Publicada la propuesta del nuevo Reglamento UE de Máquinas: Lo que hay que saber

PILZ
THE SPIRIT OF SAFETY

Jan Puig

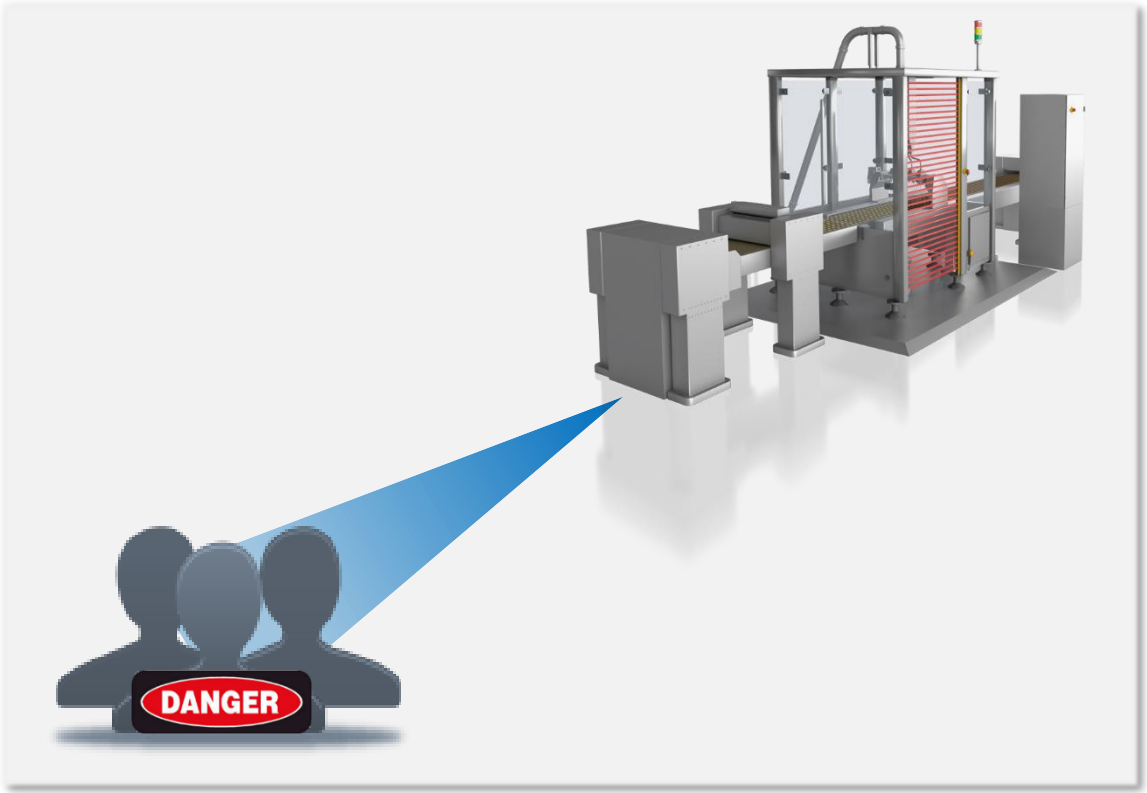

We
automate.
Safely.

Seguridad y Protección

Safety

Proteger a las **personas** de las máquinas.
ej. protección de posibles daños severos causados por partes móviles de la máquina.

Security



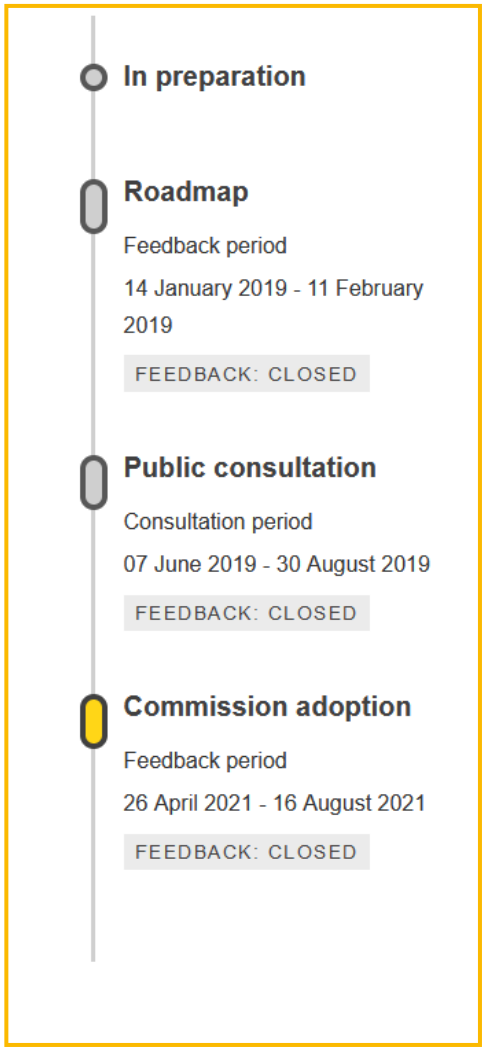
Proteger a las **máquinas** de las personas.
ej. protección contra acessos no autorizados o personal no cualificado para realizar tareas de mantenimiento.

1

Introducción

Planificación estimativa

Roadmap 2022 - 2026



Abril 2021

01

- Publicación Draft

2022

02

- Procedimiento decisión compartido parlamento EU + Consejo EU

2023

03

- Publicación como Reglamento EU
- NO transposición a los estados miembros como ley

¿2025/26?

