

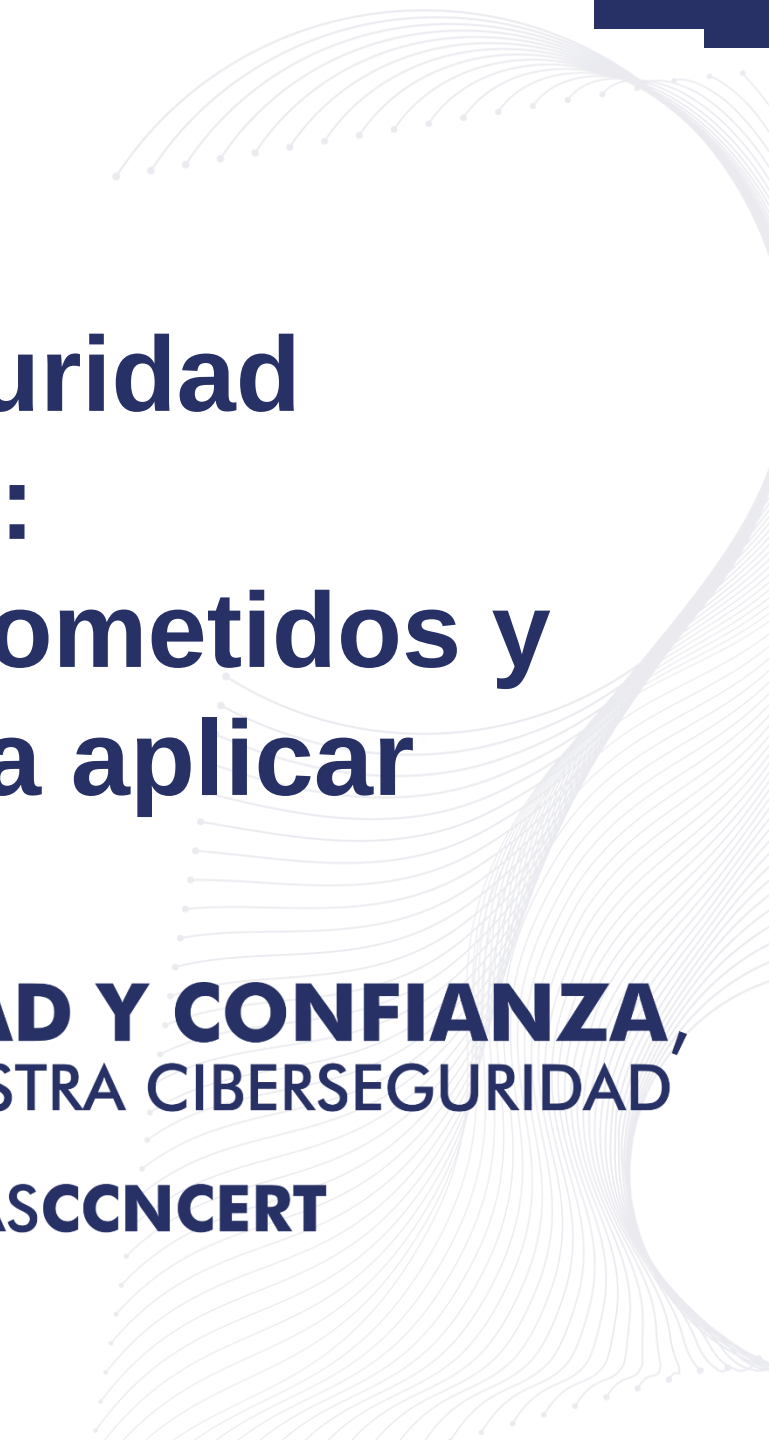
**XIII
JORNADAS
STIC
CCN-CERT**



**Ciberseguridad
Industrial:
Errores cometidos y
cambios a aplicar**

**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCCNCERT





Edorta Echave García

**Centro Ciberseguridad Industrial
Grupo LKS Next**

edorta.echave@es.cci-es.org

edorta.echave@secureit.es

Índice

1. Aproximación y necesidades

2. Tecnología

3. Procesos

4. Personas

5. Conclusiones



Aproximación y necesidades



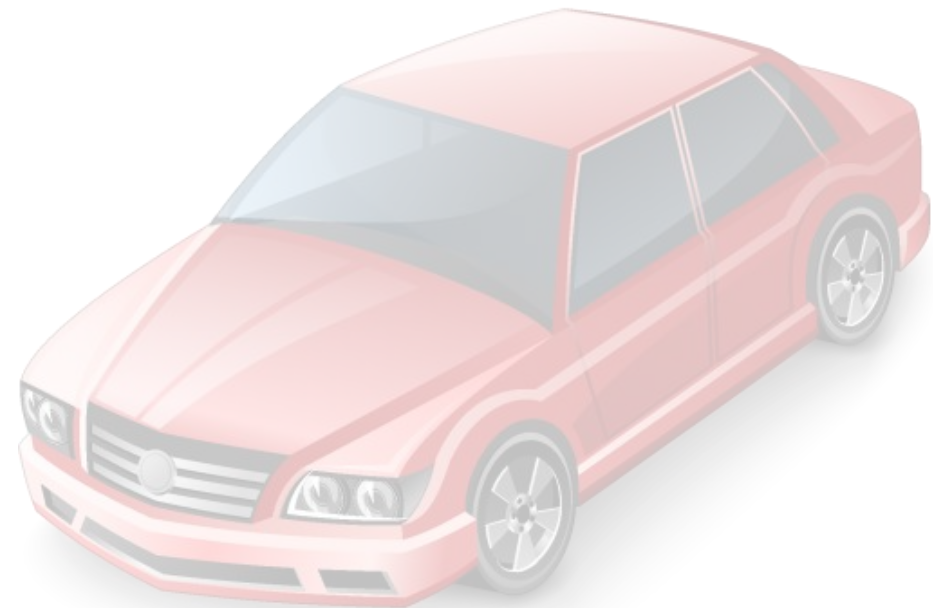
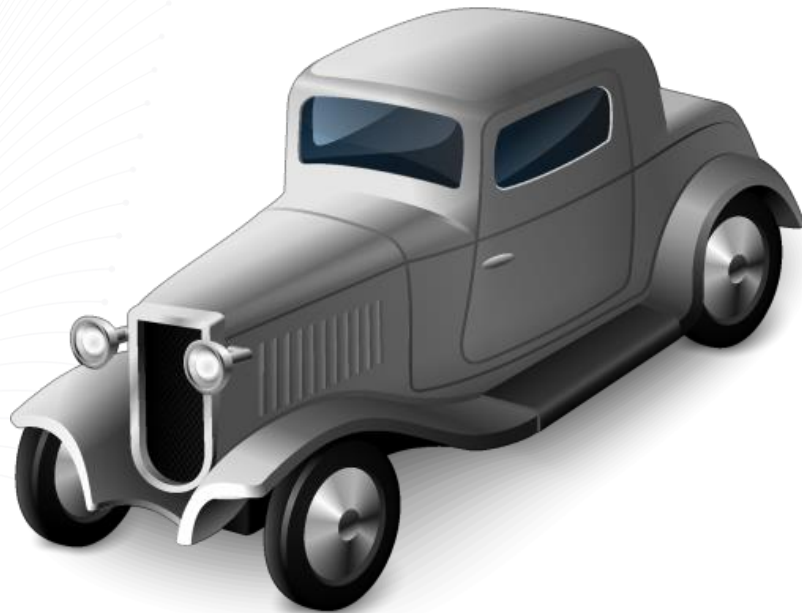
Aproximación y necesidades



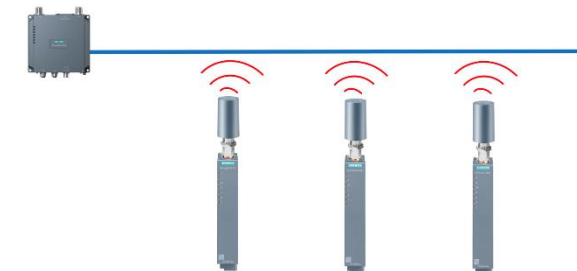
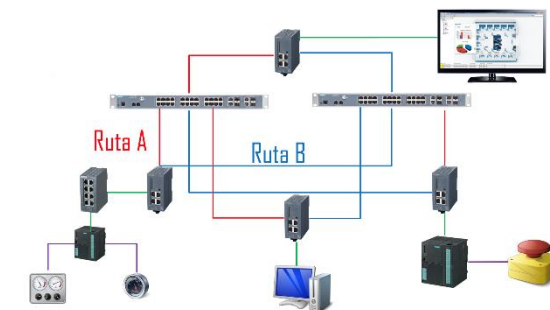
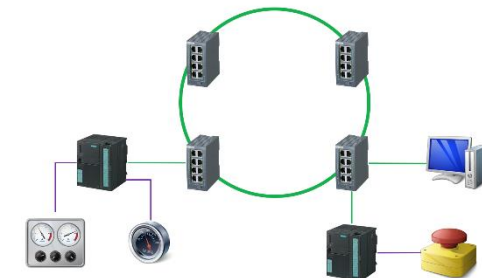
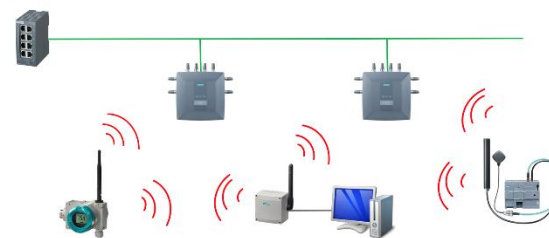
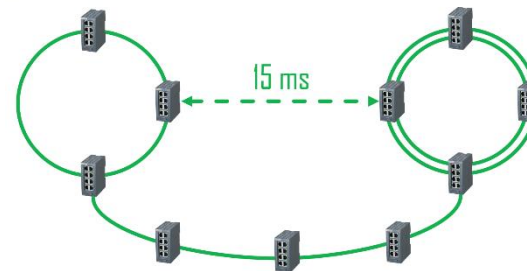
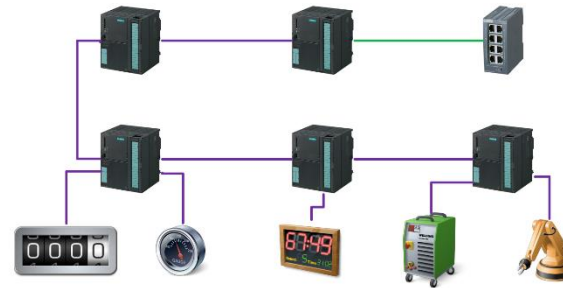
HONDA



Tecnología



Tecnología



PROFI[®]
NET

PROFI[®]
BUS



EtherCAT[®]

Safety over
EtherCAT[®]

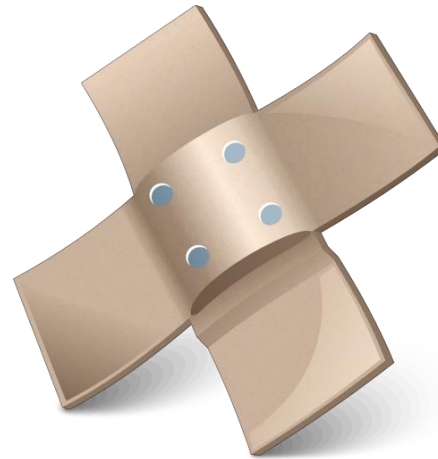
ETHERNET
POWERLINK

EtherNet/IP[™]

IO-Link

OPC UA[™]

Tecnología



PROFI[®]
NET

PROFI[®]
BUS



EtherCAT[®]

Safety over
EtherCAT[®]

ETHERNET
POWERLINK

EtherNet/IP[™]

IO-Link

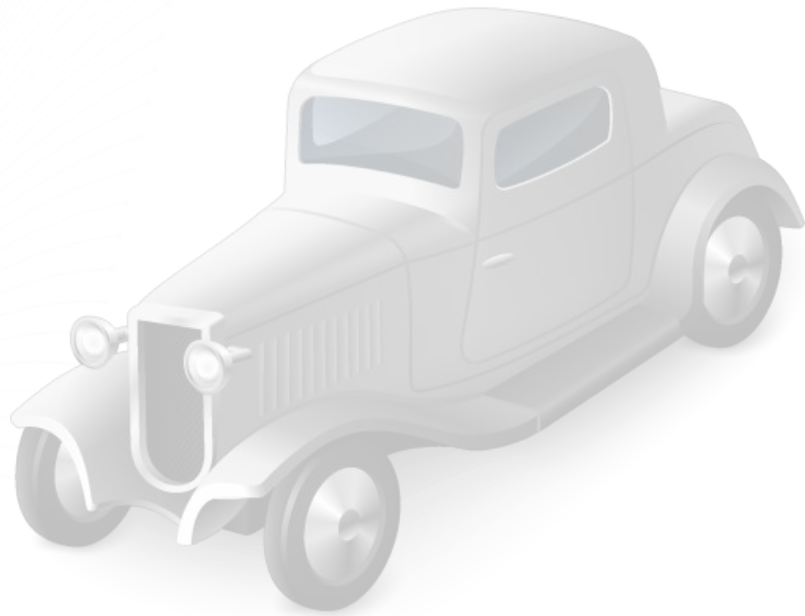
OPC UA[™]



URGENT/11



Tecnología



Tecnología



Procesos



KISS

Keep It Simple, Stupid

Procesos

Automotive Giants Hit by Massive Data Breach

Sunday, July 22, 2018



Security researcher UpGuard Cyber Risk disclosed Friday that sensitive documents from more than 100 manufacturing companies, including GM, Fiat Chrysler, Ford, Tesla, Toyota and VW were exposed on a publicly accessible server belonging to Level One Robotics.

The exposure via Level One Robotics, which provides industrial automation services, came through rsync, a common file transfer protocol that is used to back up large data sets, according to UpGuard Cyber Risk, news website Tech Crunch reported.

The breach exposed 157 gigabytes of data—a treasure trove of 10 years of assembly line schematics, factory floor plans and layouts, robotic configurations and documentation, ID badge request forms, VPN access request forms. The breach even included sensitive non-disclosed agreements, including one from Tesla.

Procesos

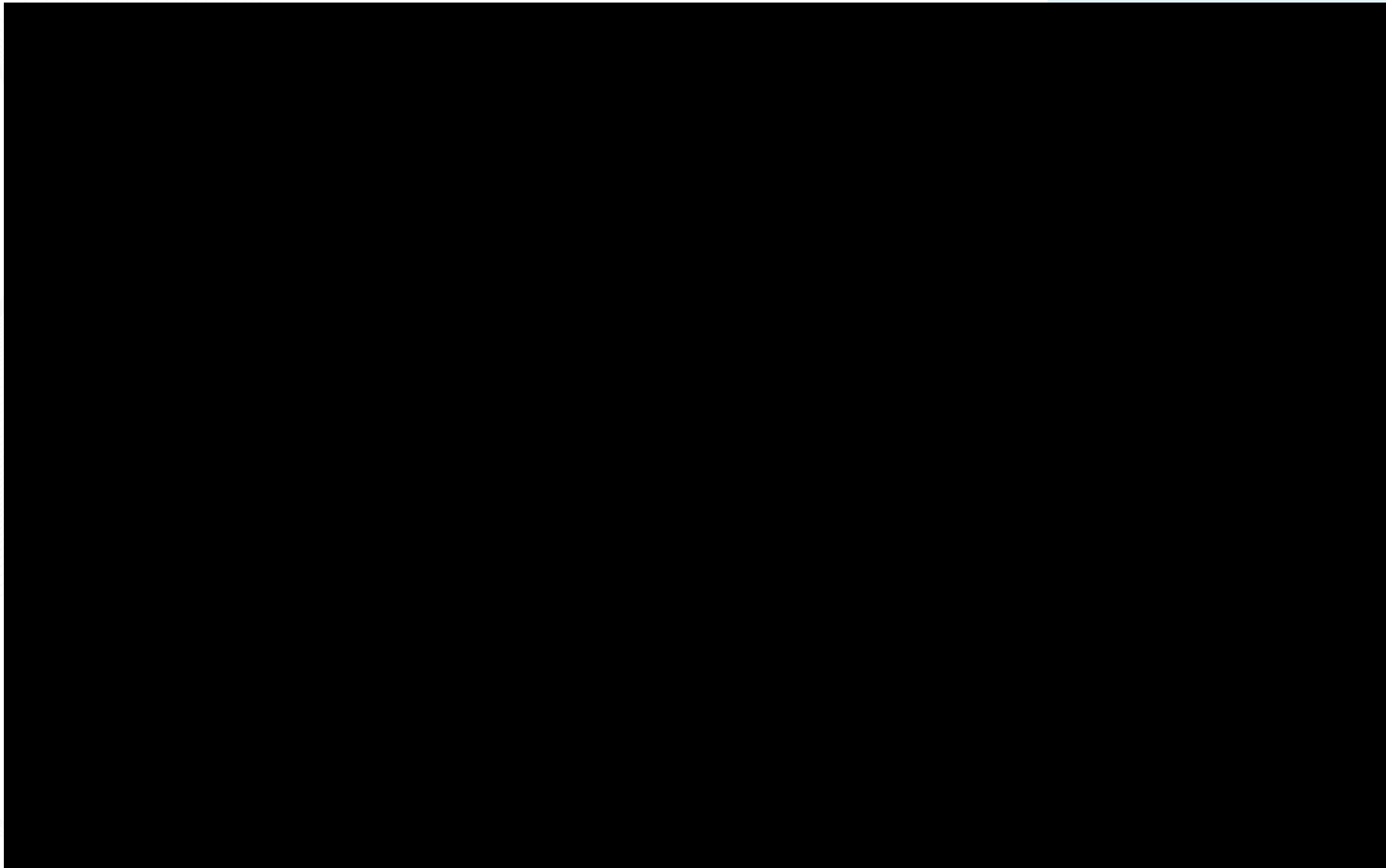
September 26, 2019

Airbus Hit by Series of Cyber Attacks on Suppliers: Security Sources

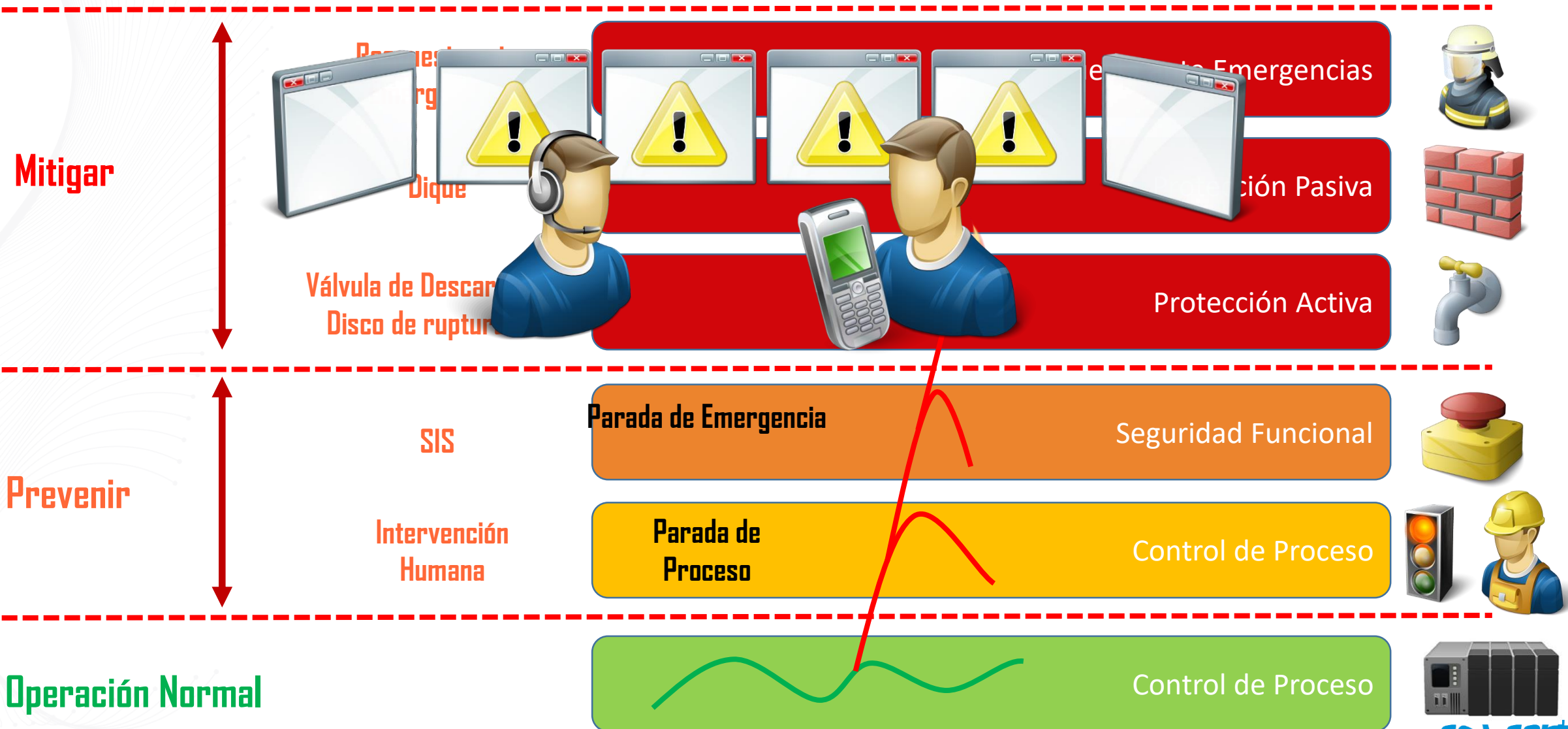
European aerospace giant Airbus has been hit by a series of attacks by hackers who have targeted its suppliers in their search for technical secrets, security sources told AFP, adding they suspected a China link.

Hackers have targeted British engine-maker Rolls-Royce and the French technology consultancy and supplier Expleo, as well as two other French contractors working for Airbus that AFP was unable to identify.

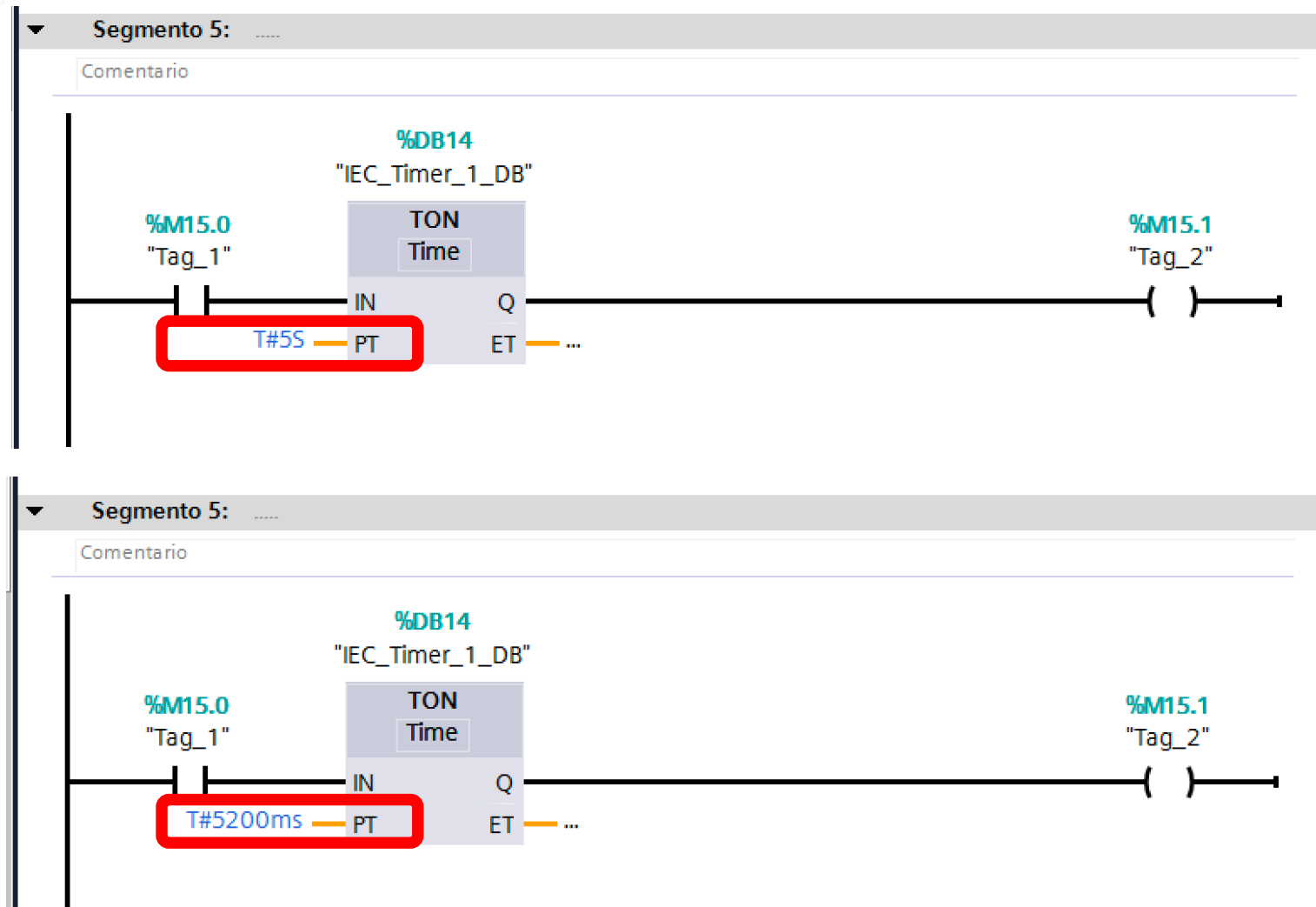
There have been four major attacks on Airbus in the last 12 months, according to two security sources involved in investigating the hacking.



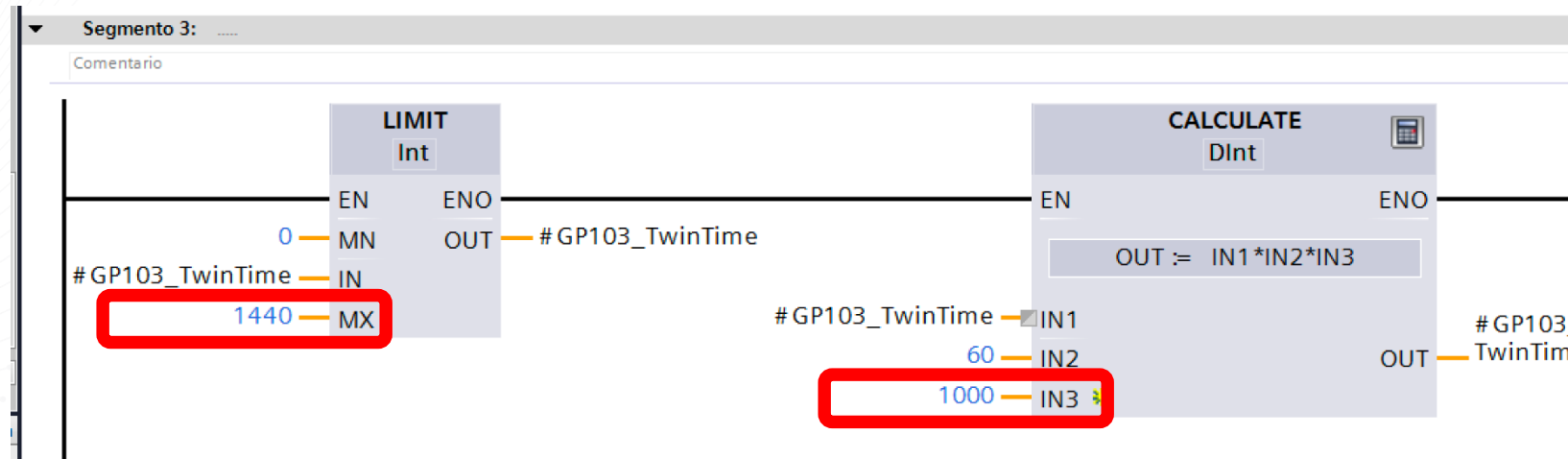
Procesos



Procesos



Procesos



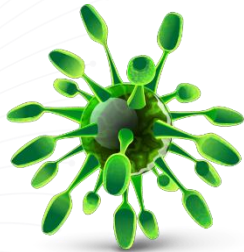
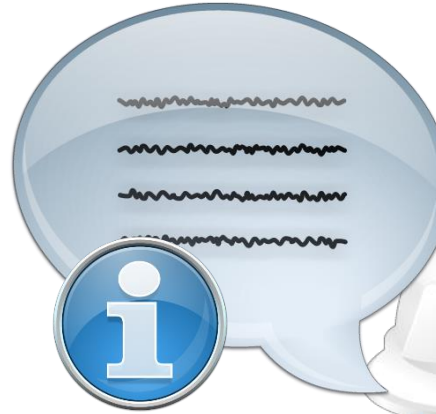
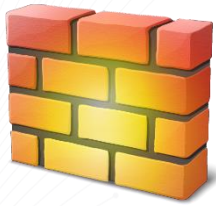
Personas



Personas



Personas



Personas



Conclusiones

“Nada podemos esperar, sino de nosotros mismos”

J.G. Artigas, 1764-1850

“Defendamos nuestros entornos, quizás, no haciéndolos más seguros, sino menos vulnerables”.

Edorta Echave 11/12/19

COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

XIII JORNADAS STIC CCN-CERT

ccn-cert
centro criptológico nacional