CONFERENCIA

Vulnerabilidad de infraestructuras críticas de energía interdependientes

JOSÉ MARÍA YUSTA LOYO

Dr. Ingeniero Industrial

Profesor Titular de Universidad

http://unizar.es / jmyusta

http://redcrit.unizar.es

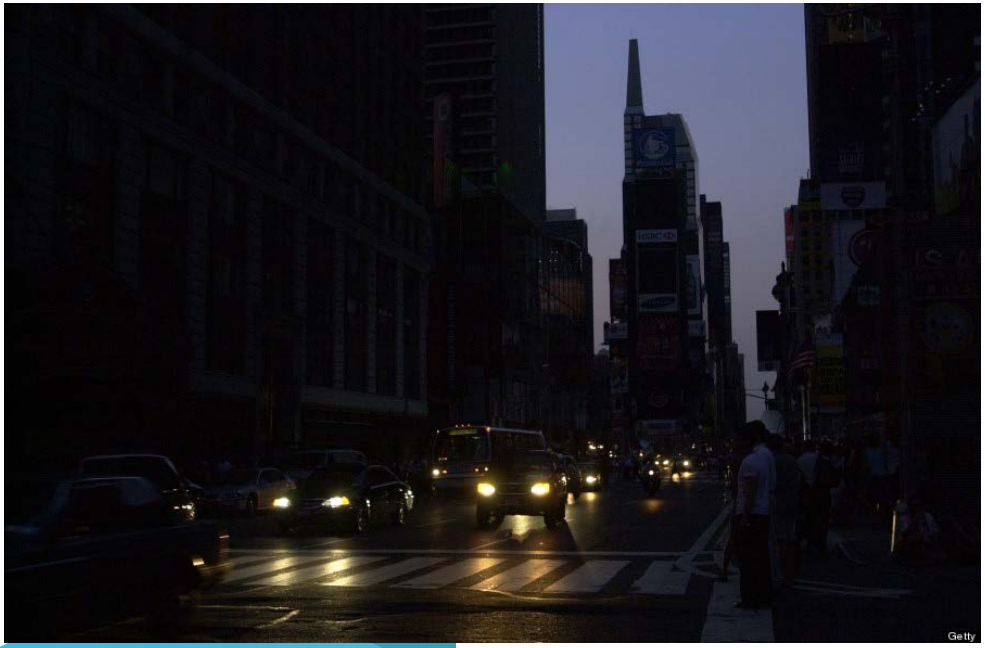
Universidad Zaragoza

XX SEMINARIO ECONOMIA Y DEFENSA, 2018

Zaragoza, España

14/8/2003

AP / Chad Rachman



Getty

28/9/2003

Blackout in Brazil

A widespread power outage Tuesday affected more than 60 million people in Brazil and Paraguay after transmission problems at a hydroelectric dam.

Area most affected by blackout

SOURCE: ESRI AP

10/11/2009

30/07/2012

Un fallo en la red eléctrica alemana causa un apagón en nueve países de Europa

UNA **FILIAL DE E.ON** PODRÍA HABER SIDO LA CAUSANTE DEL CORTE DE SUMINISTRO

Madrid, Cataluña, Valencia, Castilla La Mancha y Castilla y León sufrieron el apagón

Campo de torres elécticas en Stommeln, Alemania.FOTO: EFE

MADRID. Un fallo en la red de suministro eléctrico en Alemania, cuyo origen aún no ha sido determinado, provocó la madrugada del sábado un apagón generalizado, que afectó a unos diez millones de personas en nueve países europeos.

Una filial de la compañía eléctrica alemana E.ON admitió ayer la posibilidad de haber provocado los apagones eléctricos que afectaron a gran parte de Europa occidental, especialmente a Alemania, Francia y España. Según explicó la filial E.ON Netz, la presunta causa de estos apagones fue "una sobrecarga de la red en el norte y oeste de Alemania" que podría estar relacionada con unas operaciones llevadas a cabo por esta compañía.

4/11/2006

EL PAÍS

INTERNACIONAL

Irán sufre un ataque informático contra sus instalaciones nucleares

El potente virus Stuxnet afecta ya a unos 30.000 ordenadores en el país

ÁNGELES ESPINOSA

Teherán - 28 SEP 2010

Irán asegura que sus instalaciones nucleares están a salvo, pero ha reconocido que Stuxnet ha afectado al menos 30.000 ordenadores dentro de su territorio y continúa propagándose. Aunque el nombre suene a videojuego, se trata de algo mucho más peligroso: el primer *gusano* informático que ataca plantas industriales. Y haciendo realidad lo que hasta ahora pertenecía al mundo de la ciencia-ficción, algunos expertos advierten de su capacidad para hacer estallar la instalación infectada. "Es parte de la ciberguerra de Occidente contra Irán", ha denunciado Mahmud Liayí, un alto cargo del Ministerio de Industria.

2010

Iranian hackers infiltrated U.S. power grid, dam computers, reports say

Disturbing Calpine attack targeted company with plants in U.S. and Canada

The Associated Press Posted: Dec 22, 2015 11:12 AM ET | Last Updated: Dec 22, 2015 11:12 AM ET

About a dozen times in the last decade, sophisticated foreign hackers have gained enough remote access to control the operations networks that keep the lights on, according to top experts who spoke only on condition of anonymity due to the sensitive nature of the subject matter, the Associated Press found. (Colin Perkel/Canadian Press)

2015

certsi_
CERT DE SEGURIDAD E INDUSTRIA

Alerta Incidentes Servicios

Inicio / Alerta Temprana / Bitacora Ciberseguridad / Ciberataque contra una fábrica de acero alema

Ciberataque contra una fábrica de acero alemana causa "daños masivos"

17/12/2014

2014

La Oficina Federal para la Seguridad de la Información en Alemania ha informado sobre una ataque informático sufrido por una fábrica de acero alemana que causó daño físico masivo al sistema. Los atacantes utilizaron una técnica de spear-phishing para acceder a la red corporativa de la fábrica, para después acceder al sistema de control industrial de la misma. El ataque afectó a numerosos sistemas, incluso imposibilitando el apagado controlado del alto horno y causando un daño masivo a la infraestructura de la fábrica. El informe omite la identidad de la fábrica afectada o detalles adicionales.

Referencias:

17/12/2014bund.de	Die Lage der IT-Sicherheit in Deutschland 2014
19/12/2014pcworld.com	Cyberattack on German steel factory causes 'massi...
22/12/2014bbc.com	Hack attack causes 'massive damage' at steel work...
22/12/2014securityaffairs.co	Cyber attack on German steel factory caused sever...
08/01/2015wired.com	A Cyberattack Has Caused Confirmed Physical Da...

Etiquetas: Cibercrimen Incidente Sistema de Control Industrial

ATAQUES INFORMÁTICOS ›

Los ciberataques a infraestructuras estratégicas se multiplican por siete en solo dos años

Detectadas casi mil ofensivas contra los operadores de estas instalaciones desde 2014

J. J. GÁLVEZ
Periodista

León - 29 MAY 2017 - 01:17 CEST

Los ciberataques a las infraestructuras extracríticas de España —centrales eléctricas y nucleares, plantas de agua, aeropuertos y hospitales, entre otras— no paran de aumentar. A un ritmo mayor del previsto por el Gobierno. Según los datos del Instituto Nacional de Ciberseguridad (Incibe), las ofensivas a través de la red contra los operadores de estas instalaciones se han multiplicado por siete en solo dos años. Han pasado de 63 en 2014, a 134 en 2015 y a 479 en 2016. Y, además, en el primer cuatrimestre de 2017 se han registrado 247, por lo que de seguir así se superarán los 700 incidentes este ejercicio y se batirá otro récord.

incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD

2017

BLACK ENERGY

UN TROYANO EN SISTEMAS CRÍTICOS

BLACKENERGY ES UN TROYANO ALTAMENTE SOFISTICADO, MODULAR Y CON MÚLTIPLES FUNCIONALIDADES ENTRE ELLAS EL CIBERESPIONAJE Y EL SABOTAJE INDUSTRIAL.

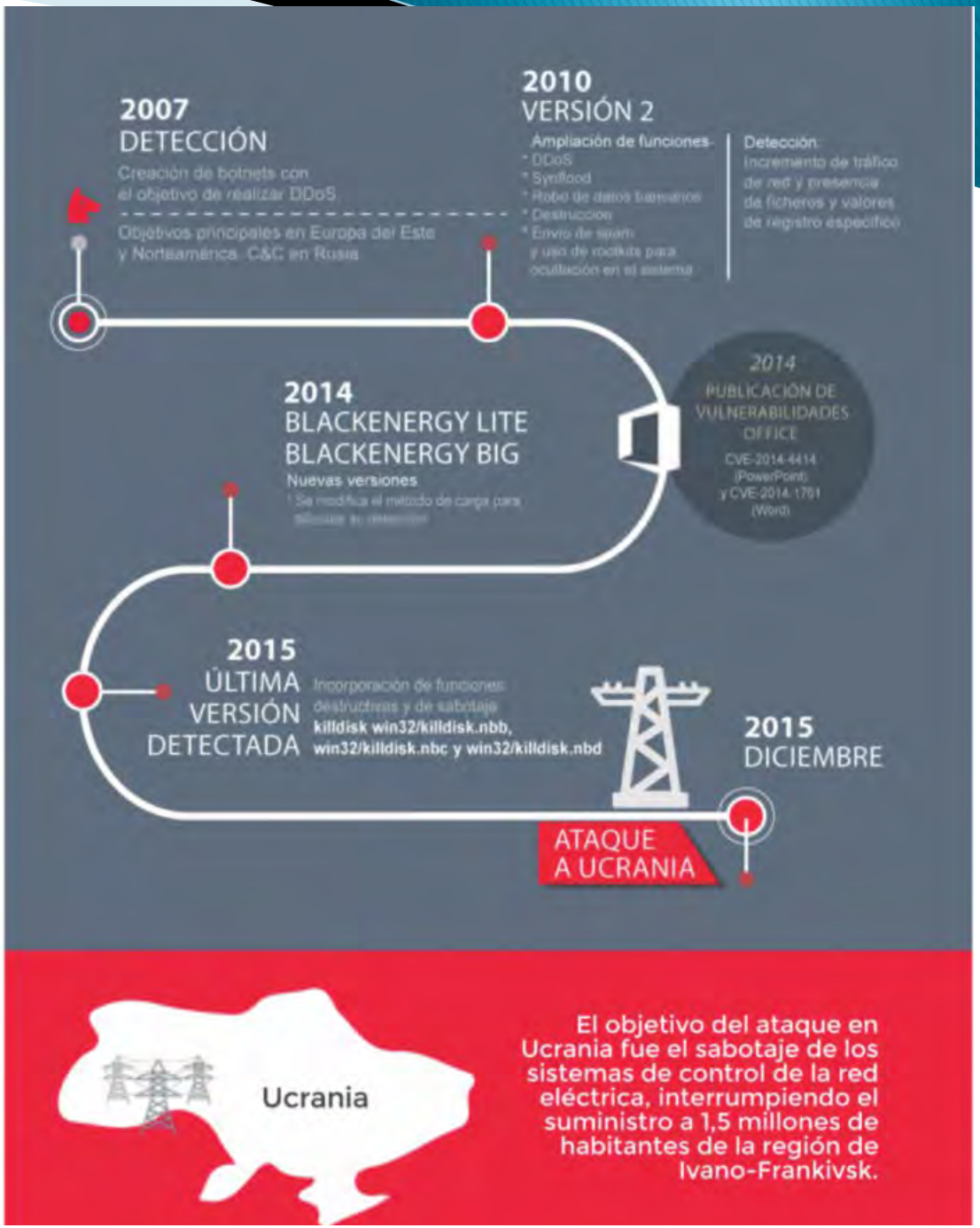
EVOLUCIÓN

Desde su aparición en 2007 como simple troyano para crear botnets utilizadas en DDoS, Blackenergy ha evolucionado hasta adoptar un sofisticado diseño modular que incorpora un rootkit y avanzadas funcionalidades para posibilitar ataques de spam, fraude bancario y ataques dirigidos. En 2015 demostró capacidad de APT para infectar sistemas SCADA con un ataque a una central eléctrica en Ucrania.

BLACK ENERGY

UN TROYANO EN SISTEMAS CRÍTICOS

2015



Official website of the Department of Homeland Security

ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

HOME | ABOUT | ICSJWG | INFORMATION PRODUCTS | TRAINING | FAQ

Control Systems

- Home
- Calendar
- ICSJWG
- Information Products
- Training
- Recommended Practices
- Assessments
- Standards & References
- Related Sites
- FAQ

Alert (IR-ALERT-H-16-056-01)

More Alerts

Cyber-Attack Against Ukrainian Critical Infrastructure

Original release date: February 25, 2016

Print | Tweet | Send | Share

Legal Notice

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

SUMMARY

On December 23, 2015, Ukrainian power companies experienced unscheduled power outages impacting a large number of customers in Ukraine. In addition, there have also been reports of malware found in Ukrainian companies in a variety of critical infrastructure sectors. Public reports indicate that the BlackEnergy (BE) malware was discovered on the

CIBERTERRORISMO

El gran apagón

17/01/2016 - 00:00 Por Carlos Manuel Sánchez - XL Semanal

El sistema eléctrico está en peligro. La digitalización de las redes tiene grandes ventajas, pero ha creado también nuevas debilidades. Militares, ingenieros y otros expertos advierten: la posibilidad de un gran ataque ciberterrorista es muy real. Y abre la puerta a un escenario apocalíptico. ¿Estamos preparados?

La preocupación no es exclusiva de Estados Unidos. En España, el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), del Ministerio del Interior, gestionó en 2015 al menos 63 ataques de alto nivel contra operadores esenciales de transporte, gas, petróleo, electricidad, agua, industria química, nuclear, alimentación, banca... El mapa del riesgo español tiene 93 operadores de infraestructuras críticas. El 80 por ciento son empresas privadas.

«El incidente más importante fue una delicada amenaza de seguridad en el sector energético que, de haberse producido, podría haber afectado a un servicio esencial consumido en miles de hogares y empresas». El CNPIC también ha reforzado la atención en el transporte, después del caos ferroviario producido por un sabotaje en la línea del AVE que paralizó 40 trenes y afectó a 13.000 pasajeros en octubre, a pesar de que no fuera un ataque informático, sino físico, pues los asaltantes cortaron los cables de fibra óptica que comunican al maquinista con el centro de control. En todo caso, no fue un robo, pues el valor de la fibra era despreciable.

2015


CIBERSEGURIDAD
La red eléctrica israelí sufre un ciberataque masivo que deja inoperativos sus sistemas
by MONICA VALLE on ENERO 28, 2016
1 COMMENT

2016

certsi_

CERT DE SEGURIDAD E INDUSTRIA

Alerta Incidentes Servicios

Inicio / Alerta Temprana / Bitacora Ciberseguridad / Ransomware afecta distribución eléctrica er

Ransomware afecta distribución eléctrica en Israel

25/01/2016

Un ransomware, distribuido a través de una campaña de phising, logró colarse en la infraestructura de la Electricity Authority de Israel. La infección se detectó el lunes 25 de enero, día en el que para atajarla tuvieron que desconectar partes de la red eléctrica del país. No se han identificado responsables de este ciberataque.

Referencias:

27/01/2016 arstechnica.com/	Israel's electric authority hit by "severe" hack attack...
27/01/2016 ics.sans.org	Context for the Claim of a Cyber Attack on the Isra...
27/01/2016 news.softpedia.com/	Israel's Power Grid Hit with Ransomware

Etiquetas: Malware Infraestructuras Críticas

2016

CNPIC
CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD

El sector energético sufre uno de cada tres ciberataques informáticos en el mundo

CONCHA RASO | 10:57 - 27/10/2016 | 0 Comentarios

Fuente: http://www.eleconomista.es/tecnologia/noticias/7919421/10/16/El-sector-sufre-el-35-de-los-ataques-informaticos.html

COLOMBIA

Ejército frustra atentado del Eln contra torres eléctricas en Antioquia

El Ejército frustró un nuevo atentado terrorista del Eln contra dos torres de la interconexión eléctrica San Carlos-Cer una zona rural del departamento de Antioquia, informaron fuentes militares.

Por EFE

Viernes 12 de enero de 2018, a las 11:48

AUMENTA ATENTADOS CONTRA INFRAESTRUCTURA ELÉCTRICA

Nacional 16.02.2018

Grave crisis eléctrica en región Caribe por atentados del Eln

La guerrilla destruyó dos torres de interconexión y averió otras dos, por lo que fue necesario poner las térmicas a toda marcha.

entsoe

Network Codes Data Outlooks Regions

[Press Release] Continuing frequency deviation in the Continental European Power System originating in Serbia/Kosovo: Political solution urgently needed in addition to technical.

Mar 6, 2018 -

The Continental European (CE) Power System -a large synchronized area stretching from Spain to Turkey and from Poland to Netherlands; encompassing 25 countries- is experiencing a continuous system frequency deviation from the mean value of 50 Hz, and this since mid of January 2018.

The power deviations are originating from the control area called Serbia, Macedonia, Montenegro (SMM block) and specifically Kosovo and Serbia.

The power deviations have led to a slight decrease in the electric frequency average.

This average frequency deviation, that has never happened in any similar way in the CE Power system, must cease. The missing energy amounts currently to 113 GWh. The question of who will compensate for this loss has to be answered.

The decrease in frequency average is affecting also those electric clocks that are steered by the frequency of the power system and not by a quartz crystal: they show currently a delay of close to six minutes.

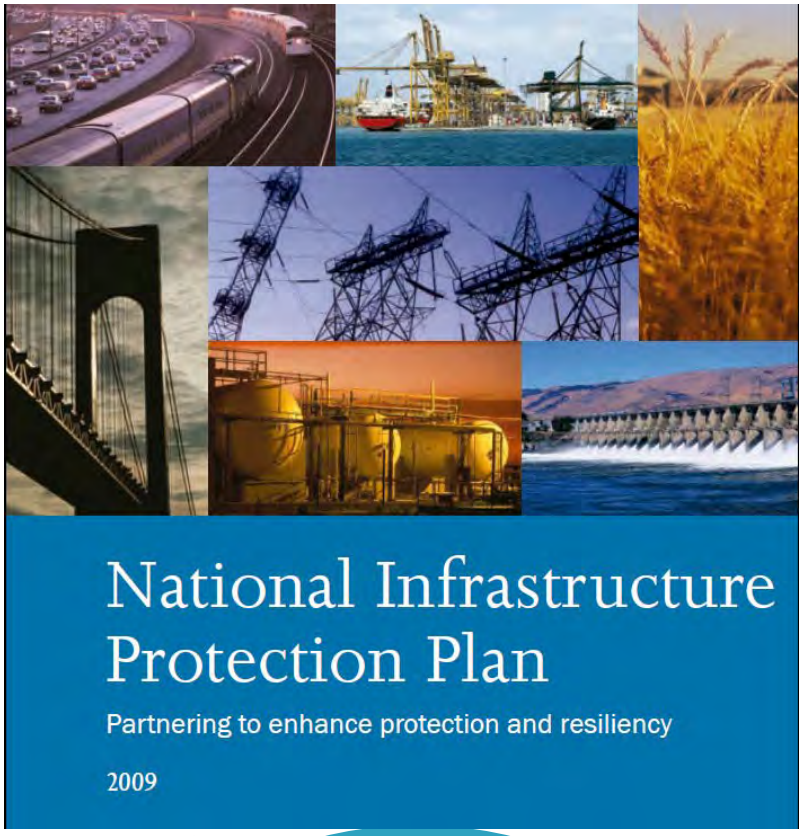
ENTSO-E, the association of the European TSOs, is exploring all technical options to address the deviation issue with the concerned TSOs.

23.12.2008 ES Diario Oficial de la Unión Europea

DIRECTIVA 2008/114/CE DEL CONSEJO

de 8 de diciembre de 2008

sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección



GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
SECRETARÍA DE ESTADO PARA LA SOCIEDAD DE LA INFORMACIÓN Y LA AGENDA DIGITAL

Ministerio de Energía, Turismo y Agenda Digital

Inicio | El Ministerio | Energía | Sociedad de la Información y Agenda Digital | Turismo |

Estás en: **Sociedad de la Información y Agenda Digital** > **Participación Pública** > Audiencia pública del Anteproyectro de L...

SOCIEDAD DE LA INFORMACIÓN Y AGENDA DIGITAL

- Secretaría de Estado
- Jefaturas Provinciales de Inspección de las Telecomunicaciones
- Servicios
- Procedimientos en la Sede
- Legislación

Participación Pública

Volver

AUDIENCIA PÚBLICA DEL ANTEPROYECTRO DE LEY SOBRE LA SEGURIDAD DE LAS REDES Y SISTEMAS DE INFORMACIÓN

De acuerdo con el artículo 26.6 de la Ley 50/1997, de 27 de noviembre, del gobierno, se sustancia la audiencia pública del anteproyecto de Ley sobre la seguridad de las redes y sistemas de información. Esta ley transpone al Ordenamiento jurídico español la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

CNPIC

CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD

.: CNPIC Index :.

www.cnpic-es.es/index.html

CNPIC

CENTRO NACIONAL PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

MENÚ

- Inicio
- Presentación
- Preguntas Frecuentes
- Legislación Aplicable
- Enlaces Nacionales
- Internacional
- Ciberseguridad
- Eventos
- Archivo
- Contacto

CNPIC - Inicio

El Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) es el órgano que se encarga de impulsar, coordinar y supervisar todas las actividades que tiene encomendadas la Secretaría de Estado de Seguridad del Ministerio del Interior en relación con la protección de las infraestructuras críticas españolas.

Nuestro objetivo principal es impulsar y coordinar los mecanismos necesarios para garantizar la seguridad de las infraestructuras que proporcionan los servicios esenciales a nuestra sociedad, fomentando para ello la participación de todos y cada uno de los agentes del sistema en sus correspondientes ámbitos competenciales. Mediante la integración de todos estos esfuerzos, se pretende fomentar un modelo de seguridad basado en la confianza mutua, creando una asociación público-privada que permita minimizar las vulnerabilidades de las infraestructuras críticas ubicadas en el territorio nacional.

Legislación Española

- Ley 8/2011 por la que se establecen medidas para la Protección de las Infraestructuras Críticas
- R.D. 704/2011 por la que se aprueba el Reglamento para la Protección de las Infraestructuras Críticas
- Acuerdo Consejo de Ministros sobre Protección de Infraestructuras Críticas
- Ley de Seguridad Nacional
- Estrategia de Seguridad Energética Nacional
- Estrategia de Seguridad Nacional
- Estrategia de Ciberseguridad Nacional
- Estrategia de Seguridad Marítima Nacional
- Ley de Seguridad Privada
- Ley 17/2015 del Sistema Nacional de Protección Civil.
- R.D. 407/1992 Norma Básica de Protección Civil
- R.D. 393/2007 Norma Básica de Autoprotección de Centros y Establecimientos
- R.D. 1468/2008 que modifica R.D. 393/2007
- R.D. 399/2007 Protocolo Intervención Unidad Militar Emergencia
- Contenidos mínimos PSO
- Contenidos mínimos PPE
- Guía de Buenas Prácticas para la elaboración de los Contenidos Mínimos de los Planes de Seguridad del Operador
- Guía de Buenas Prácticas para la elaboración de los Contenidos Mínimos de los Planes de Protección Específicos

CNPIC
CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD

MENÚ

- Inicio
- Presentación
- Preguntas Frecuentes
- Legislación Aplicable
- Enlaces Nacionales
- Internacional
- Ciberseguridad
- Eventos
- Archivo
- Contacto

CNPIC - Inicio

El Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC) es el **órgano responsable del impulso, coordinación y supervisión de todas las políticas y actividades relacionadas con la protección de las infraestructuras críticas españolas y con la ciberseguridad en el seno del Ministerio del Interior**. El CNPIC depende del **Secretario de Estado de Seguridad**, máximo responsable del Sistema Nacional de Protección de las Infraestructuras Críticas y de las políticas de ciberseguridad del Ministerio.

El CNPIC fue creado en el año 2007, mediante **Acuerdo de Consejo de Ministros de 2 de noviembre**, siendo sus competencias reguladas por la **Ley 8/2011**, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y por el **Real Decreto 704/2011**, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

Panel II: Ciberseguridad en las infraestructuras críticas: protegiéndonos en el ciberespacio

5º Congreso de Protección de Infraestructuras Críticas y Servicios Esenciales

Ciberseguridad, un pilar fundamental para la Protección de Infraestructuras Críticas y Esenciales de nuestro país

21/12/2017 - E.G/ B.V/ D.M/ J.S. Fotos:Mar Sáez

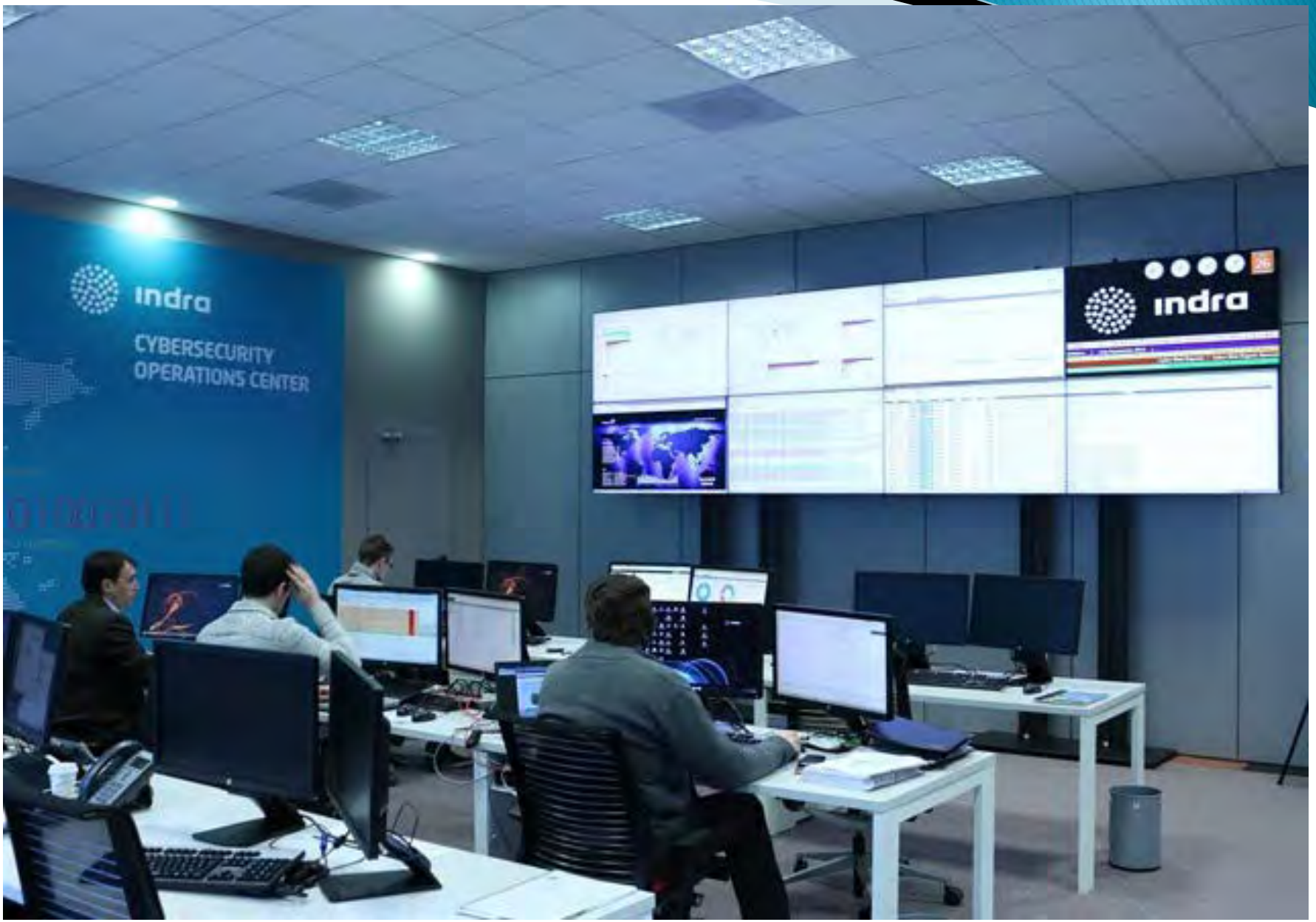
Luis Jiménez (CCN), Enrique Cabeiro (Mando Conjunto de Ciberdefensa), José Valiente (CCI), Alberto Hernández (Incibe) y Miguel Ángel Abad (OCC).


