Aplicando Análisis de Riesgos a un entorno de Hogar Inteligente: Caso de Estudio MARISMA-CPS

José Luis Ruiz Catalán
Grupo de Investigación GSyA
Universidad de Castilla-La Mancha
Ciudad Real, España
joseluis.ruiz@uclm.es

Carlos Pedraza Antona
Grupo de Investigación GSyA
Universidad de Castilla-La Mancha
Ciudad Real, España
carlos.pedraza@uclm.es

David G. Rosado
Grupo de Investigación GSyA
Universidad de Castilla-La Mancha
Ciudad Real, España
david.grosado@uclm.es

Antonio Santos-Olmo
Grupo de Investigación GSyA
Universidad de Castilla-La Mancha
Ciudad Real, España
antonio.santosolmo@uclm.es

Luis E. Sánchez
Grupo de Investigación GSyA
Universidad de Castilla-La Mancha
Ciudad Real, España
luise.sanchez@uclm.es

Carlos Blanco
Grupo de Investigación GSyA
University of Cantabria
Santander, España
carlos.blanco@unican.es

***Abstract*—Los sistemas ciberfísicos (CPS) son sistemas inteligentes que integran redes físicas y computacionales, impactando infraestructuras críticas como el transporte, la salud, la energía y la manufactura avanzada. Los CPS enfrentan desafíos significativos de seguridad debido a la conectividad entre los mundos cibernético y físico. Los métodos tradicionales de evaluación de riesgos de TI son inadecuados para los CPS, lo que requiere nuevos enfoques. Aplicamos una técnica novedosa de análisis de riesgos para CPS basada en MARISMA y la herramienta eMARISMA. Esta técnica incorpora elementos reutilizables y adaptables para gestionar y controlar los riesgos de CPS, alineados con los marcos de NIST y ENISA. Un estudio de caso en un hogar inteligente demuestra la adaptabilidad del patrón a varios entornos de CPS, mostrando cómo los riesgos de seguridad en hogares inteligentes pueden identificarse y gestionarse de manera efectiva.**

***Index Terms*—Análisis de riesgos, Evaluación de riesgos, MARISMA, Sistema ciberfísico, Hogar inteligente**

I. Introducción

Los sistemas ciberfísicos (CPS) son sistemas inteligentes que integran capacidades de computación, almacenamiento y comunicación para monitorear y gestionar objetos del mundo físico [1], [2], creando aplicaciones y servicios innovadores para ciudadanos, negocios y gobierno [3]–[5].

Mientras que la investigación actual se centra principalmente en lograr estabilidad, robustez, rendimiento y eficiencia para los sistemas físicos [6], la cuestión de la ciberseguridad en los CPS ha sido ampliamente pasada por alto [7].

Los CPS poseen características únicas como restricciones de respuesta en tiempo real, alta disponibilidad, predictibilidad y confiabilidad, que son críticas para las decisiones de ciberseguridad [8]. Los avances en tecnología aumentan el riesgo de ciberataques, incluyendo la explotación de capacidades de automatización [9]. Proteger los CPS se complica aún más por su necesidad de operar bajo condiciones diversas, exponiéndolos a una variedad de mecanismos de ciberataques [10]. Los métodos de evaluación estática proporcionan solo estimaciones aproximadas del riesgo a lo largo del tiempo, careciendo de precisión para momentos específicos [11]. Por lo tanto, los métodos de evaluación dinámica capaces de predecir situaciones futuras son necesarios para mejorar la efectividad de la evaluación de riesgos. Esto es particularmente importante, ya que los ciberataques actuales apuntan a sistemas similares e intentan ajustar el proceso de Análisis y Gestión de Riesgos (RAM) actualizando sus variables y salvaguardas. Sin embargo, la evaluación dinámica es difícil de implementar y los enfoques RAM actuales típicamente no la abordan [12].

Los métodos tradicionales de evaluación de riesgos para sistemas de TI no pueden aplicarse directamente a los CPS, lo que conlleva riesgos de seguridad significativos. Una evaluación de riesgos efectiva para los CPS debería proporcionar una comprensión integral de su estado de seguridad y apoyar la asignación eficiente de recursos protectores [13]. Muchas propuestas existentes de RAM para TI enfrentan desafíos prácticos de implementación en sistemas dinámicos como los CPS [14]–[16], careciendo de herramientas adecuadas y utilizables adaptadas a entornos específicos. Para abordar estos problemas, desarrollamos la metodología MARISMA (Metodología para el Análisis de Riesgos en Sistemas de Información, utilizando Meta-Patrón y Adaptabilidad).

Trabajos previos definieron y adaptaron la metodología MARISMA y el meta-patrón para un entorno de Big Data [17] y para un entorno de CPS [18], aplicándolos exitosamente a casos reales. Este documento se enfoca en el uso del patrón MARISMA-CPS, con el objetivo de proporcionar un entorno completo de RAM basado en la metodología MARISMA para otro estudio de caso, un hogar inteligente. El patrón propuesto permite una gestión y control efectivos de riesgos en CPS, alineándose con los principales estándares de CPS, IoT y gestión de riesgos como ISO/IEC 27.000, IEC 62443, las recomendaciones de seguridad de IoT de ENISA y el marco de CPS de NIST.

El resto de este trabajo está organizado de la siguiente man-

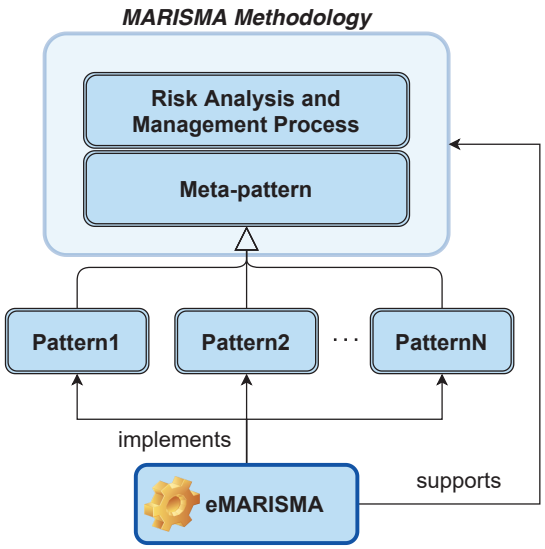

Fig. 1. Esquema general del framework MARISMA.

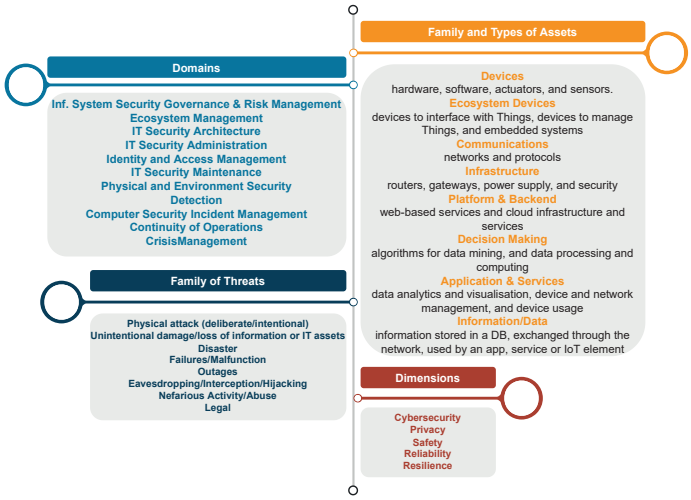

Fig. 2. Componentes del patrón MARISMA-CPS.

era: primero, se presenta una visión general de las principales características del marco MARISMA, así como una breve descripción del patrón MARISMA-CPS. Luego, se presenta un caso de estudio y se muestran los resultados de la aplicación del patrón MARISMA-CPS a este estudio de caso. Finalmente, se incluye una sección de conclusiones y trabajos futuros.

II. MARISMA Framework y patrón MARISMA-CPS

MARISMA es una metodología RAM que puede adaptarse a cualquier tipo de entorno de TI [19]. Define el meta-patrón, en el cual los controles de seguridad se consideran desde el inicio del proceso de análisis de riesgos, y permite la reutilización de artefactos y la definición de patrones para contextos específicos. Además, al estar soportado por la herramienta eMARISMA, el proceso y la toma de decisiones se vuelven ágiles y simples (ver Fig. 1).

La adaptabilidad de MARISMA a diferentes contextos se debe principalmente a la definición del patrón. El patrón hereda los elementos comunes a cualquier proceso de RAM definidos en el meta-patrón, y luego los completa o adapta a un contexto específico.

Para el patrón MARISMA-CPS [18] nos hemos guiado por las recomendaciones de ENISA y NIST para IoT y los estándares ISO/IEC 27.000 e IEC 62443, donde establecen conjuntos de posibles controles, taxonomías de activos, amenazas, dimensiones, etc. que pueden servir como una primera aproximación para la construcción del patrón (ver Fig. 2).

Vamos a utilizar el patrón ya construido [18], por lo que lo aplicaremos a la vida real, instanciando el patrón a un caso concreto, para lo cual hemos elegido un hogar inteligente. Para ello, es necesario estudiar en profundidad los tipos de activos involucrados en el sistema y analizar e identificar los tipos de amenazas que pueden afectar al sistema y causar daños a los activos en este entorno, lo cual se mostrará en la siguiente sección.

III. Caso de Estudio: Hogar Inteligente

Un hogar inteligente es un entorno doméstico que integra tecnología avanzada para automatizar y controlar varios sistemas y dispositivos, optimizando la eficiencia y la comodidad del usuario. Esta configuración incluye iluminación automatizada, control climático, sistemas de seguridad y más, todos interconectados y capaces de tomar decisiones autónomas. El objetivo principal es minimizar la intervención manual mediante la implementación de sistemas de automatización y control remoto. Esto mejora la conveniencia, eficiencia energética y seguridad del hogar, proporcionando una experiencia de vida inteligente y sin interrupciones. El objetivo de este escenario es mostrar el potencial de la tecnología de hogares inteligentes para crear un entorno de vida más eficiente, cómodo y seguro.

A. Definiendo dimensiones para el caso de estudio

Para poder realizar el análisis de riesgos, MARISMA-CPS primero define un conjunto de dimensiones (mostrado en Fig. 2) que deben establecerse para el caso de estudio y que se muestran en la Tabla I.

B. Definiendo activos para el caso de estudio

Los hogares inteligentes tienen activos esenciales para su operación, por lo que necesitan protección. Muchos de estos activos son comunes tanto a hogares inteligentes como convencionales, pero hay otros específicos para hogares inteligentes, ya que pueden tomar decisiones de forma autónoma debido a su conectividad inteligente. Estos activos incluyen, por ejemplo, sistemas de iluminación automatizada, sistemas de control climático, cámaras de seguridad, sistemas de identificación y más (ver Tabla II, en inglés, por la configuración actual de eMARISMA junto a los resultadoss mostrados).

Siguiendo la jerarquía del patrón, se debe definir los activos específicos del caso de estudio (el patrón solamente define familias y tipos de activos), categorizándolos en sus tipos de activos. Una vez que se han identificado y clasificado los

TABLE I
DESCRIPCIÓN DE LAS DIMENSIONES PARA EL CASO DE ESTUDIO

Dimensiones	Descripción
Ciberseguridad	Los sistemas, dispositivos e información sensible deben protegerse usando técnicas y herramientas para asegurar la confidencialidad, integridad y disponibilidad.
Privacidad	Se maneja, almacena y transmite una gran cantidad de datos personales relacionados con el uso, información financiera, comportamiento, imagen y conversaciones. Por lo tanto, asegurar la privacidad de estos datos es esencial.
Safety	Es necesario garantizar que el sistema no funcione de manera que pueda llevar a estados peligrosos, lo que lo haría susceptible de causar pérdidas económicas y accidentes domésticos.
Fiabilidad	Debe asegurarse tanto en el software como en el hardware. El software garantiza la funcionalidad del dispositivo y la coordinación adecuada entre los dispositivos del hogar y los usuarios. El hardware permite el funcionamiento de los servicios y la transmisión de información sensible a los dispositivos del hogar.
Resiliencia	El hogar inteligente debe asegurar la resiliencia cibernética asegurando la disponibilidad y continuidad de los servicios que dependen de los activos de TIC.

activos, incorporarlos a la herramienta eMARISMA es sencillo porque la herramienta facilita su definición y clasificación siguiendo una estructura jerárquica entre familias, tipos de activos y activos definidos en el patrón.

Al usar el patrón MARISMA-CPS para el análisis de riesgos, tan pronto como se agregan los activos a la herramienta, las relaciones establecidas en el patrón entre activos, amenazas y dimensiones permiten que la herramienta comience a ejecutar el análisis de riesgos con los activos del caso de estudio. La herramienta muestra en tiempo real los resultados actuales de riesgo para este conjunto de activos, así como una lista de controles apropiados para proteger este conjunto de activos.

C. Definiendo amenazas para el caso de estudio

Para proceder con el proceso de análisis de riesgos, el primer paso es identificar el conjunto de amenazas que pueden afectar el sistema bajo análisis. Basándose en los tipos de amenazas descritas en el patrón MARISMA-CPS, se identifican las amenazas que afectan al caso de estudio específico, teniendo en cuenta los activos a proteger (ver Tabla III). Dado que todos los tipos de amenazas a los CPS ya están definidas en el patrón precargado de la herramienta eMARISMA, solo se seleccionan aquellos tipos de amenazas que afectan al caso de estudio, especificando los valores para el porcentaje de degradación del activo (daño causado al activo) y la probabilidad de ocurrencia (probabilidad de que ocurra un ataque). Estos valores van de 0 a 100, incrementados en 10 (como se muestra en la Fig. 3). Inicialmente, estos valores se cargan automáticamente gracias al conocimiento y experiencia de numerosas aplicaciones de MARISMA a diferentes sectores con tipos de amenazas similares o iguales, pero pueden ser modificadas por el contexto y experiencia de los expertos.

La herramienta inicialmente carga valores predeterminados para las tasas de degradación y ocurrencia, basándose en la ex-

TABLE II
DESCRIPCIÓN DE ACTIVOS PARA EL CASO DE ESTUDIO

Familia de Activos	Tipo de Activos	Activos
Devices	Software	Firmware of IoT Devices
	Hardware	Lighting, motion detectors, Video recording and streaming, Air conditioners, refrigerators, kitchen robot, input devices multipurpose, intelligent and control devices, wearable external devices and electromagnetic receivers and emitters
	Actuators	Electric (linear, rotary), magnetic, piezoelectric, electromechanical and electroactive Polymers actuators.
	Sensors	Light, motion, temperature, contact, humidity, position, proximity, electromagnetic, accelerometer, gyroscope, air quality, gas, biomedical and optic sensors
Ecosystem Devices	Device to interface with Things	Multipurpose, intelligent and control devices, Identification systems and Air conditioners
	Device to manage Thing	Air conditioners, alarm systems, Lighting
	Embedded systems	Supportive devices
Communications	Networks	WiFi, Bluetooth, Zigbee and NFC
	Protocols	MQTT, CoAP, HTTP, HTTPS, LWM2M y SNMTP
Infrastructure	Routers	Backbone network devices
	Gateways	IoT Gateways
	Power supply	Power and climate regulation systems
	Security	Biometric scanners, CCTV, Automated door lock system, Alarm system
Platform & Backend	Web-based service	Information, control and smart systems
	Cloud infrastructure and services	Power information system, security system, communication and control systems, log information system
Decision making	Algorithms for data mining	IoT Gateways
	Data processing and computing	Tracking logs
Applications & Services	Data analytics and visualization	Multipurpose, intelligent and control devices
	Device and network management	Mobile applications for smartphone, tablets and web-based application for PCs
	Device usage	Automation equipment and smart use
Information/ Data	Information stored in a database (at rest)	Data on the state of home, usage data, private data of the home users, media data, financial data
	Information sent or exchanged through the network (in transit)	Data on the state of the devices, media data and financial data
	Information used by an application, service, or IoT element (in use)	Data of the devices

TABLE III
DESCRIPCIÓN DE TIPOS DE AMENAZAS PARA EL CASO DE ESTUDIO

Familia de Amenazas	**Tipo de Amenazas**	**Amenazas**
Physical attack	Device modification; Device destruction (sabotage)	Theft Device and Data
Damage loss (IT assets)	Data/Sensitive information leakage	Smart home system configuration error; House user's errors; Non-compliance
Disaster	Disaster natural; Environment Disaster	Fire, Flood, Earthquake
Failures/ Malfunction	Software vulnerabilities; third parties failures	Cloud service providers, IoT device manufacturer; Network providers; IoT device management software; Power suppliers; Software failures; Inadequate firmware; Device failure; Network components failure; Insufficient maintenance; Overload; Absence of audit logs
Outages	Failures of devices; Failure of system; Loss of support services; Network or cloud outage	Communication between IoT and non-IoT
Eavesdropping/ Interception/ Hijacking	Communication protocol hijacking; Network reconnaissance; Interception of information; Session hijacking; Information gathering; Replay of messages; Man-in-the-middle; Spoofing; Tampering; Repudiation; Information disclosure; Denial of Service (DoS); Elevation of Privilege	Hijacking to Networks/session and IoT devices; Skimming
Nefarious Activity/ Abuse	Malware; Exploit Kits; Targeted attacks; DDoS; Counterfeit by malicious devices; Attacks on privacy; Modification of information	Denial of Service; Social Engineering: Phishing; Baiting and Device cloning (RFID); Malware; Virus and Ransomware; Unauthorised access control; IoT Device tampering
Legal	Violation of rules and regulations/Breach of legislation; Failure to meet contractual requirements; Abuse of personal data	Theft or exposure house user's data

periencia de análisis previa y el aprendizaje de la herramienta. La herramienta eMARISMA permite la modificación de estos valores predeterminados por parte de expertos en seguridad RAM, quienes aplican su juicio y conocimiento sobre las amenazas potenciales que afectan al sistema, el daño que podrían causar y su probabilidad de ocurrencia. Para abordar amenazas que no impactan el sistema, asignarles un valor bajo o incluso 0% es válido.

Tomando como ejemplo la amenaza de "attacks on privacy" de la familia de amenazas "Nefarious Activity/Abuse", los expertos pueden actualizar la probabilidad de ocurrencia y el porcentaje de degradación hasta un 100% basándose en su

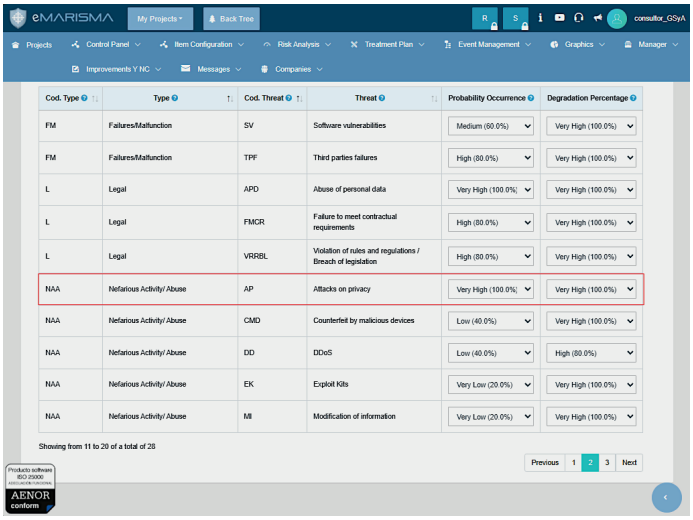

Fig. 3. Ocurrencia y degradación para los tipos de amenazas con eMARISMA

experiencia (ver Fig. 3). Los expertos reconocen que acceder a los datos privados de los usuarios puede amenazar su seguridad en aspectos legales, financieros, de imagen personal, honor y predicción de comportamiento, lo que podría llevar a otros tipos de ataques como robos en el hogar basados en patrones de entrada y salida.

Por lo tanto, estas amenazas son altamente críticas y requieren atención urgente. Es crucial darse cuenta de que los dispositivos inteligentes se han convertido en un punto clave para los ataques a la privacidad debido a su vulnerabilidad percibida y facilidad de acceso. Los valores especificados para probabilidad y degradación están adaptados a tipos de amenazas específicos y afectarán a todas las relaciones que involucren tipos de activos afectados por esas amenazas.

D. Análisis de Riesgo para el caso de estudio

El siguiente paso en el análisis de riesgos es determinar el impacto de las amenazas en cada activo afectado, considerando diversas dimensiones. Esto permite calcular el daño total o la degradación infligida al activo cuando la amenaza apunta al sistema, basado en el daño evaluado para cada dimensión. La herramienta muestra las relaciones entre amenazas, activos y dimensiones, junto con los valores asignados en el paso anterior. Los valores predeterminados para cada dimensión se derivan de los porcentajes de degradación y las tasas de ocurrencia.

Por ejemplo, la amenaza "Attacks on privacy" (bajo el tipo de amenaza "Nefarious Activity/Abuse" y tiene una probabilidad de ocurrencia del 100%), puede observarse, en Fig. 4, cómo el porcentaje de degradación depende de las dimensiones y del tipo de activo. Para este tipo de amenaza, involucra a las familias de activos "Cámaras de seguridad", "Dispositivos con micrófonos", "Dispositivos del ecosistema" y "Comunicaciones". El tipo de amenaza "Nefarious Activity/Abuse" se encontró con una probabilidad de degradación del 100%, afectando todas las dimensiones relevantes. Sin

embargo, dependiendo del activo específico afectado, estos valores de degradación por dimensión pueden ajustarse. Por ejemplo, para el tipo de activo ”Cámaras de seguridad”, se considera una degradación del 100% en las dimensiones ”Privacidad” y ”Safety” debido al impacto severo en la privacidad de los miembros del hogar y su seguridad si la amenaza se materializa. Por lo tanto, en estos casos se asigna un porcentaje más alto de degradación.

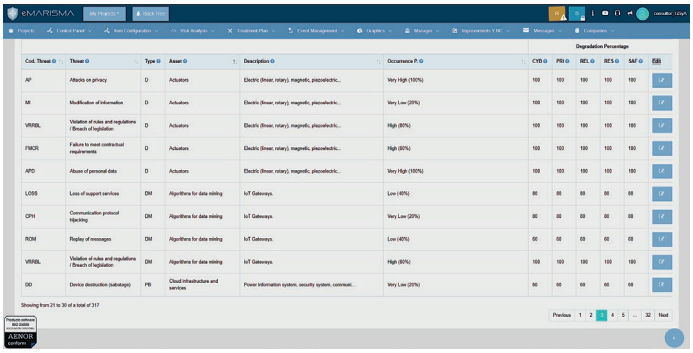

Fig. 4. Porcentage de degradación x dimensiones x activos x amenazas en eMARISMA.

E. Análisis de Riesgos: Resultados

Para concluir el análisis de riesgos, se debe realizar una verificación interna (utilizando una lista de verificación de seguridad) para descubrir el nivel real de seguridad en un Hogar Inteligente. Esta verificación se lleva a cabo basada en el patrón definido, ya que el patrón ha establecido un conjunto de dominios, objetivos de control y controles, que son los tres niveles en los que se divide la lista de verificación. Esta revisión se realiza para descubrir la cobertura de seguridad actual, es decir, cuántos de los controles establecidos en el patrón se cumplen en el hogar inteligente bajo análisis.

El resultado de la lista de verificación proporciona una visión general del nivel de seguridad del sistema, identificando de un vistazo los principales puntos fuertes y débiles, proporcionando así herramientas importantes para la toma de decisiones. También sirve para identificar, a través de recomendaciones, los controles que deben implementarse para mejorar la seguridad, proteger los activos y reducir el riesgo. La herramienta proporciona un panel que muestra los niveles de cobertura de los controles por dominio, permitiendo una evaluación visual y detallada, como se muestra en la Fig. 6.

Además, permite visualizar el nivel actual a través de un diagrama de Kiviat por dominio (ver Fig. 7). Una vez que se ha calculado el riesgo con todos los elementos añadidos, la herramienta también muestra una gran cantidad de información tanto en forma textual como visual, permitiendo al experto en seguridad conocer siempre el nivel de riesgo al que está expuesto el sistema bajo análisis. La herramienta, entre muchas otras posibilidades, muestra el nivel de riesgo por activo (ver Fig. 5), o el nivel de riesgo por amenaza , facilitando la priorización de las acciones correctivas.

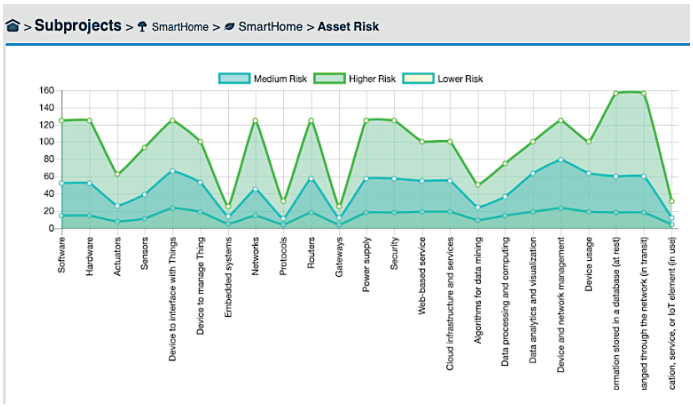

Fig. 5. Riesgo calculado por tipo de activo usando eMARISMA.

Por ejemplo, para el dominio ”IT Security Architecture (ISAR)” hay una cobertura del 87%, que coincide con el porcentaje promedio de los objetivos de control definidos para este dominio, como se puede ver en el diagrama Kiviat para el dominio ISAR de la Fig. 8.

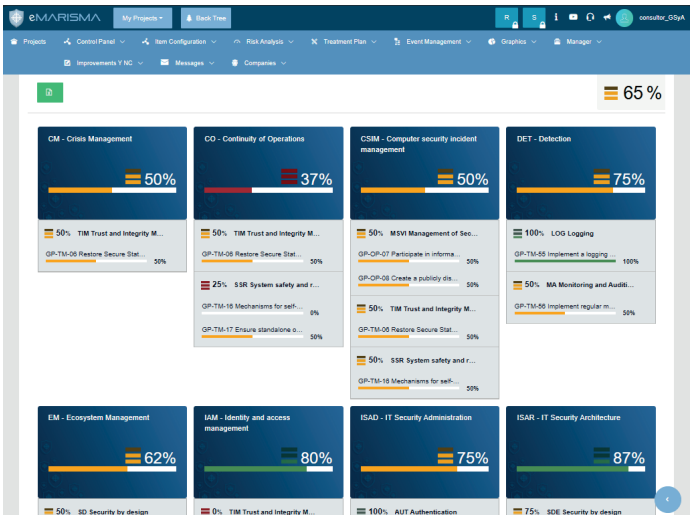

Fig. 6. Dashboard muestra los niveles de cobertura de lso controles para el caso de estudio.

IV. Conclusiones y trabajo futuro

El estudio demuestra que el patrón MARISMA-CPS, originalmente diseñado para sistemas ciberfísicos, es altamente adaptable y reutilizable en diferentes contextos, como el de un Smart Home. La aplicación exitosa del patrón en este nuevo entorno resalta su versatilidad y capacidad para gestionar y mitigar riesgos de seguridad en una variedad de escenarios, más allá de su uso inicial. Esta flexibilidad sugiere que el patrón MARISMA-CPS puede ser aplicado a otros dominios, facilitando un análisis de riesgos preciso y eficiente, sin requerir un conocimiento sectorial especializado.

En cuanto al trabajo futuro, se propone aplicar el patrón MARISMA-CPS en otros dominios como ciudades inteligentes y redes descentralizadas, con el objetivo de refinar

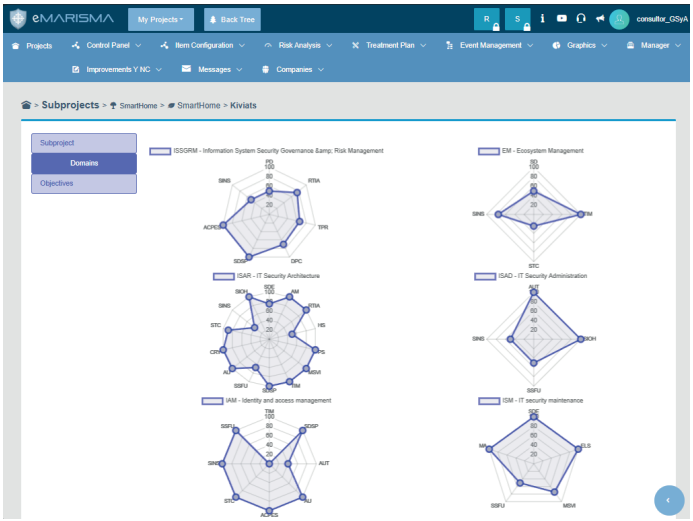

Fig. 7. Niveles de cobertura por dominios con diagramas Kiviat para el caso de estudio.

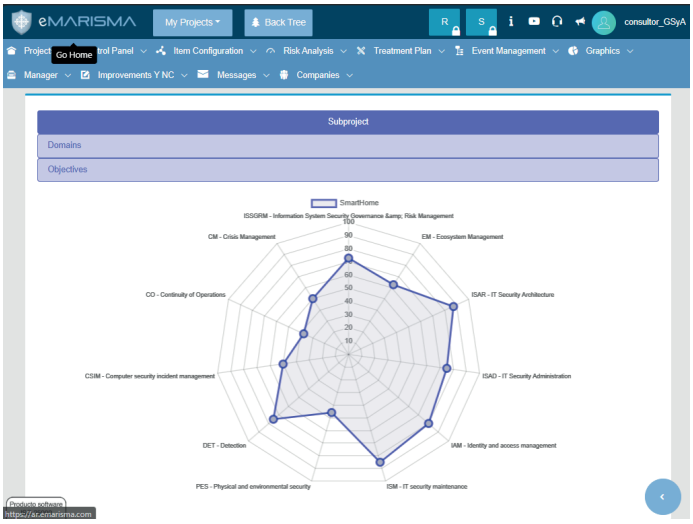

Fig. 8. Niveles de cobertura por objetivos de control con diagramas Kiviat para el caso de estudio.

y validar aún más el patrón. Además, se planea el desarrollo de sub-patrones especializados para sectores específicos como salud, manufactura y energía, aprovechando las capacidades de herencia y reutilización del marco MARISMA.

Agradecimientos

Este trabajo ha sido financiado por los proyectos Di4SPDS (CHIST-ERA grant - PCI2023145980-2) financiado por MCIN/AEI/10.13039/501100011033 y cofinanciado por la Unión Europea, AETHER-UCLM (PID2020-112540RB-C42) financiado por MCIN/AEI/10.13039/501100011033; ALBA-UCLM (TED2021-130355B-C31) y ALBA-UC (TED2021-130355B-C33) financiado por MICIN/AEI/10.13039/501100011033/ Unión Europea NextGenerationEU/PRTR; y MESIAS (2022-GRIN-34202) financiado por FEDER.

References

[1] H. Orojloo and M. A. Azgomi, "A game-theoretic approach to model and quantify the security of cyber-physical systems," *Computers in Industry*, vol. 88, pp. 44–57, 2017.

[2] R. Alguliyev, Y. Imamverdiyev, and L. Sukhostat, "Cyber-physical systems and their security issues," *Computers in Industry*, vol. 100, pp. 212–223, 2018.

[3] V. S. Abhijith, B. Sowmiya, S. Sudersan, M. Thangavel, and P. Varalakshmi, "A review on security issues in healthcare cyber-physical systems," in *Cyber Intelligence and Information Retrieval*. Singapore: Springer Singapore, 2022, pp. 37–48.

[4] R. Kumar, B. Narra, R. Kela, and S. Singh, "Afmt: Maintaining the safety-security of industrial control systems," *Computers in Industry*, vol. 136, p. 103584, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0166361521001913

[5] N. F. M. Osman, A. A. A. Elamin, E. S. A. Ahmed, and R. A. Saeed, "Cyber-physical system for smart grid," in *Artificial Intelligence Paradigms for Smart Cyber-Physical Systems*. IGI Global, 2021, pp. 301–323.

[6] Z. Ying, Q. Li, S. Meng, Z. Ni, and Z. Sun, "A survey of information intelligent system security risk assessment models, standards and methods," in *Cloud Computing, Smart Grid and Innovative Frontiers in Telecommunications*. Springer International Publishing, 2020, pp. 603–611.

[7] T. K. Ananda, G. Simran T., T. Sukumara, D. Sasikala, and R. Kumar P., "Robustness evaluation of cyber physical systems through network protocol fuzzing," in *International Conference on Advances in Computing and Communication Engineering (ICACCE)*, 2019, pp. 1–6.

[8] Y. Lu and L. D. Xu, "Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2103–2115, apr 2019.

[9] M. Lezzi, M. Lazoi, and A. Corallo, "Cybersecurity for Industry 4.0 in the current literature: A reference framework," *Computers in Industry*, vol. 103, pp. 97–110, dec 2018.

[10] E. Griffor, D. Wollman, and C. Greer, "Framework for Cyber-Physical Systems: Volume 1, Overview," National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep. June, jun 2017.

[11] W. Wu, R. Kang, and Z. Li, "Risk assessment method for cyber security of cyber physical systems," in *1st International Conference on Reliability Systems Engineering, ICRSE 2015*. IEEE, oct 2015, pp. 1–5.

[12] A. Jamshidi, D. Ait-kadi, A. Ruiz, and M. L. Rebaiaia, "Dynamic risk assessment of complex systems using fcm," *International Journal of Production Research*, vol. 56, no. 3, pp. 1070–1088, 2018.

[13] A. Santos-Olmo, L. E. Sánchez, D. G. Rosado, M. A. Serrano, C. Blanco, H. Mouratidis, and E. Fernández-Medina, "Towards an integrated risk analysis security framework according to a systematic analysis of existing proposals," *Frontiers Comput. Sci.*, vol. 18, no. 3, 2024.

[14] T. E. Abioye, O. T. Arogundade, S. Misra, K. Adesemowo, and R. Damaševičius, "Cloud-based business process security risk management: A systematic review, taxonomy, and future directions," *Computers*, vol. 10, no. 12, 2021.

[15] B. M. Bhatti, S. Mubarak, and S. Nagalingam, "Information security risk management in it outsourcing - a quarter-century systematic literature review," *Journal of Global Information Technology Management*, vol. 24, no. 4, pp. 259–298, 2021.

[16] M. N. Aleksandrov, V. A. Vasiliev, and S. V. Aleksandrova, "Implementation of the risk-based approach methodology in information security management systems," in *2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT QM IS)*, 2021, pp. 137–139.

[17] D. G. Rosado, J. Moreno, L. E. Sánchez, A. Santos-Olmo, M. A. Serrano, and E. Fernández-Medina, "Marisma-bida pattern: Integrated risk analysis for big data," *Computers & Security*, vol. 102, 2021.

[18] D. G. Rosado, A. Santos-Olmo, L. E. Sánchez, M. A. Serrano, C. Blanco, H. Mouratidis, and E. Fernández-Medina, "Managing cybersecurity risks of cyber-physical systems: The marisma-cps pattern," *Computers in Industry*, vol. 142, p. 103715, 2022.

[19] A. Santos-Olmo, L. Sánchez, D. Rosado, E. Fernández-Medina, and M. Piattini, "Applying the Action-Research Method to Develop a Methodology to Reduce the Installation and Maintenance Times of Information Security Management Systems," *Future Internet*, vol. 8, no. 3, p. 36, jul 2016.