04

- Artículos 49 + 50
- Periodo de transición
- 30 meses desde publicación oficial

Fase Consultiva

Statistics

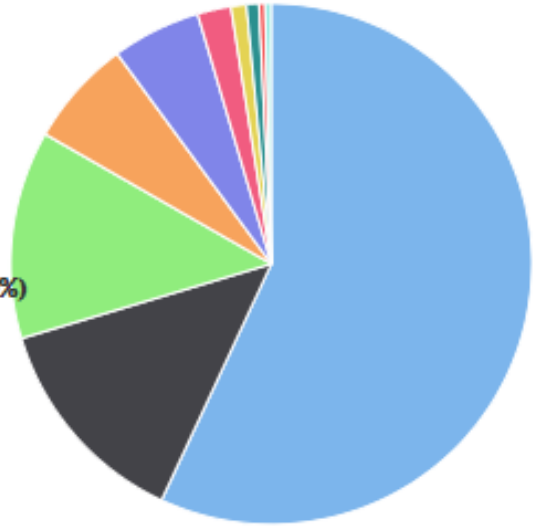
Total of valid feedback instances received: 527

The number feedback instances shown includes only the valid ones, respecting the feedback rules.
The data is regularly updated.

By category of respondent

- Company/business organisation: 300 (56.93%)
- Business association: 71 (13.47%)
- EU citizen: 68 (12.90%)
- Public authority: 35 (6.64%)
- Other: 29 (5.50%)
- Non-governmental organisation (NGO): 11 (2.09%)
- Trade union: 5 (0.95%)
- Academic/research Institution: 4 (0.76%)
- Non-EU citizen: 2 (0.38%)

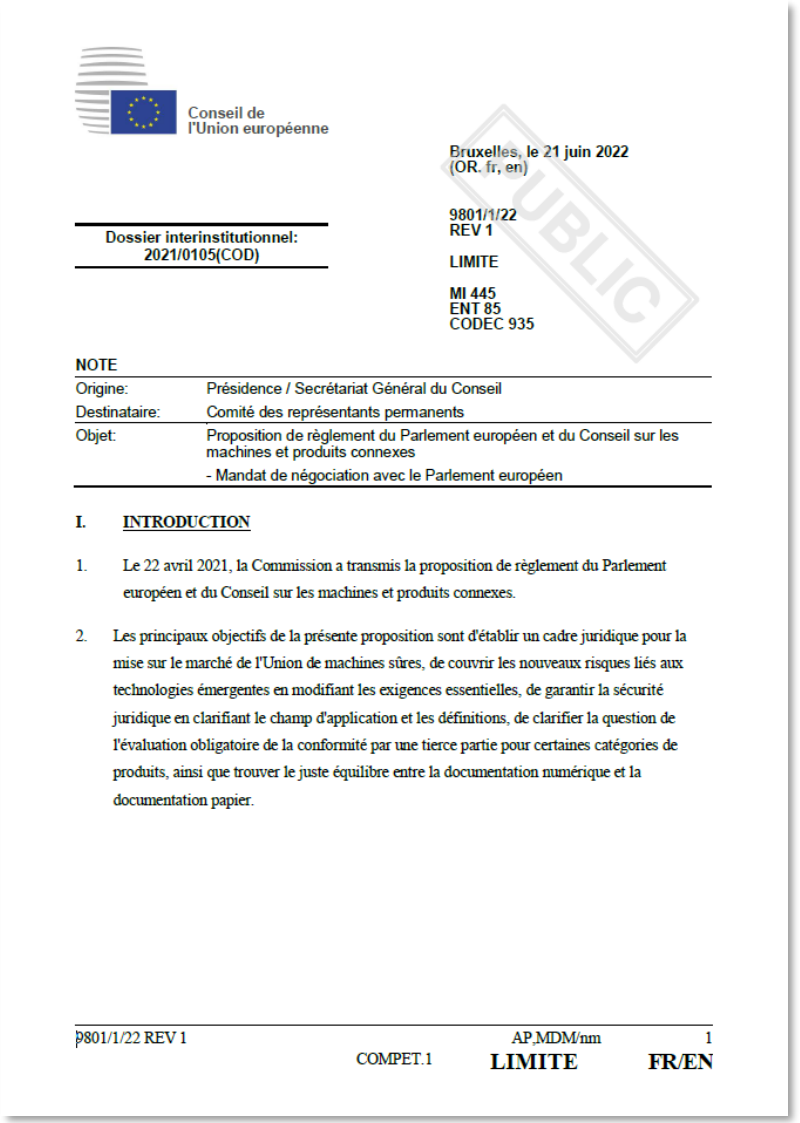
1 / 2



Revisión de la Directiva de Máquinas 2006/42/EC

Propuesta 2022-06 (Propuesta => cambios son aun posibles)

A finales de junio, los representantes de los Estados miembros en el Comité de Representantes Permanentes (COREPER), adoptaron la posición final de los Estados miembros y el mandato de la Presidencia del Consejo para las negociaciones con la Comisión y el Parlamento de la UE.



Conseil de
l'Union européenne

Bruxelles, le 21 juin 2022
(OR. fr, en)

PUBLIC

Dossier interinstitutionnel:
2021/0105(COD)

9801/1/22
REV 1

LIMITE

MI 445
ENT 85
CODEC 935

NOTE

Origine:	Présidence / Secrétariat Général du Conseil
Destinataire:	Comité des représentants permanents
Objet:	Proposition de règlement du Parlement européen et du Conseil sur les machines et produits connexes - Mandat de négociation avec le Parlement européen

I. INTRODUCTION

1. Le 22 avril 2021, la Commission a transmis la proposition de règlement du Parlement européen et du Conseil sur les machines et produits connexes.

2. Les principaux objectifs de la présente proposition sont d'établir un cadre juridique pour la mise sur le marché de l'Union de machines sûres, de couvrir les nouveaux risques liés aux technologies émergentes en modifiant les exigences essentielles, de garantir la sécurité juridique en clarifiant le champ d'application et les définitions, de clarifier la question de l'évaluation obligatoire de la conformité par une tierce partie pour certaines catégories de produits, ainsi que trouver le juste équilibre entre la documentation numérique et la documentation papier.

