Sistema de Infraestructura del Conocimiento para la Experimentación Real mediante Células de Automatización Industrial

SICERCAI

Un nuevo paradigma a aplicar para la mejora de la Ciberseguridad en Sistemas de Control Industrial.

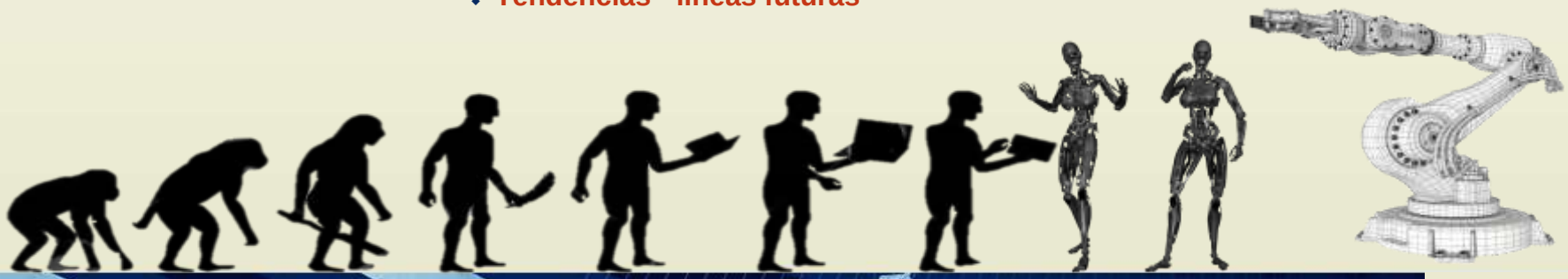
Junio 2021

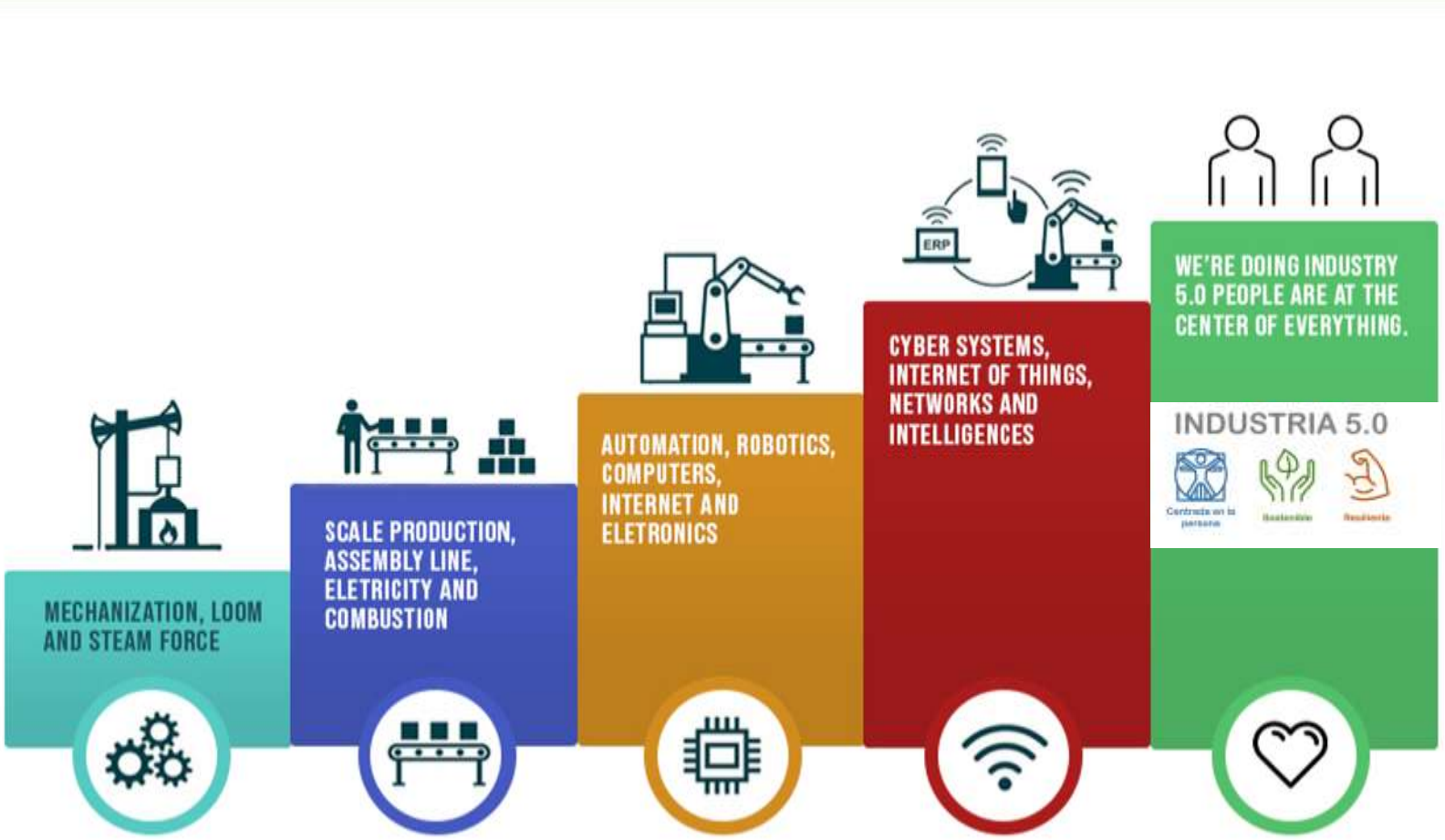
Síntesis curricular:

