TOWARDS A NATIONAL ECOSYSTEMIC ANALYSIS

Nicolas MAYER
Senior R&T Associate
LIST

11/04/2022

LUXEMBOURG
INSTITUTE OF SCIENCE
AND TECHNOLOGY
LIST

LEGAL CONTEXT: CURRENT SITUATION

NIS Directive

Member States shall ensure that operators of essential services "*take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations*". In addition, the article points out that "*those measures shall ensure a level of security of network and information systems appropriate to the risk posed*". [Article 14]

Supervision of the operators of essential services (OSE) required and operated by the Competent Authority (CA) of the different countries. [Article 15]

Adoption at the national level

Loi du 28 mai 2019 […] concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne [LU]

7 avril 2019. - Loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique [BE]

SUPERVISION CONTEXT

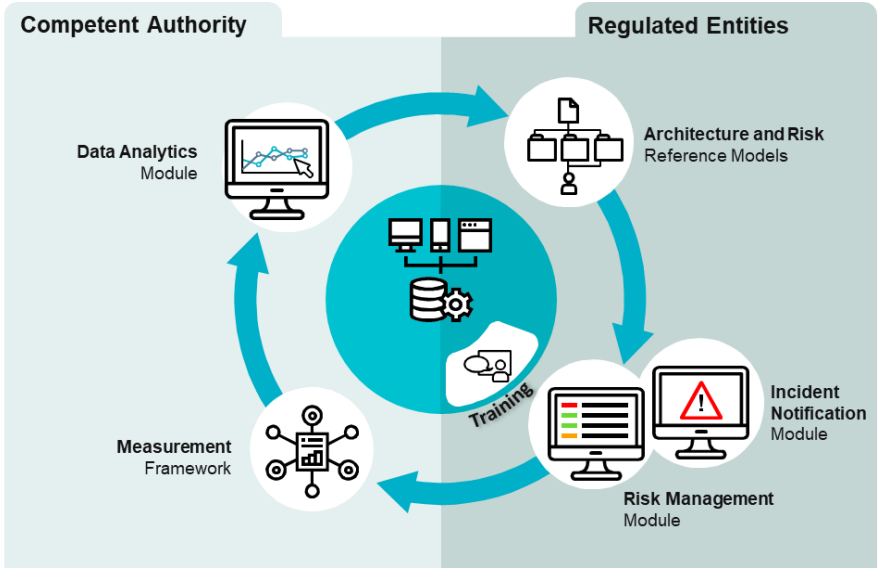
SERIMA, a platform to support both the CA and the regulated entities

How to support regulated entities in managing the risks posed to security of network and IS?

- Built on top of sectoral knowledge
- Integration with other standards and regulations
- Open to evolutions of the regulation and of the technology

How to support the competent authority in gathering, analysing and benchmarking risk reports?

- From raw data to relevant measurements
- Individual report generation for the regulated entities



Fonds National de la Recherche Luxembourg

Supported by the National Research Fund, Luxembourg, and financed by the RegTech4ILR project (PUBLIC2-17/IS/11816300)

LEGAL CONTEXT: COMING SITUATION

NIS 2

NIS 2 (still in negotiation) should add a specific focus on supply chain security:

The measures referred to in paragraph 1 shall include at least the following:
[…]
d) supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers such as providers of data storage and processing services or managed security services;

Member States shall ensure that […] entities shall take into account the vulnerabilities specific to each supplier and service provider […]

The proposed NIS 2 Directive would introduce express requirements to manage third party risks in supply chains and supplier relationships, thus addressing one of the most important challenges facing cybersecurity today.

CHALLENGE

Supply chain security: a more customer-centric approach

It is currently not possible for the CA to be aware of the actual risks harming the end-user (i.e. to have a customer-centric risk approach), which is by essence what is targeted by the regulations (EECC, NIS…).

The aim of the regulation is indeed to try to minimize as much as possible risks taken by the citizens related to the use of essential services, and avoid critical situations such as, e.g., the incapacity to use ventilation support machines in a hospital due to a power outage.

WEAKNESS OF THE CURRENT RM SYSTEM

Local risk management vs ecosystemic risk management

Today, risks are assessed individually by each organization.

No link established between the risk management results of interacting organizations.

Key assumption: Confidentiality of the risk management data between supplier/customer is a must-have.

How to reconcile individual security risk management established by OES in order to identify and analyse systemic risks, coming from dependencies between OES?