CURSO SUPERIOR UNIVERSITARIO PICE
PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS Y ESTRATÉGICAS
CERTIFICA:
Universidad Rey Juan Carlos


Curso de Especialización
Gestión de la Seguridad Integral en Infraestructuras Críticas y Estratégicas
GET
Grupo Estudios Técnicos
UNIVA
Diseñado para la Especialización y diferenciación de Directores de Seguridad


CURSO SUPERIOR EN PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS
2ª EDICIÓN
Dirigido a: Directores y Jefes de Seguridad, Delegados de Seguridad, Criminólogos, miembros de las FFCCSS y las FAS, alumnos de enseñanzas relativas a la seguridad.
IHS
DIRECCIÓN ACADÉMICA: FACULTAD DE DERECHO DE LA UNIVERSIDAD DE GRANADA
DIRECCIÓN TÉCNICA: CENTRO ANDALUZ DE ESTUDIOS Y ENTRENAMIENTO
COLABORA: INSTITUTO HISPANOAMERICANO DE SEGURIDAD
RED AZUL
POLICIA NACIONAL
PROGRAMA COOPERA
COMUNICACIÓN OPERATIVA
GUARDIA CIVIL - SEGURIDAD-PRIVADA
CONSEJERÍA DE JUSTICIA E INTERIOR
Dirección General de Interior, Emergencias y Protección Civil
ANDS
S.XXI


FUNDACIÓN BORREDÁ
El modelo de Protección de Infraestructuras Críticas en España
GUÍA PIC
II edición
CNPIC


indra
CYBERSECURITY
OPERATIONS CENTER
indra

GESTIÓN ESTRATÉGICA DE LA ENERGÍA ELÉCTRICA

Universidad Zaragoza

1542

- ***Threats to security of spanish energetic supply***. Inteligencia y Seguridad: Revista de Análisis y Prospectiva, nº 6, Plaza y Valdés, **2009**, Pags. 223-252
- ***Methodologies and applications for critical infrastructure protection***. Energy Policy 39 (**2011**) 6100–6119
- ***Using Interconnected Risk Maps to Assess the Threats Faced by Electricity Infrastructures.*** International Journal of Critical Infrastructure Protection 6 (**2013**) 197–216
- ***Grid Vulnerability Analysis Based on Scale-Free Graphs versus Power Flow Models***. Electric Power Systems Research 101 (**2013**) 71-79.
- ***Structural Vulnerability in Transmission Systems: Cases of Colombia and Spain***. Energy Conversion and Management 77 (**2014**) 408-418
- ***Nuevas técnicas para el análisis de la vulnerabilidad de infraestructuras energéticas ante ataques deliberados***. II Congreso Nacional de I+D en Defensa y Seguridad, DESEi+d (**2014**)
- ***Representation of electric power systems by complex networks with applications to risk vulnerability assessment.*** DYNA 82 (192) (**2015**) 68-77
- ***Vulnerability Assessment of a Large Electrical Grid by New Graph Theory Approach***, IEEE Latin America Transactions 16, 2 (**2018**) 527-535

SEGURIDAD ENERGETICA

- **DEFINICIÓN clásica:**
  Suficiente cantidad de energía a precio asequible.

- **DEFINICIÓN moderna:**
  Estabilidad de los precios, diversificación de fuentes, economía de las inversiones, seguridad de las infraestructuras, reservas y almacenamiento, eficiencia energética, mercados, sostenibilidad.

EN PLENA OLA DE FRÍO

Putin aprueba el corte total del suministro de gas ruso a Europa a través de Ucrania

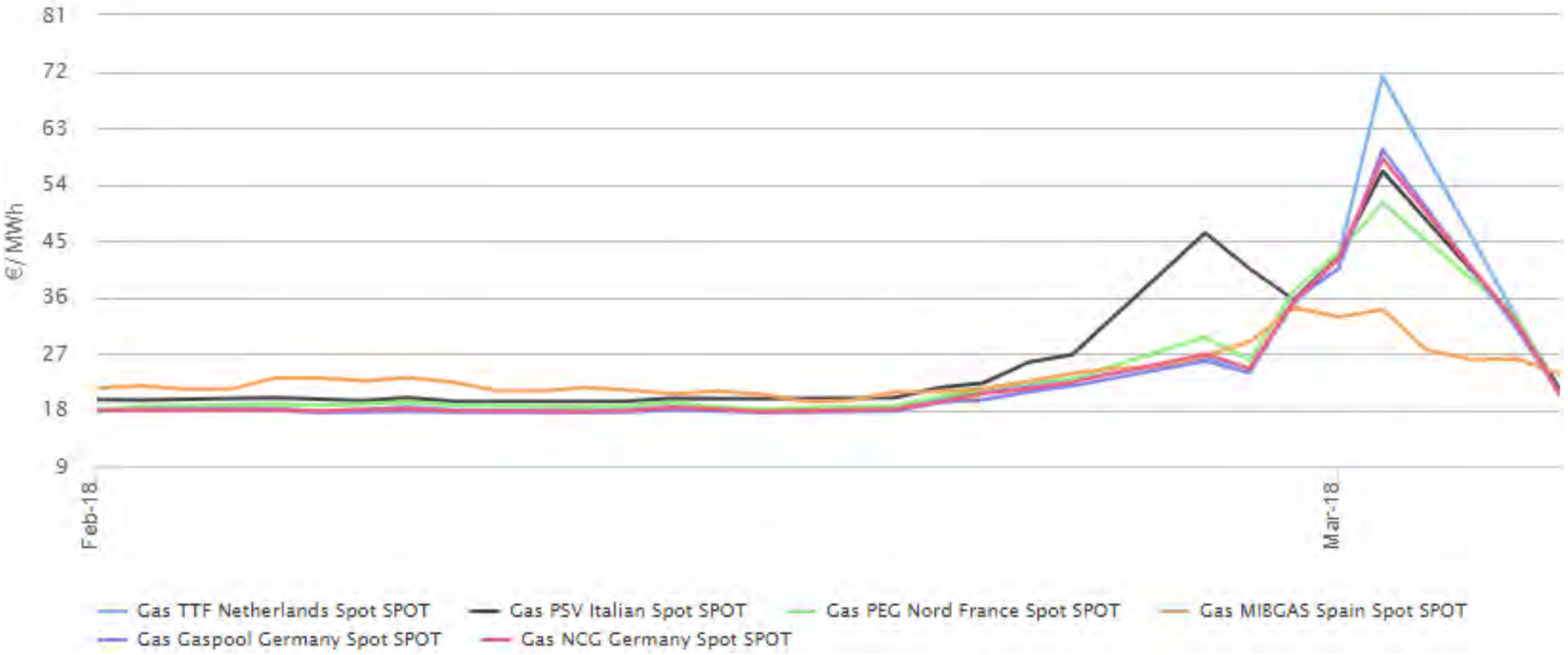
- Al menos 16 países sufren este conflicto, desde Croacia a Francia
- Pocas reservas en Bulgaria, República Checa, Hungría y Rumanía, entre otros
- Ucrania y Rusia se siguen acusando mutuamente de la crisis

Actualizado miércoles 07/01/2009 14:43

07/01/2009

Friday, Mar 2, 2018
- Gas TTF Netherlands Spot SPOT: **71,17**
- Gas Gaspool Germany Spot SPOT: **59,49**
- Gas NCG Germany Spot SPOT: **58,06**
- Gas PSV Italian Spot SPOT: **56,05**
- Gas PEG Nord France Spot SPOT: **50,99**
- Gas MIBGAS Spain Spot SPOT: **33,94**

02/03/2018



Source: M-Tech

Fecha: 19/02/2018

OFERTA DE SUMINISTRO GAS NATURAL 2018 – 2019

Opción 1… PRECIO FIJO :

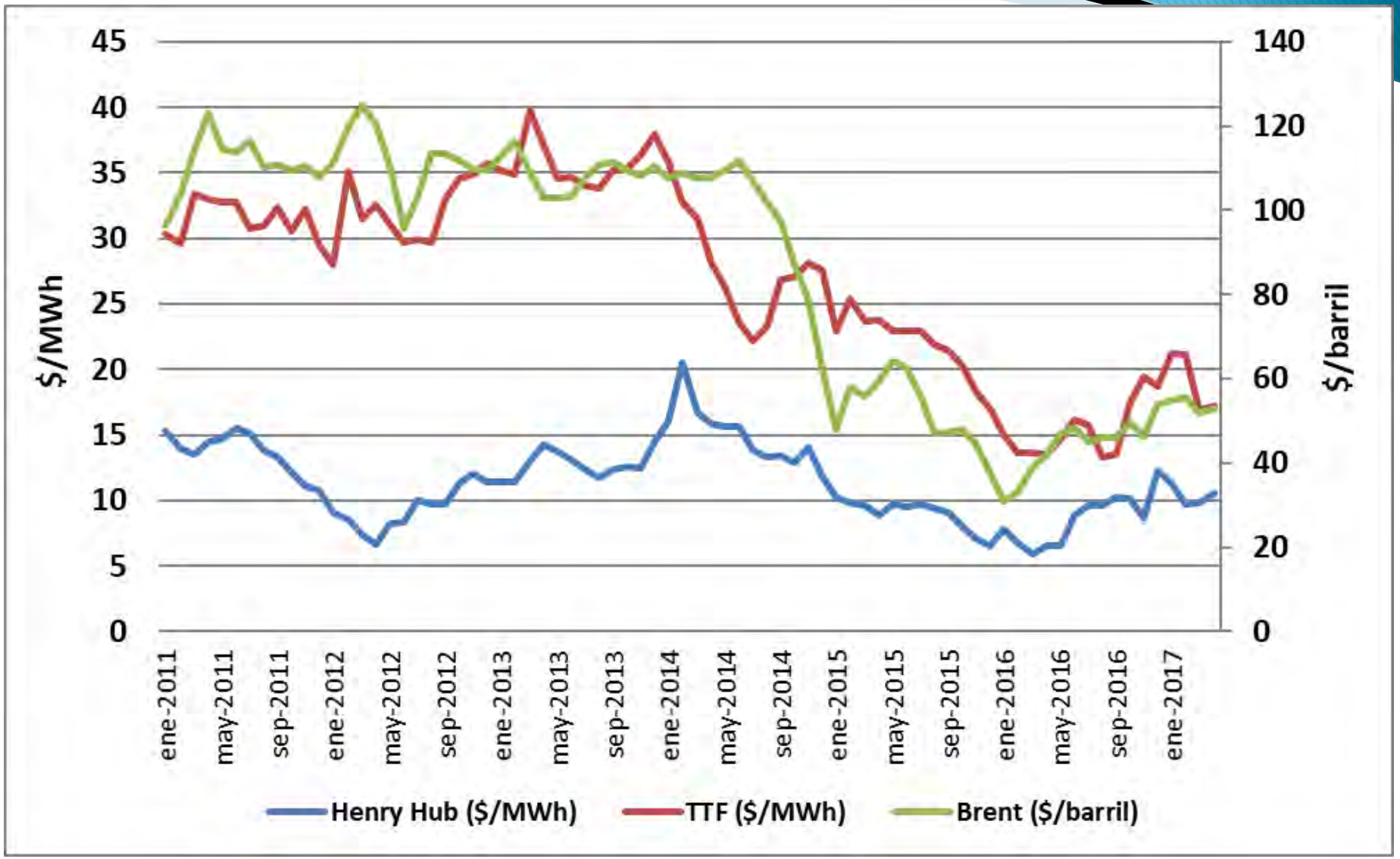
(18,99 + **V6**) = €/MWh

Opción 2…. FORMULA BRENT:

(8% Dated Brent603 + 3,2) / FX101 * 100 / 293,071 + **V6** - 0,34 = cent€/kWh

Opcion 3……FORMULA TTF DA:

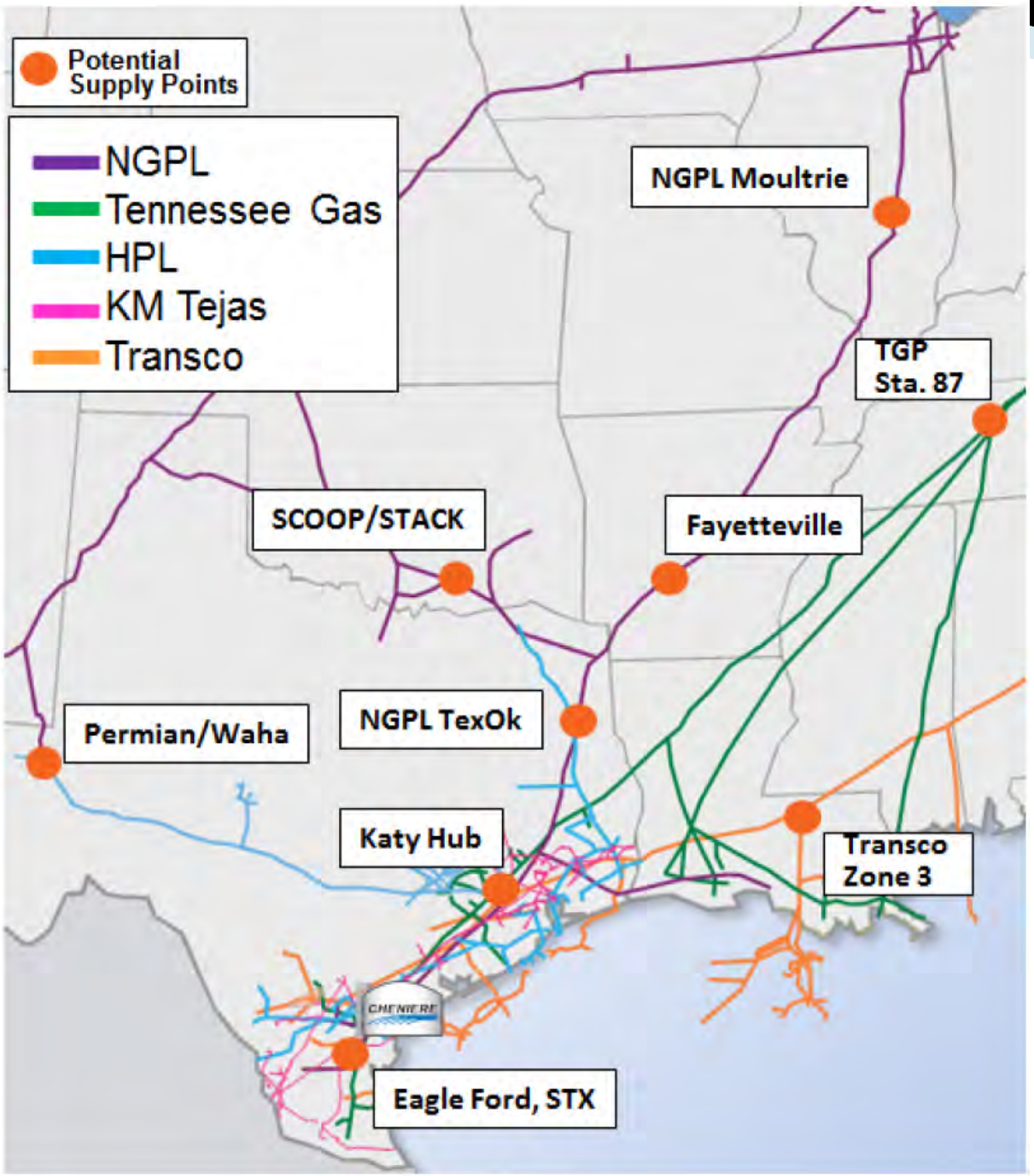
TTF Heren DA + 1,09 + **V6** = euros/MWh

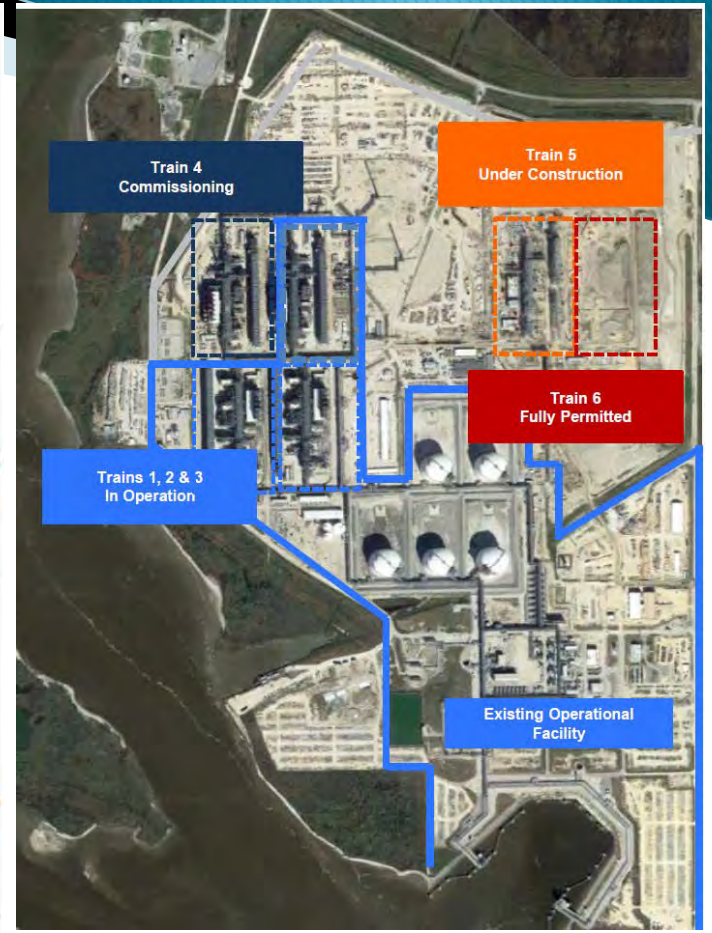

45
40
35
30
25
20
15
10
5
0
$/MWh
140
120
100
80
60
40
20
0
$/barril
ene-2011
may-2011
sep-2011
ene-2012
may-2012
sep-2012
ene-2013
may-2013
sep-2013
ene-2014
may-2014
sep-2014
ene-2015
may-2015
sep-2015
ene-2016
may-2016
sep-2016
ene-2017
Henry Hub ($/MWh)
TTF ($/MWh)
Brent ($/barril)

Cheniere LNG Cargo Destinations

More than 100 Cargoes (~400 TBtu) Exported and Delivered to 20 Countries Across the Globe

Note: As of April 30, 2017.





Sabine Pass Liquefaction Project (SPL)

Corpus Christi LNG Terminal

Corpus Christi Liquefaction SPAs

SPA progress: ~8.42 mtpa "take-or-pay" style commercial agreements
~$1.5B annual fixed fee revenue for 20 years

	PT Pertamina (Persero)	Endesa S.A.	Iberdrola S.A.	Gas Natural Fenosa	Woodside Energy Trading	Électricité de France	EDP Energias de Portugal S.A.
Annual Contract Quantity (TBtu)	79.36	117.32	39.68	78.20	44.12	40.00	40.00
Annual Fixed Fees [1]	~$278 MM	~$411 MM	~$139 MM	~$274 MM	~$154 MM	~$140 MM	~$140 MM
Fixed Fees $/MMBtu [1]	$3.50	$3.50	$3.50	$3.50	$3.50	$3.50	$3.50
LNG Cost	115% of HH	115% of HH	115% of HH	115% of HH	115% of HH	115% of HH	115% of HH
Term of Contract [2]	20 years	20 years	20 years	20 years	20 years	20 years	20 years
Guarantor	N/A	N/A	N/A	Gas Natural SDG, S.A.	Woodside Petroleum, LTD	N/A	N/A
Guarantor/Corporate Credit Rating [3]	BBB-/Baa3/BBB-	BBB/WR/BBB+	BBB+/Baa1/BBB+	BBB/Baa2/BBB+	BBB+/Baa1/BBB+	A-/A3/A-	BB+/Baa3/BBB-
Contract Start	Train 1 / Train2	Train 1	Train 1 / Train 2	Train 2	Train 2	Train 2	Train 3

ESTRATEGIA DE SEGURIDAD ENERGÉTICA NACIONAL

ESTRATEGIA DE SEGURIDAD ENERGÉTICA NACIONAL

CAPÍTULO 1

CAPÍTULO 2

ESTRATEGIA DE

SEGURIDAD ENERGÉTICA NACIONAL

CAPÍTULO 3

DESAFÍOS A LA SEGURIDAD ENERGÉTICA NACIONAL 25

CAPÍTULO 4

OBJETIVOS Y LÍNEAS DE ACCIÓN ESTRATÉGICAS 34

ESTRATEGIA DE SEGURIDAD ENERGÉTICA NACIONAL

ESTRATEGIA DE
SEGURIDAD
ENERGÉTICA
NACIONAL

RIESGOS Y AMENAZAS

▪ Actualización insuficiente e inversiones inadecuadas en infraestructuras	Económicos
▪ Volatilidad de los precios de suministro de la energía	
▪ Actividades fraudulentas en el sector energético	
▪ Inestabilidad política en los países productores	Geoestratégicos
▪ Optimización de la diversificación de los recursos energéticos	
▪ Amenazas a los países y rutas de aprovisionamiento	
▪ Conflictos políticos entre países suministradores, consumidores y de tránsito	
▪ Insuficientes interconexiones energéticas	Técnicos
▪ Riesgos de la generación eléctrica nuclear	
▪ Accidentes industriales graves	
▪ Catástrofes naturales	Ambientales
▪ Ciberamenazas	Deliberados
▪ Amenazas físicas a las infraestructuras energéticas	

INFRAESTRUCTURAS CRITICAS

Según el USA Patriot Act de 2001: Las infraestructuras críticas están compuestas por aquellos sistemas y sus activos, ya sean físicos o virtuales, tan vitales para los Estados Unidos que la inhabilitación o la destrucción de estos sistemas y sus activos tienen un alto impacto en la seguridad económica nacional, en la salud pública, en la seguridad nacional, o cualquier combinación de éstas.

Según la Directiva 2008/114/CE de la Unión Europea: Las infraestructuras críticas se definen como todo elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones.

Artículo 2. *Definiciones.*

A los efectos de la presente Ley, se entenderá por:

a) Servicio esencial: el servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.

b) Sector estratégico: cada una de las áreas diferenciadas dentro de la actividad laboral, económica y productiva, que proporciona un servicio esencial o que garantiza el ejercicio de la autoridad del Estado o de la seguridad del país. Su categorización viene determinada en el anexo de esta norma.

c) Subsector estratégico: cada uno de los ámbitos en los que se dividen los distintos sectores estratégicos, conforme a la distribución que contenga, a propuesta de los Ministerios y organismos afectados, el documento técnico que se apruebe por el Centro Nacional de Protección de las Infraestructuras Críticas.

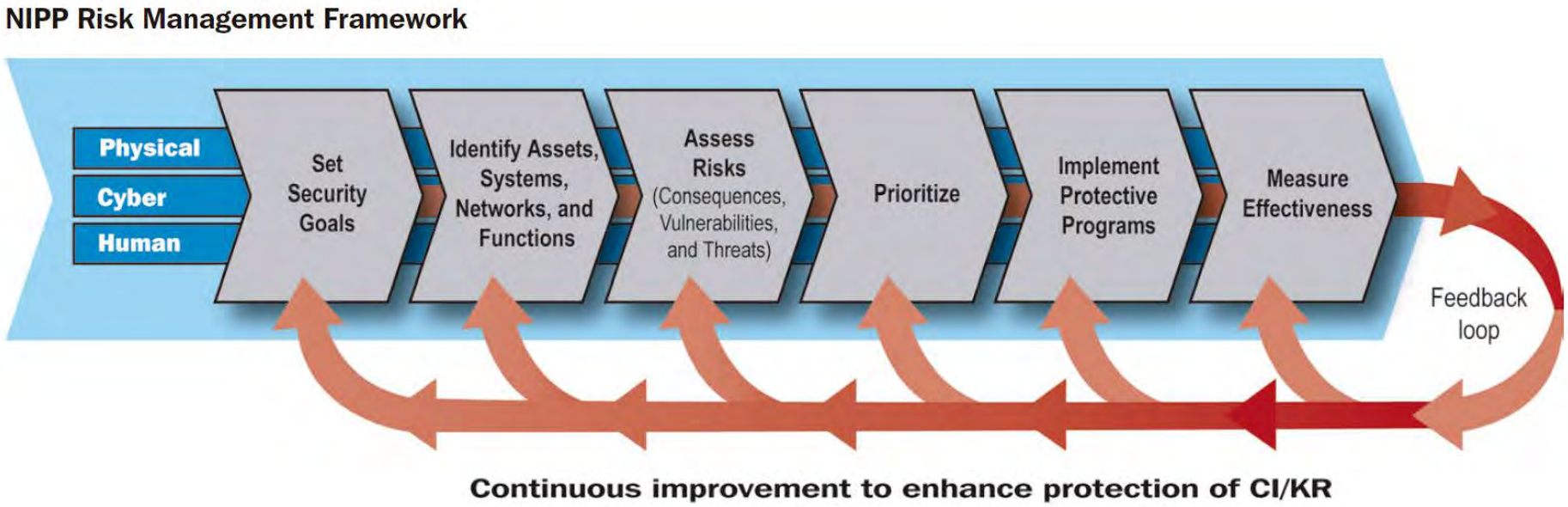
d) Infraestructuras estratégicas: las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales.

e) Infraestructuras críticas: las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

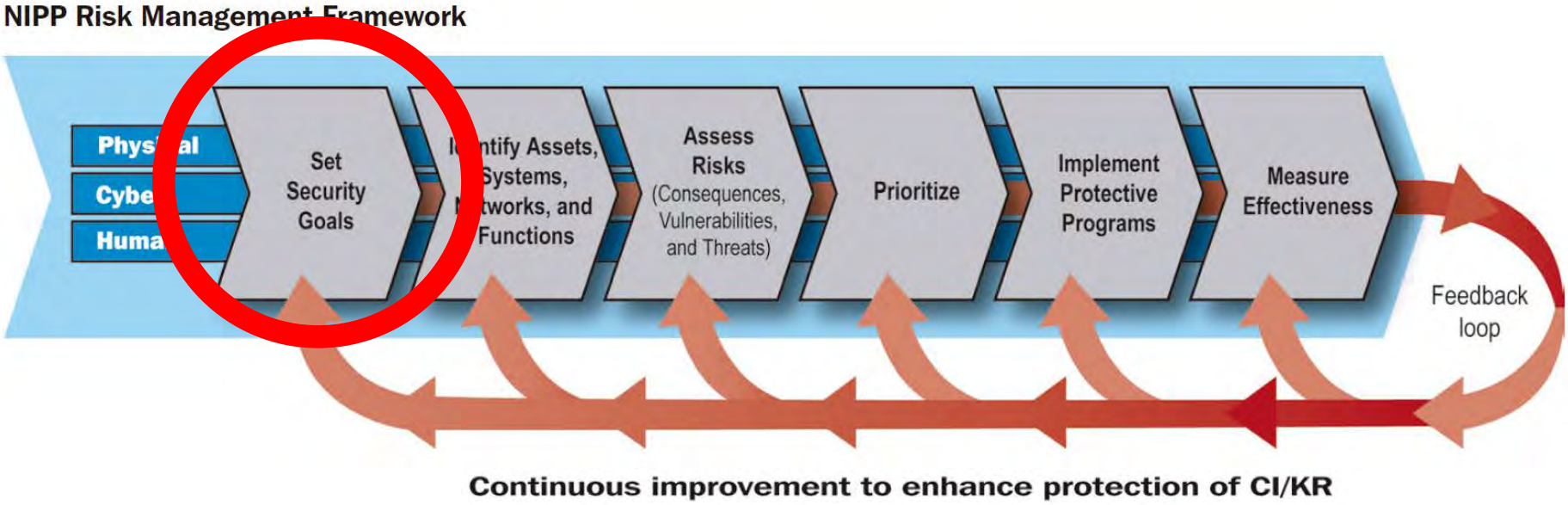
f) Infraestructuras críticas europeas: aquellas infraestructuras críticas situadas en algún Estado miembro de la Unión Europea, cuya perturbación o destrucción afectaría gravemente al menos a dos Estados miembros, todo ello con arreglo a la Directiva 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección (en adelante, Directiva 2008/114/CE).

Ley 8/2011

Un sistema de gestión de riesgos



Definir los objetivos



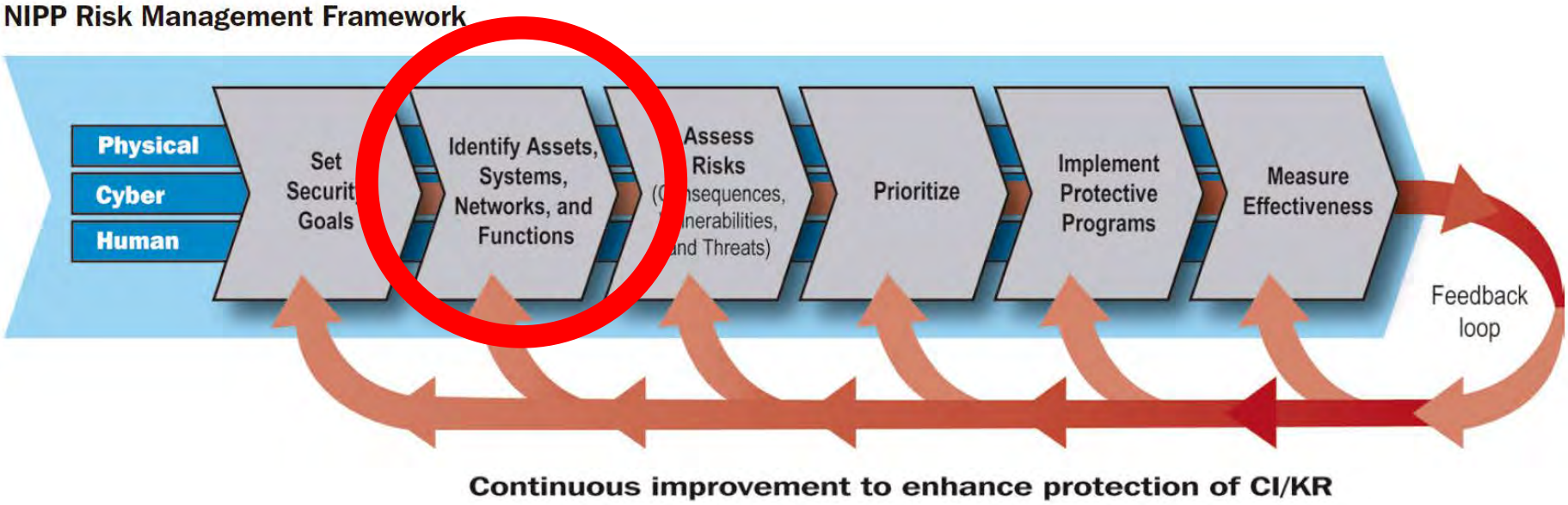
MACROSECTORS US NIPP	MACROSECTORS EU DIRECTIVE 114/08	
Agriculture and food	Energy	Electricity
Bank and finances		Oil
Communications		Natural gas
Military installations and defence	Transport	Roads and highways
Energy		Railroads
Technologies of information		Aviation
National monuments and icons		Inland waterways
Transportation systems		Shipping and ports
Drinking water treatment plants		

Sectores estratégicos y Ministerios/Organismos del sistema competentes

Sector	Ministerio/Organismo del sistema
Administración.	Ministerio Presidencia. Ministerio Interior. Ministerio Defensa. Centro Nacional de Inteligencia. Ministerio Política Territorial y Administración Pública.
Espacio.	Ministerio Defensa.
Industria nuclear.	Ministerio Industria, Turismo y Comercio. Consejo de Seguridad Nuclear.
Industria química.	Ministerio Interior.
Instalaciones de investigación.	Ministerio Ciencia e Innovación. Ministerio Medio Ambiente, y Medio Rural y Marino.
Agua.	Ministerio Medio Ambiente, y Medio Rural y Marino. Ministerio Sanidad, Política Social e Igualdad.
Energía.	Ministerio Industria, Turismo y Comercio.
Salud.	Ministerio Sanidad, Política Social e Igualdad. Ministerio Ciencia e Innovación.
Tecnologías de la Información y las Comunicaciones (TIC).	Ministerio Industria, Turismo y Comercio. Ministerio Defensa. Centro Nacional de Inteligencia. Ministerio Ciencia e Innovación. Ministerio Política Territorial y Administración Pública.
Transporte.	Ministerio Fomento.
Alimentación.	Ministerio Medio Ambiente, y Medio Rural y Marino. Ministerio Sanidad, Política Social e Igualdad. Ministerio Industria, Turismo y Comercio.
Sistema financiero y tributario.	Ministerio Economía y Hacienda.

Ley 8/2011

Identificar las amenazas

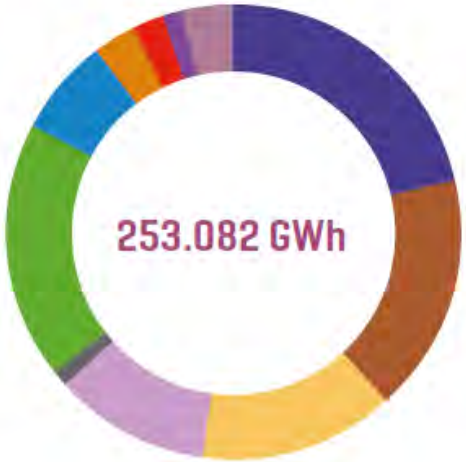



MAR CANTÁBRICO
OCEANO ATLÁNTICO
MAR MEDITERRÁNEO
ILHAS AÇORES
ILHAS DA MADEIRA
ISLAS CANARIAS
ISLAS BALEARES
ILLES BALEARS
SISTEMA ELÉCTRICO IBÉRICO
Enero - Janeiro 2014
LEYENDA - LEGENDA

COBERTURA DE LA DEMANDA ELÉCTRICA PENINSULAR AÑO 2017

%

Nuclear	21,5	Eólica	18,2
Carbón	17,0	Hidráulica (1)	7,0
Ciclo combinado	13,9	Solar fotovoltaica	3,1
Cogeneración	11,0	Solar térmica	2,1
Residuos	1,2	Otras renovables	1,4
		Saldo importador de intercambios internacionales	3,6



(1) No incluye la generación de bombeo.

INSTALACIONES DE LA RED DE TRANSPORTE DE ENERGÍA ELÉCTRICA EN ESPAÑA

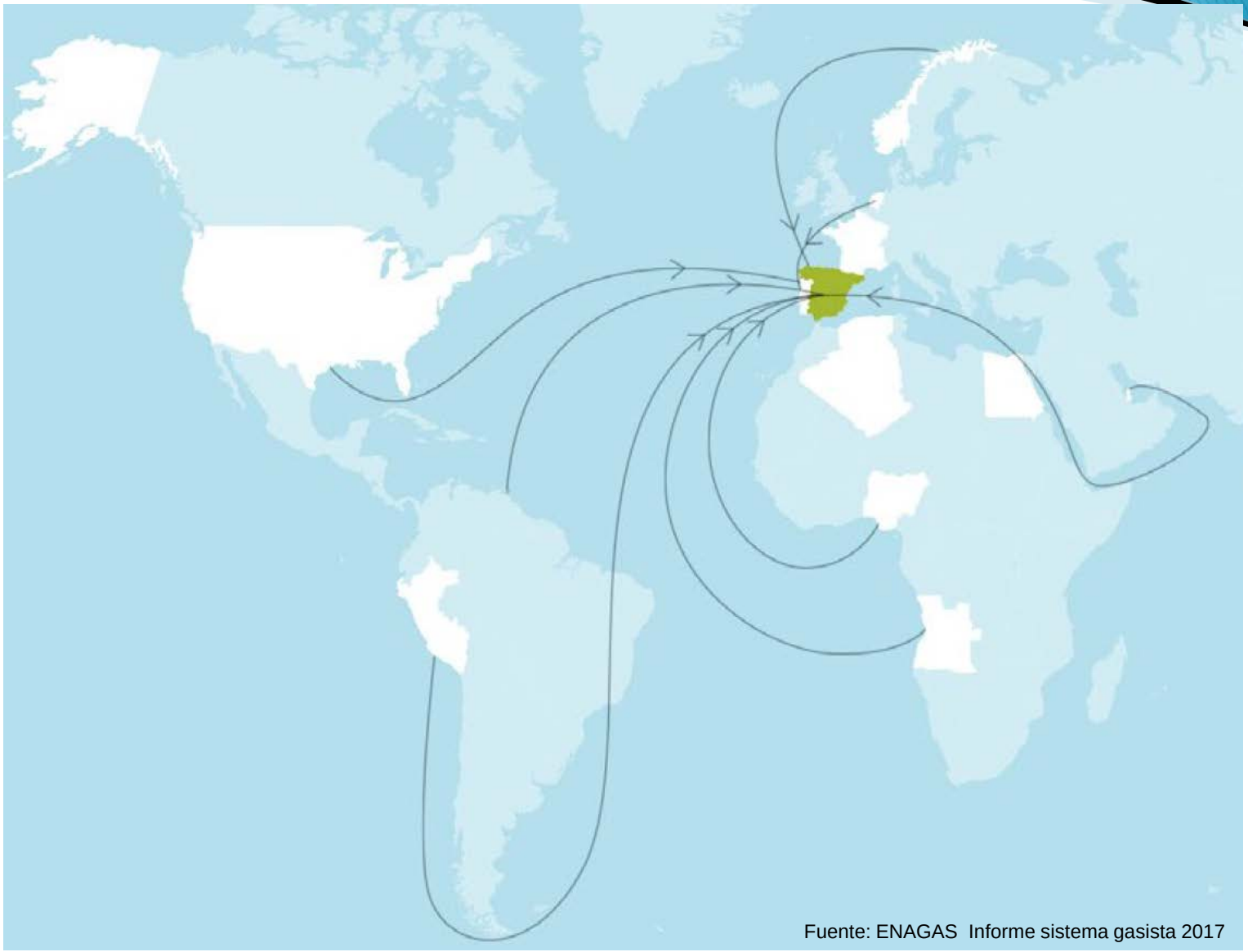
	400 kV	≤ 220 kV			
	Península	Península	Baleares	Canarias	TOTAL
Total líneas (km)	**21.729**	**19.040**	**1.808**	**1.422**	**43.998**
Líneas aéreas (km)	21.612	18.265	1.089	1.146	42.112
Cable submarino (km)	29	236	540	30	835
Cable subterráneo (km)	88	539	179	245	1.051
Transformación (MVA)	**80.208**	**613**	**3.273**	**2.560**	**86.654**

Fuente: REE Informe sistema eléctrico 2017

RED ELÉCTRICA DE ESPAÑA

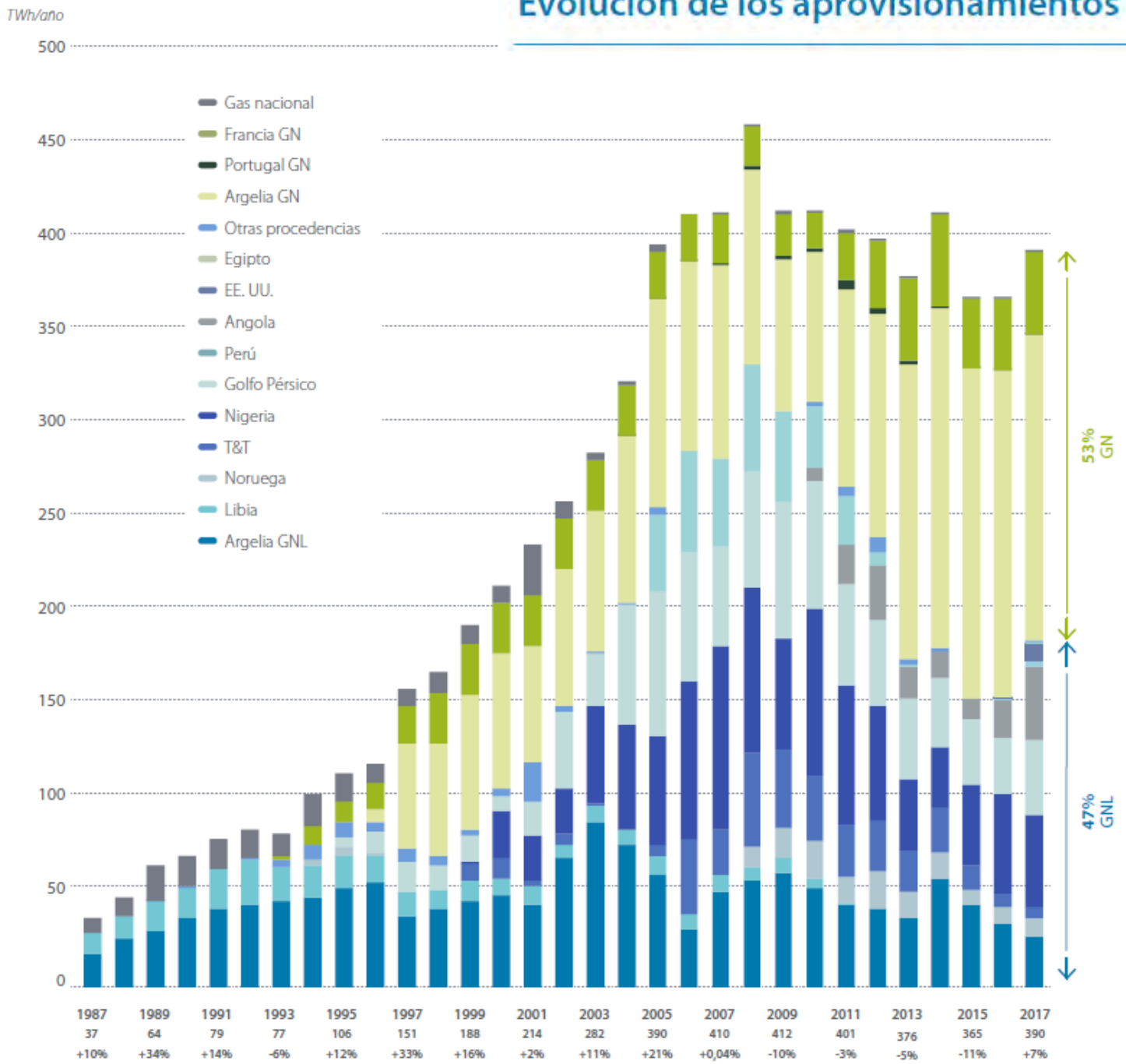
SISTEMA GASISTA ESPAÑOL

Origen de los suministros

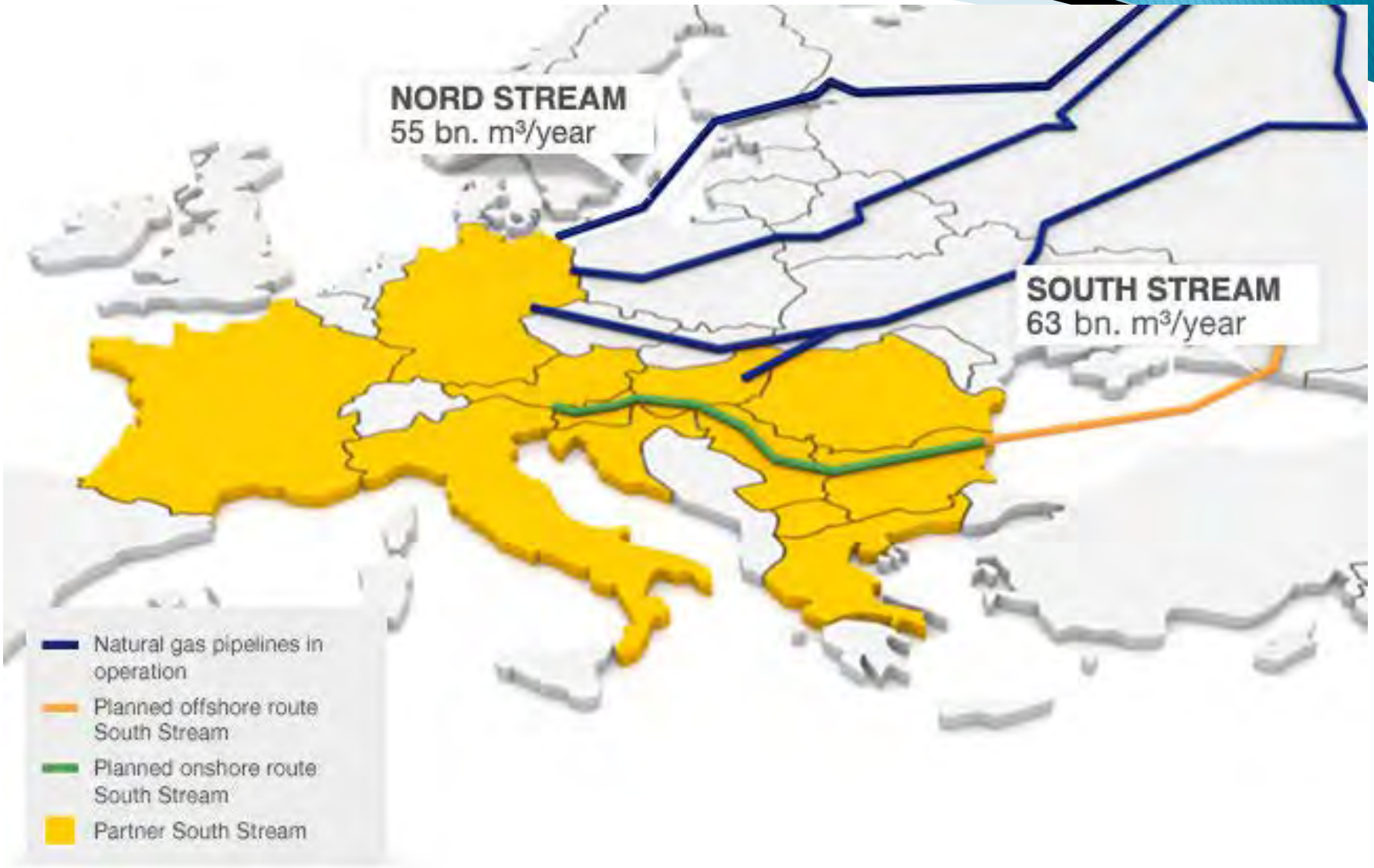


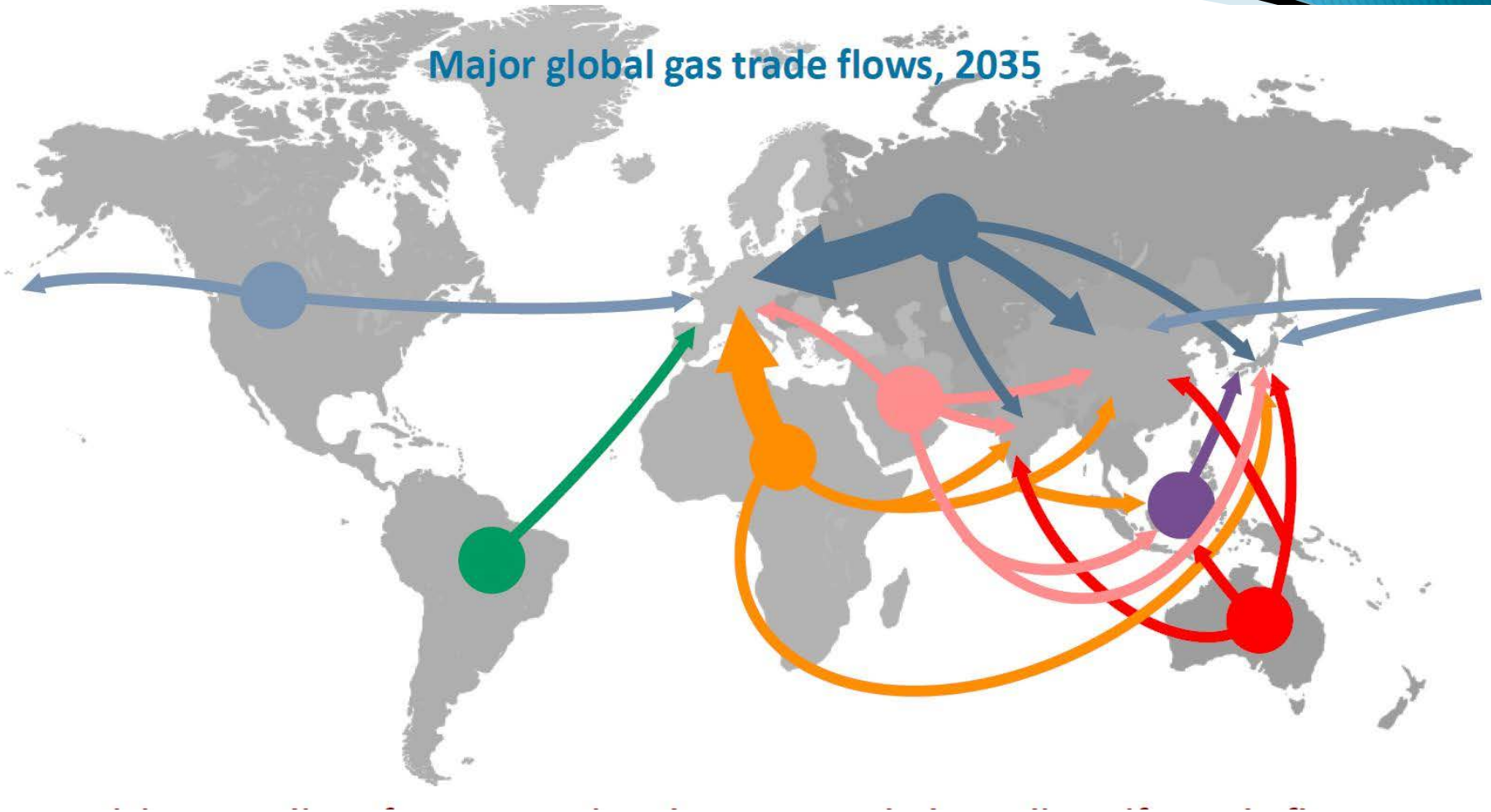
Fuente: ENAGAS Informe sistema gasista 2017

Evolución de los aprovisionamientos



Fuente: ENAGAS Informe sistema gasista 2017


NORD STREAM
55 bn. m³/year
SOUTH STREAM
63 bn. m³/year
Natural gas pipelines in operation
Planned offshore route South Stream
Planned onshore route South Stream
Partner South Stream


Major global gas trade flows, 2035

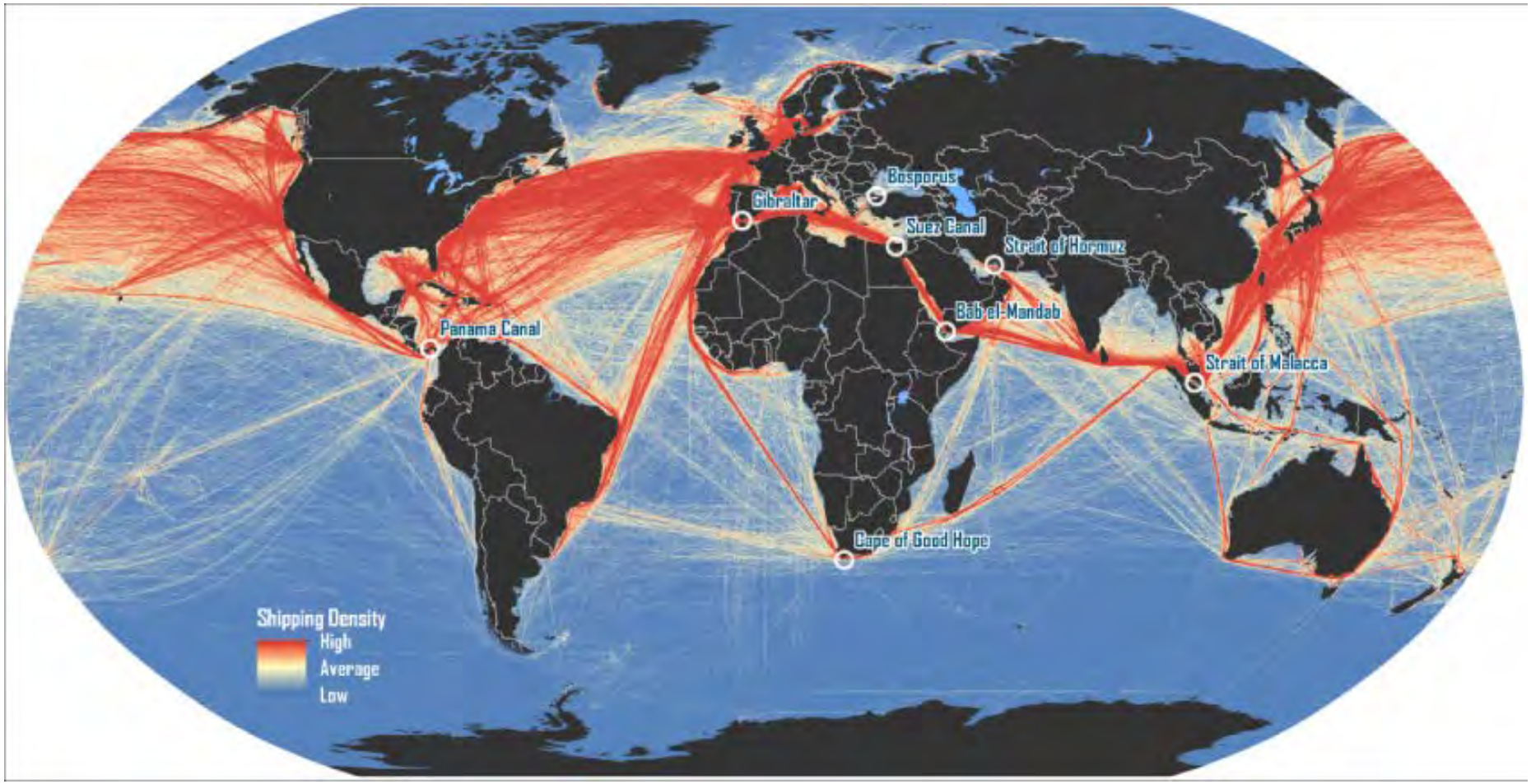

Bosporus
Gibraltar
Suez Canal
Strait of Hormuz
Bāb el-Mandab
Panama Canal
Strait of Malacca
Cape of Good Hope
Shipping Density
High
Average
Low

Table 2
Records of current national critical infrastructure plans.

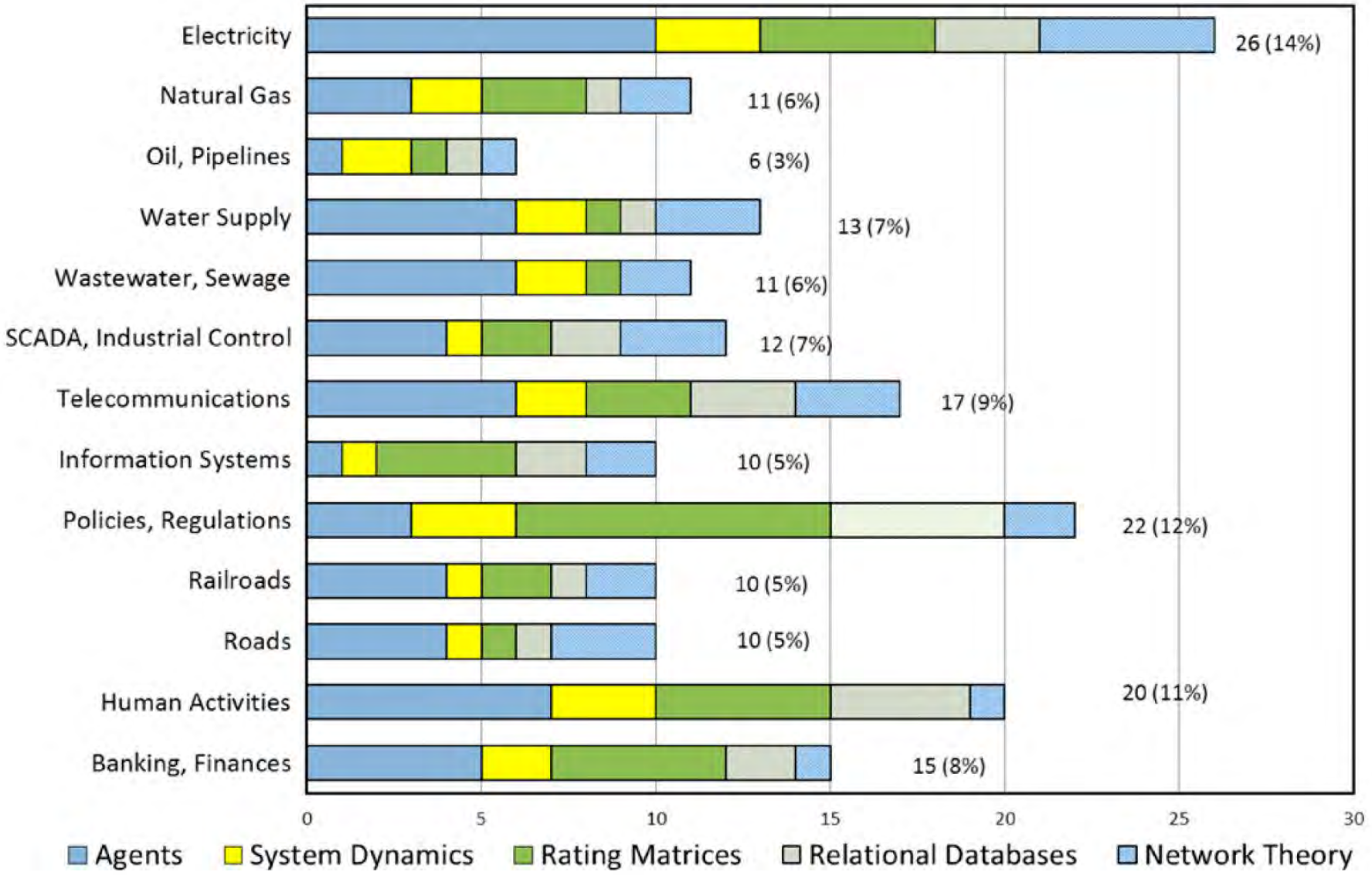
COUNTRY	PROGRAMM	PURPOSE	REFERENCES	AGENCY
Argentina	Cyberprotection	CERT/CSIRT methodology (Internet and telecommunications)	(ONTI, 2011)	Oficina Nacional de Tecnologías de Información
Australia	National Strategy for Critical Infrastructure Protection	Australia's ability to conduct national defence and homeland security	(Australian and CSIRO, 2008)	National Infrastructure Information
	Australian standard AS/NZS 4360:1999	Implementation of risk management techniques (Companies and systems)	(AS/NZS, 1999)	Public Services Companies
Brazil	Cyberprotection	CERT/CSIRT methodology (Internet and telecommunications)	(CERT.br, 2011)	Ministry of Defence
Canada	Strategy for the Protection of National Critical Infrastructure	Physical and cyber components, applied to both public and private sectors	(Abdur Rahman, 2009)	North American Electric Reliability Corporation (NERC)
	Canadian public safety agencies	Integration among federal organisations dealing with national security, emergency management, law enforcement, corrections, crime prevention and borders. respond to various security threats including terrorism, infectious diseases, natural disasters and cyber attacks	(Canadian, 2011)	Canadian Security Intelligence Service
China	Cyberprotection	CERT/CSIRT methodology (Internet and telecommunications)	(CNCERT/CC, 2011)	Computer emergency response teams within China
Colombia	Cyberprotection	CERT/CSIRT methodology (Internet and telecommunications)	(CERT-CCIT, 2011)	Ministry of Defence
France	White Paper on Defence and National Security	National infrastructure security challenges inside and outside France	(SGDSN, 2011)	Secrétariat General de la Défense Nationale
	Cyberprotection	CERT/CSIRT methodology (Internet and telecommunications)		Centre opérationnel de la sécurité des systèmes d'information & PIRANET Plan
Germany	Federal computer emergency response team (CERT-Bund)	CERT/CSIRT methodology (Internet and telecommunications)	(BSI, 2011)	Federal office for information security
Netherlands	National crisis centre	Support for risk assessment and safety advice, best practices and international contacts	(NAVI, 2011)	Nationaal Adviescentrum Vitale Infrastructuur
South Korea	Cyberprotection	CERT/CSIRT methodology (Internet and telecommunications)	(KrCERT/CC, 2011)	Korea Internet security center
Spain	Spanish national infrastructures protection plans	Coordination of activities of those involved in the protection of critical infrastructure, both in the public and the private sector	(BOE, 2011; CNPIC, 2010)	Centro Nacional de Protección de Infraestructuras Críticas
	Cyberprotection	CERT/CSIRT methodology (Internet and telecommunications)	(CCN-CERT, 2011)	Centro Nacional de Criptología
United Kingdom	Initiative for critical infrastructure sectors (communications, emergency services, energy, finance, food, government, healthcare, transportation and water)	Protection policies on sectors and resources and services that are critical at all levels of society	(CPNI, 2011)	Centre for the Protection of National Infrastructure

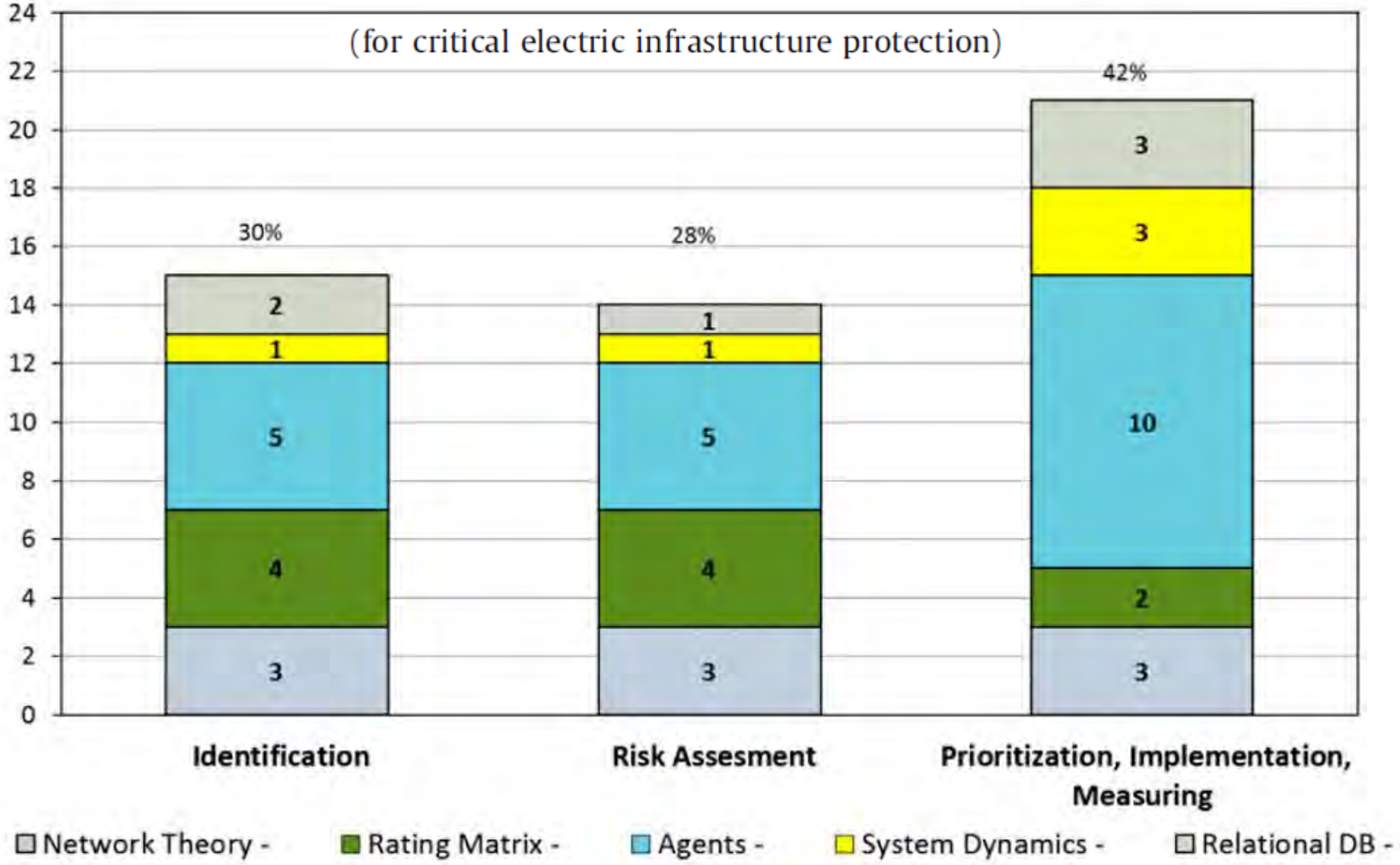
Table 3
Methodologies/applications for analysis of vulnerabilities in critical infrastructure.

APPLICATION/ METHODOLOGY	PUBLICATION	SOFTWARE	AVAILABILITY	INFRASTRUCTURE SECTOR												
				Electricity	Natural Gas	Oil, Pipelines	Drinking Water	Sewage, Wastewater	Industrial Control	Telecommunications	Computer Network, Information Systems	Railways	Highways, Roads	Human Activities	Banking, Finance	Policies, Regulations
AIMS	(Ghorbani and Marsh, 2004)	●	R					●								
Athena	(Drabble et al., 2009)	●	L	●	●	●	●	●	●	●	●	●	●	●	●	●
CASCADE	(Newman et al., 2005)	●	R	●												
CARVER2	(National Infrastructure Institute and Peimer, 2010)	●	C													
CEEESA	(Argonne Labs and Peerenboom, 2010)	●	L	●	●										●	
CERT/ CSIRT	(Alberts et al., 2004)		C											●	●	
CI[3]	(Argonne Labs et al., 2007)	●	L	●	●		●	●	●	●						
CIMS	(Idaho and Dudenhoeffer, 2006)	●	C	●					●					●		
CIP/DSS	(Argonne Labs et al., 2008a)	●	L	●	●	●	●	●	●	●		●	●	●	●	●
CIPMA	(Australian and CSIRO, 2008)	●	L	●	●	●				●	●				●	●
CISIA	(Panzieri et al., 2005)	●	R	●				●	●							
COMM-ASPEN	(Sandia Labs et al., 2004)	●	D	●						●					●	
DEW	(Broadwater, 2006)	●	L	●					●							
DUTCH NRA	(Pruyt and Wijnmalen, 2010)		L	●		●	●						●	●		●
EAR-PILAR	(Mañas, 2007)	●	C								●			●		●
ECI-GIS	(Peggion et al., 2008)	●	D											●	●	●
EMCAS	(Argonne Labs and Conzelmann, 2008)	●	C	●						●					●	
FAIT	(Sandia Labs and Brown, 2005a)	●	L	●	●			●				●				
FINSIM	(Los Alamos Labs and Flaim, 2006)	●	R							●					●	
FMEA/FMECA	(Milulak, 2004)		C						●	●				●	●	
Fort Future	(USACE et al., 2010)	●	L	●	●	●	●	●	●	●	●	●	●	●	●	●
FTA	(ISOGRAPH Inc, 2010)		C						●	●				●	●	
GAMS-CERO-ERA	(ERA, 2010; Pragma, 2010)		C											●	●	●
GIS Inter-operability	(Li et al., 2007)		R									●	●			
GoRAF	(Donzelli and Setola, 2007)	●	R	●			●		●					●		
CERT Initiatives	(CCN-CERT, 2011; CNPIC, 2010; Zielstra, 2010)		C						●		●			●		●
HAZOP	(ISOGRAPH Inc, 2008)		C	●	●	●			●	●				●		●
IEISS	(Los Alamos Labs et al., 2006)	●	L	●	●		●	●								●
IIM	(Quarles and Haimes, 2007)	●	R	●			●			●	●		●			●
Infrastructure Disruptions	(Beyeler and Brown, 2004)	●	R											●		●
IRAM	(Ezell and Wiese, 2000)	●	R				●	●								
IntePoint Vu	(IntePoint and Armstrong, 2010)	●	C	●						●		●	●	●		
Knowledge Management & Visualisation	(Dodrill et al., 2007)	●	R	●												●
LUND	(Johansson, 2010)		R	●								●	●			
MARGERIT V2	(CCN Criptología, 2010)		C								●			●	●	●
MIA	(ENEA et al., 2010)		R	●						●	●					●
MIN	(Pengcheng et al., 2005)	●	R										●	●		
Modular Dynamic Model	(Beyeler et al., 2002)	●	R	●												
MUNICIPAL	(Lee et al., 2005)	●	R	●						●	●					
N-ABLE	(Sandia Labs and Brown, 2005b)	●	L	●								●			●	
NEMO	(SPARTA Inc et al., 2005)	●	L	●	●		●					●				●

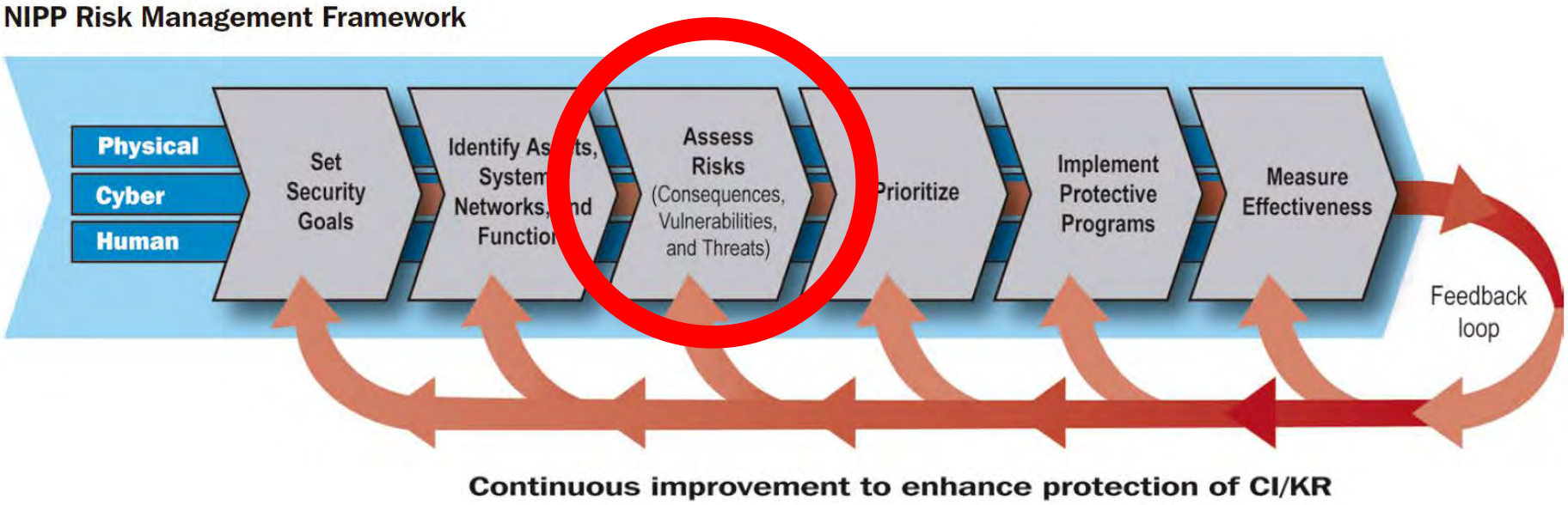
Of the 55 applications and platforms, 69% are software tools and 31% are analytical and generic methodologies. A first discussion is driven from the following perspectives:

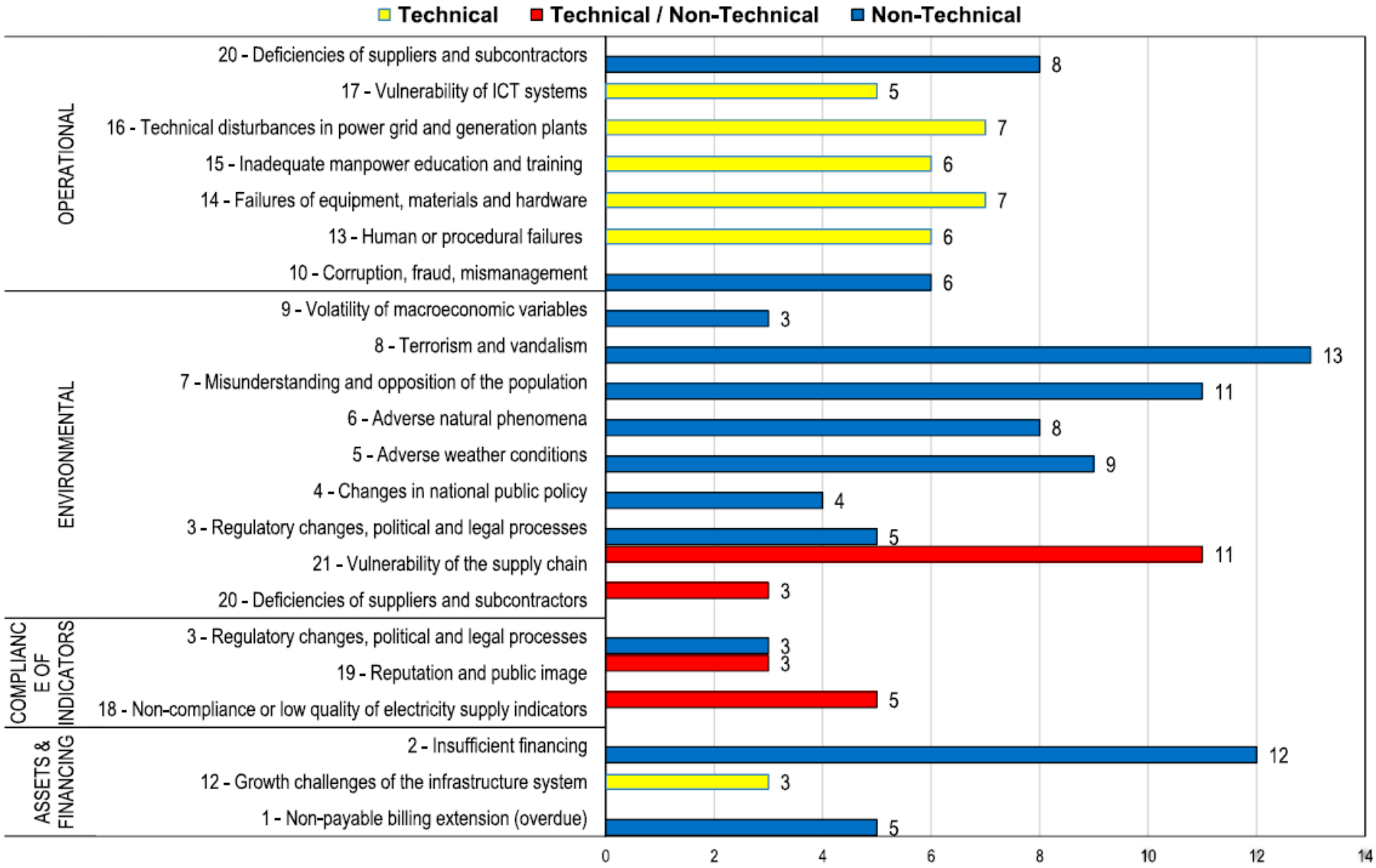
- Availability and maturity of applications.
- Combination of mathematical models and complimentary computational techniques that are currently used in research on critical infrastructure protection.
- Use of mathematical/computational models applied to the list of critical infrastructure sectors.
- Usage of modelling techniques in each stage of the risk management framework.

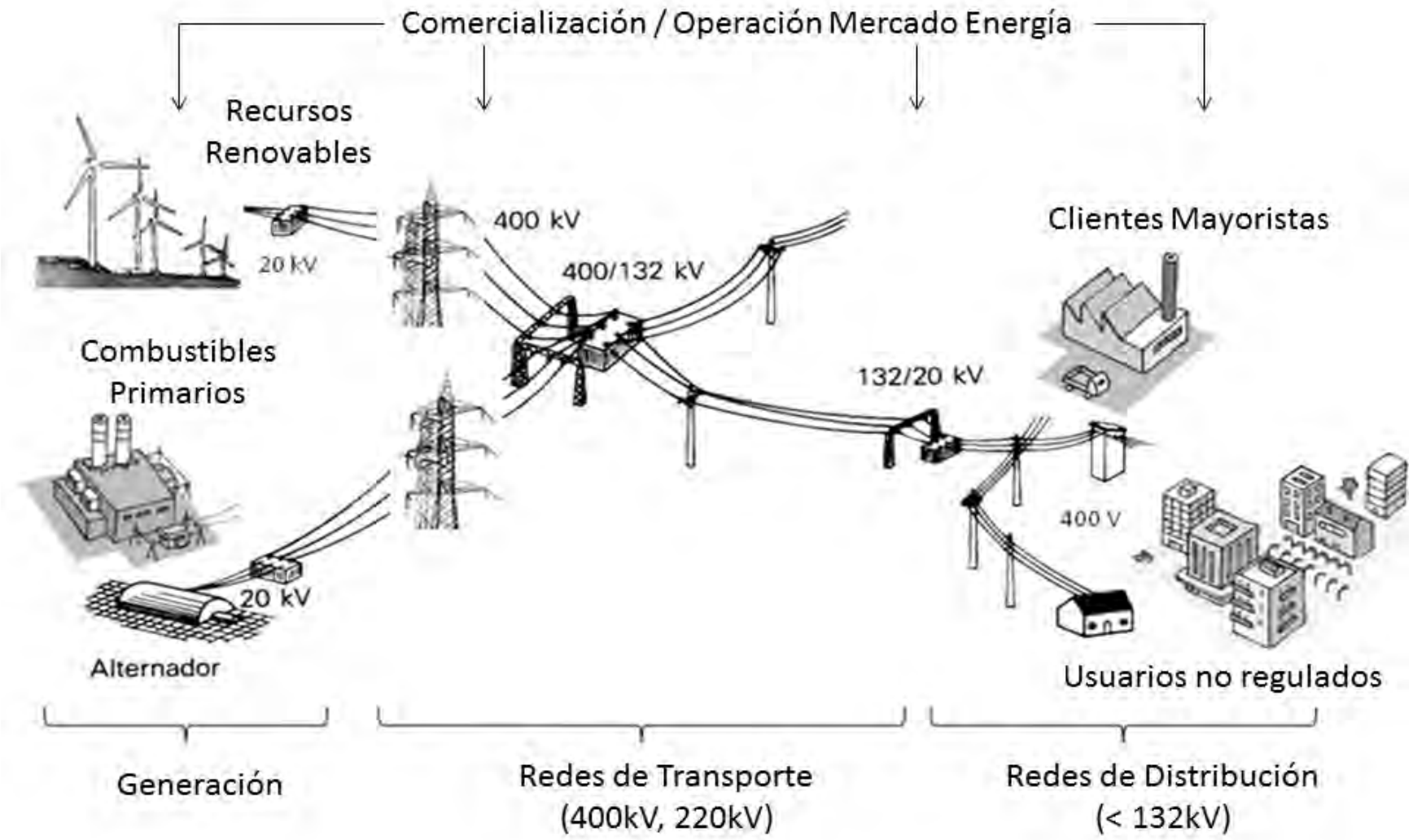

Electricity
Natural Gas
Oil, Pipelines
Water Supply
Wastewater, Sewage
SCADA, Industrial Control
Telecommunications
Information Systems
Policies, Regulations
Railroads
Roads
Human Activities
Banking, Finances
26 (14%)
11 (6%)
6 (3%)
13 (7%)
11 (6%)
12 (7%)
17 (9%)
10 (5%)
22 (12%)
10 (5%)
10 (5%)
20 (11%)
15 (8%)
0
5
10
15
20
25
30
Agents
System Dynamics
Rating Matrices
Relational Databases
Network Theory

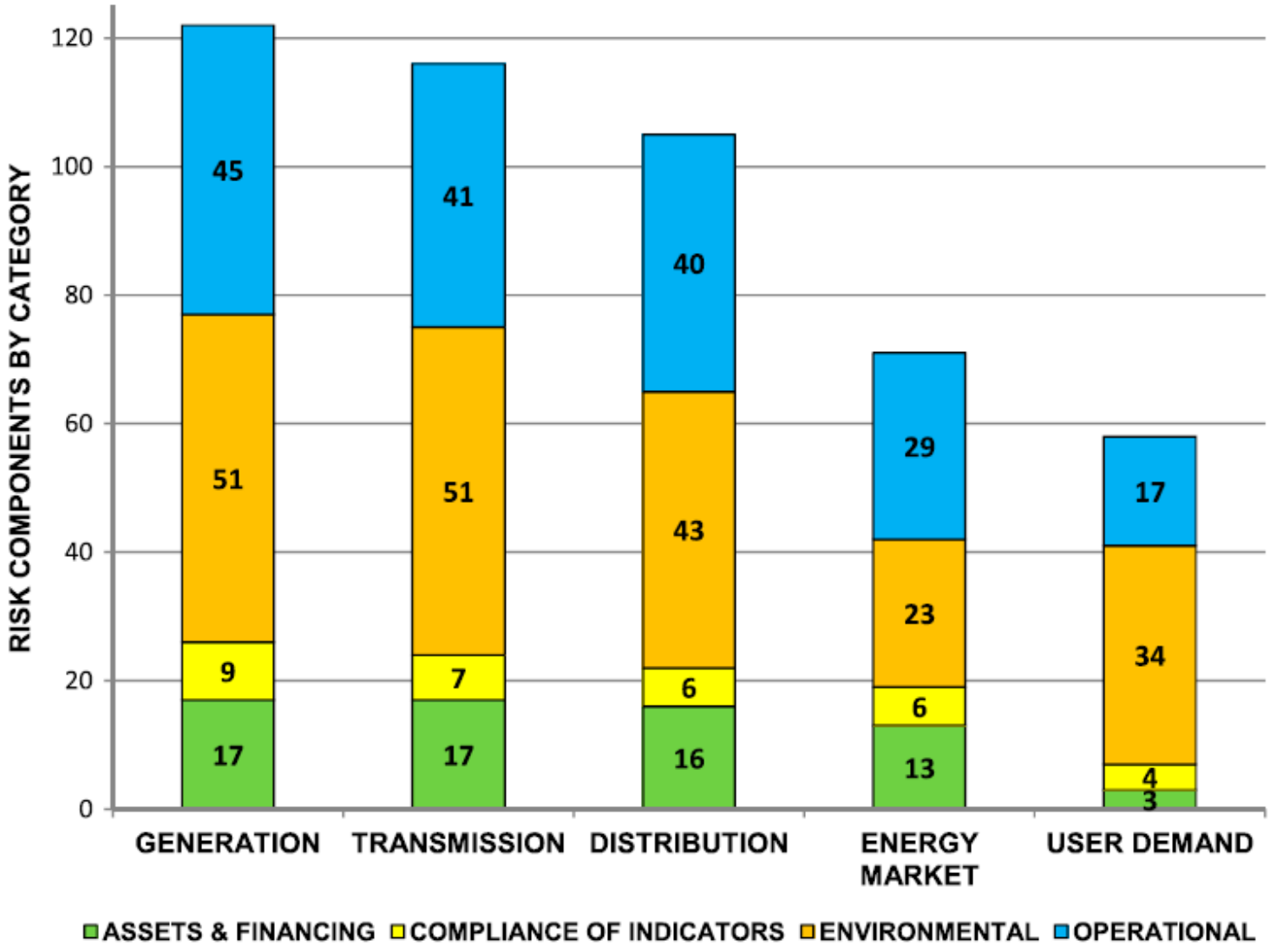

(for critical electric infrastructure protection)
24
22
20
18
16
14
12
10
8
6
4
2
0
30%
28%
42%
2
1
5
4
3
1
1
5
4
3
3
3
10
2
3
Identification
Risk Assesment
Prioritization, Implementation, Measuring
Network Theory -
Rating Matrix -
Agents -
System Dynamics -
Relational DB -

Evaluar las amenazas




Technical
Technical / Non-Technical
Non-Technical
OPERATIONAL
20 - Deficiencies of suppliers and subcontractors
17 - Vulnerability of ICT systems
16 - Technical disturbances in power grid and generation plants
15 - Inadequate manpower education and training
14 - Failures of equipment, materials and hardware
13 - Human or procedural failures
10 - Corruption, fraud, mismanagement
ENVIRONMENTAL
9 - Volatility of macroeconomic variables
8 - Terrorism and vandalism
7 - Misunderstanding and opposition of the population
6 - Adverse natural phenomena
5 - Adverse weather conditions
4 - Changes in national public policy
3 - Regulatory changes, political and legal processes
21 - Vulnerability of the supply chain
20 - Deficiencies of suppliers and subcontractors
COMPLIANCE OF INDICATORS
3 - Regulatory changes, political and legal processes
19 - Reputation and public image
18 - Non-compliance or low quality of electricity supply indicators
ASSETS & FINANCING
2 - Insufficient financing
12 - Growth challenges of the infrastructure system
1 - Non-payable billing extension (overdue)
8
5
7
6
7
6
6
3
13
11
8
9
4
5
11
3
3
3
5
12
3
5
0
2
4
6
8
10
12
14


Comercialización / Operación Mercado Energía
Recursos Renovables
20 kV
400 kV
400/132 kV
Clientes Mayoristas
Combustibles Primarios
132/20 kV
400 V
20 kV
Alternador
Usuarios no regulados
Generación
Redes de Transporte (400kV, 220kV)
Redes de Distribución (< 132kV)


RISK COMPONENTS BY CATEGORY
120
100
80
60
40
20
0
45
51
9
17
41
51
7
17
40
43
6
16
29
23
6
13
17
34
4
3
GENERATION
TRANSMISSION
DISTRIBUTION
ENERGY MARKET
USER DEMAND
ASSETS & FINANCING
COMPLIANCE OF INDICATORS
ENVIRONMENTAL
OPERATIONAL

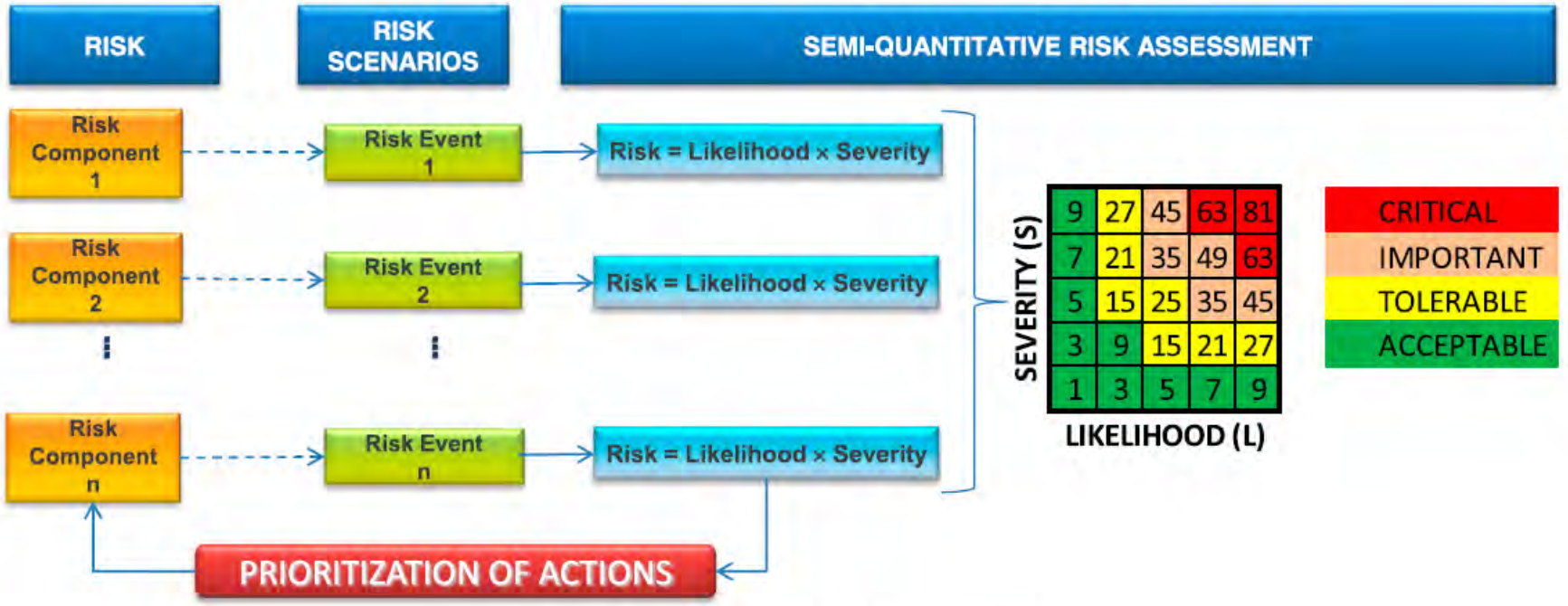


Fig. 3 – Risk component breakdown structure.

Table 1 – Likelihood (L) scales for semi-quantitative risk assessment.

Likelihood (L)	Remote	Unlikely	Credible	Probable	True
Scale	1	3	5	7	9
Frequency	One event every 10 years or more	One event every 7–10 years	One event every 3–7 years	One event every 1–3 years	One or more events every 1 year

Table 2 – Severity (S) scales for semi-quantitative risk assessment.

Severity (S)	Low	Moderate	Medium	High	Critical
Scale	1	3	5	7	9
Economic resources	Losses less than 1M €	Losses between 1M € and 3M €	Losses between 3M € and 10M €	Losses between 10M € and 20M €	Losses more than 20M €
Technical resources	No services are affected. Enterprise information is not compromised	No services are affected. Enterprise information may be somewhat compromised	No services are affected. Enterprise information is lost but can be recovered	Some services are affected. Enterprise information is also compromised	Some services are affected. Enterprise information is lost and cannot be recovered
Human resources	No effects on employees or stakeholders	Integrity of employees or stakeholders may be temporarily affected, but no intervention is required for recovery	Integrity of employees or stakeholders may be temporarily affected, but intervention is required for recovery without consequences	Integrity of employees or stakeholders may be permanently affected. Intervention is strongly required for recovery	Loss of human life
Material resources	No effect on service operations. Relationships with energy consumers are not affected	Effect on service operations is evident. Relationships with energy consumers are not affected	Effect on service operations is evident. Relationships with energy consumers are somewhat affected	Service operations have collapsed. Relationships with energy consumers have deteriorated	Service operations have crashed. Relationships with energy consumers and market regulators are shattered

Table 4 – Semi-quantitative assessments of the risks in the interconnected risk map.

No	Description of risk	Risk	Judgment
1	Non-payable billing extension (overdue)	7.1	Acceptable
2	Insufficient financing	4.4	Acceptable
3	Regulatory changes, political and legal processes	4.8	Acceptable
4	Changes in national public policy	12.0	Tolerable
5	Adverse weather conditions	19.1	Tolerable
6	Adverse natural phenomena	36.0	Important
7	Misunderstanding and opposition of the population	18.1	Tolerable
8	Terrorism and vandalism	50.0	Critical
9	Volatility of macroeconomic variables	18.3	Tolerable
10	Corruption, fraud, mismanagement	34.4	Important
11	Gaps in information and knowledge management	24.3	Tolerable
12	Growth challenges of the infrastructure system	6.0	Acceptable
13	Human or procedural failures	35.9	Important
14	Failures of equipment, materials and hardware	20.1	Tolerable
15	Inadequate manpower education and training	27.2	Tolerable
16	Technical disturbances in power grid and generation plants	34.6	Important
17	Vulnerability of ICT systems	33.9	Important
18	Non-compliance or low quality of electricity supply indicators	33.5	Important
19	Reputation and public image	8.3	Acceptable
20	Deficiencies of suppliers and subcontractors	29.4	Important
21	Vulnerability of the supply chain	33.5	Important

No.	Type	Category	Risk	Risk Component	Score	Range
30	NT	EN	5 - Adverse weather conditions	Ice storms and/or snow	6.0	--
31	NT	EN	5 - Adverse weather conditions	Wind gusts	25.0	-
32	NT	EN	5 - Adverse weather conditions	Environmental pollution	11.0	-
33	NT	EN	5 - Adverse weather conditions	Excess salinity	11.5	-
34	NT	EN	5 - Adverse weather conditions	Cold waves	1.5	--
35	NT	EN	5 - Adverse weather conditions	Heat waves	18.8	-
36	NT	EN	5 - Adverse weather conditions	Solar radiation	18.8	-
37	NT	EN	5 - Adverse weather conditions	Strong storms	35.0	+
38	NT	EN	5 - Adverse weather conditions	Lightning	44.0	+
39	NT	EN	6 - Adverse natural phenomena	Earthquakes	31.3	+
40	NT	EN	6 - Adverse natural phenomena	Landslides	49.0	+
41	NT	EN	6 - Adverse natural phenomena	Avalanches or sudden rises of river levels	64.8	++
42	NT	EN	6 - Adverse natural phenomena	Flood or flooding	64.8	++
43	NT	EN	6 - Adverse natural phenomena	Volcanic eruptions	14.3	-
44	NT	EN	6 - Adverse natural phenomena	Forest fires	37.0	+
45	NT	EN	6 - Adverse natural phenomena	Solar magnetic disturbances	2.0	--
46	NT	EN	6 - Adverse natural phenomena	Vegetation protruding into easement area of the electricity infrastructure	25.0	+

No.	Type	Category	Risk	Risk Component	Score	Range
57	NT	EN	8 - Terrorism and vandalism	Armed attacks or seizure of facilities, including generation plants	6.0	--
58	NT	EN	8 - Terrorism and vandalism	Attacks on the electricity transmission infrastructure	60.0	++
59	NT	EN	8 - Terrorism and vandalism	Kidnapping of employees and collaborators	62.5	++
60	NT	EN	8 - Terrorism and vandalism	Minefields	55.0	++
61	NT	EN	8 - Terrorism and vandalism	Extortion	62.5	++
62	NT	EN	8 - Terrorism and vandalism	Lockdowns or armed strikes	55.0	++
63	NT	EN	8 - Terrorism and vandalism	Crossfire	34.5	+
64	NT	EN	8 - Terrorism and vandalism	Armed attacks on transmission towers, substations and generation facilities	55.0	++
65	NT	EN	8 - Terrorism and vandalism	Easements or land invasion of forced displacement	29.0	+
66	NT	EN	8 - Terrorism and vandalism	Assault	62.5	++
67	NT	EN	8 - Terrorism and vandalism	Illicit crops that constrain access to infrastructure assets	17.5	-
68	NT	EN	8 - Terrorism and vandalism	Actions by contractors outside the law or contrary to the interests of the infrastructure owner or operator	40.0	+
69	NT	EN	8 - Terrorism and vandalism	Armed attacks (including thrown explosives)	40.0	+

THE WALL STREET JOURNAL.

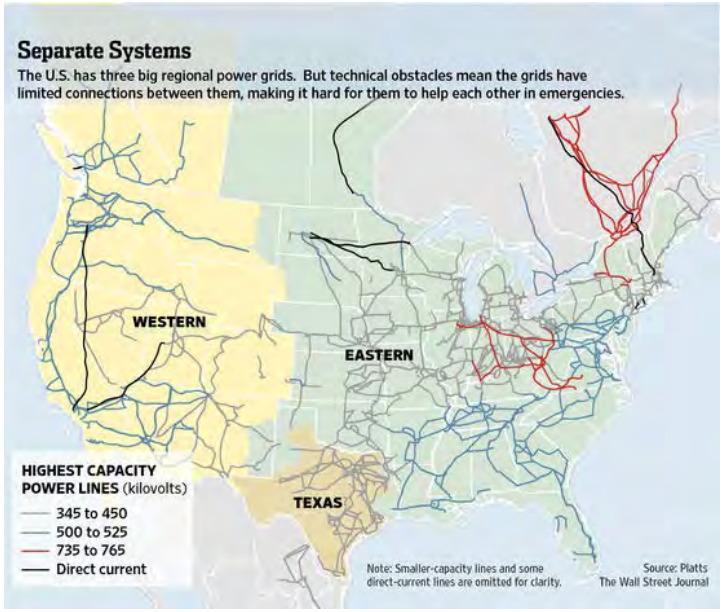
U.S. Risks National Blackout From Small-Scale Attack

Federal Analysis Says Sabotage of Nine Key Substations Is Sufficient for Broad Outage

By REBECCA SMITH
March 12, 2014 7:03 p.m. ET

The U.S. could suffer a coast-to-coast blackout if saboteurs knocked out just nine of the country's 55,000 electric-transmission substations on a scorching summer day, according to a previously unreported federal analysis.

The study by the Federal Energy Regulatory Commission concluded that coordinated attacks in each of the nation's three separate electric systems could cause the entire power network to collapse, people familiar with the research said.



THE WALL STREET JOURNAL.

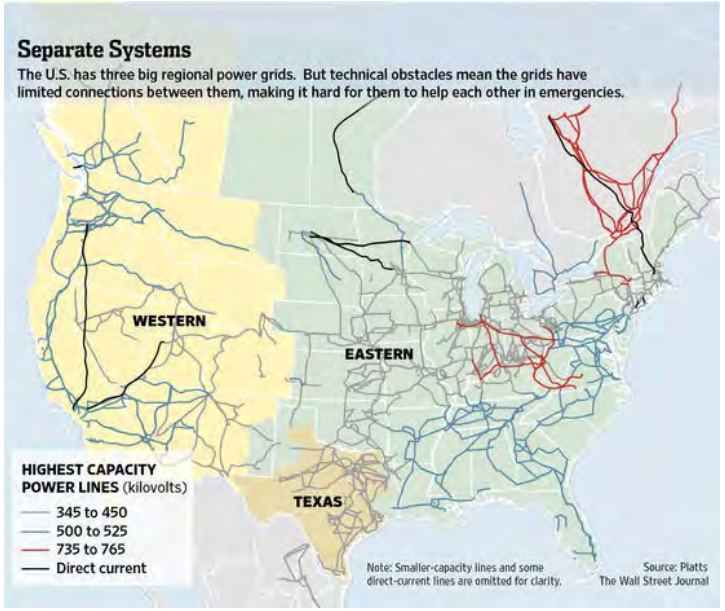
U.S. Risks National Blackout From Small-Scale Attack

Federal Analysis Says Sabotage of Nine Key Substations Is Sufficient for Broad Outage

By REBECCA SMITH
March 12, 2014 7:03 p.m. ET

The U.S. could suffer a coast-to-coast blackout if saboteurs knocked out just nine of the country's 55,000 electric-transmission substations on a scorching summer day, according to a previously unreported federal analysis.

The study by the Federal Energy Regulatory Commission concluded that coordinated attacks in each of the nation's three separate electric systems could cause the entire power network to collapse, people familiar with the research said.



THE WALL STREET JOURNAL.

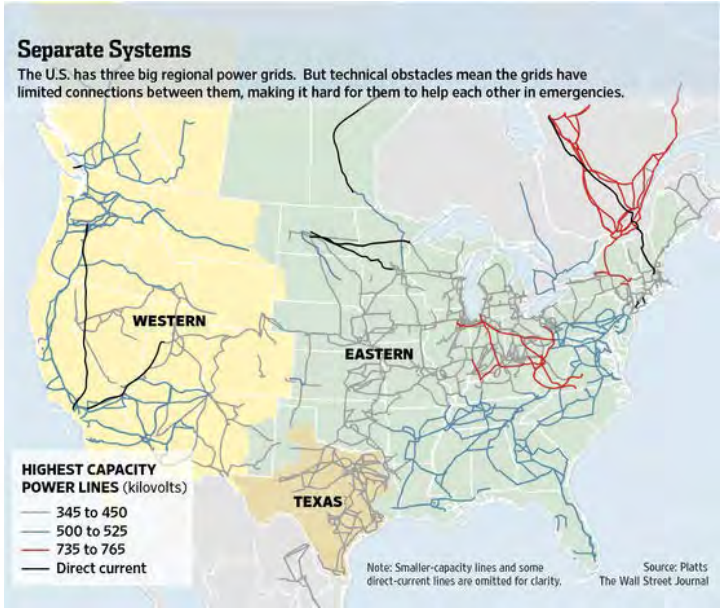
U.S. Risks National Blackout From Small-Scale Attack

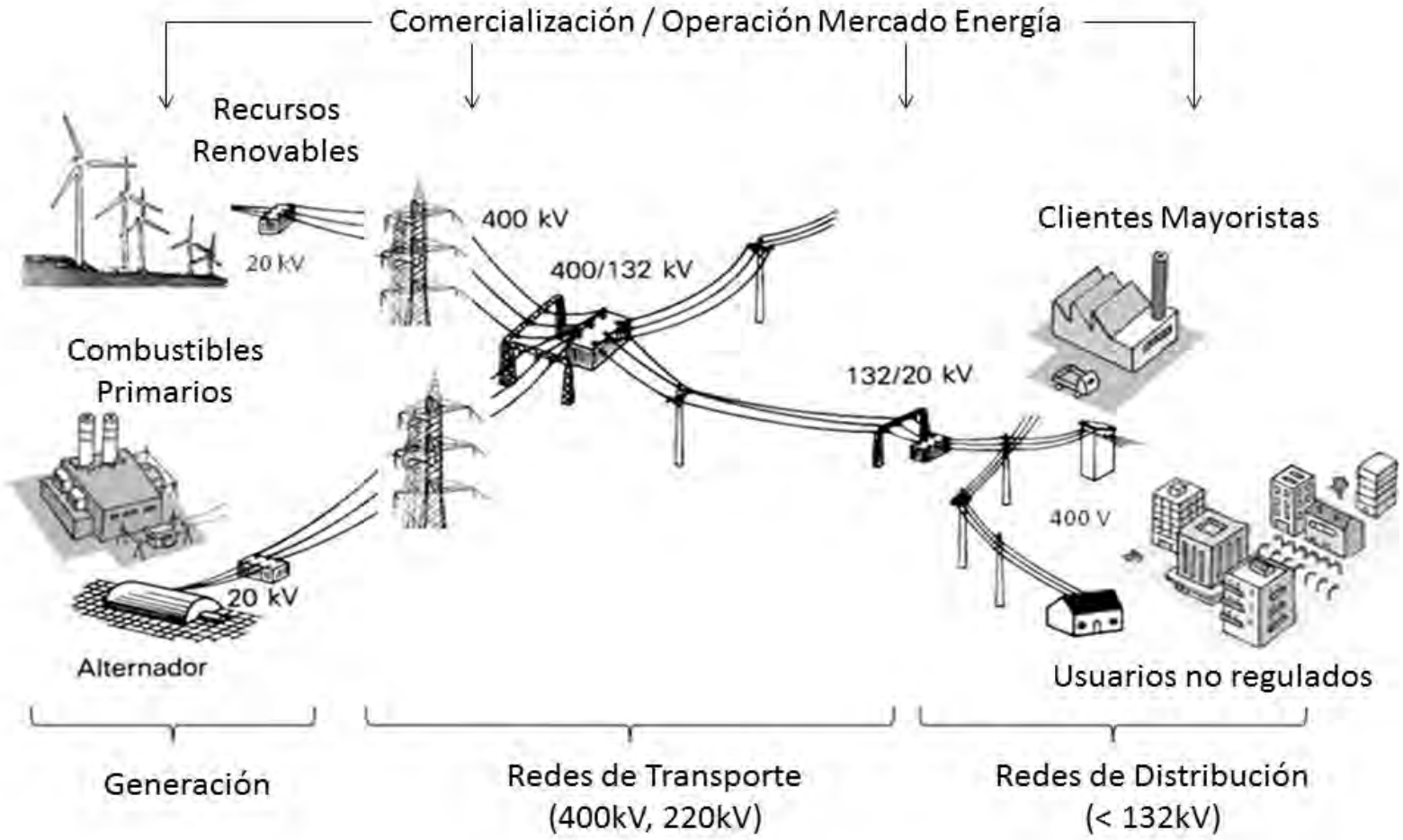
Federal Analysis Says Sabotage of Nine Key Substations Is Sufficient for Broad Outage

By REBECCA SMITH
March 12, 2014 7:03 p.m. ET

The U.S. could suffer a coast-to-coast blackout if saboteurs knocked out just nine of the country's 55,000 electric-transmission substations on a scorching summer day, according to a previously unreported federal analysis.

The study by the Federal Energy Regulatory Commission concluded that coordinated attacks in each of the nation's three separate electric systems could cause the entire power network to collapse, people familiar with the research said.




Comercialización / Operación Mercado Energía
Recursos Renovables
20 kV
400 kV
400/132 kV
Clientes Mayoristas
Combustibles Primarios
132/20 kV
400 V
20 kV
Alternador
Usuarios no regulados
Generación
Redes de Transporte (400kV, 220kV)
Redes de Distribución (< 132kV)

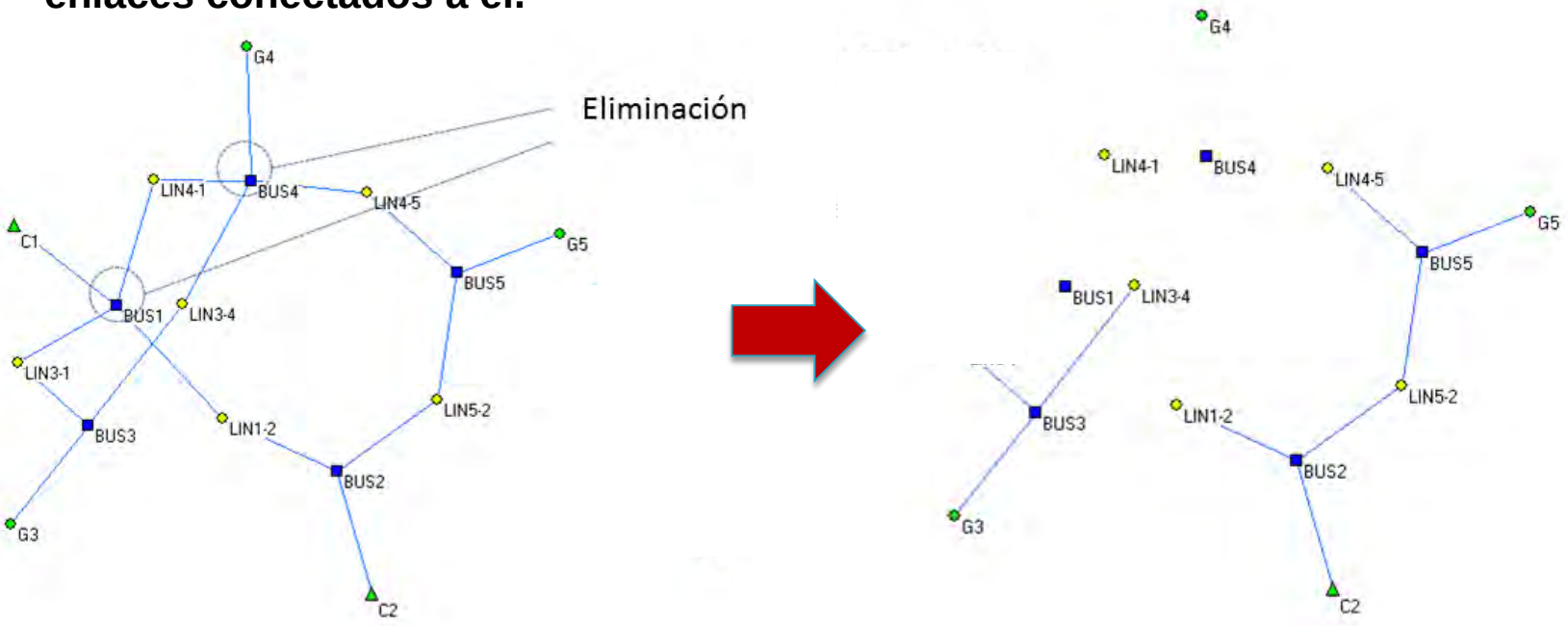
G.J. Correa, J.M. Yusta. *Grid Vulnerability Analysis Based on Scale-Free Graphs versus Power Flow Models*.
Electric Power Systems Research 101 (2013) 71-79.

VULNERABILIDAD CONTRA FALLOS Y ATAQUES EN LA RED

- **Validación de la aplicación de teoría de grafos como herramienta adecuada para el análisis de vulnerabilidad en el sector de infraestructura eléctrica.**

- **Funcionamiento de las redes complejas en eventos de eliminación de nodos de manera aleatoria ("tolerancia contra errores o fallos") o de manera deliberada ("tolerancia contra ataques").**

- **Partiendo de una red conectada, en cada iteración se elimina un nodo. El aislamiento (o desaparición) de ese nodo implica la eliminación de todos los enlaces conectados a él.**



INDICADORES DE EVALUACIÓN EN EL GRAFO DE LIBRE ESCALA

Medidas estadísticas que se obtienen para cada grafo

- Distancia Geodésica: $$d_{ij}\underset{i=2\mathrm{L}\ N}{} = \min_{j\in N(i)}\left(d_j\right)_i$$
- Distancia Media Geodésica: $$\bar{d} = \frac{1}{N\cdot\left(N-1\right)}\sum_{i\neq j} d_{ij}$$
- Eficiencia Geodésica: $$\bar{e} = \frac{1}{N\cdot\left(N-1\right)}\sum_{i\neq j}\frac{1}{d_{ij}}$$

Con estos indicadores se obtienen posteriores mediciones que reflejan la evolución del grafo en condiciones de aislamientos sucesivos de los nodos que lo conforman.

INDICADORES DE EVALUACIÓN EN EL GRAFO DE LIBRE ESCALA

Evolución de ciertos indicadores estadísticos de las redes complejas en caso de eventos de eliminación sistemática de sus nodos.

- Índice de Vulnerabilidad Geodésica ($\bar{v}$):

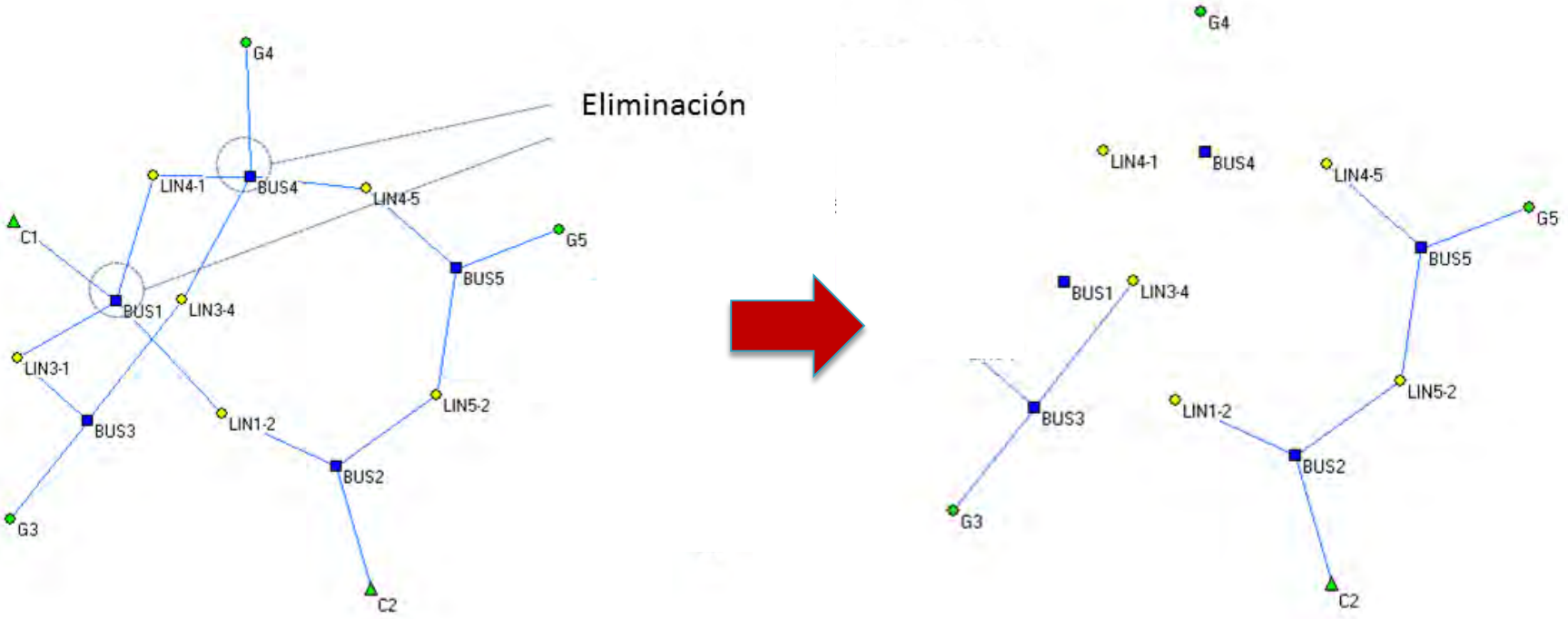
$$\bar{v} = 1 - \frac{\sum_{i \neq j} \left(\frac{1}{d_{ij}^{LC}} \right)}{\sum_{i \neq j} \left(\frac{1}{d_{ij}^{BC}} \right)}$$

- Índice de Impacto en la conectividad (S):

$$S = 1 - \frac{N^{LC}}{N}$$

- Índice de Desconexión de Cargas (PLS):

$$PLS = 1 - \frac{\sum_{i} \sqrt{\left(P_{Di}^{LC}\right)^2 + \left(Q_{Di}^{LC}\right)^2}}{\sum_{i} \sqrt{\left(P_{Di}^{BC}\right)^2 + \left(Q_{Di}^{BC}\right)^2}}$$


G4
LIN4-1
BUS4
LIN4-5
C1
G5
BUS5
BUS1
LIN3-4
LIN3-1
LIN5-2
BUS3
LIN1-2
BUS2
G3
C2
Eliminación
G4
LIN4-1
BUS4
LIN4-5
G5
BUS5
BUS1
LIN3-4
LIN5-2
BUS3
LIN1-2
BUS2
G3
C2

G.J. Correa, J.M. Yusta. *Grid Vulnerability Analysis Based on Scale-Free Graphs versus Power Flow Models*. Electric Power Systems Research 101 (2013) 71-79.

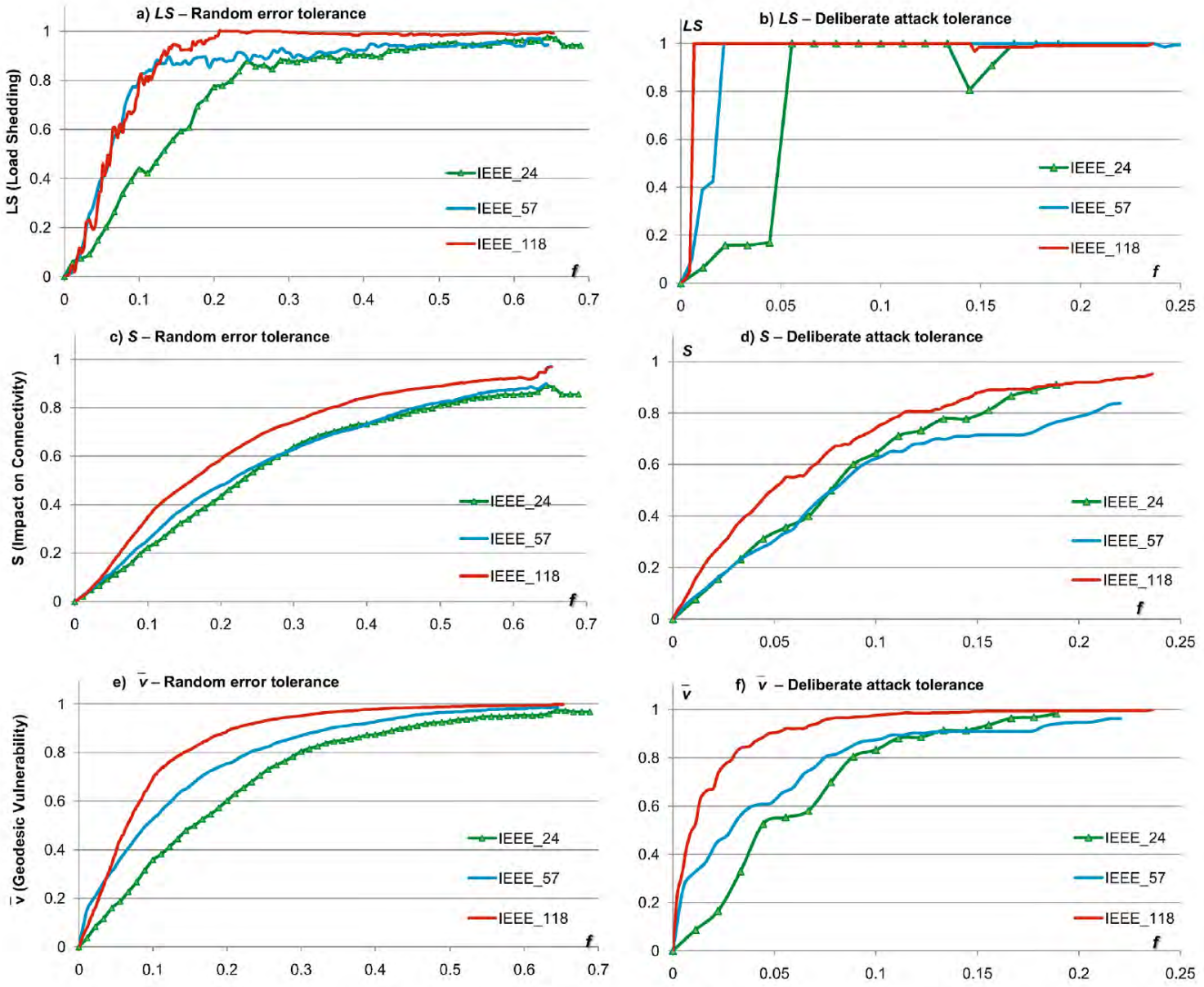


Fig. 5. Graphical representation of indexes *LS*, *S* and $\bar{v}$ in IEEE test networks.

G.J. Correa, J.M. Yusta. *Grid Vulnerability Analysis Based on Scale-Free Graphs versus Power Flow Models*.
Electric Power Systems Research 101 (2013) 71-79.

Table 2
Iterative process for random errors and deliberate attacks on IEEE test networks (time in minutes).

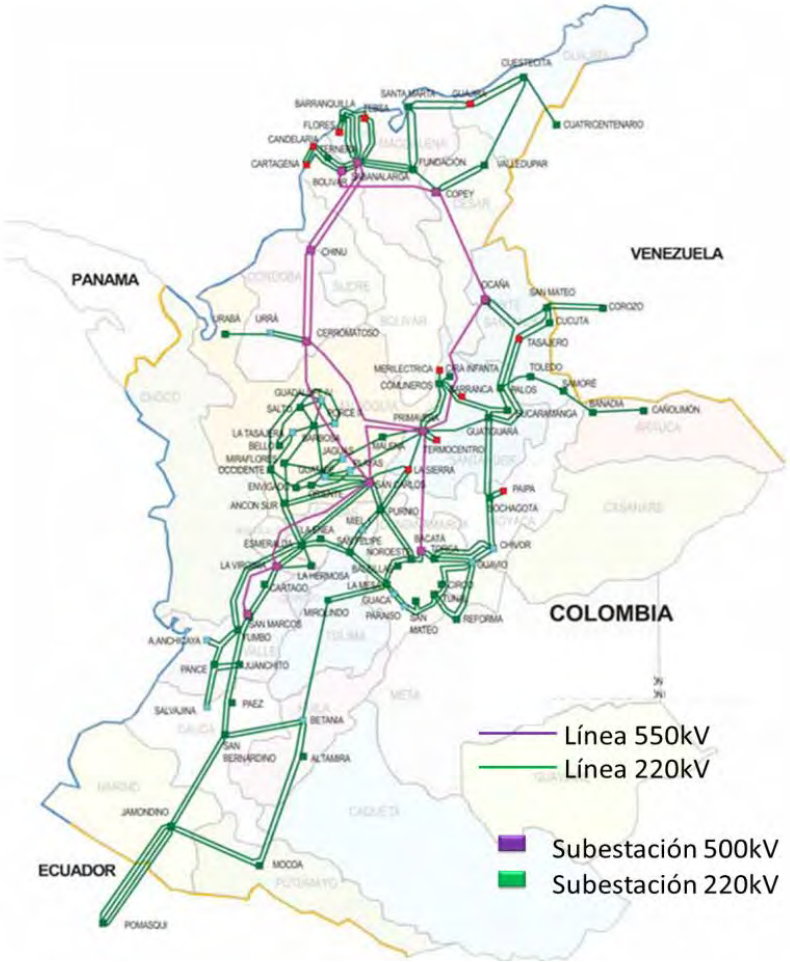
Disruption strategy	Algorithm execution	IEEE 14	IEEE 24	IEEE 30	IEEE 57	IEEE 118	IEEE 300
Random (35 samples)	Average iterations per sample	33	62	67	120	293	635
	Power flow routine time	35′	80′	90′	570′	1140′	3150′
	Graph theory index calculations time	6′	11′	12′	21′	51′	151′
Deliberate (1 sample)	Iterations per sample	10	18	26	42	107	213
	Power flow routine time	1′	2′	2′	4′	12′	21′
	Graph theory index calculations time	0.1′	0.2′	0.2′	0.5′	1′	2′

Table 3
Pearson correlation between electric index *LS* and graph theory measures $S(\rho_1)$ and $\bar{v}(\rho_2)$.

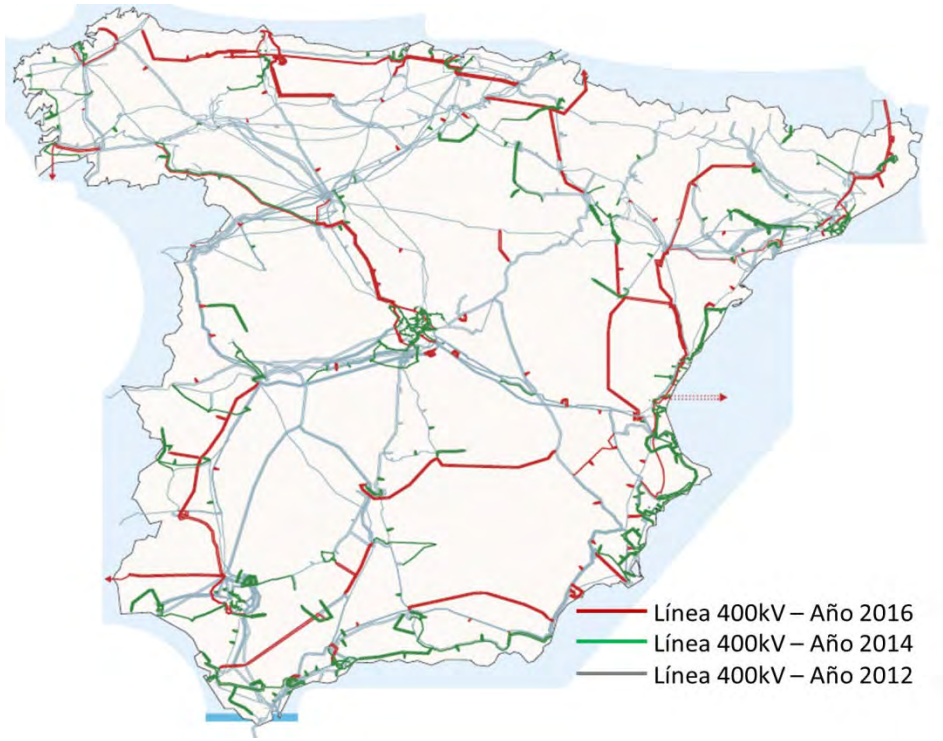
Disruption strategy	Correlation	IEEE 14	IEEE 24	IEEE 30	IEEE 57	IEEE 118	IEEE 300
Random	ρ_1	0.9485	0.9532	0.9503	0.8047	0.8584	0.9742
	ρ_2	0.9903	0.9826	0.9920	0.9099	0.9828	0.9867
Deliberate	ρ_1	0.8566	0.8268	0.3941	0.6266	0.4264	0.7130
	ρ_2	0.9491	0.8780	0.6586	0.7897	0.7321	0.9012

G.J. Correa, J.M. Yusta. *Structural Vulnerability in Transmission Systems: Cases of Colombia and Spain*.
Energy Conversion and Management 77 (2014) 408-418

RED DE TRANSPORTE ALTA TENSIÓN (COLOMBIA, ESPAÑA)



Redes de transporte 220kV y 500kV en Zonas Interconectadas de Colombia

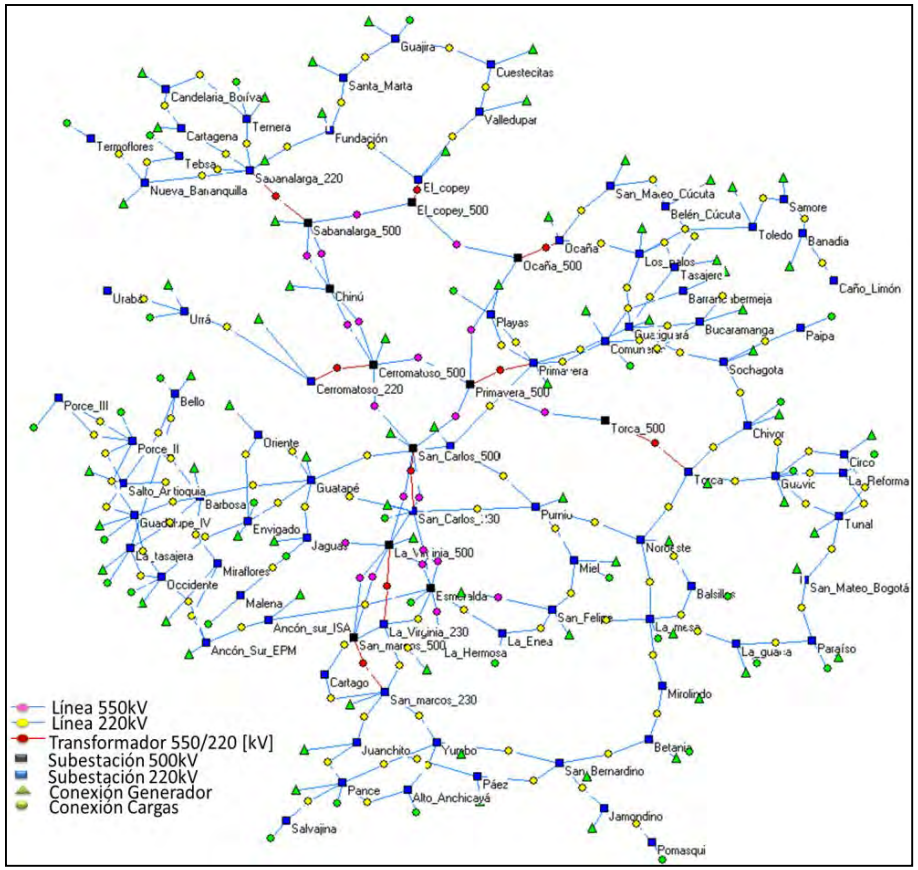


Red peninsular de alta tensión 400kV en España

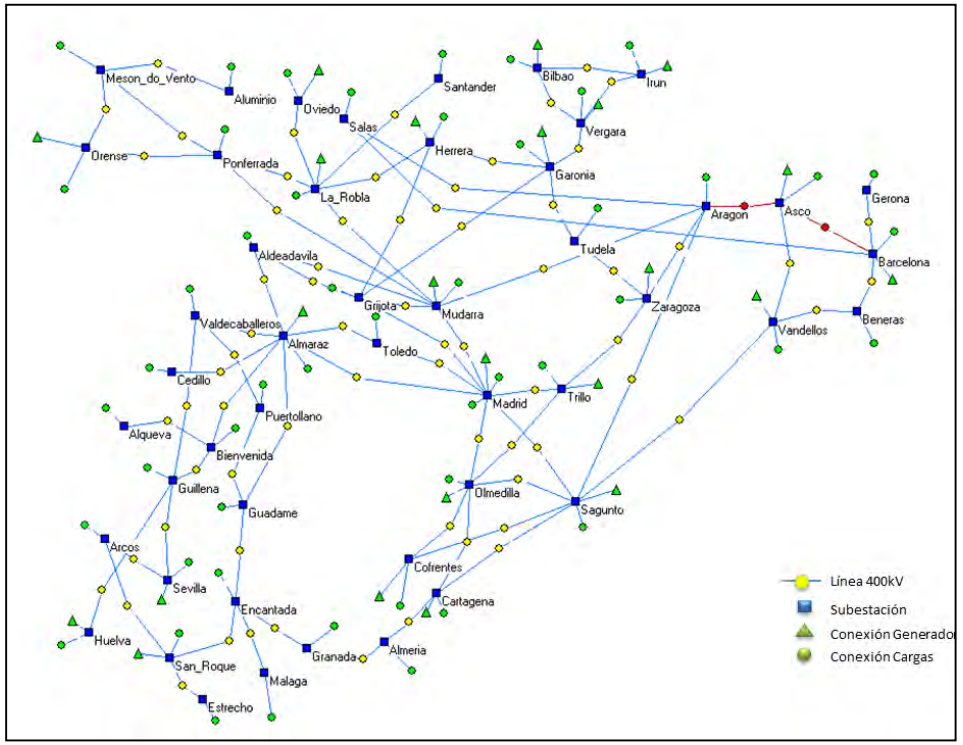
G.J. Correa, J.M. Yusta. *Structural Vulnerability in Transmission Systems: Cases of Colombia and Spain*.
Energy Conversion and Management 77 (2014) 408-418

RED DE TRANSPORTE ALTA TENSIÓN (COLOMBIA, ESPAÑA)

Grafos de Libre Escala representativos de las redes de transporte (caso base)



Red colombiana 220kV y 500kV

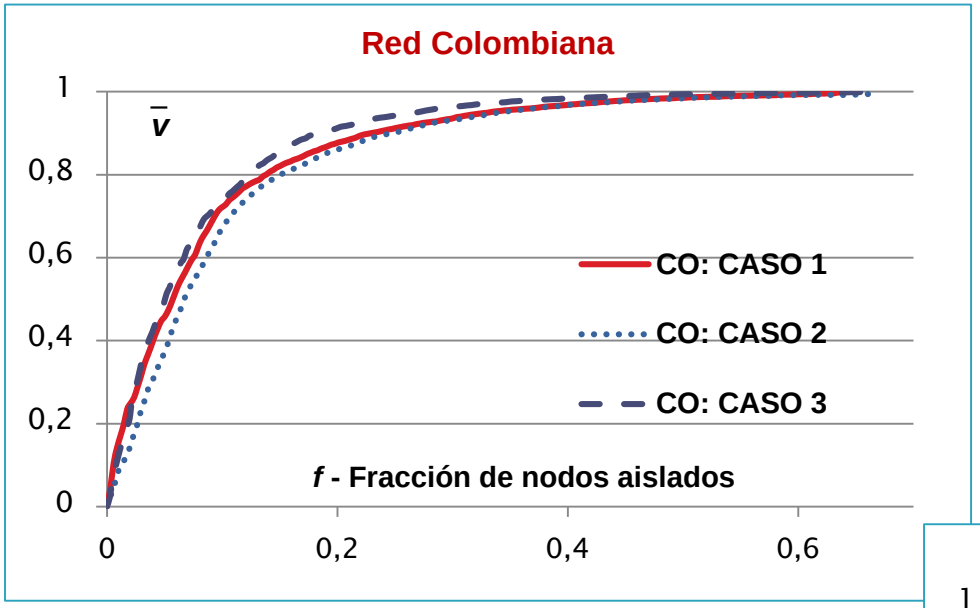


Red española 400kV

RED DE TRANSPORTE ALTA TENSIÓN (COLOMBIA, ESPAÑA)

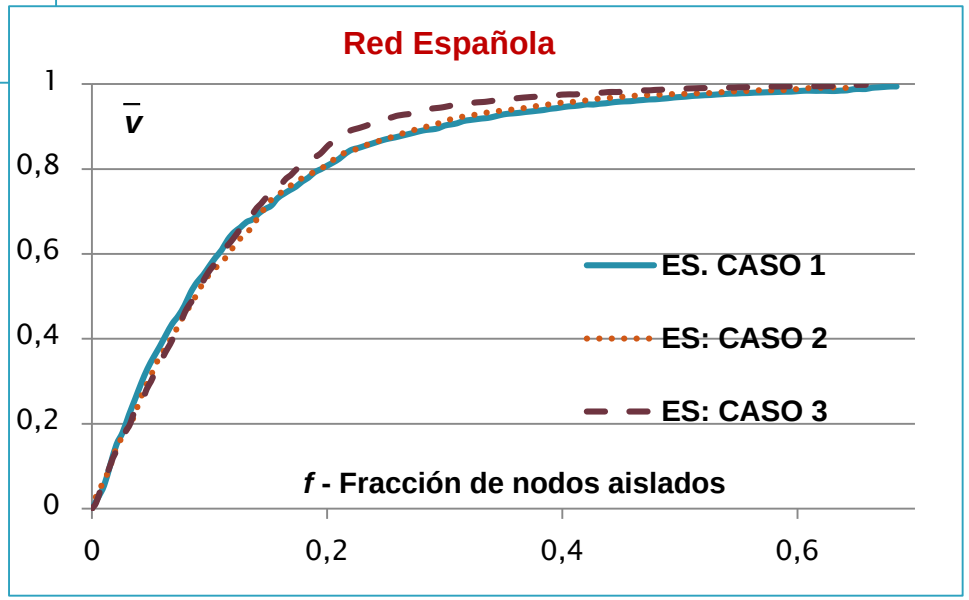
- **Caso 1:** Condición actual de la Red de Transporte (94 buses en Colombia, 48 buses en España)
- **Caso 2:** Planes de mejora de robustez de la red actual, según la planificación establecida en los documentos gubernamentales (UPME 2010-2024, MINETUR 2008-2016)
- **Caso 3:** Planificación de la expansión de las redes actuales, según los documentos gubernamentales (117 buses en Colombia, 76 buses en España)

VULNERABILIDAD GEODÉSICA (FALLOS ALEATORIOS)



Caso 1 *vs* Caso 2:
Leve mejora de la vulnerabilidad

Caso 1 *vs* Caso 3:
La red expandida es más vulnerable (es menos compacta)



VULNERABILIDAD GEODÉSICA (FALLOS ALEATORIOS)

Algunos escenarios de riesgo tienen la consecuencia de aislar un área geográfica que comprometa una pequeña cantidad de nodos (5% ó 10% de los nodos de la red)

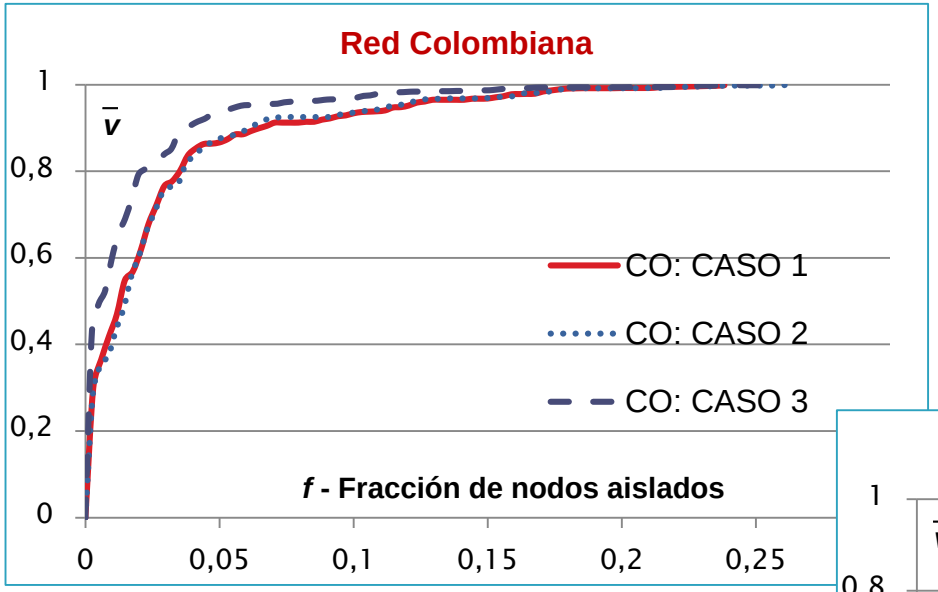
RED	f = 5%	f = 10%	f = 20%	f = 30%
España (Caso 1)	0.34	0.57	0.81	0.90
España (Caso 2)	0.31	0.55	0.81	0.91
España (Caso 3)	0.30	0.54	0.86	0.95
Colombia (Caso 1)	0.47	0.71	0.88	0.93
Colombia (Caso 2)	0.40	0.65	0.87	0.93
Colombia (Caso 3)	0.51	0.73	0.91	0.96

Menor vulnerabilidad $\bar{v}$ para una red más mallada:

- **Nuevas líneas de transporte, sin aumentar el número de subestaciones.**
- **Mayor valor promedio del grado de conexión $\bar{k}$**

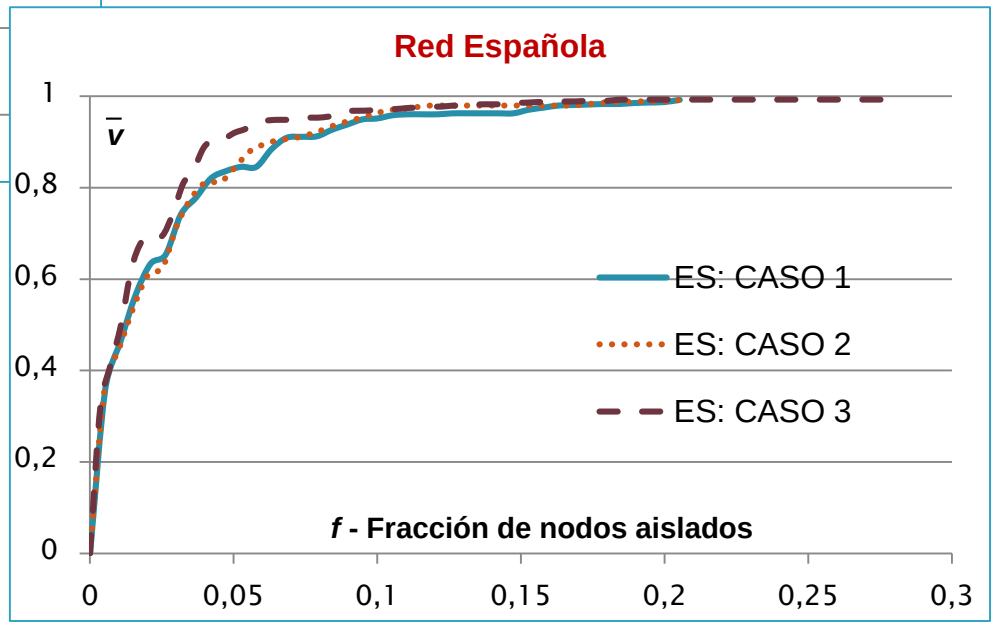
G.J. Correa, J.M. Yusta. *Structural Vulnerability in Transmission Systems: Cases of Colombia and Spain*. Energy Conversion and Management 77 (2014) 408-418

VULNERABILIDAD GEODÉSICA (ATAQUES DELIBERADOS)



Caso 1 *vs* Caso 2:
Curvas superpuestas (no implica mayor protección frente a los ataques deliberados)

Caso 1 *vs* Caso 3:
La red expandida es más vulnerable (es menos compacta)



G.J. Correa, J.M. Yusta. *Structural Vulnerability in Transmission Systems: Cases of Colombia and Spain*. Energy Conversion and Management 77 (2014) 408-418

VULNERABILIDAD GEODÉSICA (ATAQUES DELIBERADOS)

Mayor resiliencia en escenarios de riesgos aleatorios (fenómenos naturales, fallos técnicos, fallos humanos, etc) que frente a amenazas de ataques malintencionados (vandalismo, terrorismo, ciberataques)

RED	f = 0.5%	f = 1%	f = 2%	f = 5%	f = 10%
España (Caso 1)	0.36	0.45	0.62	0.84	0.95
España (Caso 2)	0.36	0.45	0.62	0.84	0.95
España (Caso 3)	0.40	0.50	0.69	0.92	0.97
Colombia (Caso 1)	0.36	0.45	0.70	0.87	0.97
Colombia (Caso 2)	0.36	0.43	0.70	0.87	0.97
Colombia (Caso 3)	0.49	0.60	0.79	0.92	0.97

En España y Colombia, la planificación de las inversiones en expansión del sistema implica la aparición de buses que concentran altos grados de conectividad

CONCLUSIONES

- **Una aplicación de la metodología desarrollada para evaluar la vulnerabilidad estructural en grandes redes eléctricas ha facilitado conclusiones sobre la efectividad de las inversiones en la topología de las infraestructuras, según la aplicación de los planes de expansión de las redes.**

- **La estrategia de aumentar la robustez a las redes, es decir, mejorar el mallado y el grado de conectividad de los buses, proporciona leves mejoras en la vulnerabilidad de la red frente a fallos aleatorios; sin embargo, no se evidencian mejoras en el caso de ataques deliberados a la infraestructura.**

GESTIÓN ESTRATÉGICA DE LA ENERGÍA ELÉCTRICA

Universidad Zaragoza
1542

Proyecto 2017-2019

REDCRIT:

REDES DE LIBRE ESCALA PARA EL ANÁLISIS DE VULNERABILIDAD Y RESILIENCIA DE INFRAESTRUCTURAS ENERGÉTICAS INTERDEPENDIENTES *ENE2016-77172-R*

Financiado por:

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD

Apoyado por:

CNPIC
CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD

RED ELÉCTRICA DE ESPAÑA

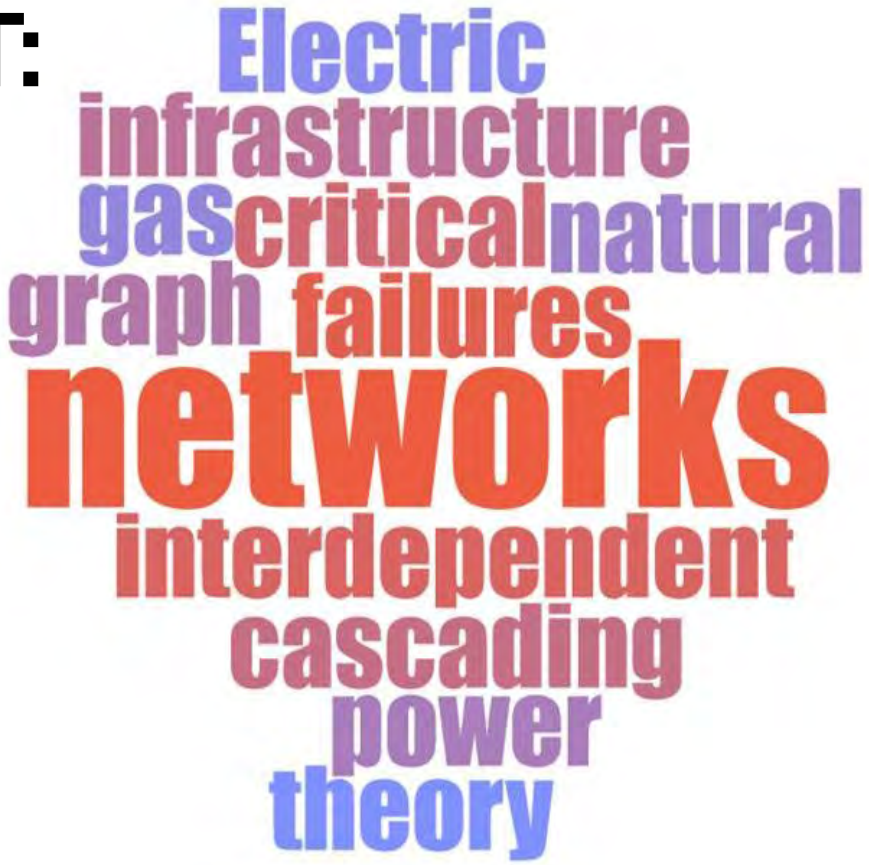
José María Yusta Loyo / XX Seminario Economía y Defensa / Zaragoza, Marzo de 2018

GESTIÓN ESTRATÉGICA DE LA ENERGÍA ELÉCTRICA

Universidad Zaragoza
1542

Proyecto 2017-2019

REDCRIT:



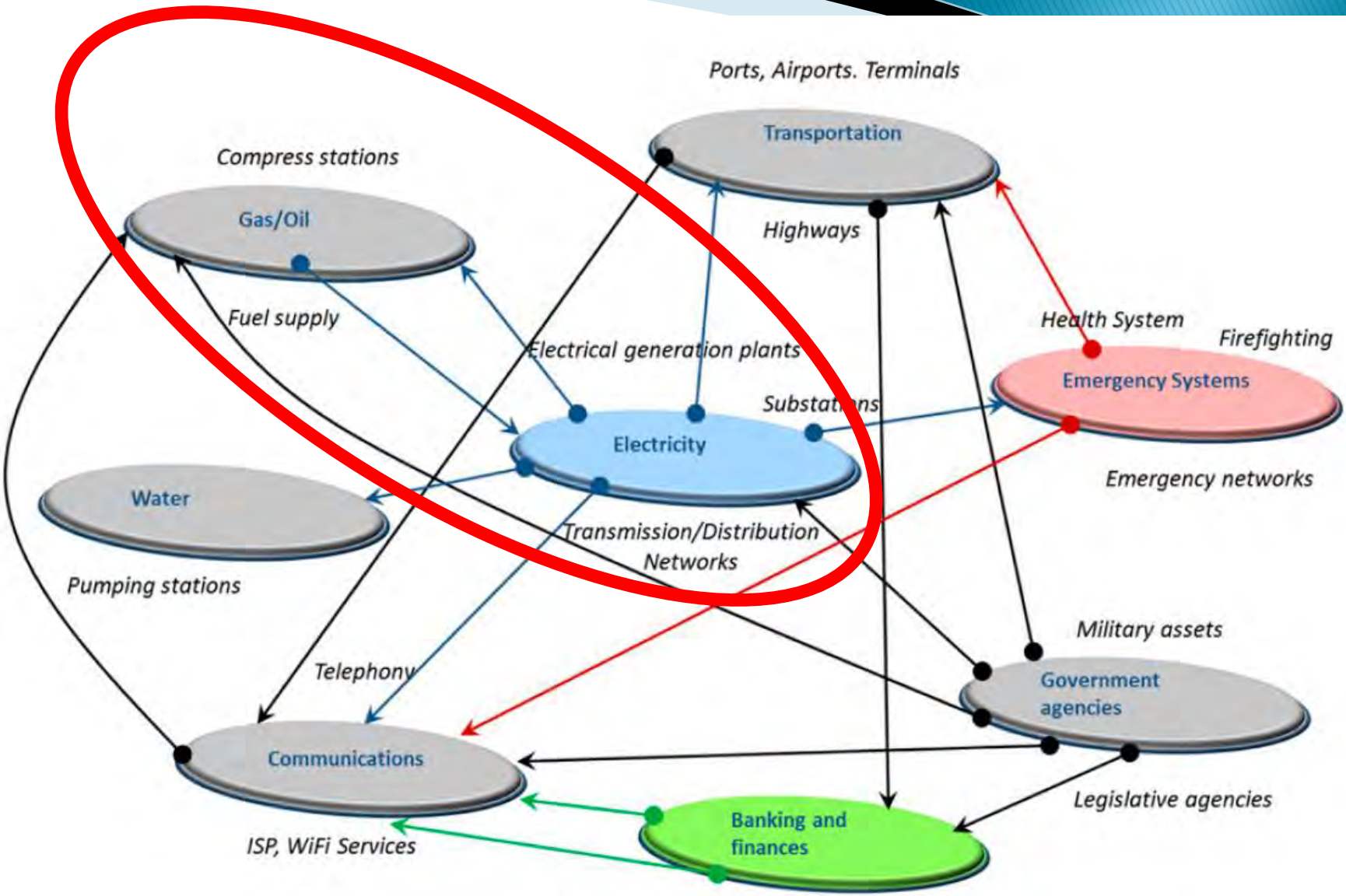


Fig. 1. Example of interdependence between energy systems and other critical infrastructure.

GESTIÓN ESTRATÉGICA DE LA ENERGÍA ELÉCTRICA

Universidad Zaragoza
1542

Proyecto 2017-2019

REDCRIT

- Aplicar los avances obtenidos por el grupo de investigación para sustituir las herramientas computacionales de flujos de cargas tradicionalmente utilizadas en el análisis de contingencias de redes eléctricas por los nuevos métodos basados en la teoría de redes complejas, aplicados al análisis de vulnerabilidad de las topologías de redes interdependientes.
- **Estudio más rápido de la resiliencia de las redes ante contingencias N-t**, **es decir, ante fallos en cascada de las redes.**

GESTIÓN ESTRATÉGICA DE LA ENERGÍA ELÉCTRICA

Universidad Zaragoza
1542

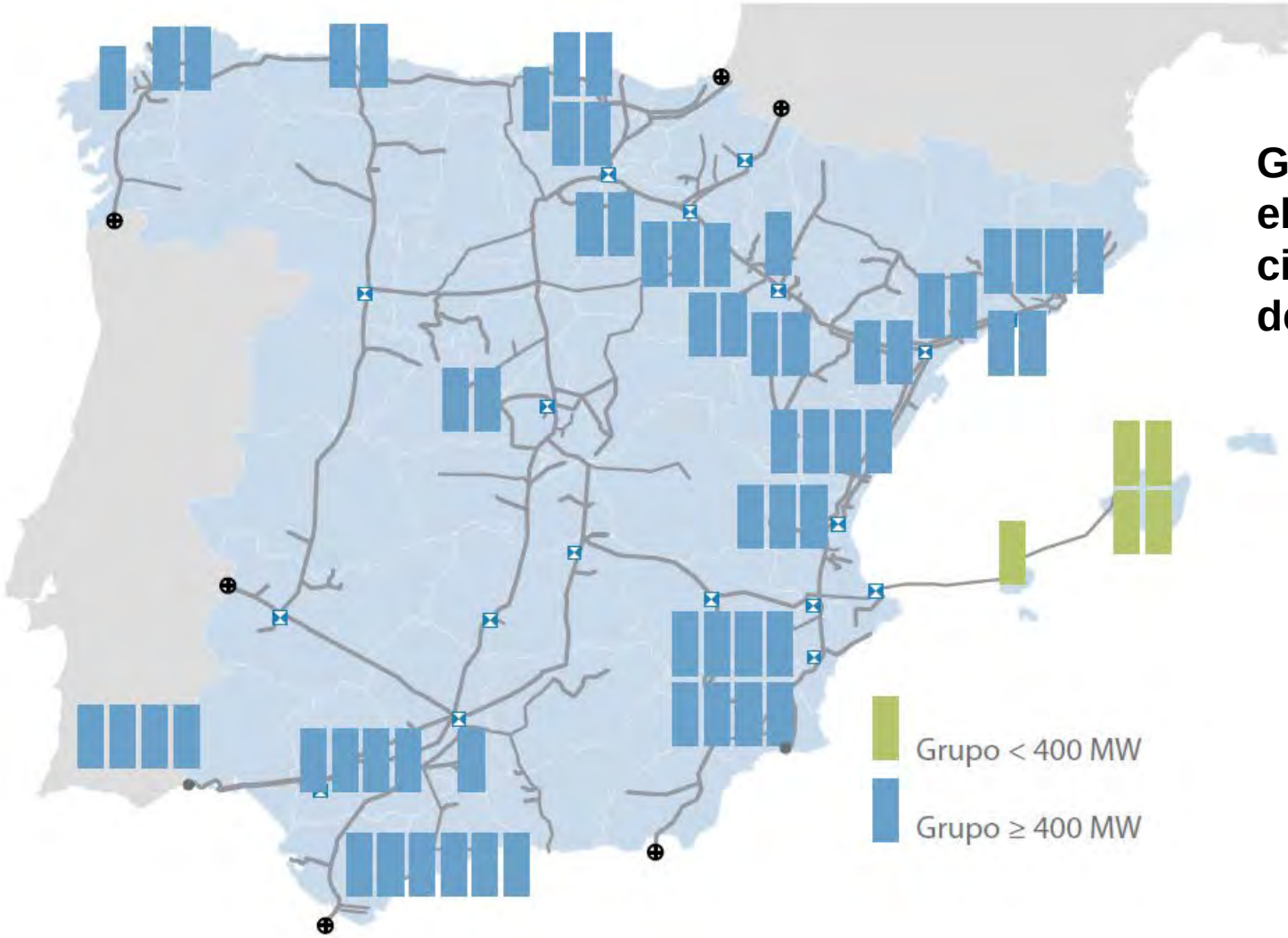
Proyecto 2017-2019

REDCRIT

- Validar una metodología para redes dependientes, donde se analizarán conjuntamente las redes eléctricas y de transporte de gas natural.
- **En España el 25% de la potencia eléctrica instalada en centrales de generación corresponde a centrales de gas natural** y cubrió en años anteriores hasta el 32% de la demanda eléctrica anual del país.

Potencia instalada: 26.251 MW

(67 grupos)



Generación eléctrica con ciclos combinados de gas natural

GESTIÓN ESTRATÉGICA DE LA ENERGÍA ELÉCTRICA

Universidad Zaragoza
1542

Proyecto 2017-2019

REDCRIT

- La metodología desarrollada se aplicará a las redes reales de transporte de gas y electricidad en España para **identificar los elementos críticos de ambos sistemas** y obtener conclusiones sobre la **efectividad de las inversiones propuestas** por los correspondientes gestores de las redes, Enagás S.A. y Red Eléctrica de España S.A. respectivamente.

http://redcrit.unizar.es

REDCRIT: Research on critical energy infrastructures

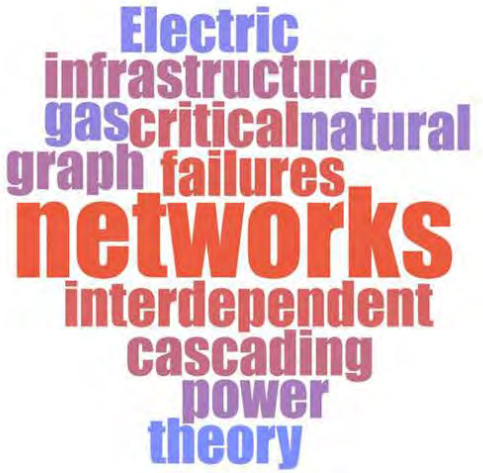
University of Zaragoza, Spain

Buscar ...

PROJECT GOALS TEAM ARTICLES MAPS & LINKS EVENTS

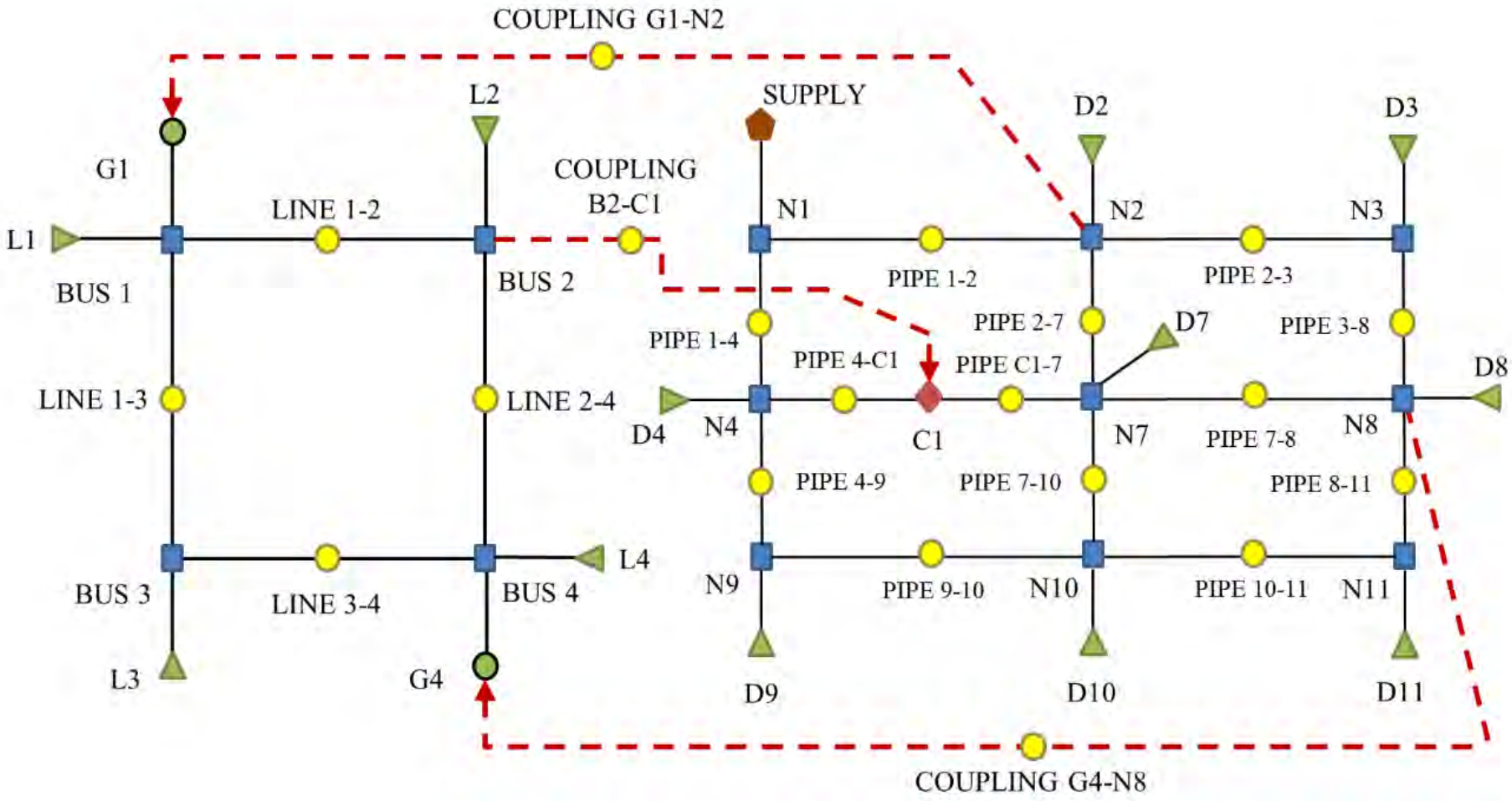
Team

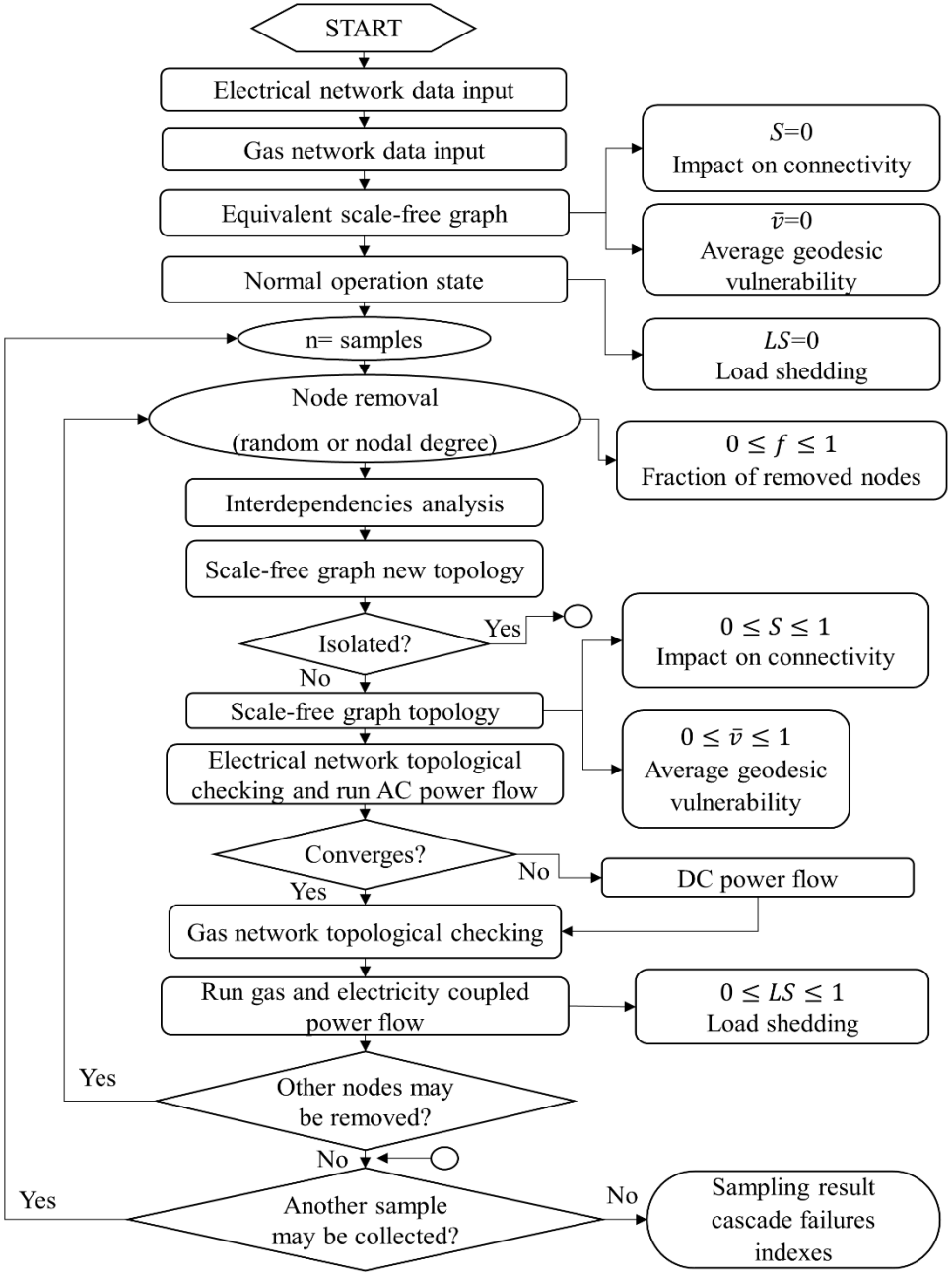
♦ Jose M. Yusta, Associate Professor, Dept. Electrical Engineering, Universidad de Zaragoza (project coordinator)
♦ Jose A. Dominguez-Navarro, Associate Professor, Dept. Electrical Engineering, Universidad de Zaragoza (project coordinator)
♦ Jose L. Bernal-Agustin, Associate Professor, Dept. Electrical Engineering, Universidad de Zaragoza
♦ Ignacio J. Ramirez-Rosado, Professor, Dept. Electrical Engineering, Universidad de Zaragoza
♦ Rodolfo Dufo-Lopez, Associate Professor, Dept. Electrical Engineering, Universidad de Zaragoza
♦ Iván R. Cristóbal-Monreal, Associate Professor, Centro Universitario de la Defensa, Academia General Militar
♦ Juan M. Lujano-Rojas, Researcher, Dept. Electrical Engineering, Universidad de Zaragoza
♦ Jesús Beyza-Bravo, PhD student, Dept. Electrical Engineering, Universidad de Zaragoza

