectors

- Through viral cybersecurity requirements that are passed down the supply chain



# Will it work?

Hopefully so!

It worked quite well in the financial sector...

It is working in the automotive sector...

**Will it be easy and painless?**

Probably not...

It wasn't for the financial sector.

It isn't for the automotive sector.