9801/1/22 REV 1 AP,MDM/nm 1
COMPET.1 **LIMITE** **FR/EN**

Objetivos

An initiative of the European Commission

NEW LEGAL FRAMEWORK (NLF)

- Mejorar el control para **proteger usuarios y fabricantes** de productos no seguros, incluyendo aquellos importados de fuera la UE.
- Establecer reglas claras y trasparentes para la **acreditación** de entes competentes de certificación
- Incrementar la **calidad y fiabilidad de los procedimientos de Evaluación de Conformidad**
- Marco legal **uniformizado, consistente y sencillo** de implementar

TÉCNICOS

- En la UE, los fabricantes son requeridos de realizar una evaluación de riesgos para mitigar y reducir los mismos en la medida de lo posible.
- Los fabricantes de maquinaria son responsables de especificar el uso de sus productos, y anticipar posibles formas de mal uso razonable.
- El fabricante debe tener en cuenta la severidad de los peligros para la integridad y salud de los operarios, así como de la probabilidad de ocurrencia.

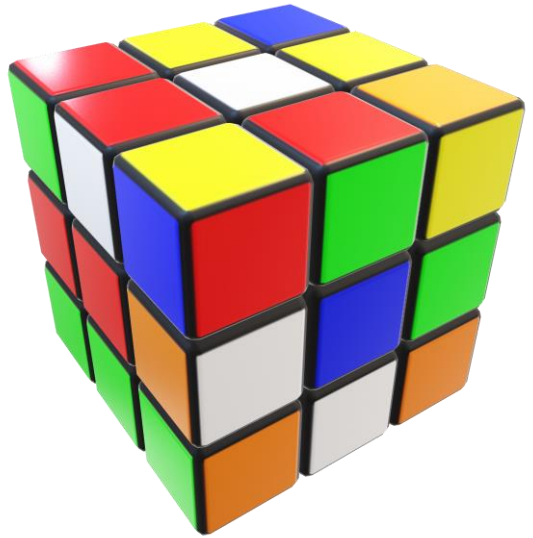
2

Aspectos técnicos

Novedades Relevantes de Seguridad – Anexo I

- Listado de productos para máquinas ~~de alto riesgo~~ ahora en **Anexo I clasificadas en dos capítulos:**

  - **Parte A → Aplica el Artículo 21 (2)**
    - *24. Safety components with fully or partially self-evolving behaviour using machine learning approaches ensuring safety functions*
    - *25. Machinery embedding systems with fully or partially self-evolving behaviour using machine learning approaches ensuring safety functions that have not been placed independently on the market, in respect only to those systems.*



24.	~~Software~~ Safety components with fully or partially self-evolving behaviour using machine learning approaches ~~or logic Systems~~ ensuring safety functions~~, including AI systems~~
25.	Machinery embedding ~~AI~~ Systems with fully or partially self-evolving behaviour using machine learning approaches ensuring safety functions that have not been placed independently on the market, in respect only to those systems.

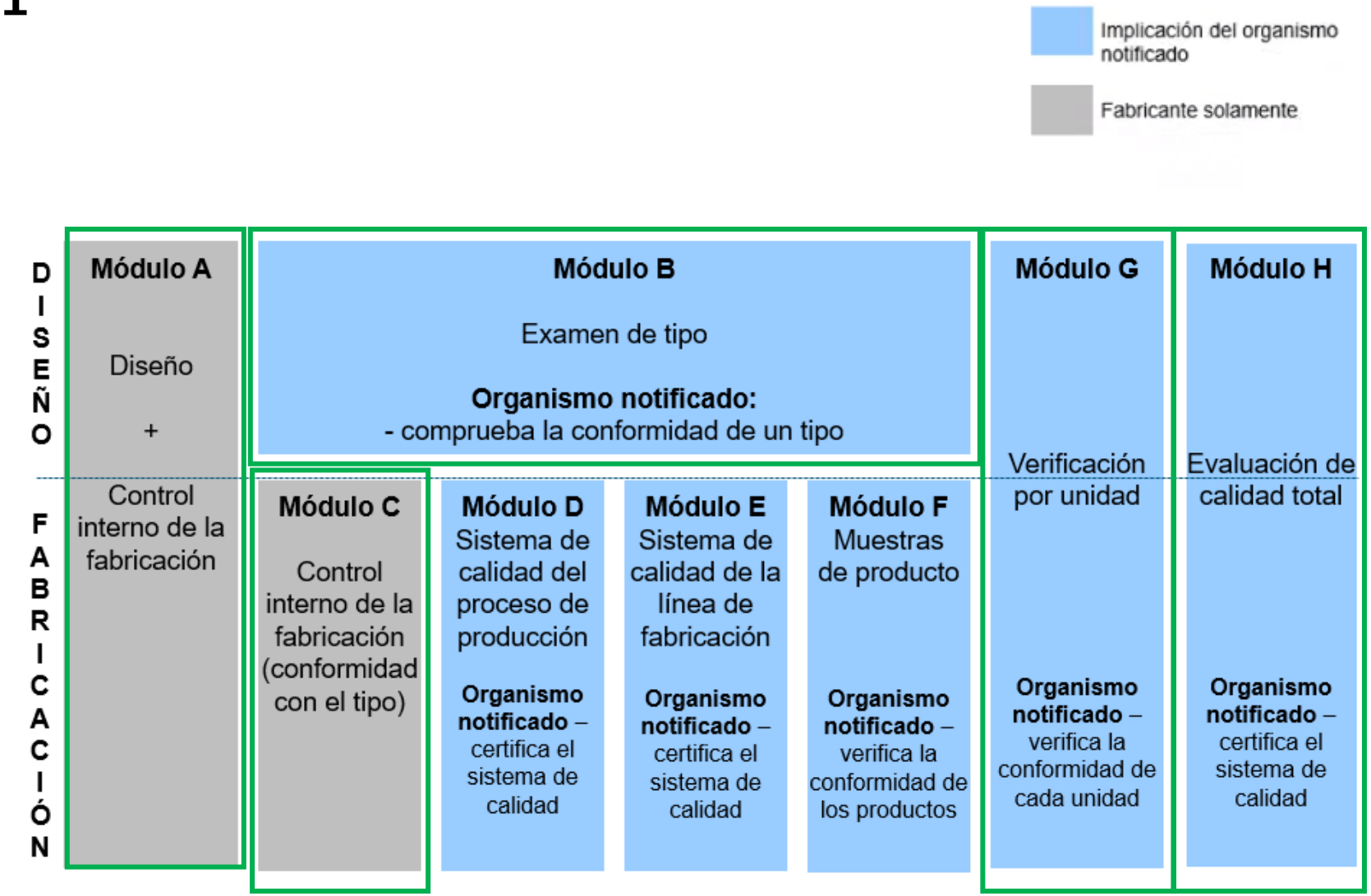
Novedades Relevantes de Seguridad – Anexo I

