TENDENCIAS EN DISEÑO DE LA RESILIENCIA DE REDES INTELIGENTES

Raúl Pastor, Doctorando de ingeniería y organización industrial – UC3M
J. Javier Larrañeta, Secretario general de la Plataforma Tecnológica de Seguridad Industrial – PESI
J. María Álvarez-Rodríguez, Profesor asociado. Departamento de Ciencias de la Computación – UC3M

La resiliencia de un sistema es su capacidad para recuperarse y minimizar las consecuencias tras un evento de riesgo acontecido. Cuando el sistema de interés (SOI) es una zona urbana o industrial, los sistemas energéticos renovables (SRs) pueden contribuir a su resiliencia a través de una operación coordinada tras el evento de riesgo, entre otras acciones preventivas articulables desde fase de rediseño de esas zonas.

Los SRs, y en concreto las redes, tanto las térmicas de frío y calor, como las eléctricas, y en el futuro puede que las de gases renovables, deben cooperar para satisfacer la demanda instantánea del SOI optimizando el uso de los recursos disponibles y esto es posible mediante una correcta gestión de los requisitos en parte derivados del uso de modelos de simulación desde fase de diseño de los SRs.

Por analogía al modo de operación normal, los requisitos exigidos a los SRs en circunstancias post siniestro vendrán determinados por un modelo de gobernanza de los riesgos, las necesidades del SOI para su recuperación, la fiabilidad y seguridad de los propios SRs (particularización del modelo de referencia de la plataforma PESI).

Con el enfoque puesto en el análisis de fiabilidad y seguridad de las redes inteligentes, se propone presentar en el Congreso de Redes Inteligentes el grado de uso de modelos a través del análisis de publicaciones recientes definiendo así una primera ontología facilitadora de la interoperabilidad de los SRs y de sus Gemelos Digitales en el contexto de la Ciudad Inteligente y la Industria 4.0.

Palabras clave: Resiliencia, Redes Inteligentes, Smart Grids, Gemelo Digital, Ciudades Inteligentes, Seguridad

INTRODUCCIÓN Y ANTECEDENTES

La resiliencia de un sistema es su capacidad para recuperarse y minimizar las consecuencias tras un evento de riesgo acontecido. Cuando el sistema de interés (SOI en inglés) es una zona urbana o industrial, los sistemas energéticos renovables (SRs) pueden contribuir a su resiliencia a través de una operación coordinada tras el evento de riesgo, entre otras acciones preventivas articulables desde fase de rediseño de esas zonas.

Actualmente más del 30% de las inversiones para la adaptación de las redes eléctricas de transporte y distribución en EEUU se están acometiendo por razones de la resiliencia y la necesidad de adaptación a los riesgos del cambio climático como pueden ser los incendios y los eventos meteorológicos extremos, para lo que afrontarán un importante proceso de digitalización y de uso de nuevas tecnologías (McKinsey & Company, 2022).

La resiliencia es una propiedad emergente de los sistemas, esto es, solo queda descrita cuando acontecen los sucesos de riesgo y la siguiente fase de recuperación de todo o parte del sistema afectado por ese suceso, pero su carácter emergente no implica que no se deba gestionar, al contrario, sin embargo esta gestión debe estar integrada con otras disciplinas como la seguridad (prevención, security), la gestión de activos, incluso la innovación, y quedar fundamentada en la gestión de los riesgos y de las oportunidades. En ese contexto de gestión es que se pueden fijar objetivos, planificar y ejecutar las acciones derivadas, evaluar y corregir, siguiendo un modelo clásico PDCA (plan-do-check-act).

Los SRs, y en concreto las redes, tanto las térmicas de frío y calor, como las eléctricas, y en el futuro puede que las de gases renovables, deben cooperar para satisfacer la demanda instantánea del SOI optimizando el uso de los recursos disponibles y esto es posible mediante una correcta gestión de los requisitos en parte derivados del uso de modelos de simulación desde fase de diseño de los SRs, y por analogía, los requisitos exigidos a los SRs en circunstancias post siniestro vendrán determinados por un modelo de gobernanza de los riesgos como el anteriormente descrito necesariamente digitalizado dotado de sus propias simulaciones.

De entre los diferentes SRs el más normalizado y avanzado en cuanto a la digitalización de sus sistemas son las redes eléctricas inteligentes pues en ellas se concentran multitud de actores, procesos y tecnologías que necesitan intercambiar información en escalas de tiempo del 10^{-6} segundos, como requieren los dispositivos de

corte de alta frecuencia, hasta los 10^5 segundos (o el día), en que se puede almacenar y despachar la electricidad acumulada en baterías. En el caso de las redes térmicas y las de gases renovables, éstas manejan tiempos de actuación instantánea del orden de 1 segundo y de acumulación de 10^7 segundos (o meses). Son sistemas que requieren una mayor intervención humana ante un fallo. Aun teniendo los sistemas diferentes niveles de madurez en cuanto a su digitalización y normalización, los SRs deben cooperar entre sí para satisfacer la demanda instantánea del SOI optimizando el uso de los recursos disponibles en cualquier circunstancia previsible.

Dentro de la arquitectura de referencia para la redes inteligentes (CEN-CENELEC-ETSI, 2012) representada en la Figura 1, entendida ésta como un sistema de sistemas (SoS, en inglés), la capa de negocio es aquella que permite plantear precisamente una gestión de la resiliencia con objetivos concretos que serán después trasladados a funciones a través de la definición de casos de uso, y al diseño detallado hasta cubrir la especificación de los elementos de dichos sistemas.

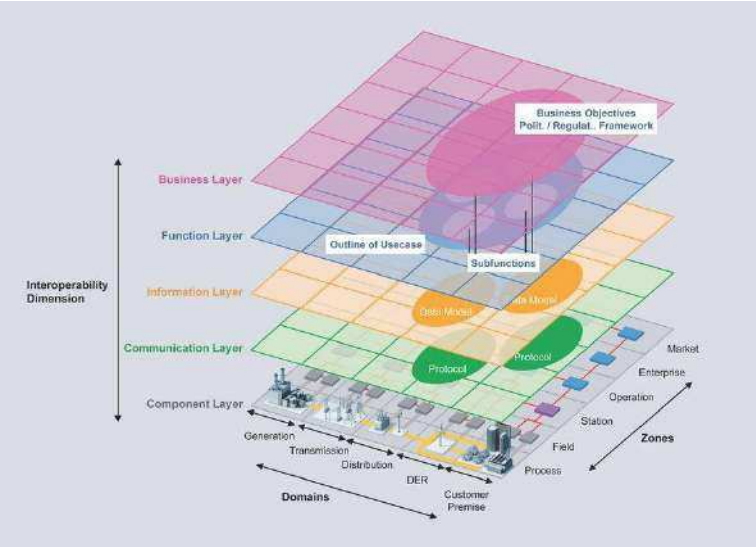

Figura 1. Arquitectura de la Red Inteligente (CEN-CENELEC-ETSI, 2012)

La Plataforma Tecnológica de la Seguridad Industrial, PESI, nos propone un modelo conceptual que denominaremos *Modelo PESI de la seguridad integral*, difundido y aceptado entre organizaciones de innovación abierta de la seguridad industrial en Europa (Larrañeta, 2022). Este modelo nos aporta un contexto para la gestión de la resiliencia de las actividades industriales y las ciudades, a través de paradigmas que motivan la investigación, el desarrollo y el uso de soluciones innovadoras de la seguridad (safety, security), que en esencia son sistemas que se deben integrar en los SRs.

La agenda estratégica de esta plataforma tecnológica nos recuerda la política europea y nacional (SEDIA, 2022) de fomento del uso de las tecnologías habilitadoras clave (KET en inglés) a lo largo del ciclo de vida de la ingeniería de todos los sistemas, los de la seguridad y del propio SOI. Son ejemplos de KETs el procesado en lenguaje natural (NLP en inglés), y la inteligencia artificial (A.I. en inglés) y el internet de las cosas (IoT en inglés).

Volviendo a la arquitectura de referencia para las redes inteligentes, y particularmente en la fase de desarrollo de la red inteligente como sistema e sistemas, a lo largo del proceso de diseño es posible aplicar estándares de modelado como UML para definir los casos de uso, y más genéricamente, RSHP (Llorens, Morato, & Génova, 2004) que permite complementar cualquier especificación y ampliarla al uso de modelos que pueden ser tanto textuales, propios del procesado en lenguaje natural (NLP), como de modelado y simulación, con tal de gestionar el conocimiento en ingeniería de los sistemas y facilitar su reusabilidad.

Los paradigmas de la Industria 4.0 y otros como el Gemelo Digital aplicado a la Ciudad Inteligente, requieren a su vez del uso de otra gama de tecnologías habilitadoras como los entornos de gestión del diseño en el ciclo de vida del producto (PLM en inglés), los específicos de modelado y simulación de la fiabilidad-disponibilidad-mantenibilidad y la seguridad-safety (RAMS en inglés), los sistemas de gestión del mantenimiento

computarizado (CMMS en inglés) y de la gestión de la información en construcción (BIM en inglés). Efectivamente esos modelos pueden ser tratados como elementos de información a través de aplicaciones que facilitan la interoperabilidad en ingeniería de sistemas y la gestión del conocimiento relacionada.

Es en el anterior contexto de gobernanza, uso de tecnologías habilitadoras y paradigmas en que las ontologías, los modelos y los requisitos, entendidas las primeras como como representaciones del conocimiento formalizables y los segundos como activos del conocimiento, pueden ser usados en las redes inteligentes como demuestra la caja de herramientas del "Smart Grid Architecture Model" SGAM (SGAM-TOOLBOX 2.0, 2022), que proporciona tanto requisitos de seguridad (security) como un modelo de la red inteligente como sistema de sistemas para la herramienta *Enterprise Architecture* ®.

Con todo lo anterior se puede decir que actualmente, y transcurrida una década desde los primeros modelos de referencia de la arquitectura redes inteligentes, estamos en una buena posición para gestionar la resiliencia desde el rediseño de los sistemas de interés urbanos e industriales, y por lo tanto de trasladar necesidades, y requisitos a la capa del negocio de las redes inteligentes usando modelos, siendo todo ello habilitador incluso de la contratación pública como pudiera ser en procesos de compra pública de innovación (Álvarez, 2012). Surge pues la pregunta de conocer hasta qué grado de está acometiendo esta ingeniería de la resiliencia en las redes inteligentes en la actualidad.

METODOLOGÍA Y MEDIOS

La metodología empleada comienza con la particularización del *Modelo PESI de la seguridad integral* que será usado para detectar las posibles contribuciones a la resiliencia que las redes inteligentes pueden aportar a los sistemas de interés urbanos e industriales. Esta particularización no es objeto de esta comunicación sino que se emplea como el marco de trabajo explícito y común al de otros SRs presentes en un mismo SOI.

La ingeniería de la resiliencia es a su vez una disciplina empleada en la ingeniería de sistemas tal cual la entienden organismos internacionales como INCOSE. De las definiciones de esa base de conocimiento y trabajos previos de los autores, se propone el uso de un modelo conceptual y simplificado de los principios de diseño de la resiliencia para las redes inteligentes.

Ambos modelos emplean una terminología específica que debe ser traducida al inglés para ser empleada en la búsqueda de bibliografía en revistas científicas y técnica empleando metadatos. La muestra puede ser clasificada según los términos que definen, en el dominio de conocimiento de las redes inteligentes, los principios de diseño de la resiliencia.

Para la obtención de textos que permitan el análisis técnico posterior o más refinado, se emplea la capacidad *Risk and Alerts* integrada en la herramienta *SES ENGINEERING Studio*® que emplea el modelo RSHP y artefactos textuales que se configuran con la herramienta *KM-KNOWLEDGE Manager*® en forma de ontología para su reutilización.

En la fase de análisis, el grado de uso de los modelos relacionados con la gestión e ingeniería de la resiliencia se concreta, entre otros, por la propia cita de terminología clave relacionada en los documentos. Se diseñan a los efectos preguntas por analogía a modelos de uso o madurez de la Industria 4.0 como el modelo HADA (MINETUR, 2022).

PARTICULARIZACIÓN DEL MODELO DE LA SEGURIDAD INTEGRAL

Se propone adaptar el *Modelo PESI de la seguridad* integral simplificando éste cuanto a la gestión de las seguridades por concreción de los activos de protección para la seguridad safety y las operaciones de seguridad (security) de los planes de emergencia respectivamente, sin atender inicialmente a los posibles riesgos del SOI sino a la necesidad de disponer de suministro a través de una red inteligente que emplea energías locales.

La red inteligente pasará a depender sin embargo de su *Capacidad* dada por sus activos físicos y software, las personas y los procesos relacionados con la operación y mantenimiento de la red, esto es, de la fiabilidad y seguridad (safety, security). Será asumido también que existen requisitos de la seguridad y fiabilidad de las redes

inteligentes y que su uso tiene o puede tener implícito el principio europeo de la sostenibilidad de no causar daño.

Según el anterior modelo, existen soluciones de la seguridad comunes para el SOI que deben ser identificadas e incluso implementadas tempranamente y esa es precisamente una de las oportunidades de las redes inteligentes para contribuir a la resiliencia pues toda acción planificada y acometida antes es más barata y protege antes. Todo ello queda representado en la Figura 2 para los SRs en general donde las fuentes de información se representan con elipses y los rectángulos representan procesos, y las flechas relaciones de inferencia o de intercambio de información.

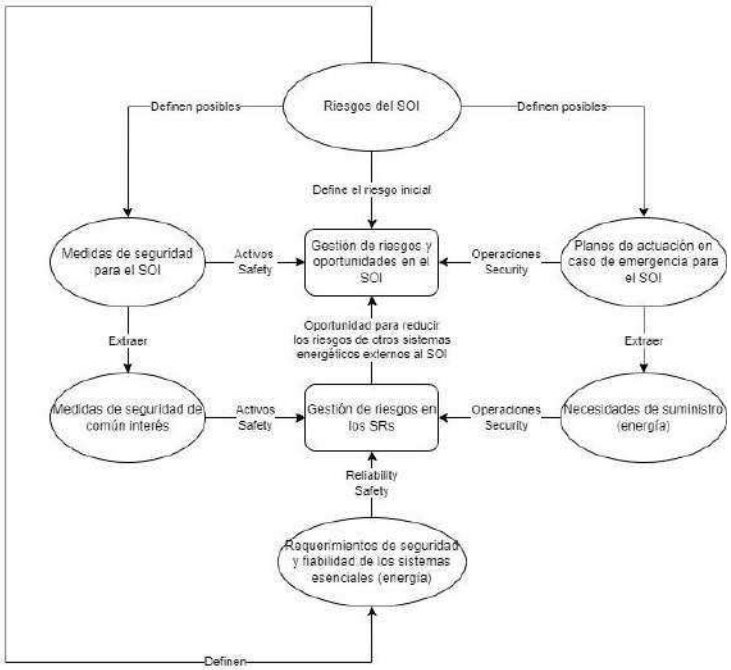

Figura 2. Adaptación del Modelo PESI de la seguridad integral para el estudio

MODELO CONCEPTUAL DE LOS PRINCIPIOS DE DISEÑO DE LA RESILIENCIA

La ingeniería de resiliencia está bien resumida en la guía de ingeniería de sistemas (INCOSE, 2015). En concreto se define esta ingeniería como un proceso cuyo resultado puede caracterizarse por un tiempo de recuperación, unas pérdidas asumibles y cierta selectividad de los riesgos por aplicación de los siguientes principios:

- *Capacidad* para soportar una amenaza, concretada en conceptos como la absorción de impactos y redundancia por parte de los sistemas.
- *Contención* para mantener fuera del sistema a la amenaza de un modo de operación o colapso inseguro, concretada por las capas de defensa.
- *Flexibilidad* para reestructurarse, concretada en una capacidad para auto reparación o reparación local de los sistemas.
- *Adaptabilidad* para prevenir un funcionamiento inseguro, concretada por conexiones flexibles, la intervención humana y la existencia de ciertos estados seguros.
- *Tolerancia* para sacar ventaja de una degradación, concretada por el funcionamiento autónomo de sistemas tras el fallo.
- *Cohesión* de los sistemas para trabajar como un todo, concretada por las conexiones de los sistemas.

En trabajos previos, los autores analizaron una veintena de publicaciones generalistas de energía relacionadas con energía y riesgos climáticos extremos derivados del Cambio Climático, el impacto económico asociado a esos riesgos y la estrategia europea para alcanzar un sistema energético más ecológico y seguro. La conclusión principal de ese estudio fue que los principios de ingeniería de la resiliencia en energía coexisten o derivan unas de las otras, siendo la *Capacidad*, concretada en diferentes activos o procesos, el principio más frecuentemente descrito y relacionado con el resto de los principios. La *Flexibilidad* y la *Adaptabilidad* se mostraron como propiedades normalmente empleadas y relacionadas entre sí. Estas conclusiones son de utilidad en la búsqueda

de bibliografía para este estudio y nos permiten justificar, aunque sea en primera aproximación, la elección de un modelo conceptual simplificado de los principios de la resiliencia para las redes inteligentes representado en la Figura 3.

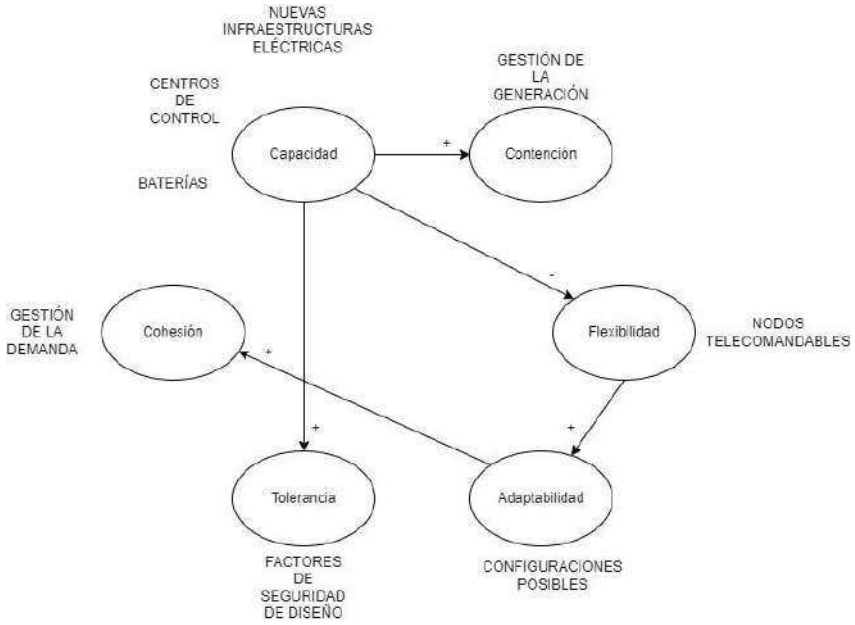

Figura 3. Modelo conceptual simplificado de los principios de diseño de la resiliencia para redes inteligentes

El modelo anterior indica que cuanta mayor *Capacidad*, el nivel *Tolerancia* exigido a los elementos de la red inteligente en su conjunto puede ser menor pues dicha capacidad implica normalmente duplicidades en los activos (de generación, distribución, almacenamiento…). La *Flexibilidad* sin embargo puede verse mermada por un exceso de concentración de *Capacidad*, siendo la topología de la red la que determine verdaderamente ese comportamiento, en tanto que la *Adaptabilidad* puede ser vista como una propiedad derivada de la *Flexibilidad* cuando la red sea capaz de operar en configuraciones más adaptadas a la demanda del SOI. Por último, la *Contención* puede ser una propiedad definida por la *Capacidad* de controlar la carga o cortar generación de los generadores que así lo permitan.

La utilidad de este modelo conceptual, que por descontado es limitado, no es otra que la de acotar el número de conceptos técnicos específicos de las redes inteligentes diseñadas con principios de la resiliencia. La elección de los términos puede ser ampliable por medio del uso de sinónimos o conceptos equivalentes, motivando, si cabe, una mejora del proceso de investigación.

SELECCIÓN DE LAS COMBINACIONES DE BÚSQUEDA DE BIBLIOGRAFÍA

La búsqueda de bibliografía en revistas científicas y técnicas emplea los siguientes términos y combinaciones como metadatos en los buscadores de las revistas científicas y técnicas entre los años 2012 y 2022 según se indica en la Tabla 1:

Temáticas (metadatos)	**Términos técnicos (metadatos)**	**Propiedad de la resiliencia representada**
Resilience, Smart grid(s),	Power management,…	Contención
	Power Switch,…	Flexibilidad
	Demand management,…	Cohesión
	Fault tolerance,…	Tolerancia
Resilience, Smart City(ies),	(Cualquiera de los anteriores)	Capacidad

Tabla 1. Metadatos y principios de la resiliencia (Fuente: elaboración propia)

Los metadatos son combinados con palabras clave según se indica en el siguiente apartado.

DEFINICIÓN DE ALERTAS DE BÚSQUEDA TEXTUAL EN LOS DOCUMENTOS

La definición terminología clave permite refinar la búsqueda de información en un buscador de bibliografía científico-técnica con metadatos. Como se ha comentado en la descripción de la metodología y medios, se emplea la capacidad *Risk and Alerts* integrada en la herramienta *SES ENGINEERING Studio®*. Dicha herramienta es capaz de proporcionar unidades de análisis (párrafos o tablas) que cumplen una o varias reglas o alertas. Tanto los términos clave como las reglas están recogidas en la Tabla 2:

Cuestión de interés	**Términos clave (para el buscador y alertas)**	**Términos de contexto (para alertas)**	**Reglas (alertas)**
Si se emplea un modelo de gestión de riesgos y las seguridades integral (Q1).	Risk management,…	Opportunity, impact, probability, safety, security, RM, GRC, FMEA, FMECA, Fault Tree, RCA	(Q1.1) Contexto el mismo párrafo o tabla que un término clave.
Si se emplean modelos de fiabilidad (Q2).	Reliability, availability, maintainability, safety,…	MTBF, MTTR, distribution, RAMS, maintenance, asset management	(Q2.1) Contexto el mismo párrafo o tabla que una término clave.
Si se consideran las operaciones de emergencia y recuperación (Q3).	Emergence, emergency, recovery,…	Recover, operation(s), activity(ies), plan(s)	(Q3.1) Contexto el mismo párrafo o tabla que un término clave. OR (Q3.2) Patrón en el mismo párrafo o tabla que un término clave: Time unt + … + Number Number + … + Time unit
Si se emplean paradigmas de la digitalización o metodologías de desarrollo (Q4).	Digital Twin, Smart City, Industry 4.0, …	DevOps, Agile, MBSE, EA, SysML, Digital Thread, Simulation, ontology, simulation model, IoT, BIM, PLM, CMMS, lifecycle/life-cycle, life cycle, system of systems / SoS, urban, village, industry(ies), industrial	(Q4.1) Contexto el mismo párrafo o tabla que un término clave. OR (Q4.2) Patrón en el mismo párrafo o tabla que un término clave: “research” OR “design” OR “development"+ **… +** un término del contexto un término del context + …+ “research” OR “design” OR “development"

Tabla 2. Refinamiento de la búsqueda y definición de alertas (Fuente: elaboración propia)

RESULTADOS

En base a los metadatos y el uso de palabras clave fue posible identificar en ScienceDirect 251 resultados que se corresponden con artículos mayoritariamente. De los anteriores, 77 resultados (el 31%) son referencias independientes, esto es, no cubren más de una combinación de búsqueda de metadatos y términos clave. De esos 77, los autores han seleccionado 20 lecturas (el 26%) indicados en la Tabla 2 donde la mitad superior de referencias provienen de la búsqueda de combinaciones de metadatos “Resilience, Smart grids,” y la segunda de “Resilience, Smart Cities,” para los diferentes términos técnicos de la Tabla 1:

		Resilience & Smart grid(s)								
Lectura seleccionada		Risk Management		Emergency, recovery			Resilience & Smart Cities			
ID	doi	Contención	Cohesión	Contención	Flexibilidad	Cohesión	Contención	Flexibilidad	Cohesión	Tolerancia
1	https://doi.org/10.1016/j.est.2022.104825.	1	1	1		1	1		1	
3	https://doi.org/10.1016/j.compeleceng.2022.107830.	1	1	1		1				
4	https://doi.org/10.1016/j.rser.2017.03.107.	1	1	1			1	1	1	
5	https://doi.org/10.1016/j.epsr.2019.02.014.	1	1	1		1	1		1	
6	https://doi.org/10.1016/j.tej.2022.107135.	1		1						
14	https://doi.org/10.1016/j.ifacol.2022.09.013.	1		1	1					
18	https://doi.org/10.1016/j.ijepes.2021.106974.			1						
19	https://doi.org/10.1016/j.ress.2016.02.009.	1	1	1			1	1		1
22	https://doi.org/10.1016/j.energy.2019.116442.	1	1	1		1	1	1	1	
25	https://doi.org/10.1016/j.scs.2021.103467.	1	1	1			1		1	
30	https://doi.org/10.1016/j.scs.2020.102412.						1	1	1	
34	https://doi.org/10.1016/j.scs.2020.102327.						1		1	
41	https://doi.org/10.1016/j.ijdrr.2022.102970.	1	1	1			1	1	1	
43	https://doi.org/10.1016/j.jum.2022.09.003.						1			
50	https://doi.org/10.1016/j.jnca.2019.06.001.							1		1
61	https://doi.org/10.1016/j.comnet.2018.08.001.									
66	https://doi.org/10.1016/j.envsci.2022.01.010.						1		1	
72	https://doi.org/10.1016/j.scs.2021.102940.									1
73	https://doi.org/10.1016/j.physa.2018.09.130.									1
77	https://doi.org/10.1016/j.future.2019.09.004.									1

Tabla 3. Tabla 3. Resultados de la clasificación de lecturas seleccionadas (Fuente: elaboración propia)

Del análisis de las lecturas clasificadas pueden deducirse primeros resultados:

- Sobre las cuestiones primera, tercera y quinta, se aprecia que son temas recurrentes.
- Para la segunda cuestión, la relativa al uso de modelos de fiabilidad para la resiliencia, no se dispone de lecturas más o menos dedicadas con las que profundizar en el análisis, en apariencia.
- En cuanto a la cuarta cuestión, relativa al gemelo digital, la red inteligente y la industria 4.0, y la resiliencia, tampoco lecturas más o menos dedicadas con las que profundizar en el análisis.

Los principios de la resiliencia de flexibilidad y tolerancia no han sido identificados lo que podría deberse a que están infrarrepresentadas en el modelo conceptual que ha dirigido la búsqueda. Por esta razón y con objeto de profundizar en el análisis con todas las lecturas, y a la vista de que hay temas que podrían quedar sin analizar si no se profundiza en la lectura, se propone el uso de alertas textuales para todas las cuestiones de interés. Hecho esto, se dispone de los siguientes resultados recogidos en la Tabla 3:

Lectura seleccionada		Q1	Q2	Q3		Q4.1	
ID	doi	Q1.1	Q2.1	Q3.1	Q3.2	Q4.1	Q4.2
1	https://doi.org/10.1016/j.est.2022.104825.						
3	https://doi.org/10.1016/j.compeleceng.2022.107830.	x	x				
4	https://doi.org/10.1016/j.rser.2017.03.107.					x	x
5	https://doi.org/10.1016/j.epsr.2019.02.014.	x	x				
6	https://doi.org/10.1016/j.tej.2022.107135.						
14	https://doi.org/10.1016/j.ifacol.2022.09.013.						
18	https://doi.org/10.1016/j.ijepes.2021.106974.						
19	https://doi.org/10.1016/j.ress.2016.02.009.	x					
22	https://doi.org/10.1016/j.energy.2019.116442.						
25	https://doi.org/10.1016/j.scs.2021.103467.						
30	https://doi.org/10.1016/j.scs.2020.102412.					x	
34	https://doi.org/10.1016/j.scs.2020.102327.	x	x			x	
41	https://doi.org/10.1016/j.ijdrr.2022.102970.					x	x
43	https://doi.org/10.1016/j.jum.2022.09.003.					x	x
50	https://doi.org/10.1016/j.jnca.2019.06.001.	x					x
61	https://doi.org/10.1016/j.comnet.2018.08.001.					x	x
66	https://doi.org/10.1016/j.envsci.2022.01.010.						
72	https://doi.org/10.1016/j.scs.2021.102940.					x	
73	https://doi.org/10.1016/j.physa.2018.09.130.						
77	https://doi.org/10.1016/j.future.2019.09.004.		x			x	x

Tabla 4. Resultados del uso de alertas textuales (Fuente: elaboración propia)

A la vista de los resultados puede deducirse que el uso de modelos de fiabilidad no es exclusivo del ámbito de las redes inteligentes, como cabía esperar, del mismo modo que el uso de paradigmas y metodologías no lo es de la ciudad inteligente. Nótese que la detección de información sobre modelos de fiabilidad no hubiera sido

posible si el uso de alertas el análisis posterior de las mismas, lo que puede ser interpretado como una ineficacia del metadatado de publicaciones en ScienceDirect.

CONCLUSIONES

La gestión de riesgos y de la seguridad, y el uso de modelos de fiabilidad forman parte de la práctica de la ingeniería de resiliencia para las redes inteligentes y ciudades inteligentes.

La relación entre la Industria 4.0, las redes inteligentes y las ciudades inteligentes parece aún poco explorada. Ciertamente los principios de la Industria 4.0 pueden relacionarse con el uso de varias tecnologías habilitadoras que también se usan en las redes inteligentes y en la ciudad inteligente, pero este hecho podría no ser suficiente como para compartir un marco de gestión de la seguridad, sin embargo, la recurrencia en el estudio de la resiliencia en la ciudad inteligente es una oportunidad para reforzar el conocimiento para las redes inteligentes, y existen datos que corroboran esta tendencia.

En cuanto a la metodología empleada para la captura de tendencias, ésta ha demostrado ser capaz de aportar valor a cuestiones relevantes de la investigación si bien requiere ser realimentada para incrementar su eficacia.

PRÓXIMOS PASOS

Los modelos conceptuales pueden ser realimentados de una forma sistemática a través de la técnica de las alertas dado que sus textos aportan nuevos términos bien contextualizados. La ontología que recoge los modelos conceptuales puede publicarse en un lenguaje de formalización SKOS-RDF para la comunidad científico-técnica (W3C, 2009).

Se está en disposición de aplicar el método de análisis antes expuesto aplicado a las redes térmicas urbanas y de gases industriales en su posible uso de los principios de la resiliencia y en su relación con las redes inteligentes, para lo que será necesario elaborar nuevos modelos conceptuales de la resiliencia para esos SRs.

En todo el proceso de investigación se tiene en cuenta que *SES ENGINEERING Studio* ® interopera a su vez con herramientas como *Enterprise Architecture*®, conocidos PLM y múltiples herramientas de modelado, simulación, gestión de requisitos, constituyendo así la base habilitadora del Gemelo Digital de los sistemas o sistemas de sistemas según se trate a la que la ontología puede contribuir.

AGRADECIMIENTOS

Los autores desean agradecer a la empresa *The Reuse Company* la licencia de uso de sus herramientas para los fines de esta comunicación.

REFERENCIAS

- Álvarez, J. M. “Métodos semánticos de reutilización de datos abiertos enlazados en las licitaciones públicas” PhD Dissertation. Oviedo: Universidad de Oviedo, 2012
- CEN-CENELEC-ETSI. “Smart Grid Reference Architecture”, 2012
- INCOSE. Systems Engineering Handbook. 2015
- Larrañeta, J. Javier. “Reflexiones sobre una nueva gobernanza y gestión de riesgos para la seguridad”, 2022, <https://www.seguritecnia.es>
- Llorens, J., J. Morato and G. Génova. “RSHP: an information representation model based on relationships” Studies in Fuzziness and Soft Computing (2004)
- McKinsey & Company. “Digitalization for sustainable infrastructure: the road ahead”, Ledzioni, 2022
- MINETUR. “HADA - Herramienta de autodiagnóstico digital avanzada” 8 de 10 de 2022, <https://hada.industriaconectada40.gob.es/hada/auth/login>
- SEDIA. TDH, 8 de octubre de 2022. <https://portalayudas.mineco.gob.es/THD/Paginas/Index.aspx>
- SGAM-TOOLBOX 2.0, 08 de octubre de 2022. <https://sgam-toolbox.org/>
- W3C. SKOS. 18 8 2009. 18 de marzo de 2022. <http://www.w3.org/TR/skos-reference>