SISTEMAS DE CONOCIMIENTO POR EXPERIMENTACIÓN REAL MEDIANTE CÉLULAS DE AUTOMATIZACIÓN INDUSTRIAL

KNOWLEDGE SYSTEMS FOR REAL EXPERIMENTATION BY MEANS OF INDUSTRIAL AUTOMATION CELLS

Santiago G.-González
Centro Nacional para la Protección de Infraestructuras y Ciberseguridad (CNPIC), Ministerio del Interior
España, santiago.gonzalez@invi.uned.es

Sebastián Dormido Canto, José Sánchez Moreno
Departamento de Informática y Automática, UNED C/ Juan del Rosal 16, 28040,Madrid,
{sebas,jsanchez}@dia.uned.es

Resumen

En la actualidad, las amenazas hacia las infraestructuras críticas están consideradas por la UE (Unión Europea) así como por otros estamentos internacionales, uno de los riesgos más graves para la estabilidad de sus estados, afectando su disfuncionalidad gravemente a la economía y la sociedad. Ello se debe, específicamente, a que los avances constantes en las tecnologías de la información y las comunicaciones se trasladan a los Sistemas de Control Industrial (SCI) proporcionando una gran flexibilidad de interconexión gracias a su escalabilidad y a modelos con una conectividad cada vez más simple e intuitiva. El uso de las redes de comunicación hace que estos sistemas sean altamente vulnerables, ya que no fueron diseñados originalmente para este tipo de expansión o formas de comunicaciones. En sus orígenes fueron diseñados con el propósito principal de otorgar la máxima disponibilidad de procesos. Sin embargo, hoy en día, la disponibilidad sigue siendo su misión principal. En este trabajo, se presenta el sistema SICERCAI[1], el cual aporta nuevas capacidades de investigación, desarrollo, simulación y banco de pruebas del funcionamiento de estos sistemas. A su vez, otorga capacidades de anticipación del comportamiento de un sistema en producción industrial y, como consecuencia directa, altas capacidades de ciberresiliencia. Como es un sistema abierto a la interconexión, permite la construcción de Células de Automatización Industrial (CAI) con elementos de los diferentes fabricantes de componentes industriales, pudiéndose agregar al sistema SICERCAI para cubrir el 100% de las posibilidades arquitectónicas existentes en la industria actual. De esta manera se consiguen recrear entornos industriales de carácter híbrido, siendo este aspecto el que más se asemeja a la realidad en la industria.

Palabras clave: Ciberseguridad, SCADA, PLC, Sistemas de Control Industrial, Infraestructuras Críticas, Ciberresiliencia, Células de Automatización Industrial.

Abstract

*This work, by the development of the SIKERCIA1 system, provides new capacities of research, development, simulation and testing of the functioning of critical infrastructures, and the capacity of anticipating the behavior of a system in industrial production. At the same time, SIKERCIA provides high capacities of cyber-resilience and also describes the condition of maturity with regard to the cybersecurity of the services implemented in SIKERCIA and catalogued as essential. All the above is provided by a system that has been tested, analyzing industrial environments. As it is a system o*pen to interconnection, it allows the construction of Industrial Automation Cells using industrial components from different manufacturers, which can be added to the SIKERCIA system to cover 100% of the existing architectural possibilities in the current industry.

Keywords: Cybersecurity, SCADA, PLC, Industrial Control System, Critical Infrastructure, Cyber-Resilience.

1 INTRODUCCIÓN

La investigación que se presenta en esta ponencia es fruto del trabajo que se está desarrollando en el área de la ciberseguridad en SCI. Este trabajo aporta capacidades de investigación, desarrollo, simulación y testeo del funcionamiento de estos sistemas catalogados como esenciales y o críticos por distintos estamentos nacionales e internacionales [2,32,33]. De

[1] Sistemas e Infraestructuras de Conocimiento por Experimentación Real a través Células de Automatización Industrial.

igual manera, se describe el estado de madurez en materia de ciberseguridad de los componentes y arquitecturas desplegados en SICERCAI. A su vez, se proporcionan altas capacidades para la realización de análisis del tipo forense, ante intervenciones no permitidas y análisis de patrones de comportamiento a través de diferentes herramientas existentes en el mercado (SIEM[2]). Desde el campo universitario, se debe tomar la iniciativa de aportar entornos de simulación [5], pruebas y testeos de componentes reales de la industria así como de las arquitecturas desplegadas al efecto. Se debe relegar a un segundo plano la importancia de los entornos virtualizados, ya que los sistemas industriales requieren de entornos reales y en completa disposición de funcionamiento operativo. Estas acciones generan confianza en el mundo de las Tecnologías de la Operación (TO). Este aporte implica un nivel extra sobre los controles a realizar en una arquitectura de red industrial. Con la CAI, desarrollada como herramienta básica para este estudio y bajo una arquitectura del fabricante SIEMENS, se ha conseguido poder implementar a nivel atómico todos y cada uno de los procesos llevados a cabo en cualquier entorno industrial:

