# MANAGING OT CYBER-SECURITY RISKS USING BOWTIES AND RISK & OPPORTUNITY BASED ASSET MANAGEMENT AT DUTCH DSO ENEXIS

Maarten HOEVE
ENCS – EU
maarten.hoeve@encs.eu

Carlos MONTE PORTELA
Enexis – NL
carlos.montes.portela@enexis.nl

Gido BROUNS
Enexis - NL
gido.brouns@enexis.nl

## *ABSTRACT*

*The increasing digitalization of the electricity grid together with the new threats, increases the cyber-security risks related to the distribution of electricity. Major investments need to be made to mitigate these risks. These investments need to be compared with other investments necessary to make the grid ready for the increased use of renewables and electric vehicles and the management of other grid related risks, such as an increasing number of outages due to ageing assets. Cyber-security risks need to be properly assessed to determine the right level of investment.*

*The Dutch DSO Enexis has developed a method to assess cyber-security risks that integrates with their Risk and Opportunity Based Asset Management process. The method uses BowTies, a general method that Enexis also uses for all non-security asset risks. The risk levels are estimated using the asset management risk matrix. In this way, they are made comparable to all other asset risks, so that rational investment decisions can be taken.*

## INTRODUCTION

The increasing digitalization of the electricity grid makes DSOs more vulnerable to cyber-attacks. More and more parts of the grid can be remotely controlled. If not properly secured, these parts could be misused in cyber-attacks. Moreover, many grid control systems have not been designed in a secure way. The systems have a long lifetime, so that there are many legacy components with lacking security, often unpatched.

With these developments, it seems reasonable to assume that the risk of cyber-attacks is also increasing. But this risk is difficult to assess. It not only depends on the vulnerability of the systems, but also on how much effort attackers are willing to spend to hack the grid control systems. The big question is: who would want to hack the electricity grid? Unlike for banks or web shops there is little commercial gain. And there were indeed no serious cyber-security incidents, at least until 2015.

In December of that year, several Ukrainian DSOs were attacked to create a blackout [1] concerning 230,000 people. And then it happened again in 2016. These attacks showed that there are attackers capable of mounting successful cyber-attacks on electricity grid operators, and that these attackers are willing to use this capability to cause power outages.

After the Ukraine attacks, most grid operators are improving the security of the grid control systems. Doing so requires major investments. Grid operators for instance need to segregate their computer networks, install advanced network monitoring systems, and introduce more secure laptops for their engineers. At the same time,

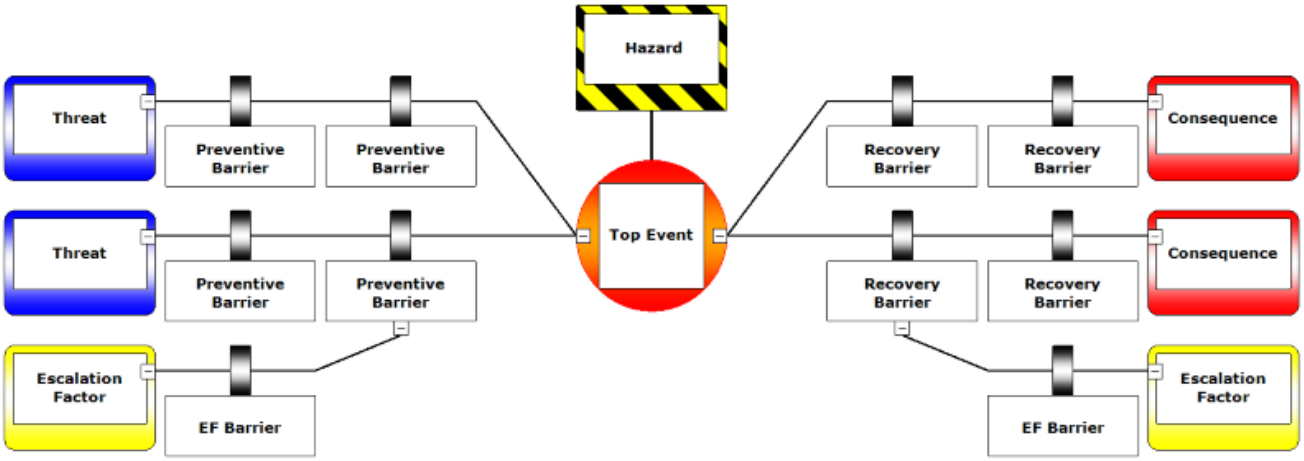


*Figure 1: BowTie diagram with the names of its parts given.*

grid operators also need to prepare for the increased use of renewables and electric vehicles. And in most countries they are closely monitored to increase the efficiency of their spending. Making a rational decision on cyber-security investments with such competing priorities, requires carefully assessing the cyber-security risks to weigh them against the investment costs.