- Listado de productos para máquinas ~~de alto riesgo~~ ahora en **Anexo I clasificadas en:**

  - **Parte B → Aplica el Artículo 21 (2a)**
    - Las ya listadas en el antiguo Anexo IV
    - Camiones de carga manual de basura o residuos que incorporen mecanismos de compresión
    - Elevadores de vehículos
    - Equipos de elevación de personas y bienes que representen un riesgo de caída vertical superior a 3m

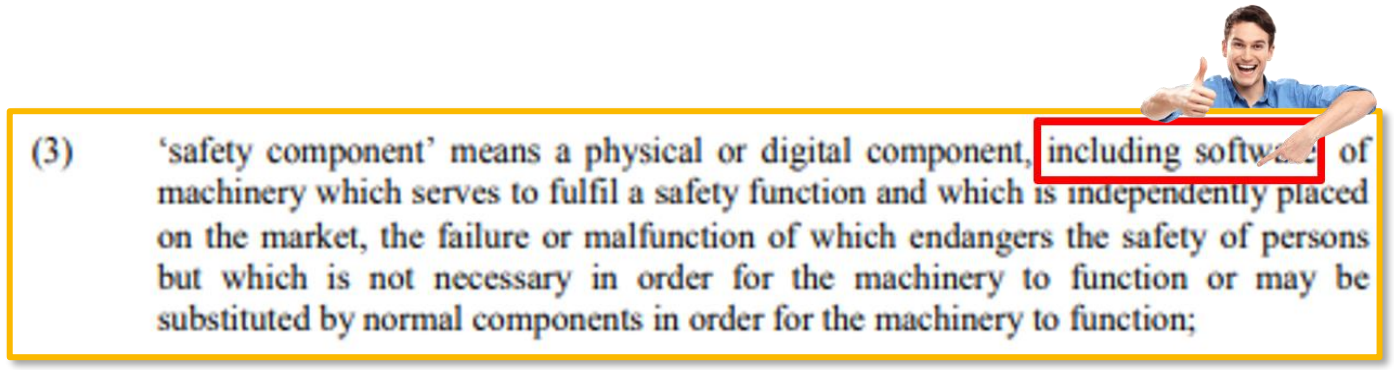
PEC ANEXO I – Artículo 21

- Parte A - Artículo 21 (2)
  - Opciones:
    - Módulos B + C
    - Módulo H
    - Módulo G
- Parte B - Artículo 21 (2a)
  - Opciones:
    - Módulo A *(solo si fabricado según normas armonizadas)*
    - Módulos B + C
    - Módulo H
    - Módulo G



Listado de Componentes de Seguridad – Anexo II

- Extensión de definición de Componente de seguridad: soporte físico o digital, incluyendo software.
- Listado de componentes en seguridad en **Anexo II**
- Se incluyen 2 nuevos apartados:
  - 18 → Software que garantice las funciones de seguridad
  - 18 a → Componente de seguridad con capacidad total o parcial para evolucionar su comportamiento de forma autónoma utilizando funciones de *machine learning*



Cuestiones a tener en cuenta

- **¿Cuándo deciden los algoritmos de machine learning (ML)?**
  - Se ha acotado la intervención del ML a los modos de funcionamiento apropiados?
- **¿Con qué datos se ha entrenado el modelo de ML?**
  - Se dispone de la experiencia real, transpuesta en datos, para alimentar correctamente el modelo?
- **¿Está programado el algoritmo para identificar tendencias que pueden llevar a situaciones peligrosas o las va a normalizar?**
  - Los fallos no solo pueden originarse por una programación incorrecta, sino también por un árbol de decisión peligroso.

Revision of Machinery Directive 2006/42/EC

Proposal 2022-06 (Proposal => changes are possible)

Article 17

Presumption of conformity of machinery products subject to this Regulation

5. Machinery and related 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

Requisitos esenciales de seguridad y salud relativos al diseño y construcción de máquinas o productos relacionados – Anexo III

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 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 the **aforementioned** 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 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.

Requisitos esenciales de seguridad y salud relativos al diseño y construcción de máquinas o productos relacionados – Anexo III

1.2. CONTROL SYSTEMS

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.