- Se podrá conectar el controlador lógico programable (PLC[3]) S7 1200 de SIEMENS utilizado a través de un servidor OPC con Matlab y Simulink. De esta manera se podrá obtener patrones de comportamiento en entornos industriales.
- Realización de simulaciones de procesos ininterrumpidos en el tiempo y de manera completamente automática.
- Simulación de procesos discretos en el tiempo. Esta simulación dependerá de los datos aportados por agentes externos (sensores).
- Diseño de controladores PID (mecanismos de control por realimentación) propios de los PLC.
- Análisis de patrones gráficos obtenidos a partir de los procesos enumerados con anterioridad.
- Conectividad local y remota bajo arquitecturas multiplataforma, otorgando la capacidad del análisis de vulnerabilidades asociadas a los SCI, a los sistemas operativos y lo que es más importante, a la combinación de ambos.
- Despliegue de sistemas SIEM [34], no solo adscritos a TI (Tecnologías de la Información) sino a su vez a TO. En definitiva, lo que esta investigación trata de determinar, es la efectividad de la anticipación mediante el conocimiento de la toma de medidas preventivas y como consecuencia directa de este aprendizaje, capacidades de resiliencia en la ciberseguridad [1,27,28,32] en la convergencia de los mundos TI y TO.

[2] Security Information and Event Management.

[3] Programmable Logic Controller.

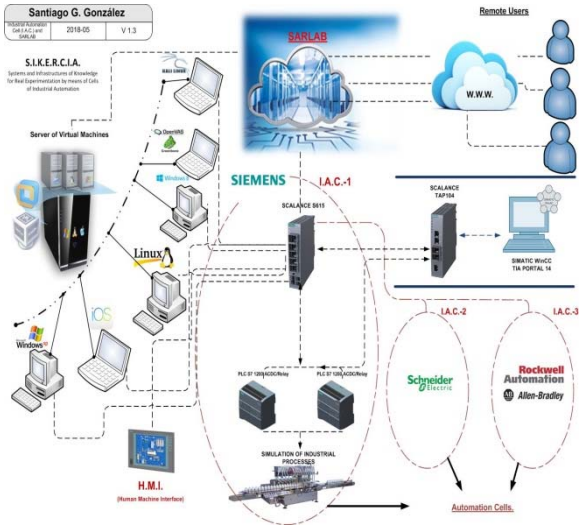

Figura 1: Esquema de SICERCAI

Esta investigación se ha llevado a cabo en un área muy específica, *la ciberseguridad industrial*. Concretamente, proporciona un valor diferenciador en el campo de los servicios esenciales [29,30,31]. Estos servicios esenciales actualmente conocidos como *infraestructuras estratégicas y / o críticas tienen como componentes del campo operacional sistemas de control industrial (SCI)para la gestión de sus procesos* [6,7,11]. Estas infraestructuras han pasado a adoptar una posición relevante en la gestión de riesgos y crisis de un Estado. Por lo tanto, la ciberseguridad, relacionada con infraestructuras-estratégicas-criticas (IEC), es clave para el funcionamiento normal del ordenamiento social de un país. Si bien las definiciones de infraestructura crítica varían de un país a otro, prácticamente todos los países identifican los tipos de infraestructura en función de los servicios que brindan [8]. Específicamente, se pueden mencionar las plantas de energía, redes de comunicaciones y tecnologías de la información, finanzas, salud, alimentos, agua, transporte, producción, almacenamiento y transporte de mercancías peligrosas. Desde el Gobierno de España, fue promulgada la *Ley para la Protección de las Infraestructuras Críticas (LPIC)* [20] y todos sus puntos se han desarrollado en el *Reglamento de Protección de la Infraestructuras Críticas* (RPIC) [26]. En España, se han definido doce Sectores Estratégicos directamente implicados en la LPIC, que a su vez se dividen en subsectores; *Administración, Espacio, Industria Nuclear, Industria Química, Instalaciones de Investigación, Agua, Energía, Salud, Tecnologías de Información y Comunicación (TIC), Transporte, Alimentos y Sistema Financiero y Tributario*.

A su vez, la *Estrategia de Seguridad Nacional (ESN)* de 2011 [28,29], enumera las ciberamenazas y los ciberataques como uno de los principales riesgos para la seguridad nacional. En 2013 se aprobó una ESN

mejorada. Esta nueva estrategia ayudó a definir nuevos escenarios estratégicos e involucrar a la sociedad civil más activamente en la seguridad nacional. En su cuarto capítulo, dedicado a líneas de acción clave, ESN *identifica la ciberseguridad como una de las doce áreas de trabajo prioritarias*. El desafío de seguridad cibernética se equipara con las amenazas tradicionales, como la lucha contra el terrorismo.

