ENCS and Enexis: bringing structure to distribution automation cybersecurity requirements

A case study

ENEXIS
ENERGIE IN GOEDE BANEN

ENCS

In March 2015, Dutch Distribution System Operator (DSO) Enexis had a challenge. It was planning to tender for the supply of new distribution automation (DA) equipment and needed to make sure the technology was secure. The problem was that, without an agreed set of requirements, it was difficult to know exactly what to ask for in the tender from a security perspective. The manufacturers could build what was needed, sure enough, but without applicable security requirements available, they needed guidance from Enexis to ensure they met their security needs.

Enexis wanted to find the right balance between mitigating cybersecurity risks and higher costs because of additional security requirements. Without guidance, Enexis ran the risk of leaving security flaws in the DA equipment or having too strict security requirements that would limit the number of possible vendors.

Fortunately, as a member of the European Network for Cyber Security (ENCS), Enexis had collaborated with six other utilities and network operators across Europe to share experiences and best practices for DA cybersecurity. This created a set of aligned requirements for just this type of process. Working closely with ENCS as an impartial third party, Enexis was able to use the requirements to successfully procure equipment that met the security requirements of Enexis taking into account the criticality of the use cases involved.

The result was a more secure DA system and a smoother procurement process, delivered at only a marginal extra cost – avoiding the inflated security premiums usually assumed to go hand-in-hand with top security.

...Working closely with ENCS as an impartial third party, Enexis was able to use the requirements to successfully procure equipment that met the security requirements of Enexis taking into account the criticality of the use cases involved.

Setting the security requirements for procurement

In 2015, ENCS asked its members about problems they had in ensuring cybersecurity was properly represented during the procurement process for DA equipment, encompassing medium voltage transport and transformer substations.

The common response was that, while DSOs wanted to hear about the equipment's cybersecurity capabilities from the manufacturers, the manufacturers were waiting for guidance from the DSOs on what security protocols they needed to build in. With no clear set of procurable requirements on either side, the cybersecurity aspect of the tender was a lengthy back-and-forth process, often producing more headaches than progress.

Inspired by the success of a similar initiative for smart meter requirements in the beginning of 2015, ENCS embarked on a project to develop a set of security requirements for the procurement of DA equipment (remote monitoring and control equipment).

Member led approach

The approach was to bring all ENCS members together to work on the project. Though vendors were to be consulted the feasibility of requirements in a market scan, ultimately it was the DSOs who led the project and determined the security measures required.

Harmonisation

Another key proof point for the project was to achieve harmonisation or consistency between the DSOs. The adoption of common requirements would not only simplify processes but could also lead to cost savings. For instance, the common security requirements used by all Austrian DSOs gives them more market power in relation to vendors. The aim was to harmonise these with other countries, with an eventual goal of having common core requirements that could be adapted to national needs.

Technology agnostic

Finally, ENCS wanted to ensure the resulting requirements were independent of any particular technology. This is because the requirements specify what security measures are needed, not how the measures should be implemented, meaning the requirements can be used for different technologies and communication protocols. This would give individual DSOs the freedom to implement security in a way that would fit with their procured solution.

That was the theory behind the project – what was needed was an opportunity to put it into practice.

Enter Enexis

Enexis one of the frontrunners in Europe in implementing DA in practice, had a procurement round starting soon after the project concluded. ENCS prepared a preliminary version of the resulting requirements so they could be incorporated into the process, tweaking them slightly according to the specifics of Enexis' architecture and risk mitigation objectives. Finding the right balance between risks and costs is something Enexis is always on the lookout for.

"Along with the other members and the ENCS team we put a lot of work into creating the tender requirements," said DSO Security Officer Philip Westbroek of Enexis. "We were optimistic about the improvements they would make, and were glad to work collaboratively with ENCS in implementing them throughout the tender. We're very happy with the results, and that's why we continued to use the requirements for conducting other tenders like the DALI tender[1] that we have recently published."

Back in 2014, Enexis had procured DA equipment for medium voltage transport systems. ENCS provided support at the time, reviewing the requirements and attending the selection interviews with manufacturers. The tender was successful, but Enexis felt that it needed an even better grip on security, and an even better way to evaluate manufacturers and their equipment in the future.