(ii) Control systems of **machinery or related product** with fully or partially **self**-evolving behaviour or logic that is designed to operate with varying levels of autonomy shall be designed and constructed in such a way that:

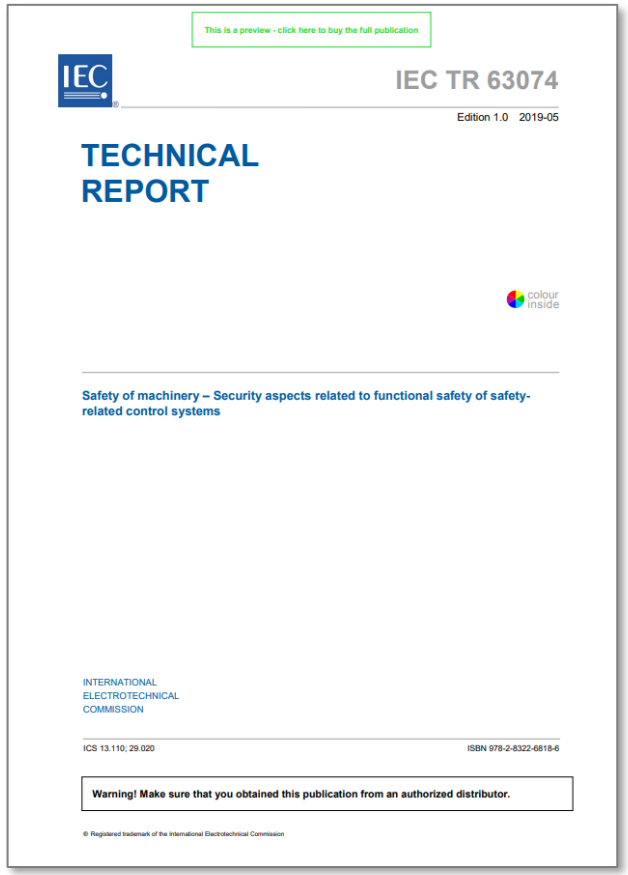
(a) they shall not cause the **machinery or related product** to perform actions beyond its defined task and movement space;

(a).1 they record recording of data on the safety related decision-making process **for software based safety systems ensuring safety function including safety components**, after the **machinery or related product** has been placed on the market or put into service, is enabled and that such data is retained for one year after its collection, exclusively to demonstrate the conformity of the **machinery or related product with this Annex further to a reasoned request from a competent national authority**

(b) it shall be possible at all times to correct the **machinery or related product** in order to maintain its inherent safety.

IEC TR 63074:2022

Safety of machinery – Security aspects



IEC TR 63074 provides **guidance** on the **application** of **IEC 62443** (all parts) with respect to aspects of security threats and vulnerabilities that could affect the functional safety implemented and realized by safety-related control systems (SCS) and result in the loss of the ability to maintain safe operation of a machine.

Security aspects related to functional safety:

- → Security risk assessment
- → Security risk response strategy
- → Security countermeasures
- → **Identification** and **authentication**
- → **Usage control**
- → Restricted data flow (= "firewall")
- → Review and maintenance of security measures

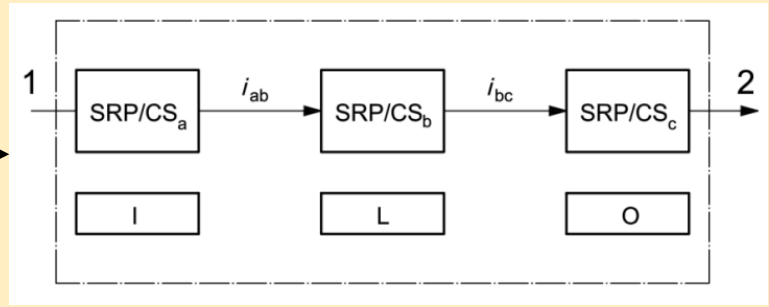
IEC TR 63074:2022

Safety of machinery – Security aspects

Machine Regulation 2021/0105

- **Security**

- **Safety**



1.1

- IEC TR 63074:2022
  Introduction

Threats, vulnerabilities and consequences

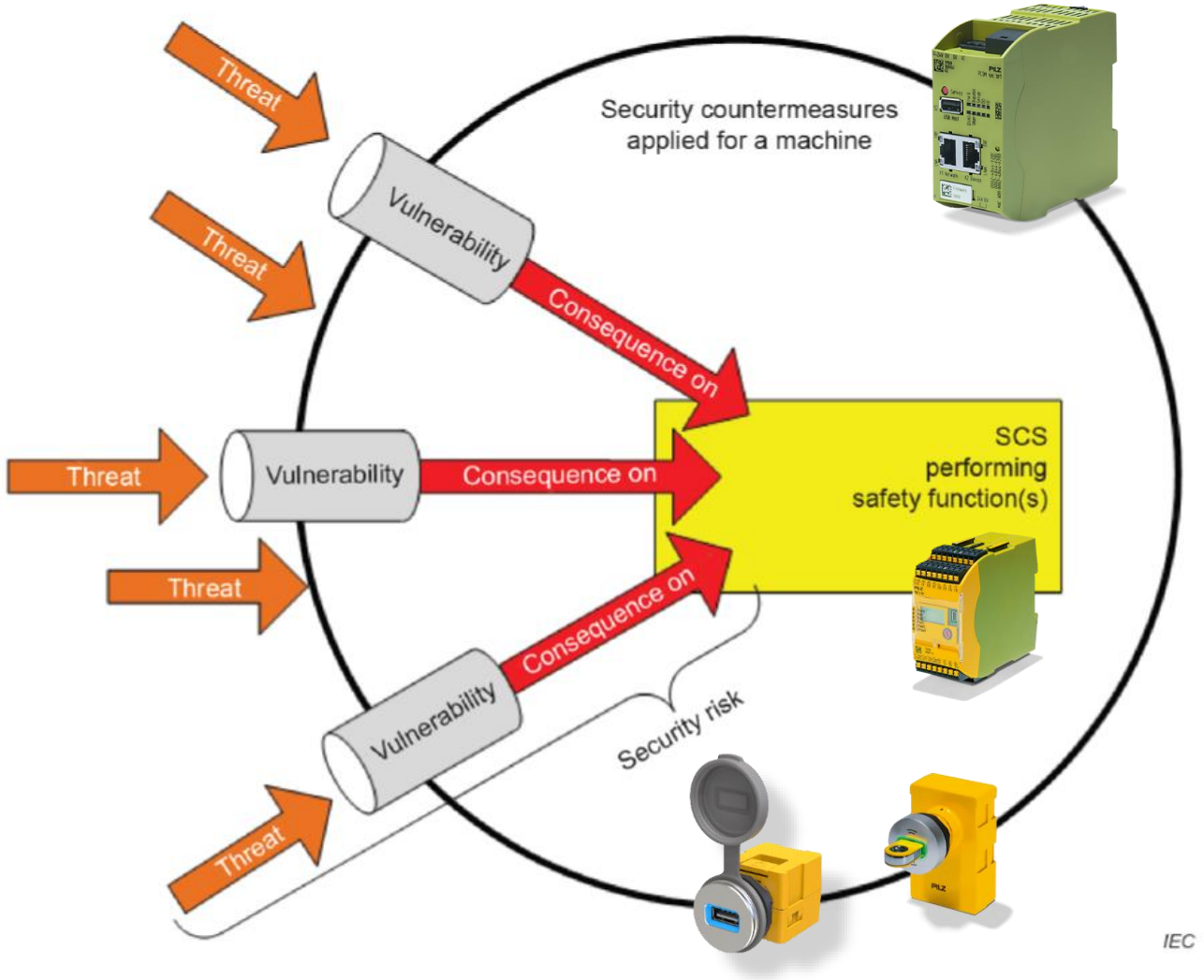


Figure 1 – Relationship between threat(s), vulnerabilities, consequence(s) and security risk(s) for SCS performing safety function(s)

Example – machine connected to cloud

Threat
- Compromise cloud account

Vulnerability
- No account management

Consequence on SRP/CS
- Person can control or modify the SRP/CS without permission.

Countermeasure
- Account management. Meaning:
  - Check and delete the accounts which have access to the machine remotely.
  - Dual approval -> authenticated person onside has to agree the access from the cloud: Security Bridge and PITreader
  - Set up mode of the SecBridge. Only an authenticated person can access the asset if set up mode is enabled.

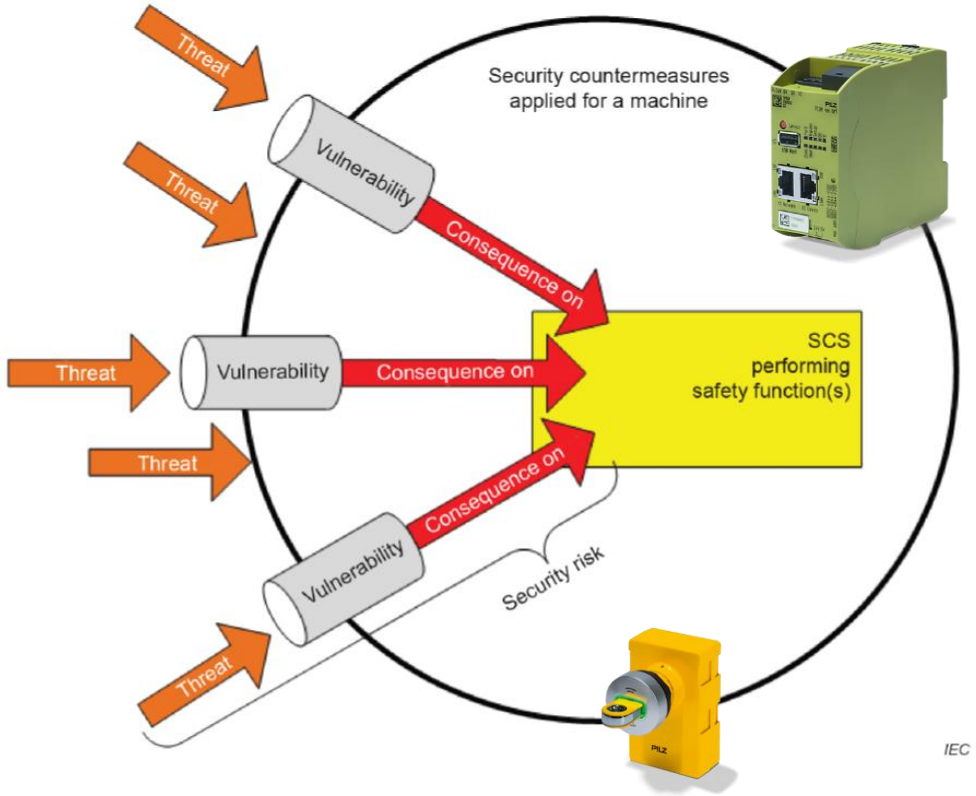


Figure 1 – Relationship between threat(s), vulnerabilities, consequence(s) and security risk(s) for SCS performing safety function(s)

Foundational requirements and influences on SRP/CS

Security countermeasures should consider table below

Table 1 – Overview of foundational requirements and possible influence(s) on a SCS