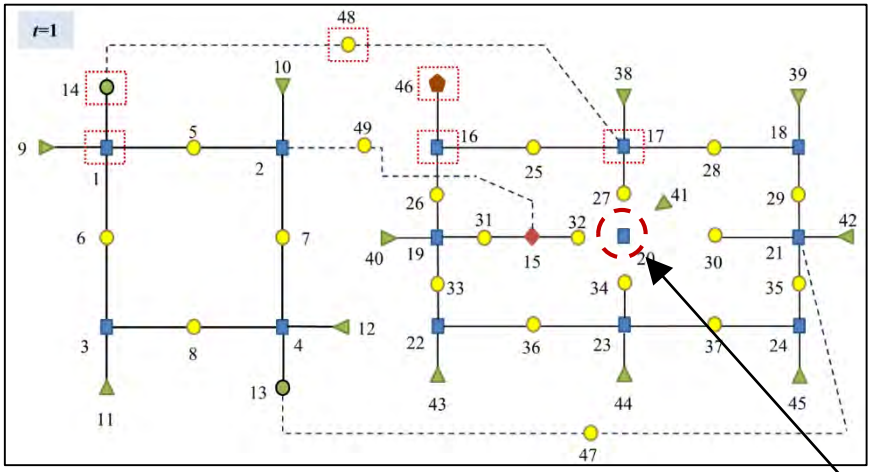


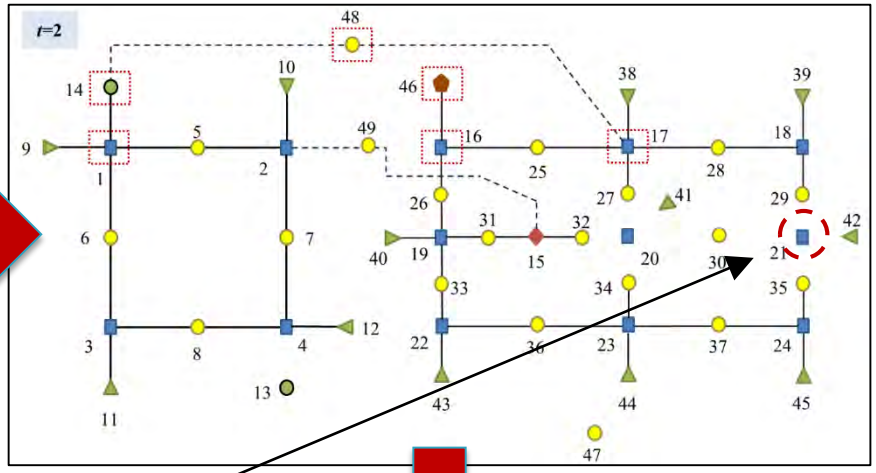
CONTACT

GRAFO DE REDES ACOPLADAS DE GAS Y ELECTRICIDAD

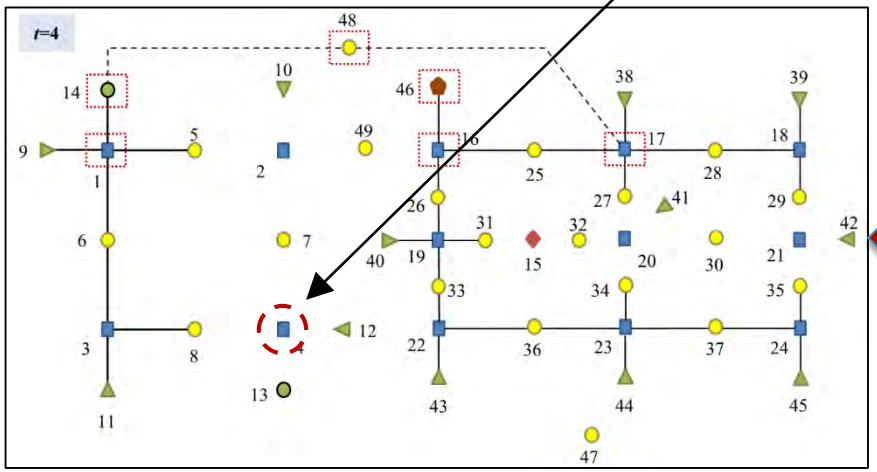


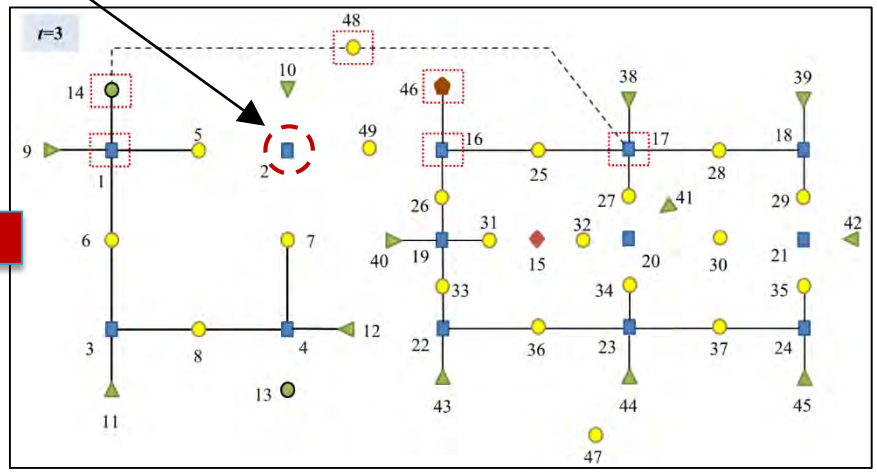

START
Electrical network data input
Gas network data input
Equivalent scale-free graph
Normal operation state
n= samples
Node removal
(random or nodal degree)
Interdependencies analysis
Scale-free graph new topology
Isolated?
Yes
No
Scale-free graph topology
Electrical network topological checking and run AC power flow
Converges?
No
Yes
Gas network topological checking
Run gas and electricity coupled power flow
Other nodes may be removed?
Yes
No
Another sample may be collected?
Yes
No
S=0
Impact on connectivity
v̄=0
Average geodesic vulnerability
LS=0
Load shedding
0 ≤ f ≤ 1
Fraction of removed nodes
0 ≤ S ≤ 1
Impact on connectivity
0 ≤ v̄ ≤ 1
Average geodesic vulnerability
DC power flow
0 ≤ LS ≤ 1
Load shedding
Sampling result
cascade failures
indexes

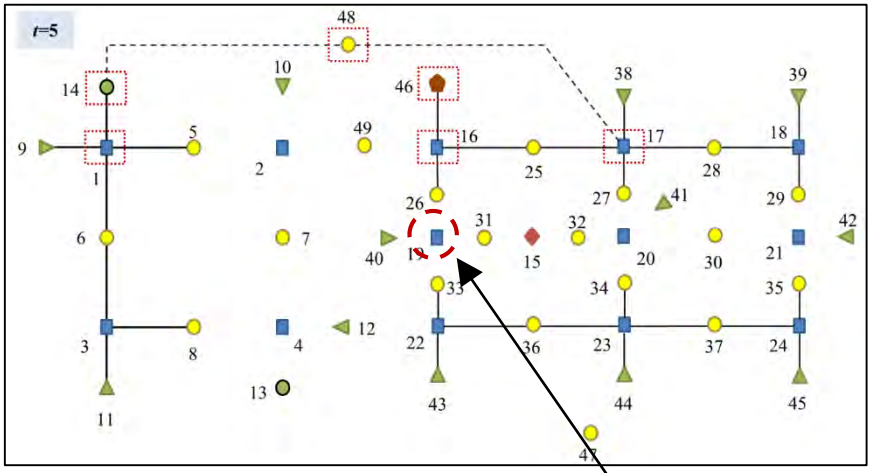


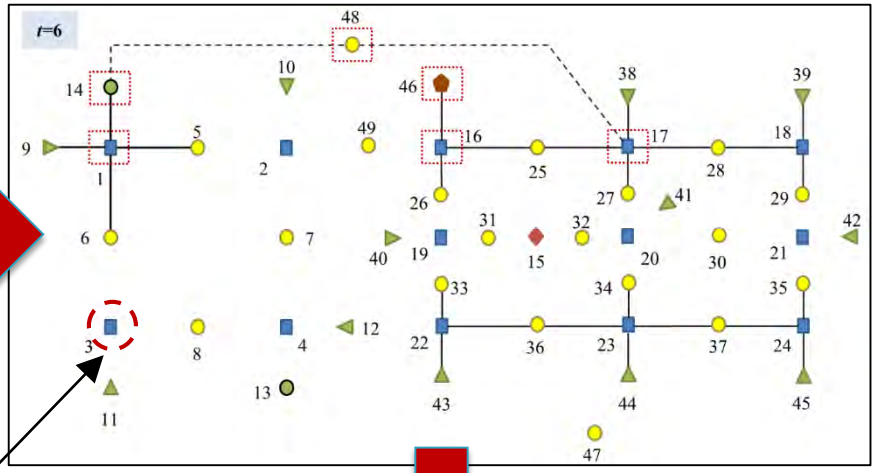


Eliminación

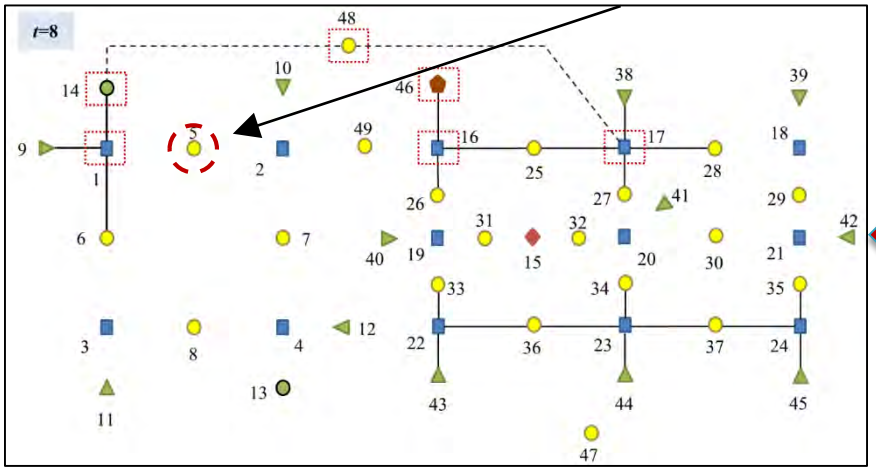


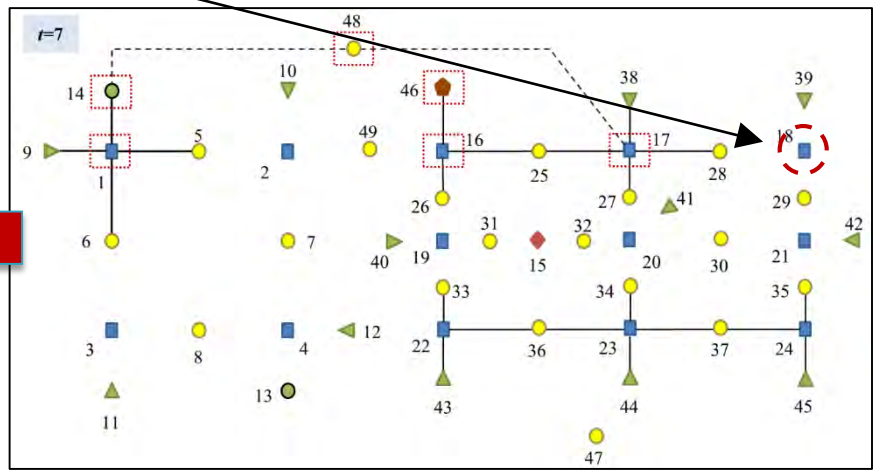


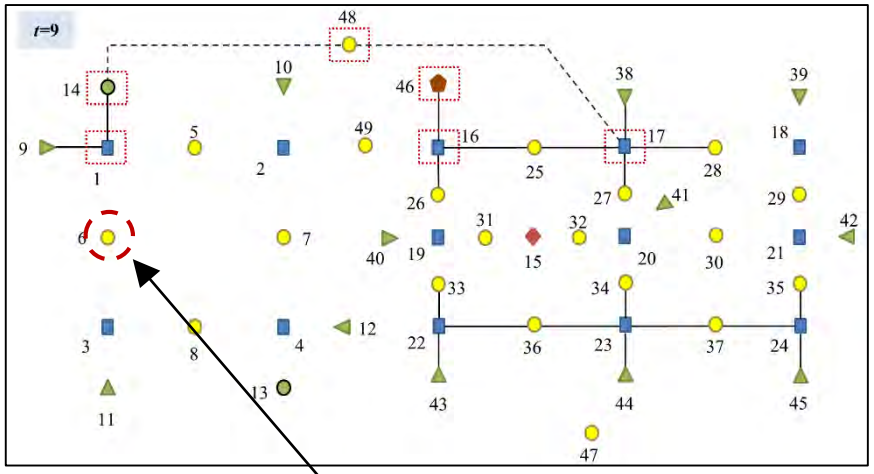




Eliminación

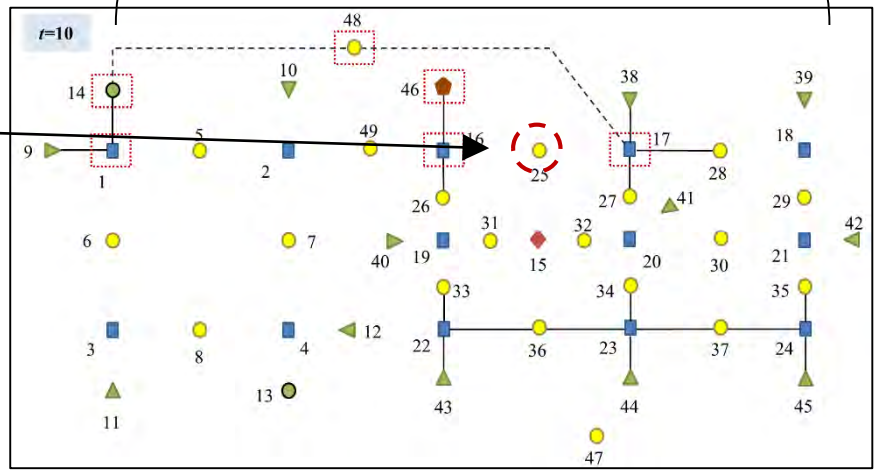


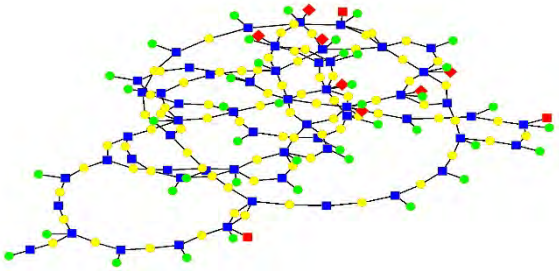
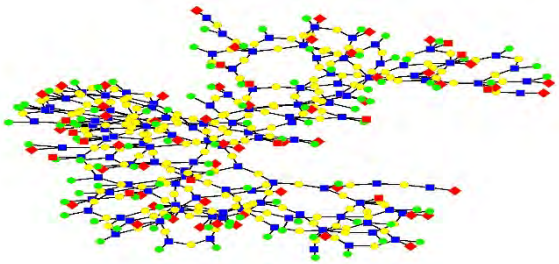
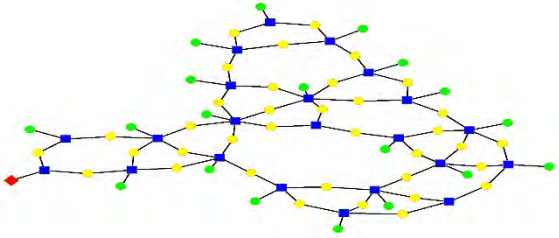
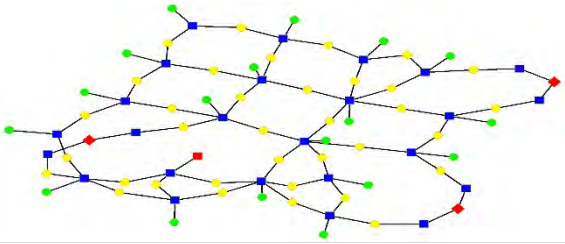


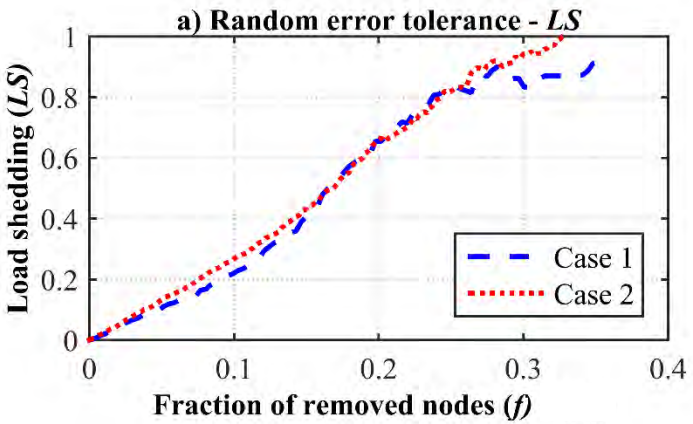


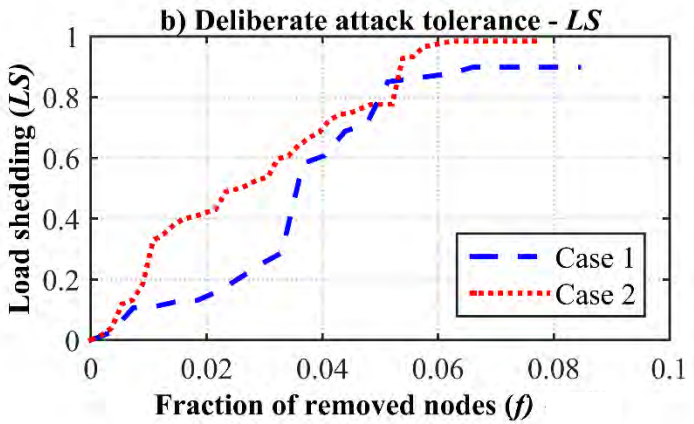
Red desacoplada

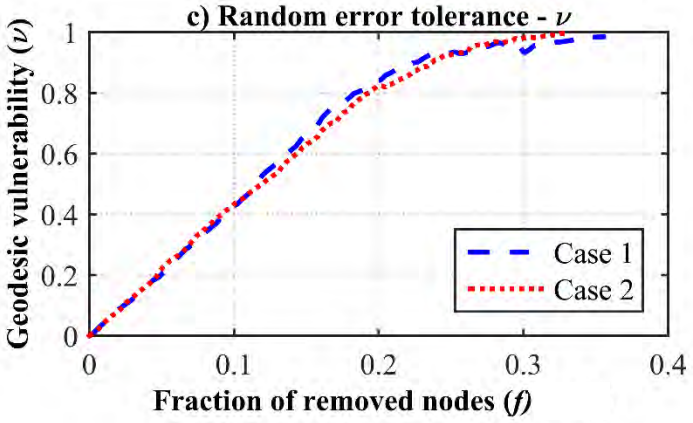
Eliminación

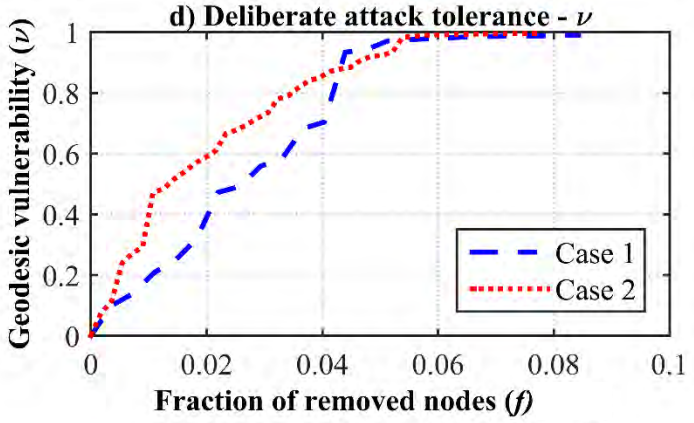


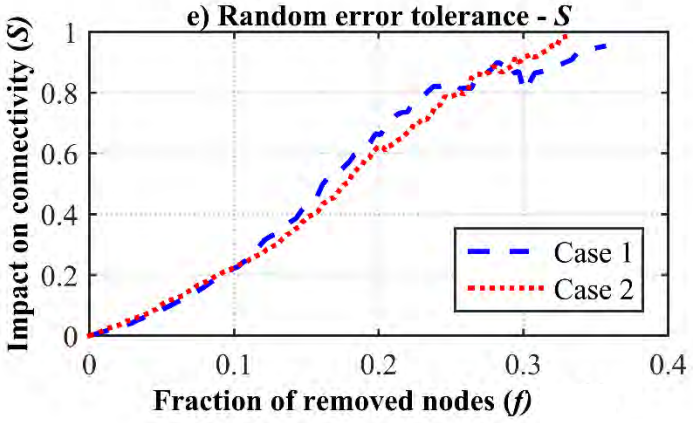
Modelo de red	Grafo de libre escala	Representación
Redes eléctricas		
57 buses: 42 cargas, 17 transformadores, 63 líneas, 3 capacitores, 7 generadores.	189 nodos, 212 enlaces	
118 buses: 99 cargas, 9 transformadores, 177 líneas, 14 capacitores, 54 generadores.	471 nodos, 539 enlaces	
Redes de gas		
22 nodos: 19 cargas no eléctricas, 1 suministro, 36 gasoductos.	78 nodos, 92 enlaces	
25 nodos: 18 cargas no eléctricas, 3 unidades de compresión, 1 suministro, 35 gasoductos.	76 nodos, 89 enlaces	

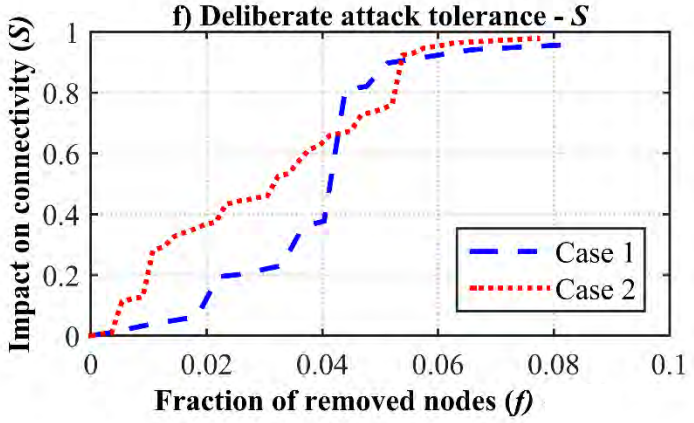

a) Random error tolerance - LS
Load shedding (LS)
Fraction of removed nodes (f)
Case 1
Case 2


b) Deliberate attack tolerance - LS
Load shedding (LS)
Fraction of removed nodes (f)
Case 1
Case 2


c) Random error tolerance - ν
Geodesic vulnerability (ν)
Fraction of removed nodes (f)
Case 1
Case 2


d) Deliberate attack tolerance - ν
Geodesic vulnerability (ν)
Fraction of removed nodes (f)
Case 1
Case 2


e) Random error tolerance - S
Impact on connectivity (S)
Fraction of removed nodes (f)
Case 1
Case 2


f) Deliberate attack tolerance - S
Impact on connectivity (S)
Fraction of removed nodes (f)
Case 1
Case 2

Estrategia de eliminación	Correlación	Caso 1	Caso 2
Aleatorio	$\rho_1(LS, v)$	0.9987	0.9992
	$\rho_1(LS, S)$	0.9759	0.9802
Deliberado	$\rho_1(LS, v)$	0.9805	0.9970
	$\rho_2(LS, S)$	0.9677	0.9754

REDES ESPAÑOLAS DE ELECTRICIDAD Y GAS NATURAL

- **Red eléctrica:** Condición actual de la Red de Transporte (611 nodos y 672 enlaces)
- **Red de gas:** Condición actual de la Red de Transporte (1380 nodos y 1402 enlaces)
- **Red acoplada:** 2031 nodos y 2154 enlaces


MAR CANTÁBRICO
OCEANO ATLÁNTICO
MAR MEDITERRÁNEO
ILHAS AÇORES
ILHAS DA MADEIRA
ISLAS CANARIAS
ISLAS BALEARES
ILLES BALEARS
SISTEMA ELÉCTRICO IBÉRICO
Enero - Janeiro 2014
LEYENDA - LEGENDA

SISTEMA GASISTA ESPAÑOL

Jose Maria Yusta Loyo

Profesor Titular de la Universidad de Zaragoza – Experto en mercados energéticos e infraestructuras críticas

SALUDO | CURRICULUM | MIS CONFERENCIAS | LIBROS | OFERTA SERVICIOS | PRENSA | CO

CONFERENCIA: "VULNERABILIDAD DE INFRAESTRUCTURAS CRÍTICAS DE ENERGÍA INTERDEPENDIENTES", XX SEMINARIO ECONOMIA Y DEFENSA, ZARAGOZA 2018

27 de febrero de 2018 | jmyusta

unizar.es / jmyusta

(http://redcrit.unizar.es)

> (VER PROGRAMA AQUI)

La conferencia ofrecerá una perspectiva de los riesgos asociados a la creciente dependencia entre los sistemas de infraestructuras de transporte de electricidad y de transporte de gas natural, materia que es objeto del proyecto de investigación REDCRIT: Scale-free networks for analysis of vulnerability and resilience of interdependent infrastructures ENE2016-77172-R.

2018