PROPOSED APPROACH

Two layers of analysis

Layer 1: Ecosystem modelling and systemic indicators

A graph-based framework dedicated to security and risk analysis of complex ecosystems (e.g., NIS essential services providers at a country level)

Layer 2: Risk cascading and ecosystem risk management

A systemic risk management approach allowing risk cascading between depending organisations and large-scale incident simulation

ECOSYSTEM MODELLING AND SYSTEMIC INDICATORS

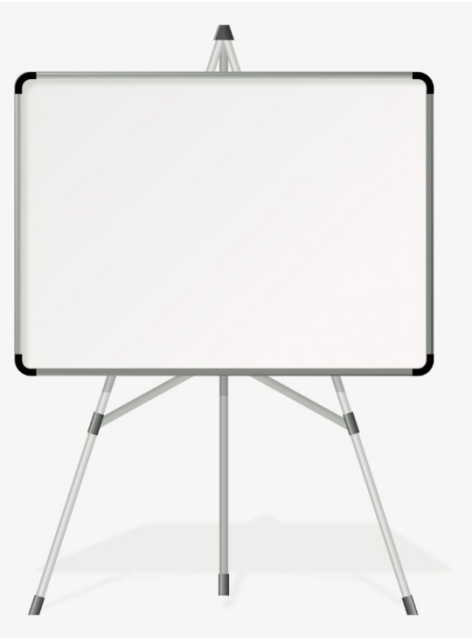
Objectives

We have developed a graph-based framework dedicated to analysis of complex ecosystem (e.g., NIS essential services providers at a country level),

Main features are ecosystem modelling, generation of KPI related to security and risks, and impact assessment (at the service level)

Target users: competent authorities, who are the sole actors allowed to have access to these data

It aims at being interopable with other applications and analysis tools of the CA, e.g., taking into account each individual risk reports or notified incidents



ECOSYSTEM MODELLING AND SYSTEMIC INDICATORS

Concepts at stake

Organization: one specific company or administration. In the frame of the NIS Directive: an OSE (or a DSP).

Service: a service delivered by an organization. In the frame of the NIS Directive: an essential service provided by an OSE.

Sector/sub-sector: the sector of activity of the organization. In the frame of the NIS directive: the NIS sector/sub-sector as depicted in Annex II of the NIS Directive about the types of entities.

Dependencies: the dependencies to services from other organizations / the services provided to other organizations.

Customers: the final users/customers (national citizens) of one or several service(s).

ECOSYSTEM MODELLING AND SYSTEMIC INDICATORS

Examples of questions of interest

What is the **criticality of an organisation / a service of a given organisation** based on the dependencies it has?

How **vulnerable to external outage** is a given organization / a service of a given organization based on the dependencies it has?

What are the **most critical organisations / services** for the ecosystem?

What are the **most vulnerable organisations / services** of the ecosystem?

What are the (internal / external) **dependencies within** a sector/sub-sector?

What are the **dependencies between** 2 sectors/sub-sectors?

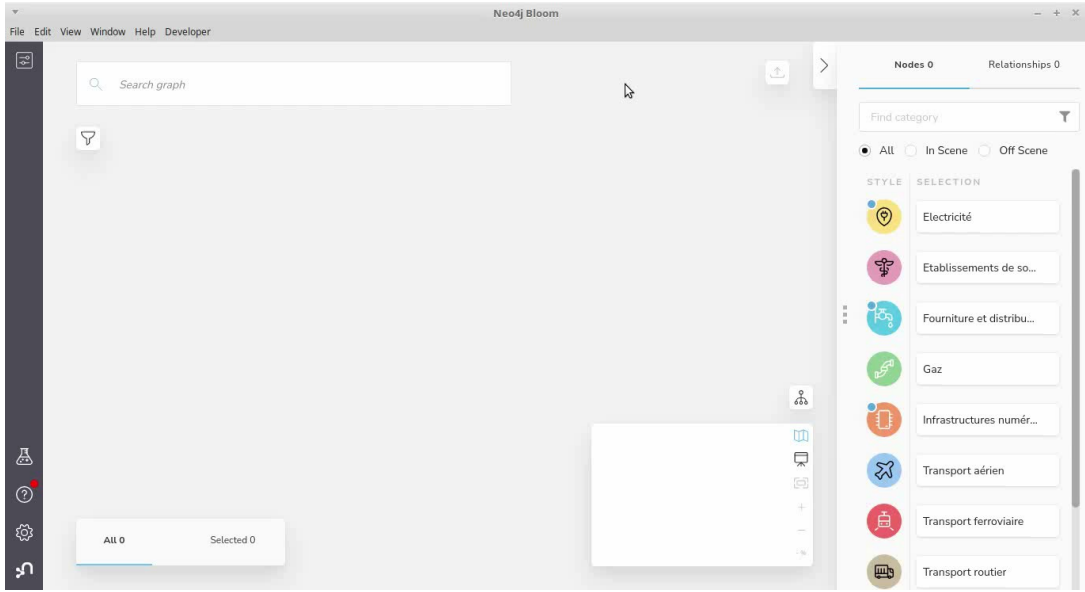
ECOSYSTEM MODELLING AND SYSTEMIC INDICATORS