Security foundational requirements	brief description	Possible influence(s) on a SCS
Identification and authentication control	Identify and authenticate all users (humans, software processes and devices) before allowing them to access to the control system.	Influence on safety integrity by modification or manipulation
Use control	Enforce the assigned privileges of an authenticated user (human, software process or device) to perform the requested action on the control system and monitor the use of these privileges.	Influence on safety integrity by modification or manipulation
System integrity	Ensure the integrity of the control system to prevent unauthorized manipulation.	Influence on safety integrity
Data confidentiality	Ensure the confidentiality of information on communication channels and in data repositories to prevent unauthorized disclosure	Possible indirect influence on safety integrity (e.g. not accessible information on the safety configuration)
Restricted data flow	Segment the control system via zones and conduits to limit the unnecessary flow of data.	Influence on safety integrity
Timely response to events	Respond to security violations by notifying the proper authority, reporting needed evidence of the violation and taking timely corrective action when incidents are discovered.	Possible indirect influence on safety integrity (e.g. by ignoring security violations, that impede to apply the appropriate counter measures)
Resource availability	Ensure the availability of the control system against the degradation or denial of essential services.	Influence on availability

Possible effects of security risk(s) to a SRP/CS

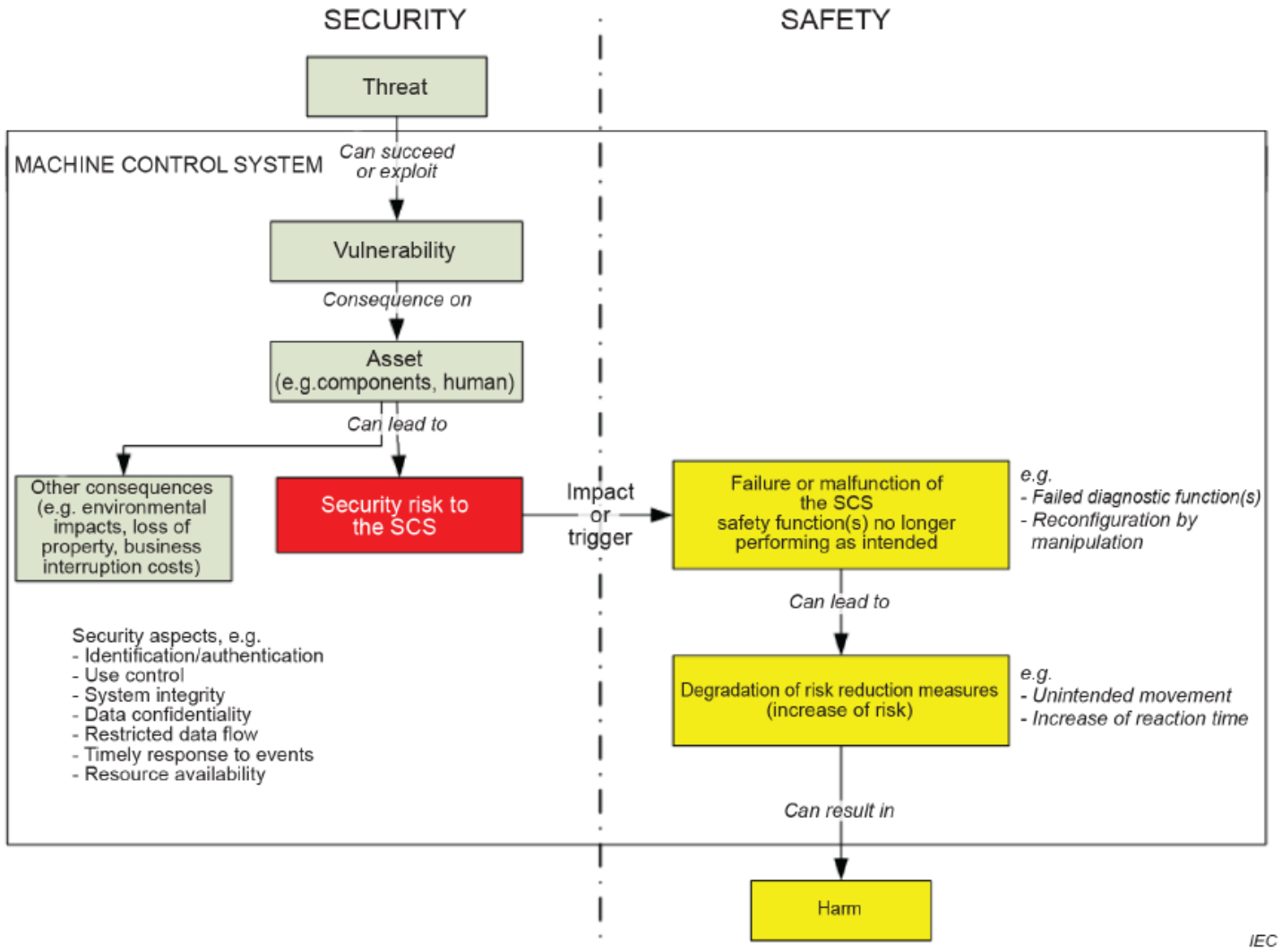
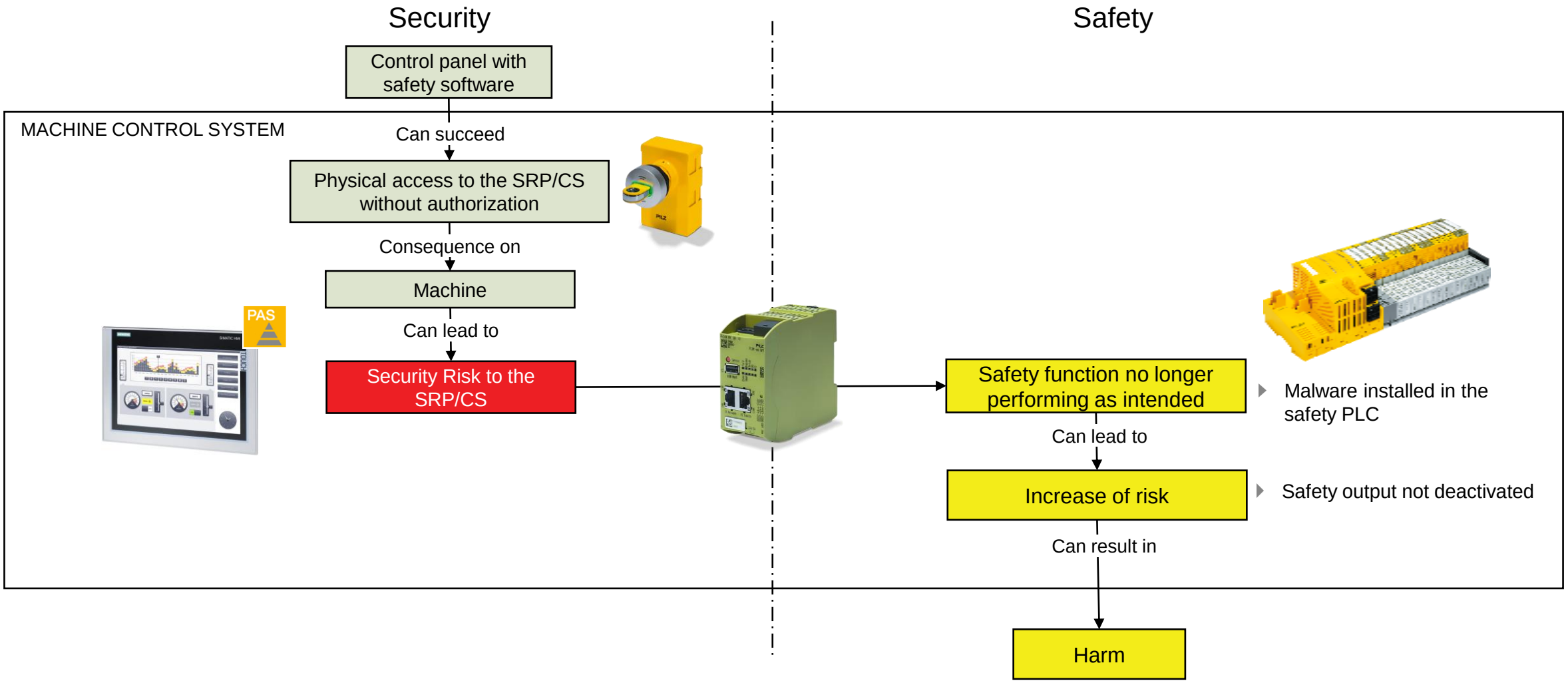