So there was a clear benchmark for success for this tender, which was for similar DA equipment in medium to low voltage transformer substations. If the overall process proved to be easier and the resulting equipment more secure, then the requirements would have been successful.

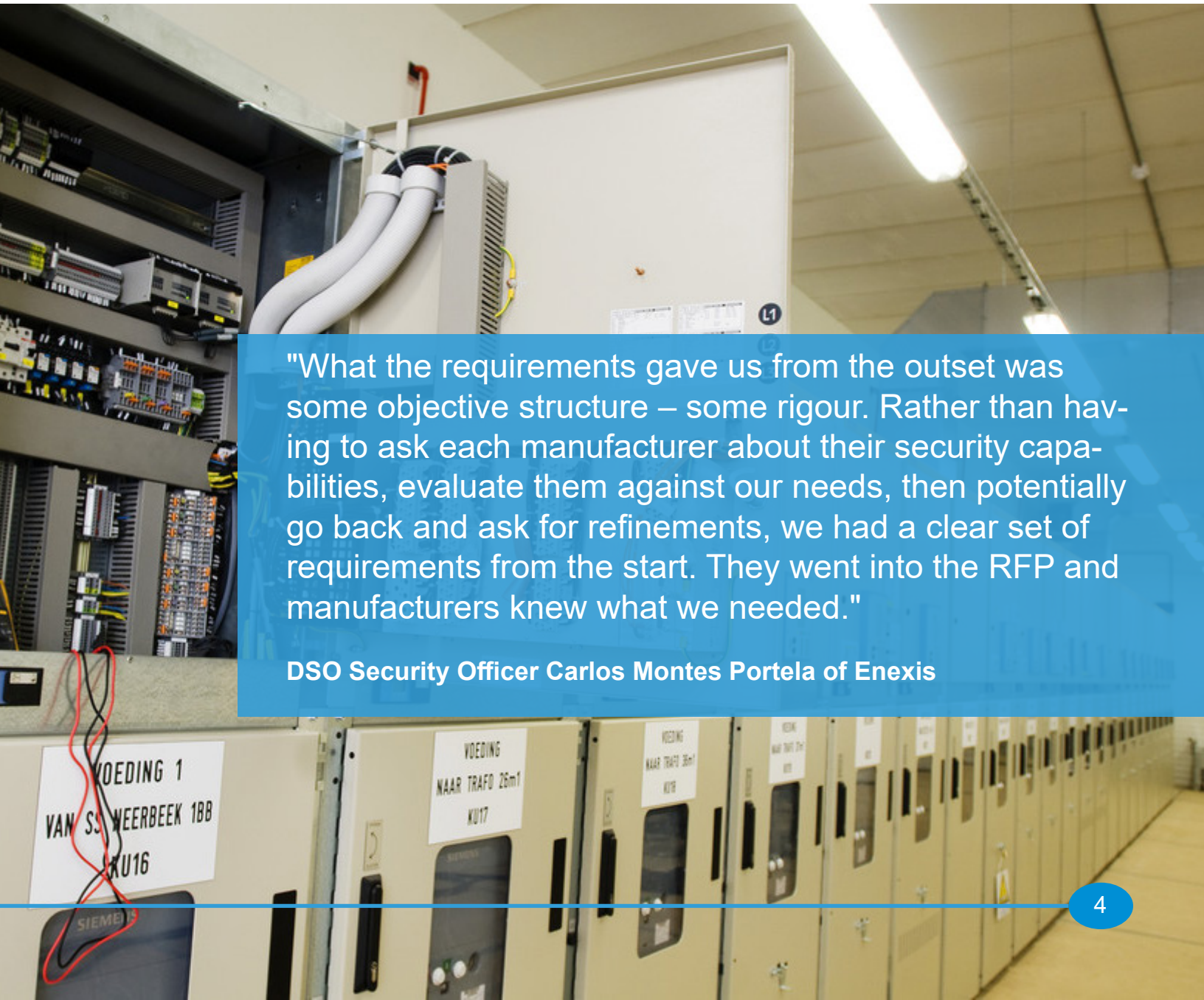
"What the requirements gave us from the outset was some objective structure – some rigour," explained DSO Security Officer Carlos Montes Portela of Enexis. "Rather than having to ask each manufacturer about their security capabilities, evaluate them against our needs, then potentially go back and ask for refinements, we had a clear set of requirements from the start. They went into the RFP and manufacturers knew what we needed."