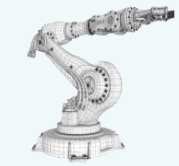
- **Master en Ingeniería de Sistemas y Control** por la Universidad UNED y U. Complutense de Madrid.
- **Doctorando Internacional en Ingeniería de Sistemas y Control** (Ciberseguridad aplicada a la Informática industrial, UNED).
- **Más de 15 años de experiencia** en Ciberseguridad de Sistemas de Información y Sistemas de Operación.
- Auditor senior en Ciberseguridad de Sistemas de Control Industrial como miembro de **Corporate Tecnology Cybersecurity Protection Service (CT CYS PRO) en SIEMENS**
- En la actualidad, **Técnico de Sistemas** | Cuerpo de Facultativos y Técnicos | Ministerio del Interior | CNP.

Agenda

- Necesidades y situaciones reales en entornos TO
  - Introducción y motivación de SICERCAI
- Visión holística de la ciberseguridad
  - SICERCAI
- Ventajas de la industria 4.0 Madurez de TI frente a TO
  - Cohesión de SICERCAI, estructura, topología
- Capacidad de prevención frente a mitigación
  - Metodología, materiales y resultados
- Contribución e innovación
  - Resultados
- CAI y laboratorio 4 tanques
  - Tendencias - líneas futuras




MECHANIZATION, LOOM AND STEAM FORCE
SCALE PRODUCTION, ASSEMBLY LINE, ELETRICITY AND COMBUSTION
AUTOMATION, ROBOTICS, COMPUTERS, INTERNET AND ELETRONICS
ERP
CYBER SYSTEMS, INTERNET OF THINGS, NETWORKS AND INTELLIGENCES
WE'RE DOING INDUSTRY 5.0 PEOPLE ARE AT THE CENTER OF EVERYTHING.
INDUSTRIA 5.0
1ª Revolución Industrial
2ª Revolución Industrial
3ª Revolución Industrial
4ª Revolución Industrial
5ª Revolución Industrial



?