2 OBJETIVOS

Desde el principio se planteó como objetivo principal, abordar la problemática desde un punto de vista global. Esto implicó la imposibilidad de afrontar por igual las peculiaridades del mundo de las TI y TO. De la convergencia llevada a cabo entre las TI y TO surge una nueva definición en el ámbito de la ciberseguridad de entornos industriales, *CTOI*[4]. Este concepto debe venir a englobar el campo tecnológico y la más pura definición de los procesos mecánicos y electrónicos soportados bajo la intercomunicación de los mismos. Como consecuencia de esta situación, los objetivos planteados y alcanzados en el trabajo de investigación llevado a cabo han sido:

1. Evaluación de la efectividad de una determinada arquitectura TI-TO desplegada, basándose en la puesta en producción real de las arquitecturas de red y operacional.
2. Análisis y desarrollo de diferentes patrones de comportamiento bajo creación de sistemas de modelado y evaluación con capacidad de ser incorporados en sistemas SIEM.
3. Portabilidad de la célula de automatización para su rápida conectividad fuera del ámbito de laboratorios remotos y virtuales [4,19,21,22,23].
4. Poner en práctica la alta capacidad de cohesión con tecnologías de diferentes fabricantes, a través de protocolos de comunicación estandarizados (PROFINET-PROFIBUS) y propietarios (S7)[5]
5. Otorgar un acceso real y remoto al entorno de programación de CAI.
6. Proporcionar capacidad de despliegue de cualquier sistema operativo cuya misión sea interactuar con el laboratorio, a través de un de un servidor de máquinas virtuales, implementando un alto grado de diversidad de configuraciones, y otorgando una autonomía completa al usuario del sistema.
7. Conceder capacidad de analizar el comportamiento en tiempo real de vulnerabilidades de los Sistemas Operativos (SO), de los sistemas de control industrial y lo más interesante, el de ambos a la vez.
8. Facilitar e informar de la manera legal y adecuada, del descubrimiento de algún tipo de vulnerabilidad TI-TO del tipo "0-Day[6]" hallada durante los despliegues.
9. Obtener patrones de comportamiento a través de diferentes fuentes:
   - Sistemas SIEM ámbito TI y su aplicación al de la Operación (TO).
   - Bases de Datos desplegada en el sistema SCADA, (acrónimo de Supervisory Control And Data Acquisition).
   - Reconocedor de patrones gráficos generados por variables de ámbito industrial.
10. Generar conocimiento extrapolable al campo universitario, infraestructuras críticas españolas, europeas y fabricantes de dispositivos Industriales [9,10,12].

3 METODOLOGÍA, MATERIALES Y ANÁLISIS

La metodología desarrollada se ha llevado a cabo de forma modular y por etapas para cumplir con los objetivos establecidos en este trabajo. Como se detalla en la descripción de los objetivos de este proyecto, fue necesario considerar, desde un punto de vista global, la unión de los mundos de TI y TO, no perdiendo de vista en ningún momento esta premisa. Como resultado del concepto CTOI, se explora una nueva forma de experimentar en el campo de la ciberseguridad industrial, creando un sistema controlado y altamente configurable para los requisitos de las pruebas que se ejecutarán [15,25]

4 SICERCAI

El sistema en su conjunto, llamado SICERCAI, otorga, a través de sus diferentes componentes, un acceso remoto y seguro, pasando por un área de configuración personalizada en función a las necesidades, al entorno de producción. Desde este entorno y tras ser administrado el acceso haciendo uso de SARLAB[7], accedemos a la parte de ingeniería industrial. Previo al acceso de la parte OT, se pone a disposición de los usuarios de un catálogo de diferentes máquinas virtuales. Estas máquinas virtuales se encuentran disponibles y son configurables de acuerdo con los objetivos previstos para la experimentación concreta. Esto proporciona

[4] Definición que agrupa los Componentes en las Tecnologías de Operación en la Industria.

[5] Protocolo de comunicación propietario de SIEMENS.

[6] Vulnerabilidad, para la cual, a día de su descubrimiento, no existe corrección para su securización.

[7] Sistema de Acceso Remoto a Laboratorios.

acceso real a las diversas celdas de automatización industrial existentes. Esta arquitectura incluye todos los componentes CTOI creados en este proyecto. Permite el desarrollo y la evaluación de las diferentes arquitecturas propuestas remotamente por la comunidad de usuarios. Otorga acceso controlado y ordenado a la comunidad que hace uso del sistema, mientras que el conocimiento generado por las diversas combinaciones de instrumentación se puede extrapolar al mundo académico, las infraestructuras críticas españolas, europeas y a los fabricantes de dispositivos industriales.