[1] In the DALI programme the MV stations are equipped with an intelligent monitoring and control unit which can, among other things, control PL (Public Lighting), read out transformer kWmax and send information from short-circuit detectors to the Operations Centre (OC). The controls for the illumination programmes are then no longer supported by tone frequency but by mobile technology. This makes new functionalities possible. More information can be found on enexis.nl/dali.

As well as building the requirements into the RFP (request for proposal), Enexis also asked ENCS to assist in the manufacturer interview process, enabling an even more objective and comprehensive evaluation of the offered solutions by the vendors.

“From our perspective, we were happy to support Enexis during the interview stage,” said Michael John, ENCS’ Director of Consulting Services. “We wanted to see the new requirements used in a tender process first hand, to make sure that we were meeting members’ needs. We wanted to make sure they did what they were supposed to, and be there to fill any gaps.”

As it happened, there weren’t any gaps, but ENCS’ presence and expertise helped the process proceed more smoothly and quickly than it might have otherwise. By having a non-profit, impartial third party, both Enexis and the manufacturer could be confident that requests were reasonable and needs were met from both sides.



"What the requirements gave us from the outset was some objective structure – some rigour. Rather than having to ask each manufacturer about their security capabilities, evaluate them against our needs, then potentially go back and ask for refinements, we had a clear set of requirements from the start. They went into the RFP and manufacturers knew what we needed."

DSO Security Officer Carlos Montes Portela of Enexis

Results

The project was a great success, providing two key results:

- The tender process was smoother and quicker: by having the cybersecurity requirements stated upfront, there was a clear idea on how to evaluate the different vendors' solutions.

- There was a clear view on the security capabilities of the solutions offered and a level playing field was created on the security part of the requirements.

By having a clearer, more rigorous process in place from the start, Enexis was able to ensure it got the best possible cybersecurity requirements for the equipment. The manufacturers involved also benefitted from having upfront requirements to meet, making it simpler for them to demonstrate suitability.

Crucially, this was achieved with only a minor extra investment.

"There's a perception in the industry that good cybersecurity comes with a hefty premium. You hear people say that best-of-breed security will double the price. Leaving aside the question of whether that's a worthwhile price to pay to keep the grid and consumers safe, that wasn't the case for Enexis in this tender," explained Philip Westbroek of Enexis.

"The added cost for security is in line with the risk reduction it brings us. We are now equipped with devices that really push us into 'state-of-the-art' territory. As these requirements are more widely used, it will become increasingly common for manufacturers to meet them as industry standard, potentially bringing that premium down further."

With Enexis' implementation of the requirements a success, ENCS hopes that both new and existing members can use them in future to get the most out of tender processes. On Enexis' part, the DALI pilot was successful, and it can now procure equipment for the rest of the programme with confidence.

As grids across Europe become more distributed, automated and smart, a collaborative approach to cybersecurity will become increasingly important to keep grids and consumers safe.

Enexis channels energy in the right direction. Enexis provides for the transmission of electricity to 2.7 million customers and of gas to over 2 million customers in the Dutch provinces Groningen, Drenthe, Overijssel, Noord-Brabant, Limburg and, through Endinet, in the Eindhoven region.
www.enexis.nl

The European Network for Cyber Security (ENCS) is a non-profit organization that brings together critical infrastructure stakeholders and security experts to deploy secure European critical energy grids and infrastructure. Founded in 2012, ENCS has dedicated researchers and test specialists who work with members and partners on applied research, defining technical security requirements, component and end-to-end testing, as well as education & training. ENCS uses its network in academia, government and business to provide cyber security solutions and counsel dedicated to the needs of national Distribution System Operators (DSO) and regulators.
www.encs.eu