☑ Necesidades y situaciones reales en entornos TO

TI

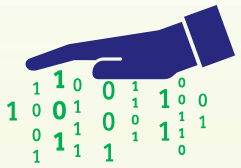
TO

Principales carencias en entornos de TO

1. Insuficientes/inexistentes segmentaciones de red
2. Gestión de activos dudosas
3. Implementación de ventanas de mantenimiento (ámbito de la seguridad)
4. Carencia de planes de administración de vulnerabilidades
5. Carencia de planes de planes de administración de parcheos y actualizaciones
6. Sistemas de identificación débiles
7. Débil seguridad física
8. Débil nivel de seguridad de aplicaciones
9. Software y componentes inseguros

¿Por qué ciberseguridad en Sistemas de Control Industrial?

Diferentes requisitos requieren conceptos diferentes o incluso adaptados

Seguridad Tecnologías Información		Seguridad Tecnologías Operación
Confidencialidad Integridad | Disponibilidad		**Disponibilidad** Integridad | Confidencialidad
Alta permisibilidad en altas latencias	**Tiempos de respuesta**	**Baja permisibilidad** en altas latencias
2/3 años, gran núm de proveedores	**Ciclo de vida**	**10/20** años proveedores muy específicos y sectoriales
Habitual e integrado en el proceso	**Evaluación del riesgo**	Realizado **si es obligatorio**
Común, fácil, definidas y automatizadas	**Antivirus/parches**	**Poco habitual**, complejo sin políticas definidas
Utilización de metodologías estándares	**Testeo y Auditorias**	**Inexistencia** de metodologías estándar
Fácil despliegue y comunmente obligatorias	**Administración de Vulnerabilidades**	**Poco habitual**, sin actuaciones forenses a penas

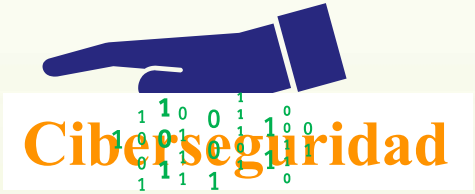
Security Topic	Office IT Systems	IACS Systems
Antivirus	Widely used and easily updated	complicated and often impossible to implement
Life Cycle	3-5 Years	5-20 Years
Awareness	Good	Not good
Patch Management	Often	Rare, approval from Plant manufacturers
Change Management	Regular and scheduled	Rare
Evaluation of log files	Established practice	Unusual practice
Time Dependency	Delays Accepted	Critical
Availability	Not always available, failures accepted	24*7
IT Security Awareness	Good	Poor
Security tests	Widespread	Rare and problematic
Testing environment	Available	Rarely available

Differences between Traditional IT Security and IACS Security
Fuente: Whitepaper IEC 62443

Introducción y motivaciones planteadas

- Los avances en las TI, proporcionan gran capacidad de interconexión a los entornos TO
- Grandes capacidades de adaptabilidad
- Importancia de ser capaces de recrear entornos reales industriales
- Heterogeneidad en componentes

Visión holística de la ciberseguridad



Holismo en Ciberseguridad
S.C.E.R.C.A.I.

- El holismo es un concepto creado en el año 1926 por Jan Christiaan Smuts
- Un sistema y sus propiedades se analizan como un todo
- De una manera Global e Integrada
- Se destierra el concepto de la funcionalidad global **como la simple suma de sus partes**

☑ Ventajas proporcionadas por la industria 4.0, Madurez de TI frente a TO

Fuente: infoPLC.net

Ventajas

- Mejora de la productividad
- Ahorro energético
- Aumento de EEE (eficiencia, eficacia y efectividad en el proceso)
- Incremento conocimiento (trabajo colaborativo)
- Creación de oportunidades de innovación
- Flexibilidad y agilidad en procesos
- Reducción de costos
- Aumento rentabilidad
- Reducción de emisiones nocivas para el planeta

SICERCAI

International Journal of Critical Infrastructure Protection 29 (2020) 100355

Contents lists available at ScienceDirect

International Journal of Critical Infrastructure Protection

journal homepage: www.elsevier.com/locate/ijcip

Obtaining high preventive and resilience capacities in critical infrastructure by industrial automation cells

Santiago G. González[a,*], S. Dormido Canto[b], José Sánchez Moreno[b]

