# Improving Cyber Security Risk Assessment by Combined Use of i* and Infrastructure Models

Christophe Ponsard[1], Valery Ramon[2] and Mounir Touzani[3]

[1]CETIC Research Centre, Avenue Jean Mermoz 28, 6041 Gosselies, Belgium
[3]INRAE, Institut national de recherche pour l'agriculture, l'alimentation et l'environnement, Toulouse, France

**Abstract**

In an ever more connected and software controlled world, managing cyber security risks has become critical. Most industrial domains have grown a cyber security risk evaluation process combining its two risk factors (1) the impact on business domain assets and (2) the feasibility of threats at infrastructure level. Many available methods and tools to conduct such analysis rely on a rather bottom-up approach, anchored at the infrastructure level with only coarse grained links with the business domain. This paper explores the benefits of a more balanced approach combining a precise modelling of the business level using i* strategic rationale model, of the technical level using an infrastructure model and of the way the infrastructure layer supports the business layer. We show better reasoning and automation to conduct and update cyber security risks analysis. We implemented our approach on the EBIOS ISO27005 compliant methodology using the open source piStar and IriusRisk community toolset. We discuss our results on a water utility case in the light of related work.

**Keywords**

Cyber Security, Risk Assessment, Goal Modelling, Model-Based System Engineering, Tool Support



## 1. Introduction

The increasing capabilities of connected computer-based systems enable a large range of features and services, but also increase their exposure to cyber security threats. Latest reports confirm the top threats (malware, web-based attacks, phishing) and their evolution towards more pervasive/targeted attacks [1]. As digital technologies have settled at the heart of our systems, ensuring their cyber security has become a key concern in many industrial sectors.

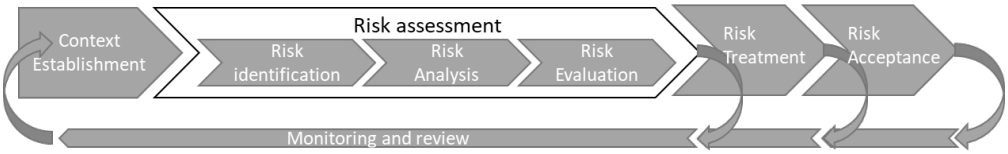


**Figure 1:** Risk analysis process following ISO 27005

Proceedings of the 14th International iStar Workshop, October 18-21, 2021, St. Johns (NL), Canada
christophe.ponsard@cetic.be (C. Ponsard); valery.ramon@cetic.be (V. Ramon); mounir.touzani@inrae.fr (M. Touzani)
0000-0002-0877-7063 (C. Ponsard)

Consequently, many cyber security frameworks and standards have been developed: the ISO27K series [2] for Information Technology (IT) and more recently Operation Technology (OT), i.e. industrial system is being addressed through ISO 63422 or the upcoming ISO 21434 for automotive. Globally, they follow a common scheme based on the risk management process of identifying risks, assessing risks, and taking steps to reduce risks to an acceptable level as depicted in Figure 1. More specifically, it aims at cancelling or at least mitigating the adverse impacts and losses that a deliberate attack, a failure/error or an accidental 'environmental' threat may cause and, where possible, reduce the probability of such events.

A (cyber security) risk analysis involves to investigate two domains:

- *The Business Domain* contains valuable assets (information, process) with different properties to be protected, typically confidentiality, integrity and availability. Analysing this dimension enables the evaluation of the impact factor of threats.
- *The Infrastructure Domain* contains the support assets on which business assets rely. It requires to capture both IT and OT infrastructure and also how it supports the business domain. It helps to evaluate potential attack scenarios and their feasibility.

The use of security modelling has been widely explored and adopted. Attack trees have been introduced to model the attack structure [3]. UML has been extended to capture security properties, e.g using UMLSec[4] and domain specific language have also been defined, e.g. CORAS [5]. Goal-Oriented Requirements Engineering (GORE) languages have also been applied: i* [6] has first been combined with UML [7] and has later developed more specific security extensions such as vulnerability centric framework [8] or Secure Tropos able to deal with socio-technical systems[9]. KAOS obstacle analysis was extended to cope with security using anti-goals [10] and was integrated in other methodologies like CAIRIS [11]. This rich set of models, some with strong semantics and analysis capabilities leads to more precise and complete analysis, and better automation. It is also increasingly possible to connect and populate the models from infrastructure, vulnerability and attack information collected from the real world.

Although not new, deploying a modelling approach may still run into different problems. This paper considers the common case of transitioning from a document-based to a model-based approach for security risk analysts in companies with limited expertise. The goal is to support a qualitative analysis by producing the risk matrix needed to drive the risk treatment phase. Based on a training program involving 30 companies, this paper explores two key issues:

- *selecting the right set of modelling notations* to capture both domain and infrastructure assets: some notations are more focused on the business or technical level. Reaching enough precision might also need to combine and map different models. We report here a modelling exercise combining generic i* modelling for the business level and a standard infrastructure notation for the technical level.
- *supporting the risk-oriented process* and its expected outputs through good automation based on the models and related tools. Our goal is to support EBIOS [12], a specific but simple and very representative implementation of ISO 27005 security risk analysis. We do not consider the risk treatment phase.

This paper is structured as follows. Section 2 gives some background on EBIOS. Section 3 details our experiment in supporting EBIOS analysis using a model-based approach. Section 4 discusses our current results in the light of related work. Section 5 draws some conclusions and presents our future work.

## 2. Background on Risk Assessment with EBIOS

EBIOS ("Expression des Besoins et Identification des Objectifs de Sécurité") is a French method developed by a specific EBIOS community and supported by ANSSI, the national cyber security authority of France [12]. It is compliant with the ISO27005 [2] which is itself based on the generic ISO31000 risk assessment process [13]. EBIOS maps well on ISO 27005. Figure 2 shows that after context establishment, it refines the risk analysis phase in two parallel activities that are then merged to perform risk analysis and treatment:

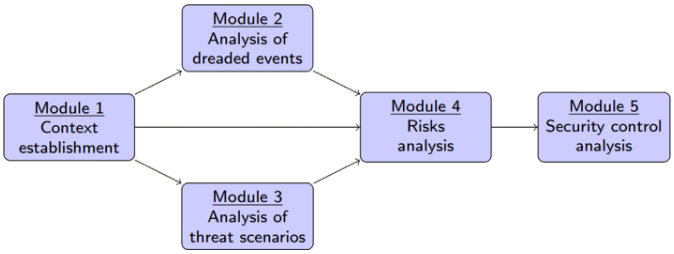


**Figure 2:** Structure of the EBIOS methodology for ISO 27005 compliant security risk analysis

- **context establishment** states organisation goals, analysis perimeter, qualitative scale to measure confidentiality, availability and integrity. Primary (i.e. business) and secondary (i.e. support) assets are identified together with their relationships (i.e. how infrastructure supports business). Secondary assets are classified according to different types (hardware, software, network, people) and the information flows may be depicted using an infrastructure network diagram. The attack complexity is stated in terms of source, expertise, resources. Existing measures are also identified.
- **dreaded event analysis**, the first part of risk estimation, is a top-down approach focusing on the business impact. It estimates the consequences of loss of confidentiality, integrity and availability on primary assets. Threat sources are also identified.
- **threat scenarios analysis**, the second part of risk estimation, is carried out in parallel with dreaded event analysis. It works bottom-up by considering the threat scenarios affecting the support assets, e.g. fishing attempt, firewall configuration problem, OS vulnerability, etc. The feasibility/likelihood is estimated on a qualitative scale defined in the context. Estimates are done before and after the application of existing measures.
- **risk analysis** combines the output of the two previous steps to estimate each risk and produce a risk analysis matrix (see Figure 5). The process can combine multiple scenarios by considering the worst case. At this step prioritisation is done and the type of action decided among the options proposed in ISO 31000 (avoid, accept, mitigate, transfer).
- **security control analysis** selects security controls for risk treatment to cover all risks requiring additional measures using different lines of defense, i.e. prevention, protection and recovery. Guidance is provided using an knowledge base and ISO 27002 list of controls. Residual risk analysis and planning steps are also covered.

## 3. Model-Driven EBIOS Using i* and Infrastructure Models

We consider a simple wastewater utility composed of an OT plant monitoring system using sensor network reporting information and possible alarms to an IT control room for processing alarms and generating accurate daily reports. The security goals are intended to ensure availability (avoid potential pollution and compliance with environmental regulations) and operational safety (integrity). Confidentiality is not considered as the collected information is intended to be public.

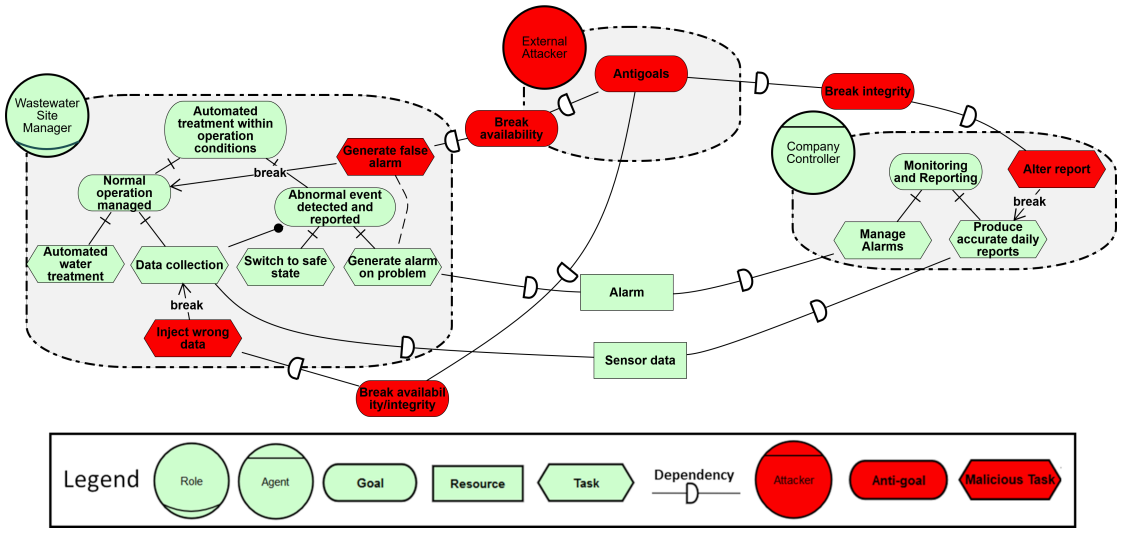


**Figure 3:** i* strategic rationale model of the wastewater treatment utility

In order to provide a simple yet effective modelling, we first capture business assets using an i* strategic rationale diagram shown in Figure 3 and produced using piStar [14]. The EBIOS system and organisation levels are captured using actors, e.g. company controller, or as role, e.g. multiple sites management. Business processes are represented as tasks (e.g collect data, manage alarms) and key information through resources (e.g. sensor or alarm data). Those are related with business goals which help assessing their value and thus the risk impact. We also enrich the model with potential attacker profiles, e.g. external attackers with their motivation using a light notation extension presented in our previous work [15] and inspired by a vulnerability centric framework [8]. An attacker agent is introduced with its motivations captured as (anti-)goals. An attack link is expressed using dependencies linking anti-goals to concrete actionable goals inside the attacked actor to break its goals. All attack-related concepts are coloured in red in order to easily identify them. Linking the business goal with attacker capabilities helps to drive the scenario analysis phase and to more precisely identify exposed support assets in the infrastructure model.

Support assets are captured through an infrastructure model using notations available in many modelling tools. Figure 4 shows such a model built using IriusRisk [16]. It follows the i* model structure: agents are used as top-level containers and an asset-refinement strategy combined with information flow analysis is used to provide a mapping between business

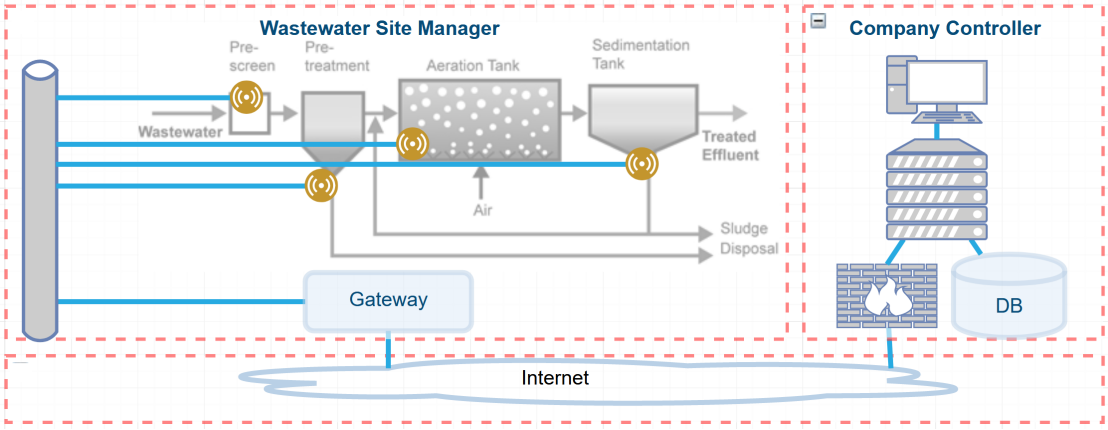


**Figure 4:** Infrastructure model of the wastewater treatment utility

goals/processes/information and supporting computation/communication/storage infrastructure without the need of the explicit mapping matrix required in a document-based EBIOS approach.

The above models can be automatically processed through their JSON or XML output format. We used a Python implementation to perform the following risk analysis steps:

- extract different security impact on business asset from the i* strategic diagram: different assets that are directly or indirectly (through dependum/needed-by links) exposed can be identified and the impact discussed and assessed.
- support IT/OT assets can be traced using the mapping and, for each asset, the technical feasibility of the identified attack can be assessed. Of course, this can require more technical information about existing vulnerabilities/exploitability which is not considered here but supported by tools such as IriusRisk.
- the feasibility and impact information are then combined using the model structure, e.g. considering the weakest link in a communication chain or the presence of technical or business level countermeasures to yield a good risk estimate for each exposed asset. The risk matrix depicted in Figure 5 can then be generated and further analysed for deciding about risk treatment phase.

| IMPACT | | | | | |
|---|---|---|---|---|---|
| | ***4. Critical*** | | Alarm unavailable | Report integrity lost | |
| | ***3. Important*** | | Sensor data integrity lost<br>Sensor data unavailable<br>Report unavailable | | |
| | ***2. Limited*** | | Sensor data unavailable | | |
| | ***1. Negligible*** | | | | |
| | | ***1. Minimal*** | ***2. Significative*** | ***3. Strong*** | ***4. Maximal*** |
| | | ***LIKELIHOOD*** | | | |

**Figure 5:** Typical resulting risk matrix

## 4. Discussion over Related Work

EBIOS provides a textual template with good guidance. However, it does not scale beyond a few primary assets while the number of risks tend to grow quickly. Event considering table-based tool support, it will still lack precision given the rough mapping of between business and support assets and the systematic worst-case risk assessment rule. In contrast, our modelling approach, yet simple, connects both worlds and drives the investigation down to infrastructure level. The richer models also enable more accurate risk estimates although still qualitative. The well-structured EBIOS guidelines [17] could be captured through GORE model patterns [18].

The security analysis of system has been widely analysed by the i* community as overviewed in [19]. As already mentioned, our work builds upon the vulnerability centric framework for dreaded events identification at the business level [8]. Work focusing of Socio-Technical System (STS) are the closest to our research. Secure Tropos has developed the STS approach for modelling and reasoning about security requirements [20]. It combines a precise modelling language capturing contracts constraining the interactions among STS actors and a tooling for reasoning on the model and detecting possible conflicts among security requirements and between security requirements and actors' business policies. Compared to secure Tropos [9], our approach has less reasoning capabilities but aims at more precise connections with infrastructure models which is missing here. However, this dimension is captured by an holistic security requirements analysis framework for STS [19]. The approach is even structured in three different layers: business, software and infrastructure, with specific specialisations of i* concepts across these layers. The approach proposes different refinement strategies based on security properties, assets or time periods. It is supported by a prototype tool. This work can help drive a better mapping between our business and at technical level (mixed software/infrastructure model), at least in a top-down way. However, we believe we should keep an infrastructure domain specific language as technical target while keeping a link with security requirements at that level using i*. The approach should also be enriched with missing bottom-up strategies to address threats originating from the technical level. The qualitative assessment proposed by EBIOS can also fit in to improve the criticality analysis.

Compared to the early CORAS method [5], our work support both business and infrastructure modelling but is more directly anchored towards the production of a risk analysis process as specified in most cyber security standards such as ISO27K or IEC 62443. Finally, compared to the complete CAIRIS platform [11], our work is purposely more lightweight and focused on a specific methodology but anchored in similar GORE modelling principles.

## 5. Conclusion and Next Steps

Our ongoing work to provide model-based support for EBIOS is showing promising results on our wastewater facility. We aim to grow our preliminary tooling into an usable prototype to conduct a validation study about 30 risks analysis that will be compared with another set of risk analysis carried out with a pure document-based approach. This will allow us to identify the real benefits, to provide better guidance and refine the tooling. Finally, the work can be generalised to other risk assessment methods, e.g. for IEC 62443 including zones and conduits.

## Acknowledgments

This work is partly funded by the CYRUS project of the Walloon Region (8227). We thanks the participants (CILE, CCB) of the Belgium NIS workshop of the water domain for their input.

## References

[1] ENISA, Threat Landscape 2020 - List of top 15 threats , 2020.
[2] ISO, ISO/IEC 27001 Information security management, https://www.iso.org/isoiec-27001-information-security.html, 2013.
[3] B. Schneier, Attack trees 24 (1999).
[4] J. Jürjens, UMLsec: Extending UML for Secure Systems Development, in: UML - The Unified Modeling Language, 2002.
[5] F. Vraalsen, et al., The CORAS Tool for Security Risk Analysis, in: Trust Management, 2005, pp. 402–405.
[6] E. Yu, J. Mylopoulos, Enterprise modelling for business redesign: The i* framework, SIGGROUP Bull. 18 (1997).
[7] E. Dubois, N. Mayer, A. Rifaut, Improving risk-based security analysis with i*, in: Social Modeling for Requirements Engineering, MIT Press, 2011.
[8] G. Elahi, E. Yu, N. Zannone, A vulnerability-centric requirements engineering framework, Requir. Eng. 15 (2010).
[9] E. Paja, et al., Sts-tool: Specifying and reasoning over socio-technical security requirements, in: Proc. of the 6th International *i** Workshop 2013, Valencia, Spain, June 17-18, 2013.
[10] A. van Lamsweerde, et al., From system goals to intruder anti-goals: Attack generation and resolution for security requirements engineering, in: RHAS, 2003.
[11] S. Faily, Designing Usable and Secure Software with IRIS and CAIRIS, Springer, 2018.
[12] ANSSI, Expression des Besoins et Identification des Objectifs de Sécurité, https://www.ssi.gouv.fr/uploads/2011/10/EBIOS-1-GuideMethodologique-2010-01-25.pdf, 2010.
[13] ISO, ISO 31000, Risk management - Principles and guidelines, https://www.iso.org/iso-31000-risk-management.html, 2018.
[14] J. Pimentel, pistar tool for i* 2.0, https://www.cin.ufpe.br/~jhcp/pistar, 2018.
[15] C. Ponsard, R. Darimont, Regulation and security modelling of essential services in network of information systems, in: Proc. of the 13th Int. iStar Workshop, 2020.
[16] S. D. Vries, et al., Irius risk, https://www.iriusrisk.com/, 2016.
[17] ANSSI, EBIOS - Knowledge Base, https://www.ssi.gouv.fr/uploads/2011/10/EBIOS-2-BasesDeConnaissances-2010-01-25.pdf, 2010.
[18] R. Darimont, W. Zhao, C. Ponsard, A. Michot, Deploying a template and pattern library for improved reuse of requirements across projects, in: 25th IEEE International Requirements Engineering Conference, RE 2017, Lisbon, Portugal, Sept. 4-8, 2017.
[19] T. Li, J. Horkoff, J. Mylopoulos, Holistic security requirements analysis for socio-technical systems, Softw. Syst. Model. 17 (2018) 1253–1285.
[20] E. Paja, F. Dalpiaz, P. Giorgini, Modelling and reasoning about security requirements in socio-technical systems, Data & Knowledge Engineering 98 (2015) 123–143.