Example of requests – knowledge of the ecosystem

What are the dependencies of the health sector on the energy sector?

In the health sector, the electricity market is shared between the following actors:

- MidElec : 50%
- WestElec: 30%
- EastElec: 20%



ECOSYSTEM MODELLING AND SYSTEMIC INDICATORS

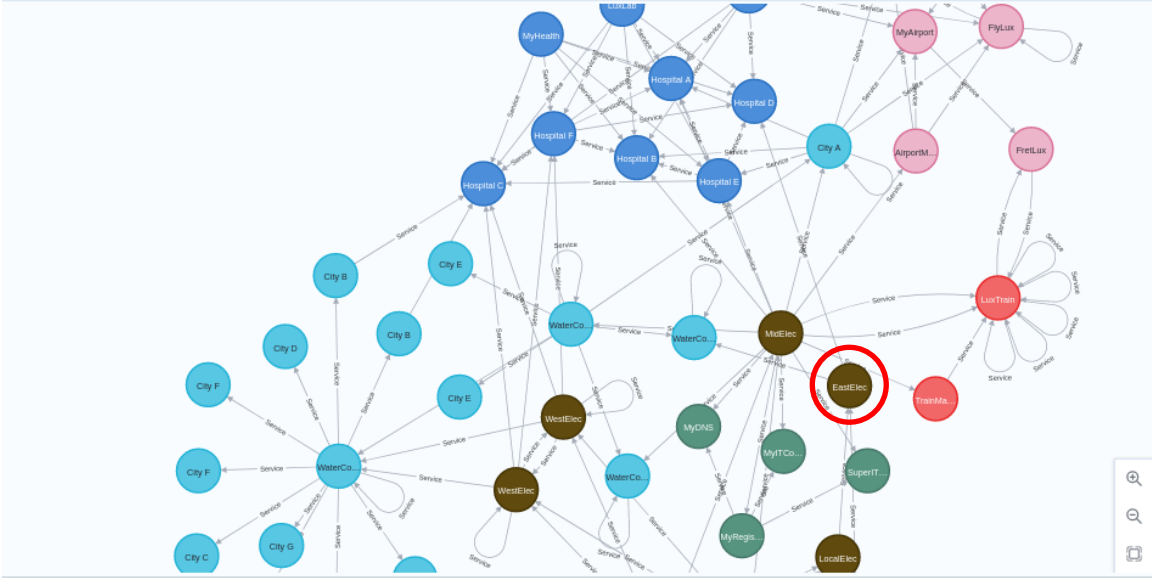
Example of requests – knowledge of the ecosystem

What is the place of *EastElec* in the ecosystem?

42 outgoing dependencies (total)
23 ingoing dependencies (total)

1 service supplied by this organization
12 services used by this organisation (total)