To perform this risk assessment, the Dutch DSO Enexis has developed a method that integrates cyber-security risks into their Risk and Opportunity Based Asset Management (ROBAM) process. The method makes cyber-security risks comparable to other types of risks, such as ageing assets or natural disasters. In that way, decisions on cyber-security investments can be made with the ROBAM process used for all grid investments, so that the right amount of resources is spent on cyber-security.

## BOWTIE METHOD

The method developed at Enexis is based on BowTies [2], a general risk assessment method that Enexis uses in their ROBAM process. Figure 1 shows a BowTie diagram with the names of its parts. The threats that can lead to a security incident are on the left-hand side, the consequences of the incident are on the right-hand side. (See Table 1 for a definition of these terms.) They are connected by a so-called top event in the center, a riskful situation in which the grid operator loses control.

The method Enexis developed to assess cyber-security risks with BowTies, starts at the center with the top event, and then works outwards determining consequences and threats, and finally determining barriers and their effectiveness. These steps will be discussed below.

### Hazards and Top Events

Hazards are derived from information assets. In BowTies, hazards are things that an organization needs for its operations, but that can cause damage if control is lost.

*Table 1: Terms used for BowTies.*

| Element | Description |
|---|---|
| Threat | Something that can cause the top event. For security usually an attacker action. |
| Preventive barrier | Something, usually a security measure, that prevents a threat leading to the top event, or that takes away the threat. |
| Consequence | Possible negative effects of the top event. |
| Recovery barrier | Something, usually a security measure, that prevents the top event leading to a consequence, or that relieves the consequence. |

Grid operators want to remotely monitor and control their substations to reduce cost and recover quicker from failures. But this creates the risk of unauthorized control through cyber-attacks. For cyber-security, the hazards can be directly related to information assets that are processed by the grid control systems. The remote control hazard for instance is related to the switching states and commands processed by the SCADA system.

To ensure all hazards were identified, a systematic analysis was made of all information assets processed by the grid control systems. This analysis was part of the IEC 62443 [3] implementation at Enexis. It was done according to the method for detailed risks assessments in IEC 62442-3-2 [4]. The OT domain was divided into systems, such as the central SCADA servers, and the different types of substations. For each system, workshops were held with employees that know the system to determine which information assets they processed.

Top events were chosen to correspond to compromises of the confidentiality, integrity, or availability of the information asset. Different top events are used for each type of compromise.

Top events were defined per security zone. It is important to have context on where an asset is compromised. Both threats and consequences are different when switching data is compromised in the central SCADA servers or in a substation. The top event thus specified where the compromise happens using the concept of "security zones" from IEC 62443 [4]. A security zone consists of components that have the same security needs. In workshops with specialists on the system, components in a system were placed into zones based on their criticality, function, physical location, and responsible department. Different top events were then defined for compromises in different zones.

### Consequences

Consequences were identified by determining the impact of a compromise of an information asset on operations. Within the BowTie approach, the top event is the moment when the system gets out of control, but before real damage is done. The damage is described in the consequences. In Figure 2, for instance, a compromise of the integrity of switching commands (the top event) can lead to the switching of circuit breakers (a consequence). Workshops were held with specialists on each system to determine for each asset what would happen if its confidentiality, integrity, or availability were compromised.

Leading in this analysis were the impact categories in the Enexis ROBAM risk matrix (see Figure 3). The impact categories (reliability, safety, compliance to law, affordability, customer satisfaction, and sustainability) are