[a] National Centre for the Protection of Infrastructures and Cybersecurity, Secretary of State for Security, Ministry of Interior Spain, CETSE, El Pardo, Madrid, 28048, Spain

[b] Department of Computer Science and Automatic Control, Universidad Nacional Educación a Distancia (UNED), Madrid, 28040, Spain

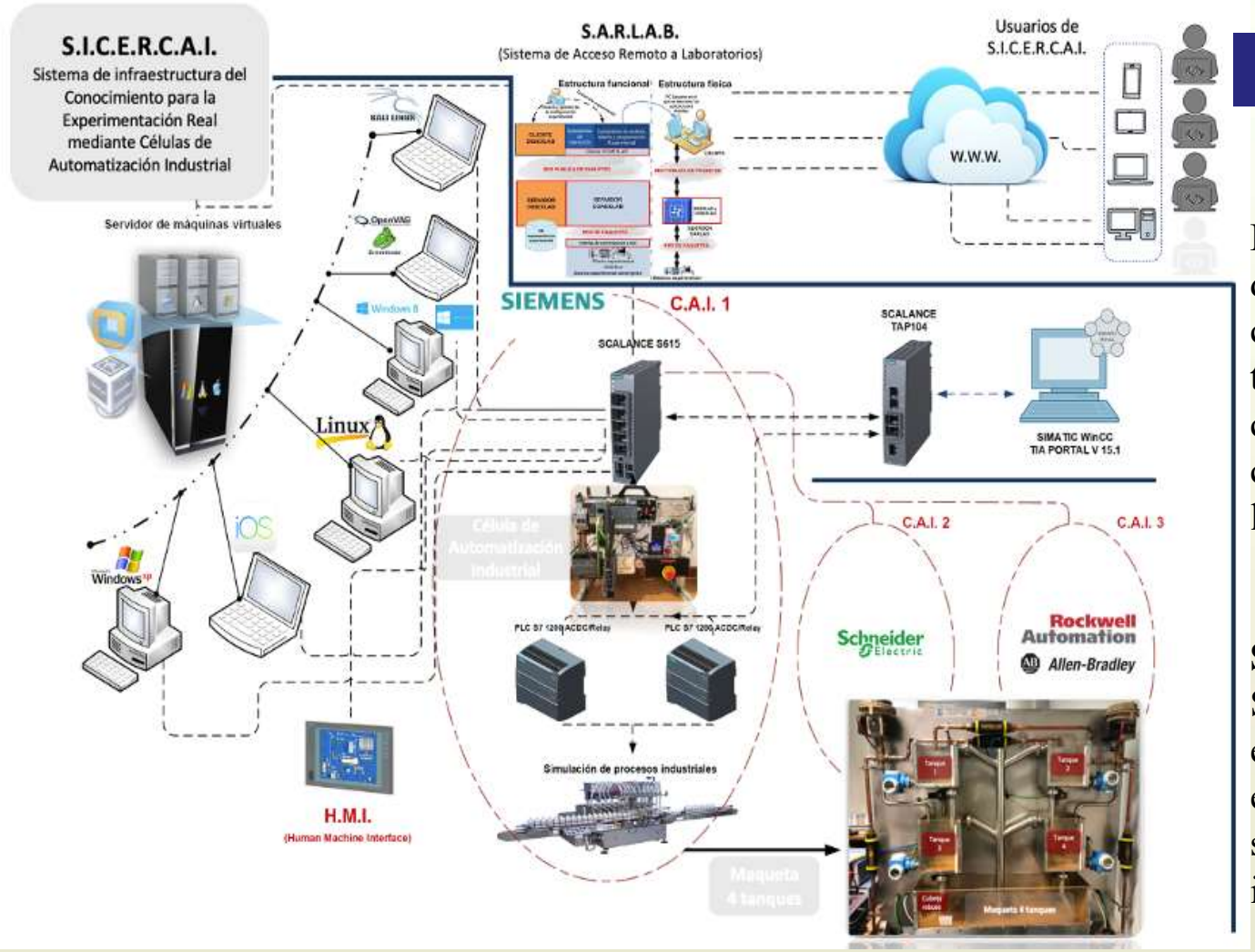
ARTICLE INFO

Article history:
Received 19 July 2019
Revised 7 March 2020
Accepted 29 March 2020
Available online 3 July 2020