342.800 final users depending of the provided service

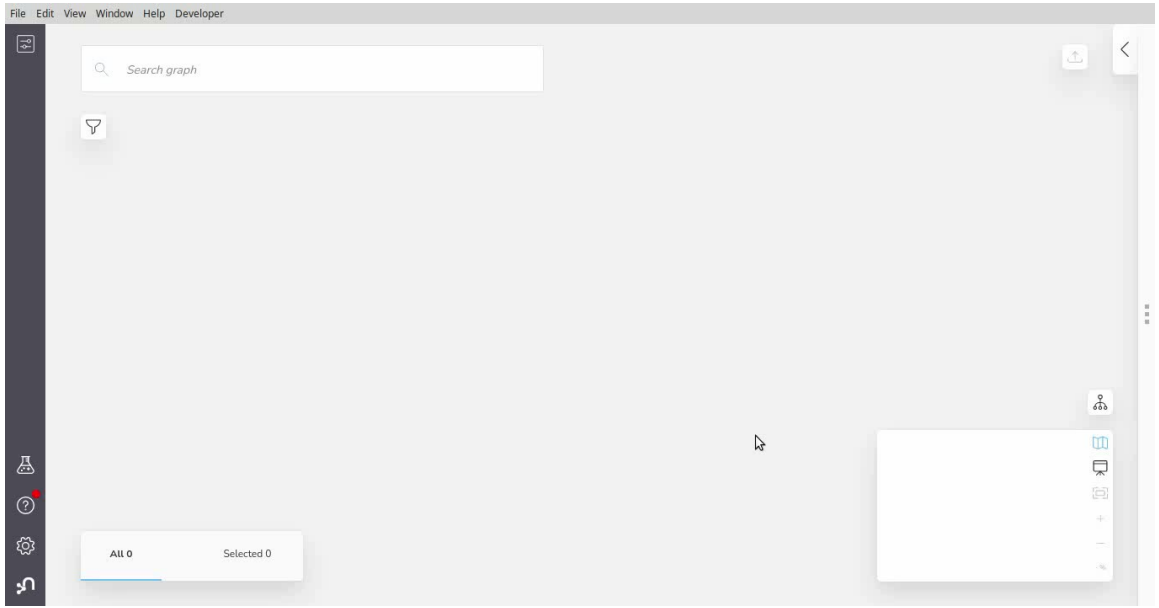


ECOSYSTEM MODELLING AND SYSTEMIC INDICATORS

Example of requests – ecosystem risks and security

How vulnerable is *Hospital A*?

Average risk level of the necessary organizations/services: 7
Number of inherited unacceptable risks: 15
Number of incidents over the past year in the necessary organizations/services: 3



ECOSYSTEM MODELLING AND SYSTEMIC INDICATORS

Open issues and future work

What are the weight of the dependencies (depending services totally down or in degraded mode)?

Integration of risk-related metrics in the graph

User-friendly environment and improvement of the modelling framework (i.e. cognitive effectiveness)

More complete and elaborated software prototype

RISK CASCADING AND ECOSYSTEM RISK MANAGEMENT

Questions and objectives

What are the new/emerging risks coming from propagation of risks due to dependencies between OES? *[Risk identification]*

Are the risk-related assumptions done by service consumers, especially likelihood of risks, sound with regard to their actual assessment by service providers? *[Risk analysis]*

What are the most critical organizations / services / assets in the ecosystem of the sector from a risk perspective? *[Risk evaluation]*

RISK CASCADING AND ECOSYSTEM RISK MANAGEMENT

Proposed approach

Step 1: Dependency modelling

=> Model of the ecosystem with a risk perspective (primary assets, supporting assets, threats…)

Step 2: Risk propagation and systemic risk analysis

=> For each risk of a service provider targeting an asset / function / service used by a service consumer, the resulting risk generated at the level of the service consumer is identified and its level analysed

Step 3: Systemic risk evaluation

=> *Consolidation at the risk identification level and at the risk analysis level by the CA*

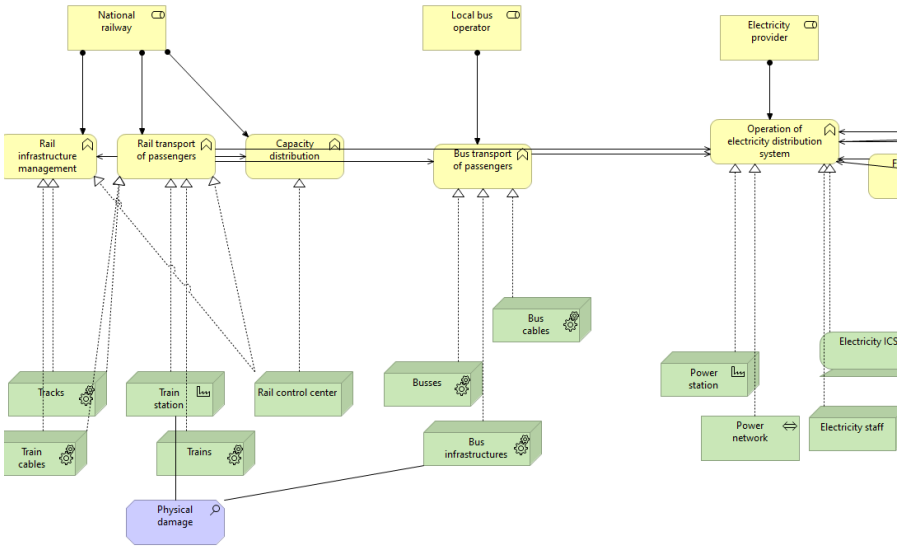
SYSTEMIC RISK MANAGEMENT METHOD

Step 1: Dependency modelling – risk perspective

Sectoral reference model established as a specialisation of an enterprise architecture model.