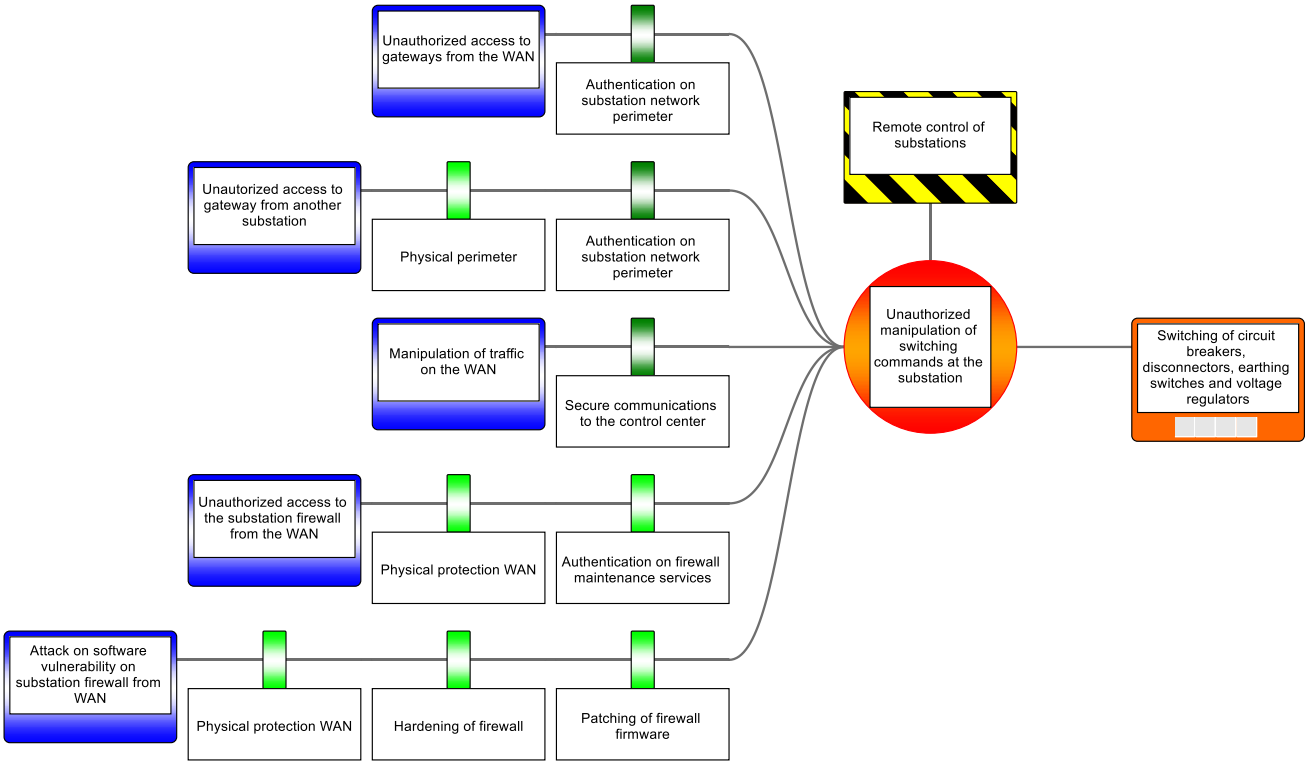


*Figure 2: Example of a filled in BowTie. The BowTie is a generic one for unauthorized access to high-voltage substations. The threats and barriers do not reflect the specific situation at Enexis.*

the core values of Enexis. They are set by the Enexis board of directors in the role of Asset Owner, and recognized by the regulator. Each category can be measured objectively. Thresholds are defined to determine the impact level in each category. In this way, the ROBAM impact categories provide a generally accepted way to assess the consequences of cyber-security incidents.

Although it always required some discussion, the specialists in the workshop could usually agree on the consequences of compromises. Most of the serious consequences came from compromises of integrity. In many cases, they could lead to disruption of electricity distribution, impacting the reliability category. A small number of risks concerning protection equipment also had very serious impact on the safety category.

In some cases the analysis showed that the impact level of such compromises was higher than the ROBAM matrix currently accommodates. The ROBAM impact levels are designed to handle accidental disruptions. The maximum impact level corresponds to an outage of a high-voltage transformer substation for sixteen hours. But in a cyber-attack, the disruptions are intentional. Attackers that penetrate into critical systems will not restrict themselves to one substation, but try to cause outages at all substations they can reach. An incident thus may affect tens or hundreds of substations. An additional impact level “catastrophic” was added properly assess such scenarios.

## Threats

Threats were determined by analyzing possible attacks on each interface to a zone. Within an IEC 62443 zoning model [4], interfaces to other zones are identified. Attacks need to come from one of these interfaces. As different security measures usually are applied at different interfaces it makes sense to assess the threats per interface.

One of the challenges in assessing security risks is to choose in what level of detail to analyze the threats. On a detailed technical level, there are too many threats to analyze. The Common Attack Pattern Enumeration and Classification (CAPEC) developed by MITRE [5] for instance includes 519 attack patterns. Analyzing all of these for each information asset and each interface is clearly not feasible. But using too generic threats may lead to some attack scenarios being overlooked.

In the BowTie approach, the detail level of threats is determined by the possible barriers. Different attack scenarios would be considered as different threats if they require different barriers to be prevented. As Enexis was choosing barriers from the IEC 62443 standard (see next section), the possible barriers were known, and the level of detail of threats could be determined well.