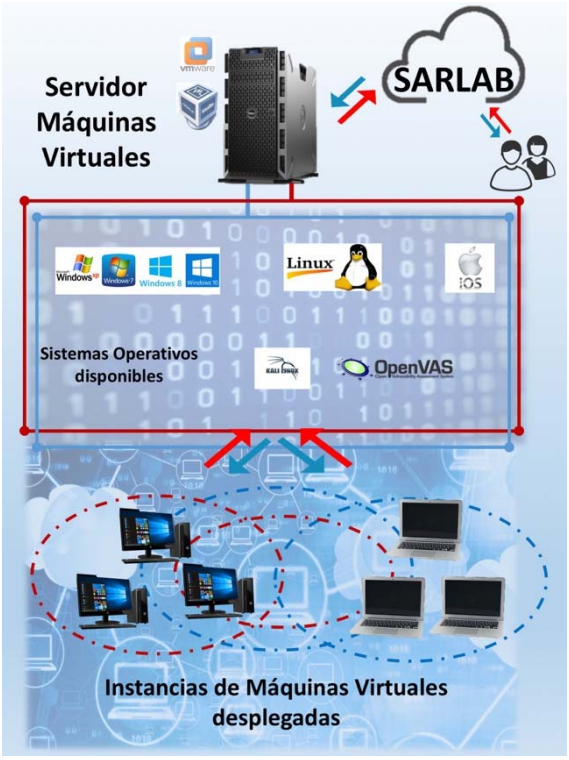

Figura 3: Esquema Servidor de máquinas virtuales.

4.1 SARLAB

SARLAB es la parte del sistema, encargado de realizar el control en las comunicaciones para la realización de un APLR[8]. Estas comunicaciones son las materializadas a través de los protocolos TCP / IP, Así mismo controla el flujo de datos entre el usuario (conectado a Internet) y SICERCAI (conectado en la red local al laboratorio desplegado y con la operatividad de campo. SARLAB también es responsable de administrar la concurrencia permitida para cada tipo de acceso a SICERCAI, brindándole la capacidad de acceso colaborativo [21,22,23].

4.2 SERVIDOR DE MÁQUINAS VIRTUALES

El servidor genera las maquinas virtuales que el usuario necesite. Se ofrece la posibilidad de usar diferentes sistemas operativos (S.O.). Los S.O. son clasificados en tres grandes grupos, siendo la funcionalidad el aspecto diferenciador:
Pentesting, sistemas de producción y sistemas de programación y adquisición de conocimiento.

1. *El área de pentesting* facilitará la evaluación del sistema operativo, siendo uno de estos SO OpenVAS que otorga funcionalidad para la creación de scripts de evaluación y búsqueda de vulnerabilidades de dispositivos industriales; un Kali Linux, varias herramientas de auditoría de red y un sistema de auditoría específico para entornos industriales, SamuraiSTFU.
2. En la parte de sistemas de producción e ingeniería operacional, se encuentran disponibles diversas versiones de sistemas operativos Windows (Windows 7, 10, etc.), que admiten una amplia gama de posibilidades relacionadas con el funcionamiento de los sistemas de acuerdo con los sistemas de programación de entornos industriales (por ejemplo, TIA Portal V13-15, WinCC), así como la simulación de redes corporativas como parte integral de las redes industriales en producción. También se extiende a los sistemas de producción en DMZ, analizando las posibles fallas de seguridad resultantes de los SO vulnerabilidades, arquitecturas de red o sistemas de programación de PLC.

En paralelo a todos estos SO, hay un sistema SCADA implementado a través de un WinCC flexible V8, una parte integral junto con el TIA Portal.

3. Finalmente la funcionalidad relativa a los sistemas de programación y adquisición de conocimiento, se implementan a través del comportamiento de cada una de las células de automatización industrial desplegadas, incluidos los accesos a componentes de automatización (modelado).

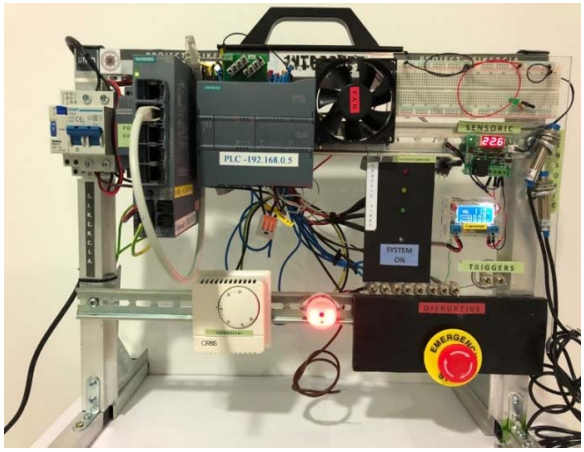

Figura 2: Célula de Automatización Industrial SIEMENS.

[8] Acceso práctico al laboratorio remoto.

4.3 CÉLULA DE AUTOMATIZACIÓN INDUSTRIAL

La CAI realizada se ha implementado con elementos de SIEMENS (controla el 33% de la tecnología industrial disponible hoy en día en el mercado).
En concreto se ha utilizado un PLC S7 1200, 1214 AC / DC Relay. Este PLC tiene un módulo de activación incorporado que es capaz de actuar directamente en las entradas digitales del del controlador lógico programable, proporcionando acceso manual a las mismas. Se ha incorporado un firewall industrial SCALANCE S615. El módulo de seguridad SCALANCE S615 tiene cinco puertos Ethernet que ofrecen protección para diversas topologías de red a través de firewall o VPN de red privada virtual (IPsec y OpenVPN) y permiten la implementación flexible de conceptos de seguridad. Los usuarios pueden configurar hasta cinco zonas seguras de red las cuales pueden ser gestionadas con reglas independientes de firewall y routing. Con la interfaz de configuración automática, el SCALANCE S615, se puede integrar y parametrizar fácilmente con la plataforma de gestión SINEMA Remote Connect. El S615 permite la creación de varias VLAN para que, de acuerdo con los permisos otorgados a las diferentes máquinas virtuales, se permita el acceso bidireccional entre el PLC-HMI (Human Machine Interface), el Sistema de Programación PLC (TIA Portal), el PLC-SCADA. La célula de automatización a su vez, consiste en un panel de sensores que proporciona señales discretas a lo largo del tiempo proporcionadas por sensores de detección de metales y sondas de temperatura, que el PLC interpreta y programa para este fin en la HMI creado en el sistema. Del mismo modo, se incorpora un indicador lumínico que emula un semáforo, cuya implementación se recrea con un TIA Portal que simula un proceso continuo. Las señales y los tiempos están programados en el PLC, que a su vez está diseñado para que, en caso de una interrupción lógica o física del sistema (ataque cibernético o intrusión física no autorizada), se restablezca y continúe funcionando. Estos entornos han sido programados para realizar simulaciones de ciberataques directos al PLC, intentando violar el firewall industrial, atacando el servidor web habilitado en el PLC o probando la combinación de los S.O., después de haber realizado cambios en las versiones de firmware de las automatizaciones industriales y actualizaciones de las máquinas de programación industrial. Los lenguajes de programación soportados por la plataforma TIA Portal, y con los que se han diseñado las funcionalidades de la CAI de SIEMENS son; FUP, KOP y AWL.

- *FUP*: es un lenguaje gráfico de Step7 que usa bloques de álgebra booleana para representar la lógica. También permite representar funciones complejas (por ejemplo, funciones matemáticas) por medio de tablas lógicas. Tiene la ventaja de mostrar las diferentes lógicas agrupadas por bloques y tener bloques complejos.
- *KOP:* Es un esquema de contactos, (escalera). Es un lenguaje gráfico de Step 7 y uno de los más extendidos de todos los lenguajes de programación.
- *AWL:* es un lenguaje de programación textual orientado a máquina. Las instrucciones son, en gran medida, equivalentes a los pasos llevados a cabo por la CPU cuando ejecuta un programa.

Figura 4: Pantalla principal del HMI.

Figura 5 : Menú del HMI.

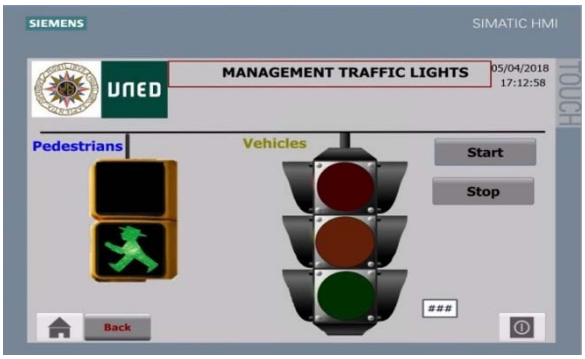

Figura 6: Pantalla de gestión del semáforo.

Para facilitar la programación, AWL se ha ampliado con estructuras de lenguaje de alto nivel (como acceso estructurado a datos y parámetros de bloque). Es el más completo y el más complejo de seguir desde un punto de vista visual.

4.4 HMI

Para llevar a cabo el control remoto de las acciones implementadas en el autómata programable de la IAC-1 (Figura1), se ha creado una interfaz de gestión a través de un panel táctil simulado a través del TIA Portal. El TIA Portal es el sistema de ingeniería innovador que permite la configuración intuitiva y eficiente de todos los procesos de planificación y producción.
Convence por su funcionalidad comprobada y por ofrecer un entorno de ingeniería unificado para todas las tareas de control, y visualización. El TIA Portal incorpora las últimas versiones del software de ingeniería SIMATIC STEP 7, WinCC y Startdrive para la planificación, programación y diagnóstico de todos los controladores SIMATIC[9], pantallas de visualización y unidades SINAMICS[10] de última generación. La oferta de paneles SIMATIC, aportan la solución adecuada para cada aplicación, desde un simple panel de teclado a través de interfaces de operador fijas y móviles hasta un rendimiento versátil; opciones de interfaz robusta, compacta y múltiple. El panel de control remoto tiene varias pantallas de navegación, lo que brinda posibilidades de administración. Según se muestra en la Figura 4, en esta primera pantalla se puede realizar la gestión de usuarios o acceder al kernel del sistema de gestión industrial. Tras la correspondiente verificación de las credenciales, se accede a las posibilidades de administración de los procesos creados en IAC-1,mostrado en la Figura 5. Accediendo a esta funcionalidad implementada en el HMI, se activa la capacidad de administrar los derechos de los diferentes tipos de usuarios a los que se permite interactuar con célula de automatización. Esta gestión es de vital importancia desde el punto de vista de la ciberseguridad de los sistemas, ya que el núcleo de la funcionalidad industrial es accesible de forma remota. La Figura 6, muestra gráficamente la funcionalidad del semáforo y del semáforo peatonal implementado (sistemas permanentes en el tiempo).

5 RESULTADOS

Los resultados obtenidos han sido los esperados, cumpliéndose las expectativas establecidas como los objetivos en el desarrollo de este trabajo. Se han programado varios procesos a través del software de programación propietario de SIEMENS (TIA Portal[11]), que actualmente ejecuta aproximadamente el 99% de los procesos industriales logrando:

- La simulación de procesos repetitivos en el tiempo (continuo) representado por un semáforo de vehículos y peatones.
- La simulación de procesos discretos a lo largo del tiempo. Datos obtenidos por sensores de temperatura y de proximidad.
- La generación de un control PID. Control del flujo de un tanque de líquido, de acuerdo con parámetros específicos del propio PID. En este caso, se utiliza la propia CPU del PLC, proporcionando así otra capacidad de análisis en caso de disponibilidad de saturación del PLC.
- La gestión de la seguridad del propio autómata, su servidor web y módulos de programa. Esta acción muestra el primer paso para el bastionamiento del sistema industrial, proceso que es clave para el mantenimiento de su disponibilidad.
- El desarrollo de una HMI que proporciona la interfaz necesaria para transmitir las órdenes de funcionamiento de los diferentes actores del sistema de forma local y remota. La interfaz incorpora la conectividad de red (LAN, WAN, etc.).

Previo a la construcción física, la CAI se genera de forma virtual a través de TIA Portal v13, aunque en la actualidad se dispone de versiones superiores ampliando la funcionalidad de la electrónica de red. Este software es el sistema de ingeniería innovador que permite la configuración intuitiva y eficiente de todos los procesos de planificación y producción. Debido a su funcionalidad comprobada y testada en entornos de producción y al ofrecer un entorno de ingeniería unificado para todas las tareas de control, resulta altamente eficaz y eficiente su uso.
El TIA Portal incorpora las últimas versiones del software de ingeniería SIMATIC STEP 7, WinCC y Startdrive para la planificación, programación y diagnóstico de todos los controladores SIMATIC, pantallas de visualización y unidades SINAMICS de última generación. El esquema de arranque de la arquitectura SICERCAI está dotado de varios componentes claramente diferenciados que proporcionan un alto grado de independencia en el sistema y cohesión con otras entidades (otros laboratorios remotos [35], centros de investigación, incorporación de nuevas células de automatización industrial de otros fabricantes, etc.).

6 CONCLUSIONES

En el trabajo de investigación llevado a cabo, se ha presentado el desarrollo de un nuevo concepto de simulación de procesos en entornos industriales a través del aprendizaje por experimentación real. En la actualidad, con el aumento de la presencia de tecnologías de la información en el área de control industrial, los sistemas industriales están expuestos a

[9] SIMATICS Engloba a una familia de autómatas de SIEMENS.
[10] SINAMICS Engloba a una familia de accionamientos de SIEMENS.
[11] Totally Integrated Automation.

un gran número de nuevas ciberamenazas [3]. Como resultado del importante papel desempeñado por estas infraestructuras y servicios esenciales, para el desarrollo normal y la coexistencia de la sociedad, se debe tener en cuenta que los futuribles ataques cibernéticos estarán abocados a intentar conseguir la violación de la seguridad de estas infraestructuras [13]. Se debe descartar la idea de que la "seguridad por oscuridad[12]" es un método válido para la protección contra los ciberataques. Por esta razón, es muy importante estar preparado para posibles eventualidades a través de "práctica y pruebas" [14], obteniendo así un alto grado de resiliencia [1] y al mismo tiempo un alto nivel de madurez en comparación con los nuevas amenazas que darán acceso a ciberataques en los sistemas de control industrial [16,17,18,24]. La mejor defensa contra estos nuevos desafíos es la capacitación. A su vez, la implementación del conocimiento teórico sin el riesgo de poner estos análisis en práctica en las plantas de producción favorece la experimentación y la ampliación de puntos de vista. Todas estas capacidades prácticas se ofrecen a través del sistema SIKERCIA, ya que nos permite elegir cómo diseñar el entorno real a simular, incluyendo todos y cada uno de los componentes involucrados en los sistemas de control:

- Sistemas operativos (en el lado de la red de control y administración).
- Software de programación específico para componentes industriales (PLC, electrónica de red, sistema SCADA).
- Conexión a la CAI disponible.
- Sistema de análisis de tráfico de red.
- Herramientas de supervisión y análisis de vulnerabilidad como el software OpenVas.[13]

La verdadera versatilidad del sistema viene dada por la gran adaptabilidad para la incorporación de tantas CAI. como fabricantes de sistemas de control industrial y automatismos. A su vez, proporcionar todo el software involucrado en estas redes proporciona calidad adicional para el análisis de vulnerabilidad. En consecuencia, la principal contribución de esta investigación, materializada en SIKERCIA, es la provisión de un marco seguro que ayudará a poder obtener análisis que demuestren el estado real de madurez de una arquitectura industrial que los usuarios implementarán de acuerdo con sus necesidades de investigación. Las futuras líneas de investigación que se dejan abiertas en este sentido son la incorporación de nuevas CAI de diferentes fabricantes y conexiones con organizaciones más complejas y heterogéneas, como la Red Nacional de Laboratorios Industriales (RNLI) y otras existentes en algunas universidades.

[12] Es un controvertido principio de ingeniería de la seguridad, que intenta utilizar el secreto (de diseño, de implementación, etc.) para garantizar la seguridad.

13 OpenVAS (Open Vulnerability Assessment System, inicialmente denominado GNessUs), es una suite de software, que ofrece un marco de trabajo para integrar servicios y herramientas especializadas en el escaneo y gestión de vulnerabilidades de seguridad de sistemas informáticos incluidos sistemas industriales.

Agradecimientos

Trabajo financiado parcialmente por el Ministerio de Economía y Competitividad mediante los proyectos ENE2015-64914-C3-2-R y DPI2017-84259-C2-2-R.

Referencias

[1] A. Chaves, M. Rice, S. Dunlap, J. Pecarina, Improving the cyber resilience of industrial control systems, *International Journal of Critical Infrastructure Protection* 17, 2017.

[2] A. Cendoya, National Cyber Security Organization: Spain. *CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence Tallinn (Estonia),* 2016.

[3] B. Genge, I. Kiss, P. Haller, a system dynamics approach for assessing the impact of cyber-attacks on critical infrastructures, *International Journal of Critical Infrastructure Protection* 10, 2015.

[4] C. J. Del Canto, M. A. Prada, J. J. Fuertes, S. Alonso, M. Domínguez, Remote Laboratory for Cybersecurity of Industrial Control System, *IFAC-PapersOnLine* 48-29 (2015) 013–018, 2015.

[5] C. Sarno, A. Garofalo, I. Matteucci, M. Vallini, A novel security information and event management system for enhancing cyber security in a hydroelectric dam, *International Journal of Critical Infrastructure Protection* 13, 2016.

[6] *Diario Oficial de la Unión Europea, DIRECTIVA 2008/114/CE del Consejo de 8 de diciembre de 2008* sobre la identificación y designación de Infraestructuras Críticas europeas y la evaluación de la necesidad de mejorar su protección, 2008.

[8] *DIRECTIVA 2008/114/CE DEL CONSEJO de 8 de diciembre de 2008* sobre la identificación y designación de Infraestructuras Críticas europeas y la evaluación de la necesidad de mejorar su protección, 2008.

[9] D. J. Ryan, Regulating the safety and security of the critical information commons, *International Journal of Critical Infrastructure Protection* 10, 2015.

[10] D. J. Ryan, Engineering sustainable critical infrastructures, *International Journal of Critical Infrastructure Protection* 10, 2017.

[11] European Commission, *Green Paper on a European Program for Critical Infrastructure Protection,* com (2005) 0576 final, Brussels, Belgium, 2005.

[12] F. Cerezo, F. Sastrón, Laboratorios Virtuales y Docencia de la Automática en la Formación Tecnológica de Base de Alumnos

Preuniversitarios, *Revista Iberoamericana de Automática e Informática industrial* 12 (2015) 419–431, 2015.

[13] G. Stergiopoulss, P. Kotzanikolaou, M. Theocharidou, G. Lykou, D. Gritzalis, Time-based critical infrastructure dependency analysis for large-scale and cross-sectorial failures, *International Journal of Critical Infrastructure Protection* 12, 2015.

[14] G. Roldán-Molina, M. Almache-Cueva, C. Silva-Rabadão, I. Yevseyeva, V. Basto-Fernandes, A Comparison of Cybersecurity Risk Analysis Tools, International Conference on Project Management / HCist - *International Conference on Health and Social Care Information Systems and Technologies, CENTERIS / ProjMAN / HCist 2017*, 8-10 November 2017.

[15] G. Roldán-Molina, M. Almache-Cueva, C. Silva-Rabadao, I. Yevseyeva, V. Basto-Fernandes, A Comparison of Cybersecurity Risk Analysis Tools, *Procedia Computer Science*, 2017.

[16] *ICS-Cert-USA, Homeland Security*, Alert (IR-ALERT-H-16-056-01) Cyber-Attack against Ukrainian Critical Infrastructure (BlackEnergy), 2016.

[17] *ICS-Cert-USA, Homeland Security, Advisory* (ICSA-10-272-01) Primary Stuxnet Advisory Original release date: September 29, 2010 | Last revised: January 21, 2014.

[18] J. Yoon, S. Dunlap, J. Butts, M. Rice, B. Ramsey, *Evaluating the readiness of cyber first responders responsible for critical infrastructure protection* 13, 2016.

[19] J. Sánchez, F. Morilla, S. Dormido, J. Aranda, P. Ruipérez, "Virtual and remote control lab using Java: A qualitative approach" *IEEE Control System Magazine (ISSN: 0272-1708)*, vol. 22, no. 2, 2002, pp. 8-20. DOI: 10.1109/37.993309.

[20] *Ley 8/2011, de 28 de abril*, por la que se establecen medidas para la Protección de las infraestructuras críticas, BOE núm. 102, 2011.

[21] L. de la Torre, J. Sánchez, S. Dormido, what remote labs can do for you? *Physics today*, 2016.

[22] L. de la Torre, J. Sánchez, T. Andrade, M.T. Restivo, Easy Creation and Deployment of JavaScript Remote Labs with EjsS and Moodle, *International Journal of Engineering Education*, Vol. 27 No.3, pp. 528-534, 2011.

[23] L. de la Torre, T. Faustino Andrade, P. Sousa, J. Sanchez, M.T. Restivo, Assisted Creation and Deployment of JavaScript Remote Experiments, *International Journal of online Engineering*, 2016.

[24] R. Spenneberg, M. Brüggemann, H. Schwartke, PLC-Blaster: A Worm Living Solely in the PLC, *BlackHat Asia*, 2016.

[25] R. ROSS, M. McEvilley, J. Carrier Oren, Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, *NIST (National Institute of Standards Technology)* Special Publication 800-160, 2016.

[26] *Real Decreto 704/2011*, de 20 de mayo, por el que se aprueba el Reglamento de Protección de las Infraestructuras Críticas, BOE núm. 120, 2011.

[27] *Resilience team, ENISA* (European Union Agency for Network and Information Security), Communication network dependencies for ICS/SCADA Systems, 2016.

[28] *Resilience team, ENISA* (European Union Agency for Network and Information Security), Cyber Insurance: Recent Advances, Good Practices and Challenges, 2016.

[29] R. Setola, V. Rosato, E. Kyriakides, Managing the Complexity of Critical Infrastructures, a Modelling and Simulation Approach, *Studies in Systems, Decision and Control Volume* 90 2016.

[30] S. Anna, Secure Infrastructure & Services *Unit, ENISA (European Union Agency for Network and Information Security), Stocktaking*, Analysis and Recommendations on the Protection of CIIs, 2016.

[31] S. Wang, A analytical model for benchmarking the development of national infrastructure items against those in similar countries, *International Journal of Critical Infrastructure Protection* 13, 2016.

[32] *Resilience team, ENISA* (European Union Agency for Network and Information Security), Communication network dependencies for ICS/SCADA Systems, 2016.

[33] *Resilience team, ENISA* (European Union Agency for Network and Information Security), Cyber Insurance: Recent Advances, Good Practices and Challenges, 2016.

[34] R. Setola, V. Rosato, E. Kyriakides, E. Rome, Managing the Complexity of Critical Infrastructures a Modelling and Simulation Approach, *Studies in Systems, Decision and Control-Volume 90*, 2016.

[35] S. Dormido, Control learning: present and future, *Annual Reviews in Control, Vol 28 (1), pp.* 115-136, 2004.