Figure 2 – Possible effects of security risk(s) to a SCS

Possible effects of security risk(s) to a SRP/CS



Caso Real

- En febrero de 2020, tres grandes fabricantes internacionales detectaron que sus dispositivos IIoT estaban infectados con malware. TrapX Security descubrió procesos de minado de criptomonedas en varios dispositivos IIoT, como impresoras, televisores y los **vehículos de guiado autónomo (AGV).**

- Los ataques formaban parte de una campaña en la que los hackers atacaron sistemas Windows 7 con malware. (Windows 7 había dejado de recibir parches de seguridad por parte de Microsoft, pero seguía operando en millones de equipos).

- El malware se extendió tan rápidamente en el centro productivo y en los AGV que afecto las comunicaciones entre los vehículos. Los AGV se utilizaban para los procesos de intralogística, con lo que si las comunicaciones se interrumpen o si los comandos o misiones eran generadas por un malware, podría suceder que vehículos se salgan de la trayectoria ocasionando daños físicos a equipos o personas.

- No cambiar las contraseñas por defecto, no habilitar las funciones de seguridad y la falta de cortafuegos proporcionan puntos de entrada para los actores de las amenazas. La simple eliminación de las contraseñas y los controles de usuario que acogen opciones de seguridad débiles puede ayudar a mantener la seguridad de las empresas de fabricación y ayudar a prevenir el despliegue de vulnerabilidades.

Fuente: Avertum

Correlaciones – Anexo XI

ANNEX XI

CORRELATION TABLE

Directive 2006/42/EC	This Regulation
Article 1	Article 2
Article 2	Article 3
Article 3	Article 8 and Article 9
Article 4	-
Article 5	Article 7
Article 6	Article 4
Article 7	Article 17 (1)
Article 8 (1)	Article 45
Article 8 (2)	-
Article 9	-
Article 10	Article 42 (3)
Article 11	Article 41 to Article 44
Article 12	Article 21
Article 13	Article 22
Article 14	Article 24 to Article 40
Article 15	Article 23
Article 16	Article 19
Article 17	Article 20
Article 18	Article 47
Article 19	-

Directive 2006/42/EC	This Regulation
Article 20	-
Article 21	Article 51
Article 21 a	Article 45
Article 22	Article 46
Article 23	Article 48
Article 24	-
Article 25	Article 49
Article 26	-
Article 27	-
Article 28	Article 52
Article 29	Article 52
Annex I - General principles	Annex III - General principles
Annex I, Section 1	Anne III, Section 1
Annex I, Section 2	Annex III, Section 2
Annex I, Section 3	Annex III, Section 3
Annex I, Section 4	Annex III, Section 4
Annex I, Section 5	Annex III, Section 5
Annex I, Section 6	Annex III, Section 6
Annex II, Parts A and B	Annex V
Annex III	-
Annex IV	Annex I
Annex V	Annex II
Annex VI	Annex X
Annex VII, Parts A and B	Annex IV, Parts A and B

Directive 2006/42/EC	This Regulation
Annex VIII	Annex VI
Annex IX	Annex VII
Annex X	Annex VIII
Annex XI	Article 28

PILZ

THE SPIRIT OF SAFETY

www.pilz.com