In Figure 2, there are for instance unauthorized access threats corresponding to authentication measures, manipulation of communication threats corresponding to

**Risicomatrix Enexis 2018**

| Potentiële gevolgen | | | | | | | Frequentie of kans van optreden | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | Vrijwel onmogelijk | Uitzonderlijk | Zelden | Incidenteel | Jaarlijks | Maandelijks | Dagelijks |
| Categorie | Betrouw-baarheid | Veiligheid | Wettelijkheid | Betaal-baarheid | Klant-tevredenheid | Duurzaamheid | Nooit eerder van gehoord in industrie | Wel eens van gehoord in industrie | Wel eens gebeurd binnen Enexis of sector | Meerdere malen gebeurd binnen Enexis | Eén tot enkele malen per jaar binnen Enexis | Eén tot enkele malen per maand binnen Enexis | Eén tot enkele malen per dag binnen Enexis |
| | | | | | | | <0,001/jr | ≥0,001/jr <1% | ≥0,01/jr 1-10% | ≥0,1/jr 10-50% | ≥1/jr 50-90% | ≥10/jr 90-99% | ≥100/jr >99% |
| Desastreus | >20.000.000 vbm (HS/MS station >16 uur uitval) | Ongeval met een of meerdere doden tot gevolg | Stille curator; Strafzaak tegen directielid; Geldboete ACM >0,1% omzet | Schade groter dan 10M euro | Internationale commotie; >20.000 klachten | Emissie >250 kton $CO_2$ | L | M | H | ZH | O | O | O |
| Ernstig | 2.000.000 tot 20.000.000 vbm (HS/MS station 4 uur uitval) | Ongeval met ernstig, blijvend letsel (langdurig verzuim) | Aanwijzing of Waarschuwing bevoegd gezag; Geldboete 6* categorie | Schade van 1M tot 10M euro | Nationale commotie; 2.000 - 20.000 klachten; Conflict >10 gemeenten of meerdere provincies | Emissie 25 - 250 kton $CO_2$ | V | L | M | H | ZH | O | O |
| Behoorlijk | 200.000 tot 2.000.000 vbm (MS-T station 4 uur uitval) | Ongeval met letsel met verzuim | Onderzoek bevoegd gezag; Geldboete 4* of 5* categorie | Schade van 100k tot 1M euro | Regionale commotie; 200 - 2.000 klachten; Conflict 2 - 10 gemeenten of 1 provincie | Emissie 2,5 - 25 kton $CO_2$ | V | V | L | M | H | ZH | O |
| Matig | 20.000 tot 200.000 vbm (MS-D streng 4 uur uitval) | Ongeval met EHBO (geen verzuim) of Ernstig incident (HSE) | Geldboete 2* of 3* categorie | Schade van 10k tot 100k euro | Lokale commotie; Interne commotie; 20 - 200 klachten; Conflict 1 gemeente | Emissie 0,25 - 2,5 kton $CO_2$ | V | V | V | L | M | H | ZH |
| Klein | 2.000 tot 20.000 vbm (netstation 2 uur uitval) | Incident (HSE) | Geldboete 1* categorie | Schade van 1.000 tot 10.000 euro | 2 - 20 klachten | Emissie 25 - 250 ton $CO_2$ | V | V | V | V | L | M | H |

*Figure 3: Enexis risk matrix (in Dutch). The impact levels are in the rows, the probability levels in the columns.*

communication security measures, and software vulnerability threats for patching measures. As each threat corresponds to different measures, they are treated separately. But if for instance the software exploit threat would be split into different more detailed attack types (overflows, web attacks, …), all these new threats would be countered by the same measures. Hence, it is more efficient to keep them grouped together.

## Barriers

Barriers were selected from the IEC 62443-3-3 standard [6]. Barriers are measures that prevent a threat leading to a top event (preventive barriers), or prevent a top event leading to a consequence (recovery barriers). For security risks, barriers are usually security measures. Enexis selected these security measures from the IEC 62443-3-3 standard for system security requirements. The authentication barriers in Figure 2 for instance correspond to the human or software user identification and authentication requirement (SR 1.1 and 1.2) in IEC 62443-3-3. The hardening barrier corresponds to the least functionality requirement (SR 7.7).

The advantage of this standard was that the measures were tailored to industrial control systems. Moreover, the standard includes technical measures that are better suited to the detailed analysis performed than the organizational measures in the ISO 27002 [7] and 27019 [8] standards. The use of IEC 62443 also fits well in the security strategy for the Enexis OT domain, which is centered around a cyber-security management system based on IEC 62443-2-1 [3].

One lesson learned was to set a common baseline of security measures for all zones. The IEC 62443 standard assumes that security measures are chosen individually per zone. But keeping track of all measures quickly became a large burden, as some systems had up to 15 zones. Instead, a baseline of measures was selected for modern and for legacy zones that ensures the minimum level of security that Enexis aims to achieve. Only deviations from these baseline were analyzed and documented.

## Barrier Effectiveness

Barrier effectiveness was estimated based on the condition of the security measures. Estimating the effectiveness turned out to be one of the largest tasks. The effectiveness indicates how difficult it is for an attacker to bypass a barrier. Four levels of effectiveness were defined from “very poor” (can be bypassed in a few hours) to “very good” (would require at least several months to bypass). The effectiveness is indicated by the color in Figure 2: light green is good, dark green very good.

For each barrier the effectiveness was estimated together with the administrators of the systems. The effectiveness of the authentication measures in Figure 2 for instance depends on the strength of the passwords or keys used. The effectiveness of the patching barrier depend on how up to date the security patches are. In this way, barrier effectiveness captures a lot of information about the security of the system.

The barrier effectiveness was combined with threat intelligence to estimate the probability of threats. The Enexis ROBAM risk matrix requires a quantitative risk estimate, at least up to an order of magnitude. Most security risk assessment methods avoid making quantitative estimates. For the BowTie method quantitative estimates were made, in two steps.

First, the probability that attackers make a certain effort to attack a DSO was estimated based on historical incidents. For instance, the cyber-attack in Ukraine took several months of work by professional attackers. So, an attack with this much effort happened at least once in the industry. The ROBAM matrix translates this into a probability of between 0.1% and 1% per year.

Second, the amount of effort needed to accomplish a certain threat was estimated by summing up the effectiveness of all barriers between the threat and consequences.

Combined, the estimates gave a probability of each threat. Together with the impact levels for the consequences, the risk level of each threat could be determined with the ROBAM risk matrix. In this way, the risk of security threats becomes comparable to all other risks in the Enexis ROBAM risk register.

The analysis showed that all major security risks are high impact, low probability events. All security events fall in the lowest three probability categories. Because some have a very high impact level, they can still pose a serious risk.

## OUTCOME

All grid control systems at Enexis were analyzed with the BowTie method, leading to a comprehensive view of all cyber-security risks. The risks were entered in the Enexis Asset Management risk register, alongside all other risks, and are now part of the regular risk based ROBAM risk management processes.

Several of the cyber-security risks identified came out as high. Major investments are being taken to mitigate these risks, based on the risk assessment framework. The use of the same method as used throughout the Enexis ROBAM method made the decision about these investment easier. Because an accepted process was followed, there was confidence that the identified risks were correctly estimated. The regulator also appreciated the way that risks were made transparent and comparable.

Enexis will further extends the BowTie method in 2019 in two ways. Firstly, the effectiveness of barriers will be explicitly measured. Currently, effectiveness estimates are based on expert judgement. As a next step, indicators for the barrier effectiveness will be defined that can be objectively measures through penetration tests, vulnerability scans, or organizational audits. Secondly, planned improvements to barriers will be added into the BowTies. In this way, the BowTies are even more explicitly linked to improvement projects and investments.

Enexis is structurally following up the implementation of the mitigations with their IEC 62443 based cyber-security management system (CSMS). Deciding on investment is only the first step. A structured approach is needed to follow up, and ensure that the required technical and organizational changes are really made. The combination of the BowTie Risk assessment method with the IEC 62443 CSMS has led to major improvements in security for Enexis. Security risk management is now part of a regular cycle at the core of Enexis's business processes. The BowTies are reviewed periodically and after major changes in the system to assess changes in the risk. In this way, security risks can be kept at acceptable level also in the future when new threats may arise.

## REFERENCES

[1] E-ISAC, 2016, "Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use case"

[2] CGE Risk, 2016, "The bowtie method." www.cgerisk.com/knowledgebase/The_bowtie_method

[3] IEC, 2010, "IEC 62443-2-1: Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program."

[4] ISA, 2015. "ISA 62443-3-2: Security for industrial automation and control systems – Security risk assessment for systems design. Draft 6, Edit 3."

[5] MITRE, 2018, "Common Attack Pattern Enumeration and Classification." capec.mitre.org

[6] IEC, 2013, "IEC 62443-3-3: Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels."

[7] ISO/IEC, 2013, "ISO/IEC 27002: "Information technology – Security techniques – Code of practice for information security control"

[8] ISO/IEC, 2017, "ISO/IEC 27002: "Information technology -- Security techniques -- Information security controls for the energy utility industry"