Reuse and adaptation of the Archimate modelling language (Enterprise Architecture Modelling).

Ecosystem model containing the individual models of each OES, as well as a reconciled view



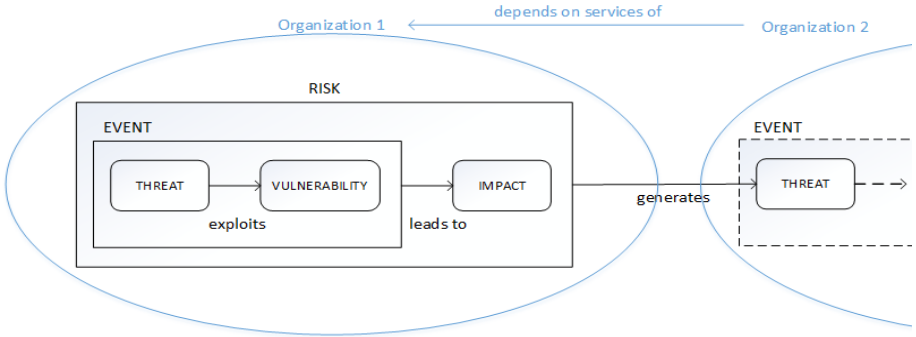
Ref.: Mayer, N., Aubert, J., Grandry, E. et al. An integrated conceptual model for information system security risk management supported by enterprise architecture management. Softw Syst Model 18, 2285–2312 (2019)

SYSTEMIC RISK MANAGEMENT METHOD

Step 2: Risk propagation and systemic risk analysis

The propagation of a risk from OES1 to OES2 leads to the generation of a new threat in OES2, which is the source of risk.

Example: *Company1* identified the risk of cut of a buried communications cable (threat), because this cable is in an area currently under work (vulnerability), leading thus to potential stop of the transmissions (impact). If *Company2* relies on the communications services of *Company1* to provide its own service(s), the previous risk generates the threat of 'loss of telecommunications services' for *Company2*.



SYSTEMIC RISK MANAGEMENT METHOD

Step 2: Risk propagation and systemic risk analysis

Threat generation based on the characteristics of the provided service:
- Active or passive provided service?
- 'Co-location' of equipement?

Threat generation based on the characteristics of the original risk:
- Security criteria harmed by the cascaded risk? (integrity, availability)
- Deliberate or accidental cause of the risk?

Threat generation based on the threat taxonomy provided by ISO/IEC 27005.

	Threat leading to loss of Integrity	Threat leading to loss of Availability
Active service	Transmission and communication errors (accidental cause) Corruption of data (deliberate cause)	Loss of essential services
Passive service	Transmission and communication errors	Loss of essential services
Co-location	*Same threat as initial threat*	*Same threat as initial threat*

SYSTEMIC RISK MANAGEMENT METHOD

Summary and future work

Summary

From an individual risk assessment to a systemic and customer-centric risk assessment.

Constraints and context of the regulation framework.

A 3 steps approach to deal with systemic security risks.

Future work

Consolidate the results and improve/complete the method.

Experiment and validate the approach.

Implementation in software prototype.

Still a lot to be done….

ROADMAP

Research still in progress

Early results obtained in:

- A FNR funded project [RegTech4ILR project (PUBLIC2-17/IS/11816300)]

- A collaborative project with ILR and IBPT

Further experiments currently performed in a European project

- PRECINCT (Preparedness and Resilience Enforcement for Critical INfrastructure Cascading Cyberphysical Threats and effects with focus on district or regional protection)

Complete method, software prototyping and local experiment

- in a new collaborative project in discussion with ILR and IBPT

- in a EU project in submission

thank you

Co-financed by the Connecting Europe Facility of the European Union

contact information

For more info, please contact us at:

Nicolas.Mayer@list.lu

NIS Directive User Community (NISDUC) has received funding from the Connecting Europe Facility (CEF) in Telecom under grant agreement INEA/CEF/ICT/A2019/2072562.

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST