Onto-CARMEN: un enfoque basado en ontologías para el razonamiento y el metamodelado de requisitos de seguridad de los sistemas ciberfísicos

Carlos Blanco[1][0000−0001−9001−0904], David G. Rosado[2][0000−0003−4613−5501], Ángel Jesús Varela-Vaca[3][0000−0001−9953−6005], María Teresa Gómez López[3][0000−0002−3562−875X], and Eduardo Fernández-Medina[2][0000−0003−2553−9320]

[1] Grupo ISTR. Universidad de Cantabria, España
carlos.blanco@unican.es
[2] Grupo GSyA. Universidad de Castilla-La Mancha, Ciudad Real, España
{david.grosado,eduardo.fdezmedina}@uclm.es
[3] Grupo IDEA. Universidad de Sevilla, España
{ajvarela,maytegomez}@us.es

Resumen En los últimos años, los sistemas ciberfísicos (CPS) están atrayendo una gran atención, especialmente en el sector industrial, ya que se han convertido en el foco de los ciberataques. Los CPS son sistemas complejos que engloban una gran variedad de componentes de hardware y software con un número incontable de configuraciones y características. Un requisito de seguridad no válido puede producir una configuración parcial o incompleta, incluso errónea, con las consiguientes consecuencias catastróficas. Por lo tanto, es crucial garantizar la validación en la especificación de los requisitos de seguridad desde las primeras etapas de diseño. Con este fin, se propone Onto-CARMEN, un enfoque semántico que proporciona un mecanismo para la especificación de los requisitos de seguridad en la parte superior de las ontologías, y el diagnóstico automático a través de axiomas semánticos y reglas SPARQL. El enfoque se ha validado utilizando los requisitos de seguridad de un caso de estudio real.

Keywords: Sistemas ciberfísicos · ciberseguridad · modelos de configuración · requisitos de seguridad · verificación de la seguridad · diagnosis

1. Introducción

Los sistemas ciberfísicos (CPS) están recibiendo una gran atención dentro de la industria, la sociedad y los gobiernos debido al enorme impacto que tienen [18], y proporcionando a los ciudadanos y las empresas una amplia gama de aplicaciones y servicios innovadores [10]. Sin embargo, el desarrollo de estos sistemas se ha realizado sin pensar en los aspectos de seguridad ni en los nuevos riesgos que implica esta automatización de procesos, que ponen en riesgo

toda la infraestructura industrial [16]. Cualquier problema de seguridad podría tener consecuencias catastróficas [2]. Por lo tanto, considerar los requisitos de seguridad desde los primeros pasos de CPS es crucial para evitar problemas de seguridad, aunque sea un reto.

La seguridad en entornos industriales se convierte en un aspecto crítico que debe ser asumido en todas las etapas [34][23]. Sin embargo, la enorme variabilidad de los componentes que intervienen y sus posibles configuraciones dificultan enormemente la definición de un conjunto correcto de requisitos de seguridad [29][32]. Para gestionar esta complejidad, es crucial disponer de un modelo que facilite, por un lado, abordar la variabilidad de los componentes CPS y sus restricciones y configuraciones, y los requisitos de seguridad y, por otro, habilitar capacidades de razonamiento que garanticen el correcto diseño de los requisitos de seguridad.

En trabajos anteriores, propusimos CARMEN [31] como marco para describir y diagnosticar los requisitos de seguridad integrando técnicas para transformar instancias de requisitos de seguridad en configuraciones que se diagnostican a través de un modelo de variabilidad específico para explicar por qué el requisito de seguridad es válido. CARMEN presenta varios inconvenientes en el uso de varios modelos interrelacionados pero desconectados, la dependencia de plantillas ad-hoc para conectar los modelos (es decir, meta-modelo de requisitos de seguridad y modelos de variabilidad), y la automatización parcial de todo el proceso de diagnóstico.

Partiendo de estas limitaciones, se propone Onto-CARMEN, un enfoque semántico que permite, por un lado, modelar los requisitos de seguridad de los CPS y su verificación y diagnóstico instantáneo en tiempo de diseño gracias a las capacidades de razonamiento que proporcionan las ontologías. Para ello, las principales aportaciones del enfoque Onto-CARMEN son: 1) El diseño e implementación de una ontología para CARMEN que permite la definición de requisitos de seguridad para CPS según las recomendaciones de seguridad de ENISA [1] y las directrices de OWASP [3]. 2) Un marco de razonamiento compuesto por reglas semánticas y SPARQL para la verificación y el diagnóstico de los requisitos de seguridad en tiempo de diseño que permiten derivar los requisitos de seguridad correctos.

El documento se ha organizado de la siguiente manera: La sección 2 introduce los antecedentes necesarios para entender la propuesta. En la sección 3 se detalla el modelo semántico y las reglas que permiten verificar y diagnosticar los requisitos de seguridad de los CPS. En la sección 4 se aplica Onto-CARMEN a un caso de uso para validar el enfoque. La sección 5 revisa los artículos más relevantes; y, por último, se extraen conclusiones y se esboza el trabajo futuro en la sección 6.

2. Antecedentes

Esta sección presenta los conceptos relacionados con la representación de ontologías y la explicación de CARMEN.

2.1. Ontología y representación del conocimiento

Una *ontología* es un modelo formal como abstracción para representar conceptos del mundo real. Especifica las propiedades de cada idea, describiendo varios aspectos y cualidades de los conceptos (clases de conceptos), restricciones sobre las propiedades, y una explicación explícita de los conceptos en un dominio.

Existen varias alternativas de lenguajes ontológicos [14], pero el lenguaje más popularizado es *OWL*. OWL (Ontology Web Language) es un lenguaje diseñado para formalizar ontologías cuya expresividad es superior a la propuesta por RDF. OWL2 es la siguiente versión de OWL e incorpora recursos expresivos no incluidos en OWL y distingue un conjunto de fragmentos útiles en aplicaciones prácticas. OWL2 es la última Recomendación del W3C para ontologías.

SPARQL [13] es un lenguaje diseñado para razonar, consultar y modificar ontologías. Es un lenguaje bastante similar a SQL, la principal diferencia es que SQL asume que los datos están implementados en tablas y SPARQL asume que los datos están implementados en grafos RDF.

2.2. CARMEN

El proceso CARMEN, por un lado, incluye un metamodelo para apoyar la definición de instancias del modelo como requisitos de seguridad para CPS. Por otro lado, CARMEN utiliza modelos de características para representar la variabilidad de las configuraciones para CPS y los requisitos de seguridad. CARMEN mapea instancias de requisitos de seguridad con conceptos de modelos de características en configuraciones de seguridad a través de "weaving template" y transformaciones. Estas configuraciones se diagnostican mediante análisis automatizados basados en motores de análisis de dominio orientados a características [9].

El metamodelo (véase la figura 1) se centra en la entidad de requisitos de seguridad que se relaciona con un conjunto de activos y características de seguridad. Los activos se han alineado con las mejores prácticas de seguridad para IoT en el contexto de infraestructuras críticas formuladas por la agencia ENISA, y las características de seguridad para CPS se obtienen de OWASP para extraer los conceptos más importantes (por ejemplo, cifrado, protocolo, red, AES, SSL/TLS, Bluetooth, alcance, vida útil).

El tipo de activo comprende cualquier activo (o conjunto de activos) presentado en un sistema CPS, es decir, usuario, aplicación, servicio, plataforma, dispositivo, infraestructura o información. Además, puede haber relaciones entre tipos de activos, como entre un dispositivo y la infraestructura que lo soporta.

La característica de seguridad representa la preocupación por la seguridad de los requisitos, por ejemplo, el tipo de cifrado para los activos de información o comunicación. Y la propiedad de seguridad se refiere a la Confidencialidad o la Integridad; debe definirse una restricción relativa al tipo de cifrado, o en el caso de la Autenticación, debe definirse una política de contraseñas.

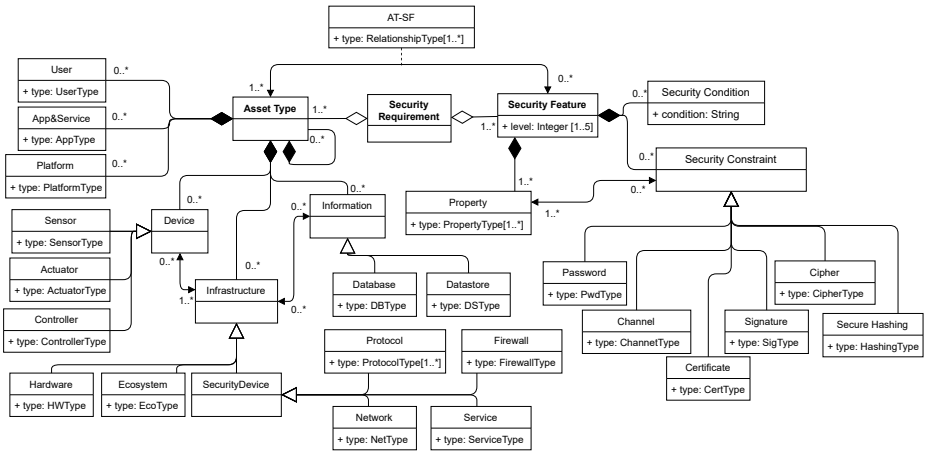

Figura 1. Metamodelo de CARMEN.

Los modelos de características [30] integrados en CARMEN, se utilizan como modelos formales para recoger la variabilidad de restricciones y relaciones entre tipos de activos y características de seguridad que deben tenerse en cuenta para las configuraciones. Por ejemplo, cuando se requiere confidencialidad, las comunicaciones forzadas deben utilizarse como canal seguro. Un modelo de rasgos es un modelo que representa un conjunto de productos pero que se define por sus rasgos y sus relaciones. Un rasgo es una característica de los sistemas que puede configurarse, por ejemplo, para elegir el protocolo de comunicación entre varias alternativas. El modelo de rasgos abarca dos partes principales: (1) los activos (cf., Activo) implicados en el requisito de seguridad, y; (2) la especificación de los requisitos de seguridad donde pueden definirse propiedades, condiciones y restricciones.

3. Onto-CARMEN

Esta sección presenta el enfoque Onto-CARMEN. En primer lugar, presentamos el proceso que lo sustenta. A continuación, se describe en detalle el modelo semántico. Y por último, se muestra el enfoque de razonamiento utilizado para verificar y diagnosticar.

3.1. Proceso

La Figura 2 representa el flujo de trabajo propuesto por el enfoque Onto-CARMEN. En primer lugar, es necesario describir los requisitos de seguridad que implican los componentes CPS y los aspectos de seguridad. Para ello, se formaliza un modelo semántico para los requisitos de seguridad en CPS en la subsección 3.2. La ontología permite la creación de individuos como nuevas instancias de requisitos de seguridad.

Para validar estos requisitos, la información recopilada en los modelos de características CARMEN se traduce en axiomas semánticos y reglas SPARQL. La subsección 3.3 proporciona los detalles necesarios para conocer las reglas semánticas y su funcionamiento. La validación mediante reglas semánticas permite realizar una primera comprobación de los requisitos de seguridad identificando la validez del requisito en (OK o KO). En el caso de que el requisito de seguridad no sea válido, las reglas semánticas permiten realizar un diagnóstico proporcionando acciones correctivas para transformarlo en válido.

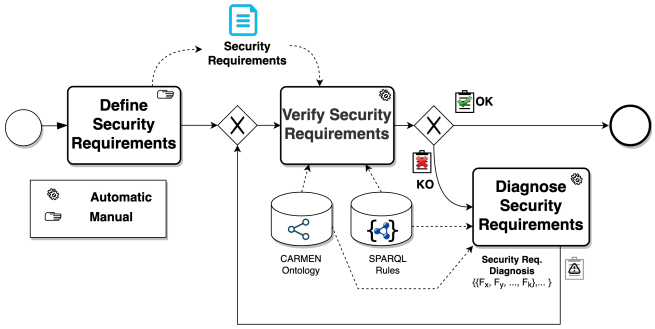

Figura 2. Proceso de Onto-CARMEN.

3.2. Modelo semántico de CARMEN

Para el diseño de la ontología hemos seguido la metodología "Ontology 101 development Process"[19], obteniendo una ontología resultante que consta de: 32 clases (que representan individuos con la misma taxonomía), 23 propiedades de objeto (relación binaria entre individuos), 23 propiedades de datos (atributos de los individuos), 22 tipos de datos definidos (para representar valores permitidos para las propiedades de datos), 12 individuos (utilizados por las clases definidas para representar niveles de seguridad y etiquetas de sostenibilidad) y 112 axiomas (restricciones de cardinalidad y valor). A continuación se describen las siete etapas de la metodología y cómo se han aplicado:

Determinar el dominio y alcance de la ontología. La ontología se centra en definir los requisitos de seguridad de CPS a partir de la identificación de los activos (usuarios, dispositivos, infraestructura, etc.) siguiendo las directrices de ENISA [1] y de las características de seguridad asociadas, siguiendo las recomendaciones de OWASP [3] para extraer los conceptos más importantes (por ejemplo, cifrado, protocolo, red, AES, SSL/TLS, Bluetooth, alcance, vida útil).

Considerar la reutilización de ontologías existentes. La flexibilidad del uso de ontologías permite la integración con otras ontologías, como el enfoque de [25]. El uso de ontologías externas enriquece o amplía conceptos fuera del

alcance de ENISA y OWASP al incluir, por ejemplo, nuevas características de seguridad para el no repudio.

Enumerar los términos importantes de la ontología. Se han extraído del metamodelo de CARMEN (Figura 1). Entre ellos se incluyen SecurityRequirement, AssetType, SecurityFeature, SecurityLevel, SustainabilityLabel, SecurityConstraint, etc.

Definir las clases y su jerarquía. Extraemos las clases ontológicas de los términos relevantes y las definimos junto con su jerarquía hasta un nivel de detalle suficiente para la clasificación de individuos. La figura 3 muestra las clases representando sus relaciones a través de propiedades de objeto o la conexión subClassOf (subclase de). Las principales clases permiten establecer las necesidades de seguridad (Security Requirement) que se definen en el entorno CPS. Para ello, se debe definir un conjunto de tipos de activos (Asset Type) implicados en la definición del requisito y las características de seguridad (Security Feature) que se deben incorporar para proteger adecuadamente dicho conjunto de activos y satisfacer la descripción del requisito.

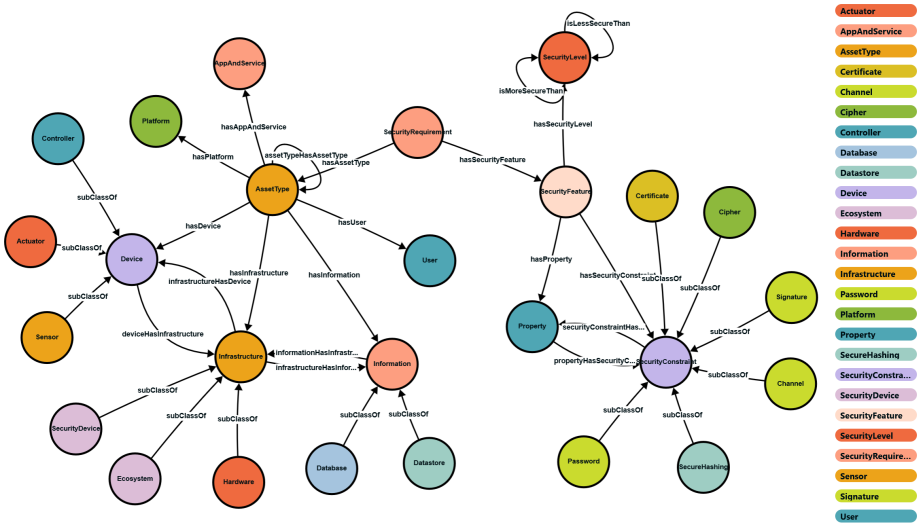

Figura 3. Vista general de la ontología.

Definir las propiedades de clases. Hemos establecido las propiedades de objetos y datos necesarias para representar las conexiones entre individuos y almacenar su información. La Tabla 1 muestra algunos ejemplos de dichas propiedades definidas. Propiedades de objeto como "hasSecurityLevel"que indica el nivel de seguridad asociado a una SecurityFeature; "hasSustainabilityLabel"que indica la etiqueta de sostenibilidad asociada a cualquier elemento o "hasAssetType"que indica el conjunto de activos implicados en un Requisito de Seguridad.

Los individuos que representan los posibles valores de SecurityLevel (low, medium, etc.) y SustainabilityLabel (A, B, C, etc.) también tienen propiedades de objeto que indican si un nivel o etiqueta es superior o inferior a otro. Por otro lado, las propiedades de datos que se han definido, se encargan en su mayoría de representar el tipo de dato del elemento (modelado como un tipo propio de dato con un conjunto de valores posibles). Por ejemplo, la clase Network tiene asociada una propiedad de datos para representar su tipo (typeNetwork) que puede tomar uno de los siguientes valores definidos en el tipo de datos NetworkType (LAN, PAN, VPN, WAN, WLAN, WPAN).

Tabla 1. Algunos ejemplos de propiedades de objetos y de datos definidas en Onto-CARMEN.

Propiedades de objetos	Descripción lógica
hasAssetType	$\exists$ hasAssetType Thing $\sqsubseteq$ SecurityRequirement $\top \sqsubseteq \forall$ hasAssetType AssetType
hasSecurityLevel	$\exists$ hasSecurityLevel Thing $\sqsubseteq$ SecurityFeature $\top \sqsubseteq \forall$ hasSecurityLevel SecurityLevel
hasSustainabilityLabel	$\exists$ hasSustainabilityLabel Thing $\top \sqsubseteq \forall$ hasSustainabilityLabel SustainabilityLabel
isLessSecureThan	$\exists$ isLessSecureThan Thing $\sqsubseteq$ SecurityLevel $\top \sqsubseteq \forall$ isLessSecureThan SecurityLevel
isLessSustainabilityThan	$\exists$ isLessSustainabilityThan Thing $\sqsubseteq$ SustainabilityLabel $\top \sqsubseteq \forall$ isLessSustainabilityThan SustainabilityLabel
isMoreSecureThan	$\exists$ isMoreSecureThan Thing $\sqsubseteq$ SecurityLevel $\top \sqsubseteq \forall$ isMoreSecureThan SecurityLevel
isMoreSustainabilityThan	$\exists$ isMoreSustainabilityThan Thing $\sqsubseteq$ SustainabilityLabel $\top \sqsubseteq \forall$ isMoreSustainabilityThan SustainabilityLabel
Propiedades de datos	**Descripción lógica**
condition	$\exists$ condition Datatype Literal $\sqsubseteq$ SecurityFeature $\top \sqsubseteq \forall$ condition Datatype string
typeNetwork	$\exists$ typeNetwork Datatype Literal $\sqsubseteq$ Network $\top \sqsubseteq \forall$ typeNetwork Datatype NetworkType

Definir axiomas. Este paso incluye la definición de restricciones de cardinalidad mínima y máxima, valores posibles para el dominio o rango y otras restricciones como transitividad, inversa, etc. Por ejemplo, la clase SecurityRequirement tiene asociada al menos un activo (cardinalidad de 1 a n), un tipo de relación (cardinalidad 1) y una característica de seguridad (cardinalidad 1). También puede tener (o no) asociada una etiqueta de sostenibilidad (cardinalidad de 0 a 1). Algunas relaciones son inversas, como propertyHasSecurityConstraint y SecurityConstraintHasProperty. Otras son transitivas, como las propiedades de objeto isLess o isMore asociadas a niveles de seguridad y etiquetas de sostenibilidad en las que se puede inferir que una es mayor o menor que la otra aunque no tengan una conexión directa.

3.3. Marco de razonamiento

Como se ha explicado anteriormente en la Sección 2, existe un conjunto de modelos de características que recogen las restricciones y relaciones entre elementos que deben tenerse en cuenta para que las configuraciones de seguridad creadas sean válidas.

En Onto-CARMEN estas restricciones se han definido mediante un conjunto de reglas SPARQL que permiten razonar sobre la ontología realizando tanto la validación de las configuraciones de seguridad como su diagnóstico y corrección de forma automatizada. Esto significa que cada regla definida comprueba una determinada situación no válida y, en caso de detectarla, realiza los cambios necesarios en la ontología (modificando propiedades, añadiendo o eliminando elementos, etc.) para convertirla en una configuración válida. Mediante razonamiento encadenado, podríamos partir de una configuración inicial que se iría enriqueciendo sucesivamente en base a la activación de reglas que evolucionarían dicha configuración a un nuevo estado en el que podrían activarse otras reglas. A nivel de implementación se ha utilizado Stardog, el cuál es un conocido sistema de gestión de datos basado en grafos y RDF que incluye un motor de razonamiento y tiene soporte para SPARQL.

A continuación, se presenta una de estas reglas a modo de ejemplo. Existe una restricción que indica que si en una característica de seguridad estamos utilizando un cifrado de tipo Camellia, el nivel de seguridad asociado a esa característica de seguridad ha de ser medio. A continuación se muestra la regla CamelliaRequiresMediumSecurityLevel, encargada de detectar situaciones en las que se está utilizando este tipo de cifrado pero el nivel de seguridad no es el adecuado y, en caso de encontrarlo, cambiaría el nivel de seguridad asociado al elemento de seguridad al correcto (medio en este caso).

Regla CamelliaRequiresMediumSecurityLevel

```
DELETE {
  ?sf ontocarmen:hasSecurityLevel ?sl . }
INSERT {
  ?sf ontocarmen:hasSecurityLevel ontocarmen:MediumSecurityLevel . }
WHERE{
   ?sf a ontocarmen:SecurityFeature .
   ?sf ontocarmen:hasSecurityLevel ?sl .
   FILTER (?sl != ontocarmen:MediumSecurityLevel) .
   ?sf ontocarmen:hasSecurityConstraint ?sc .
   ?sc a ontocarmen:Cipher .
   ?sc ontocarmen:typeCipher "Camellia" . }
```

4. Experimentación

En esta sección, se emplean varios requisitos de seguridad de un caso de estudio real para validar el enfoque en términos de representación de requisitos de seguridad y sus capacidades de razonamiento para la validación y verificación. Onto-CARMEN permite su aplicación a otros casos de estudio relacionados con

IoT / CPS, ya que al estar alineada con ENISA y OWASP incluye los elementos más relevantes a considerar en este tipo de sistemas.

Los requisitos de seguridad descritos se obtienen a partir de un sistema CPS para cultivo hidropónico [31], en el que intervienen diversos componentes, tanto hardware como software. A nivel físico tenemos: sensores de temperatura, luz y humedad; calentador, refrigerador, ultravioleta, inyector de nutrientes y bombas de agua; una placa de desarrollo Arduino que nos permite programar el microcontrolador y establecer conexiones con los sensores y actuadores mencionados y un sistema web que recibe los datos de todos los sensores y los envía (mediante conexiones inalámbricas) al sistema Big Data para su posterior almacenamiento, análisis y visualización. Además de la parte física, el controlador está conectado a un sistema de visualización y control con tecnologías Big Data donde se despliega un dashboard, un gestor de datos y un datastore (HDFS y HBASE).

- **Requisito de seguridad SR1:**
  El requisito establece que la comunicación inalámbrica entre el sensor de temperatura y el microcontrolador debe cifrarse para mantener un alto nivel de confidencialidad. Para lograrlo, hemos definido la propiedad de Confidencialidad, que está asociada a un tipo específico de cifrado (Camellia) y a un canal de comunicación seguro (HTTPS). Esta característica de seguridad se aplica a un conjunto de activos que incluye el sensor de temperatura y el Arduino, que se comunican entre sí a través de una red WLAN utilizando BLE o RFID. Esta relación entre la característica de seguridad y el conjunto de activos se denomina comunicación segura.
  En la Figura 4 se muestra cómo se aplica la regla al requisito de seguridad SR1, detectando una situación no válida ya que presenta un nivel de seguridad alto (parte superior de la figura) y cómo, tras aplicar la regla, el nivel de seguridad se ha modificado a medio (parte inferior de la figura).
- **Requisito de seguridad SR2:** Los sensores de temperatura, luz y humedad se conectan a un controlador Arduino mediante Bluetooth. La información transmitida actúa bajo el protocolo cliente/servidor HTTP pero debe asegurarse aplicando el protocolo SSL/TLS sobre HTTP, asegurando la confidencialidad. Esta información se almacena encriptada en un servidor web local con HDFS y HBASE, asegurando la integridad.
  En primer lugar, SR2 define que la comunicación debe ser confidencial con un nivel alto, por lo que se define la característica de seguridad que tiene la propiedad de confidencialidad y un canal de comunicación seguro utilizando HTTPS. Estas condiciones se comprueban utilizando las reglas SPARQL comentadas en la Sección anterior 3.3. Sin embargo, esto no es válido debido a que la base de datos y el datastore (assets) están relacionados con un elemento de seguridad con un nivel de seguridad muy alto utilizando cifrado AES128GCM, pero este cifrado sólo está indicado para un nivel de seguridad alto. Existirían dos opciones como acciones correctivas: (1) bajar el nivel de seguridad de muy alto a alto para cumplir las condiciones de AES128GCM; y (2) cambiar el tipo de cifrado a ChaCha20. La siguiente regla SPARQL

permite detectar esta situación no válida y corregirla automáticamente utilizando la primera opción (nivel de seguridad de muy alto a alto).

5. Trabajo relacionado

En este apartado analizaremos todas las propuestas existentes relacionadas con ontologías de seguridad, ontologías de requisitos de seguridad y para el análisis y gestión de riesgos, y centraremos el análisis en las propuestas sobre ontologías de seguridad para CPS.

Algunas aproximaciones se centran en el desarrollo de ontologías y requisitos de seguridad [22][26] y privacidad [11]. Algunos investigadores han desarrollado herramientas de seguridad basadas en ontologías capaces de integrarse con las etapas iniciales del proceso de desarrollo [20], para modelar patrones de seguridad, lo que proporciona una forma sistemática y reutilizable de representar el conocimiento de diseño de seguridad [28].

Existen numerosos trabajos que definen enfoques basados en ontologías para capturar requisitos de seguridad en diferentes entornos como en computación en la nube [4], para identificar y clasificar amenazas y requisitos de seguridad y evaluar la seguridad en IoT [12], o en entronos sanitarios [6][7]. También hay trabajos de ontologías de seguridad para capturar los requisitos de seguridad y evaluar la seguridad de las ciudades y hogares inteligentes [21][15].

Por otro lado, las ontologías de seguridad para el análisis y gestión de riesgos permiten obtener automáticamente una visión global de todo el sistema, infiriendo el conocimiento necesario, y finalmente estimando el nivel de riesgo del sistema analizado [24][5]. Estas propuestas hacen uso de las ontologías basadas en inteligencia de ciberamenazas [17] o en vulnerabilidades [27].

En cuanto a propuestas existentes que permitan modelar los requisitos de seguridad para CPS, podemos indicar el trabajo de Shaaban et. al. [25] quienes introducen una cadena de herramientas de seguridad basada en ontologías capaz de integrarse con las etapas iniciales del proceso de desarrollo de sistemas críticos. En [33] se razona semánticamente sobre el impacto de los ciberataques en los sistemas físicos, y en [8] aplican enfoques ontológicos y técnicas de razonamiento para lograr una mayor comprensión de los CPS.

Como hemos comentado anteriormente, la mayoria de propuestas se centran más o en políticas, o en comunicaciones, o en dominios específicos, y nuestra propuesta se centra en un entorno específico como son los sistemas CPS donde cualquier dominio que haga uso de conceptos CPS tiene cabida, además nuestra propuesta se centra en ayudar en las primeras fases de desarrollo mediante la identificación, modelado, análisis, verificación y validación de requisitos de seguridad.

6. Conclusiones

Los CPS son sistemas que ofrecen grandes oportunidades para la industria y la sociedad, pero su desarrollo no se consideran los aspectos de seguridad ni los

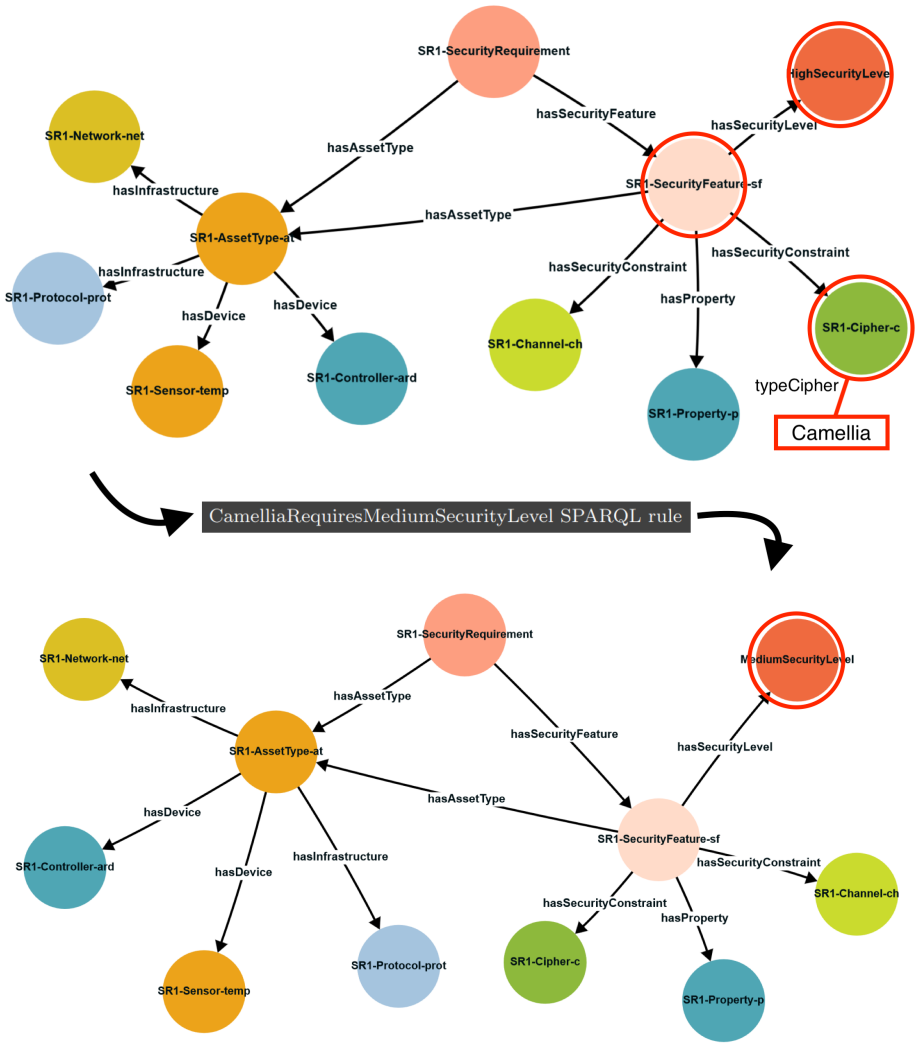

Figura 4. Aplicación de la regla CamelliaRequiresMediumSecurityLevel.

nuevos riesgos que implican. En el contexto de los requisitos de seguridad, las ontologías proporcionan una comprensión compartida de los conceptos relevantes y sus relaciones, ayudando a las partes interesadas a identificar y articular las necesidades de seguridad con mayor precisión.

En este trabajo proponemos el diseño e implementación de una ontología de seguridad (Onto-CARMEN) capaz de capturar las necesidades de seguridad de los sistemas CPS a través de la definición de requisitos de seguridad. Además, se propone un marco de razonamiento para la verificación y diagnóstico de los requisitos de seguridad en tiempo de diseño, permitiendo conocer en todo momento si la definición del requisito es adecuada y cumple con las reglas ontológicas, y también permite detectar definiciones incorrectas de requisitos de seguridad, derivando o recomendando requisitos de seguridad correctos de acuerdo a la ontología definida.

Como trabajo futuro, incorporaremos otras ontologías de seguridad existentes, como las de análisis y gestión de riesgos, para extender y enriquecer Onto-CARMEN incorporando conocimiento de inteligencia de amenazas.Además se pretende incorporar conceptos de sostenibilidad y eficiencia y consumo energético para predecir y recomendar los mejores y más eficientes mecanismos y configuraciones de seguridad para un entorno CPS específico.

Agradecimientos Este trabajo es parte de los proyectos ALBA-UCLM(TED2021-130355B-C31), ALBA-UC(TED2021-130355A-C33), ALBA-US(TED2021-130355B-C32) financiados por MCIN/AEI/10.13039/501100011033/ Unión Europea Next-GenerationEU/PRTR, AETHER-UCLM(PID2020-112540RB-C42/ AEI/10.13039 /501100011033), AETHER-US(PID2020-112540RB-C44/ AEI/10.13039/501100011033), COPERNICA (P20_01224) y METAMORFOSIS (US-1381375).

Referencias

1. Baseline security recommendations for IoT (Apr 2018), https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
2. Cyber-physical systems security: Limitations, issues and future trends. Microprocessors and Microsystems **77**, 103201 (2020). https://doi.org/https://doi.org/10.1016/j.micpro.2020.103201
3. OWASP Internet of Things Project. Available from OWASP (2021), https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Main
4. Ageed, Z.S., Ibrahim, R.K., Sadeeq, M.A.M.: Unified Ontology Implementation of Cloud Computing for Distributed Systems. Current Journal of Applied Science and Technology pp. 82–97 (nov). https://doi.org/10.9734/cjast/2020/v39i3431039
5. Alanen, J., Linnosmaa, J., Malm, T., Papakonstantinou, N., Ahonen, T., Heikkilä, E., Tiusanen, R.: Hybrid ontology for safety, security, and dependability risk assessments and Security Threat Analysis (STA) method for industrial control systems. Reliability Engineering & System Safety p. 108270 (apr). https://doi.org/10.1016/j.ress.2021.108270

6. Alenezi, M.: An Ontological Framework for Healthcare Web Applications Security. International Journal of Advanced Computer Science and Applications (6), 511–516. https://doi.org/10.14569/IJACSA.2021.0120658
7. Alsubaei, F., Abuhussein, A., Shiva, S.: Ontology-based security recommendation for the internet of medical things. IEEE Access **7**, 48948–48960 (2019). https://doi.org/10.1109/ACCESS.2019.2910087
8. Balduccini, M., Griffor, E., Huth, M., Vishik, C., Burns, M., Wollman, D.: Ontology-based Reasoning about the Trustworthiness of Cyber-physical Systems. Living in the Internet of Things: Cybersecurity of the IoT - 2018 **2018**(CP740), 12 (10 pp.)–12 (10 pp.) (2018). https://doi.org/10.1049/cp.2018.0012
9. Benavides, D., Segura, S., Ruiz-Cortés, A.: Automated analysis of feature models 20 years later: A literature review. Information Systems **35**(6), 615 – 636 (2010). https://doi.org/https://doi.org/10.1016/j.is.2010.01.001
10. Colombo, A.W., Veltink, G.J., Roa, J., Caliusco, M.L.: Learning industrial cyber-physical systems and industry 4.0-compliant solutions. In: 2020 IEEE Conference on Industrial Cyberphysical Systems (ICPS). vol. 1, pp. 384–390. IEEE (2020)
11. Gharib, M., Giorgini, P., Mylopoulos, J.: COPri v.2 — A core ontology for privacy requirements. Data & Knowledge Engineering **133**, 101888 (may 2021). https://doi.org/10.1016/j.datak.2021.101888
12. Gonzalez-Gil, P., Skarmeta, A.F., Martinez, J.A.: Towards an ontology for iot context-based security evaluation. In: 2019 Global IoT Summit (GIoTS). pp. 1–6 (2019). https://doi.org/10.1109/GIOTS.2019.8766400
13. Harris, S., Seaborne, A.: SPARQL 1.1 Query Language (Mar 2013), https://www.w3.org/TR/2013/REC-sparql11-query-20130321/
14. Kalibatiene, D., Vasilecas, O.: Survey on ontology languages. In: Perspectives in Business Informatics Research - 10th International Conference, BIR 2011, Riga, Latvia, October 6-8, 2011. Proceedings. vol. 90, pp. 124–141. Springer (2011). https://doi.org/10.1007/978-3-642-24511-4_10
15. Khan, Y.I., Ndubuaku, M.U.: Ontology-based automation of security guidelines for smart homes. In: 2018 IEEE 4th World Forum on Internet of Things (WF-IoT). pp. 35–40 (2018). https://doi.org/10.1109/WF-IoT.2018.8355214
16. Lezzi, M., Lazoi, M., Corallo, A.: Cybersecurity for industry 4.0 in the current literature: A reference framework. Computers in Industry **103**, 97 – 110 (2018). https://doi.org/https://doi.org/10.1016/j.compind.2018.09.004
17. Merah, Y., Kenaza, T.: Ontology-based Cyber Risk Monitoring Using Cyber Threat Intelligence. ACM International Conference Proceeding Series (aug). https://doi.org/10.1145/3465481.3470024
18. Mörth, O., Emmanouilidis, C., Hafner, N., Schadler, M.: Cyber-physical systems for performance monitoring in production intralogistics. Computers & Industrial Engineering **142**, 106333 (2020). https://doi.org/https://doi.org/10.1016/j.cie.2020.106333
19. Noy, N., (Hrsg.), D.M.: Ontology development 101: A guide to creating your first ontology. Technical report. Stanford knowledge systems laboratory technical report KSL-01-05 (2001)
20. Peldszus, S., Bürger, J., Kehrer, T., Jürjens, J.: Ontology-driven evolution of software security. Data & Knowledge Engineering **134**, 101907 (2021). https://doi.org/https://doi.org/10.1016/j.datak.2021.101907
21. Qamar, T., Bawany, N.: A Cyber Security Ontology for Smart City. International Journal on Information Technologies and Security **12**(3), 63–74 (2020)

22. Rashid, A., Ali, R., Lages, W.: Ontology-based security requirements engineering for software-intensive systems. IEEE Transactions on Software Engineering **45**(2), 187–215 (2019). https://doi.org/10.1109/TSE.2017.2763965
23. ur Rehman, S., Allgaier, C., Gruhn, V.: Security requirements engineering: A framework for cyber-physical systems. In: 2018 International Conference on Frontiers of Information Technology (FIT). pp. 315–320. IEEE (2018)
24. Sánchez-Zas, C., Villagrá, V.A., Vega-Barbas, M., Larriva-Novo, X., Moreno, J.I., Berrocal, J.: Ontology-based approach to real-time risk management and cyber-situational awareness. Future Generation Computer Systems **141**, 462–472 (2023). https://doi.org/https://doi.org/10.1016/j.future.2022.12.006
25. Shaaban, A.M., Gruber, T., Schmittner, C.: Ontology-based security tool for critical cyber-physical systems. In: 23rd International Systems and Software Product Line Conference - Volume B. p. 207–210. SPLC '19, Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3307630.3342397
26. Shaaban, A.M., Gruber, T., Schmittner, C.: Ontology-based security tool for critical cyber-physical systems. In: 23rd International Systems and Software Product Line Conference - Volume B. p. 207–210. SPLC '19, Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3307630.3342397
27. Syed, R.: Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system. Information & Management **57**(6), 103334 (2020). https://doi.org/https://doi.org/10.1016/j.im.2020.103334
28. Vale, A.P., Fernandez, E.B.: An Ontology for Security Patterns. Proceedings - International Conference of the Chilean Computer Science Society, SCCC **2019-November** (nov 2019). https://doi.org/10.1109/SCCC49216.2019.8966393
29. Valle, P., Arrieta, A., Arratibel, M.: Automated misconfiguration repair of configurable cyber-physical systems with search: an industrial case study on elevator dispatching algorithms. CoRR **abs/2301.01487** (2023). https://doi.org/10.48550/arXiv.2301.01487
30. Varela-Vaca, Á.J., Gasca, R.M.: Formalization of security patterns as a means to infer security controls in business processes. Logic Journal of the IGPL **23**(1), 57–72 (2015). https://doi.org/10.1093/jigpal/jzu042
31. Varela-Vaca, Á.J., Rosado, D.G., Sánchez, L.E., Gómez-López, M.T., Gasca, R.M., Fernández-Medina, E.: Carmen: A framework for the verification and diagnosis of the specification of security requirements in cyber-physical systems. Computers in Industry **132**, 103524 (2021). https://doi.org/https://doi.org/10.1016/j.compind.2021.103524
32. Varela-Vaca, Á.J., Rosado, D.G., Sánchez, L.E., Gómez-López, M.T., Gasca, R.M., Fernández-Medina, E.: Definition and verification of security configurations of cyber-physical systems. In: Computer Security. pp. 135–155. Springer International Publishing, Cham (2020). https://doi.org/https://doi.org/10.1007/978-3-030-64330-0_9
33. Venkata, R.Y., Kamongi, P., Kavi, K.: An ontology-driven framework for security and resiliency in cyber physical systems. ICSEA **2018**, 23 (2018)
34. Zunino, C., Valenzano, A., Obermaisser, R., Petersen, S.: Factory communications at the dawn of the fourth industrial revolution. Computer Standards & Interfaces **71**, 103433 (2020). https://doi.org/https://doi.org/10.1016/j.csi.2020.103433