Keywords:
Cybersecurity
Industrial control system
Critical infrastructure
National Security
Cyber Resilience

ABSTRACT

The advances in Information Technologies (ITs) are providing Industrial Control Systems (ICS) with a great capacity for interconnection and adaptability. However, the use of communication networks makes ICS highly vulnerable. Consequently, it is essential to develop methodologies for the identification and subsequent classification of the ICS that intervene in critical infrastructure assets with any level of complexity, scalability and heterogeneity. The System and Infrastructure of Knowledge for Real Experimentation by means of Cells of Industrial Automation (SIKRECIA), described in this work, provides new capabilities for research, development, simulation and testing of the functioning of these systems, and the ability to foresee the behavior of a specific system in industrial production. The scenarios recreated through SIKRECIA have the ability to anticipate new threats that affect the ICS of critical infrastructures. Using SIKRECIA, a specific vulnerability of a PLC has been verified through the engineering programmed for the management of a traffic light control system. The results obtained demonstrate the high dependence between IT and OT (Operation Technologies) systems and therefore the importance of being able to recreate those environments before entering into operation. As SIKRECIA is an open system, it can use components from different industrial manufacturers to cover the existing architectures in the process industry.



Arquitectura de RED

Lo importante para que la digitalización funcione es una colaboración exitosa entre las tecnología TO e TI y que cada una de las partes comprenda las necesidades de la otra.

SARLAB

Sub-sistema, modular y escalable que proporciona un ecosistema completo de soluciones para las TI involucradas.

☑ Capacidad de prevención frente a mitigación

Ciber-Inteligencia

Detección y gestión de las nuevas amenazas y vulnerabilidades para dar una respuesta actualizada y dinámica **frente a los riesgos a los que está expuesta la organización**

Ciber-resiliencia

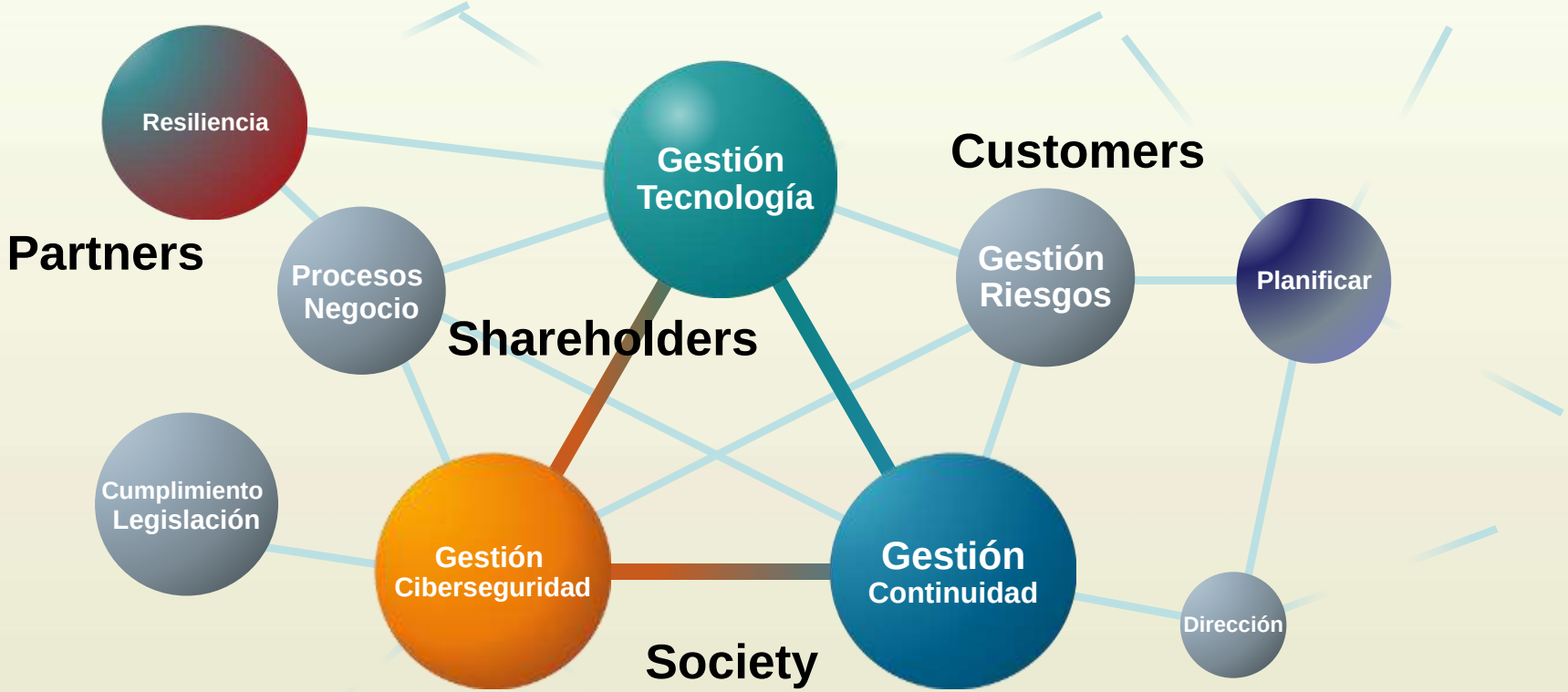
Anticipar, en materia de ciber-resiliencia, significa tener la capacidad de prevenir que se hagan realidad las amenazas, **recurriendo a procedimientos establecidos por la propia organización y a tecnologías de ciberseguridad avanzada** que ayuden a gestionar los diferentes tipos de riesgos detectados

☑ Contribución e innovación

S. I. C. E. R. C. A. I.

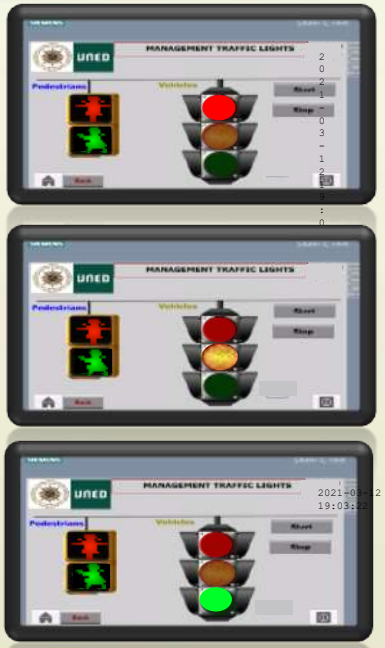
- Nuevo concepto de simulación en entornos industriales
- Heterogéneo
- Gran adaptabilidad y altas capacidades de cohesión con diferentes fabricantes
- 100% seguro

Componentes Clave
Resiliencia Funcional en Ciberseguridad



Célula Automatización Industrial
Maqueta 4 tanques mezcla de fluidos

☑ CAI y Laboratorio 4 tanques



Si quieres ir rápido, camina solo, pero si quieres llegar lejos, ve acompañado.

Proverbio africano

Muchas gracias por su atención !!!

Santiago G. González

Doctorando en Ingeniaría de Sistemas y Control

Ciberseguridad en SACI | IC

Email: Santiago.gonzalez@invi.uned.es
Linkedin:www.linkedin.com/in/santiago-g-gonzalez

Firmado digitalmente por GONZALEZ GONZALEZ SANTIAGO - 03465430C el día 07/06/2021 con un certificado emitido por AC FNMT Usuarios

Junio 2021