The DNO's ultimate guide to IP network integration for smart grid deployments

First edition

Headquarters, Operations & Sales

Phone: +44 (0)1291 623 813
Email: hello@txo.com

TXO.com

Registered in England & Wales:
Company Registration No: 05479601
VAT Registration No: GB840431165

In order to maintain a modern day network in line with the latest technologies, for most utility companies moving operational technology (OT) to a modern, fully IP based solution is now more of a necessity than a choice.

The OT network for most utilities evolves over time, resulting in a unique mix of technologies. Depending on the age of your company, your OT network could consist of analogue, digital, IP, copper, fibre, microwave radio and scanning VHF/UHF radio systems and so on.

When making the shift to an IP based network we believe that making maximum use of your existing communications infrastructure is critical for reducing risk, cost and deployment time. Upgrading and replacement must also be considered where new technology brings benefits such as improved security, bandwidth or latency. Smart grid deployments need the kind of transparent interconnection that IP provides to connect the various types of equipment and sensors that will be deployed to make the grid "smart". IP-based communication delivers reliability, network flexibility and security to pave the way for future smart grids. In terms of reliability, IP is the best communication protocol for this as it has more tools than any other to help maintain a network.

In this ultimate guide we cover the process for making a successful transition to full IP. Covering the detail and analysis it takes to get right and also outlining the importance of working with an experienced partner.

1. Review of requirements

You may already have a good understanding of your current OT network requirements. But even so, it's imperative to review the current system with all stakeholders. You should consider both the current and known future requirements of your OT network. After this, a comprehensive specification for the network can be drawn up. Firstly, you'll need to identify the individuals or groups with an interest in the OT network. This stakeholder group may be broader than you think, so cast the net wide. Business areas to bring into the review may include, but certainly will not be restricted to: Operations, Communications, IT, Cybersecurity, Finance, and anyone else involved in active asset replacement projects.

The objective is to extract and detail each stakeholder's requirements from the OT network. Note that some of these requirements may include blockers such as financial constraints or security policy restrictions. Some will be competing e.g. ease of operational use vs. cybersecurity.

It is common for a utility's OT network to be geographically dispersed. Therefore it is useful to identify the endpoints and the equipment at each end. You should also bear in mind that any developments in planning, such as asset replacement programmes or OT network enhancements, may have an impact. We understand it can be difficult to juggle so many stakeholders, and so working with a third party to manage the process and ensure all requirements are surfaced during this discovery phase can be very helpful.

Now that the technical requirements have been identified, different protocols are likely to be required to pass over the network. From legacy systems; analogue protocols such as RS232/422, DNP3 and the like, along with current layer 2/3 IP connectivity. Not all endpoints have the same demand upon the OT network so you should record details on bandwidth, bit rate, latency with any other key parameters e.g. jitter for your equipment.
You will also have resilience requirements to consider. These include power, diverse routing or duplicated equipment delivering an overall network availability target. Not all parts of the network will require the same level of protection.

It is crucial to remember that the topic of the moment in critical national infrastructure is cybersecurity. The requirements for which are constantly evolving and may ultimately be reflected in regulation – a major reason why DNOs are being urged to switch to full IP sooner rather than later.

The cybersecurity requirements applicable to your organisation should be well understood by your company's IT/security team. What will need to be clear is the impact this has on operational requirements. Different utilities have different standards to comply with, so you'll need to check the relevant standards and take on board those relevant to your network. Utility companies should already be in compliance or working towards IEC-62443.

Finally, it is important to capture all the data types that are expected to be passed over the network. The demand that each makes on your network in terms of data rates, latency along with the source and destination points for each. Examples include SCADA, Voice, CCTV and access control.

This review will produce a comprehensive requirements document which the OT network design will be required to deliver.

2. Specify system

The requirements gathering phase will have you close to a system specification. From here, more detail will need to be added to move toward a high-level design for your OT network.

A specification for each network node is required, starting from endpoints across the OT network, as traffic aggregates toward the central management location. Decisions on the core topology must be made particularly for resilience and in determining where high speed nodes need to be located on the network. As these build, the overall network topology will form; clearly showing all network nodes and end points and the capacity requirements between each. If your solution to resilience in the core network is a ring, then data capacity must account for ALL traffic going in one direction.

A common requirement for utilities is resilience in power with up to 72-hour duration. It makes good sense to uncover:

- Which nodes in your OT network require this?
- Is it only required on the core network and key locations?
- How will resilience be managed overall?

It is usually a combination of topology, duplicated equipment, standby equipment, and routing strategies. Define the proposed solution for each node in the network including routing plans. You will be developing an IP plan at this stage and an IP range will need allocating to the OT network, this may be assigned by your IT team.

Note that your new network may need to be backwards compatible for quite some time, so account for this in the specification. There is a lot of work to be done during this stage but it's so worth it – the outcome will be a full specification of the new OT network down to node level.

3. Audit

Auditing the existing OT network will identify how closely it matches the new requirements. Bear in mind your existing network may not be performing as well as it should be. It is highly recommended that a full technical performance is undertaken as maintenance regimes may not have checked circuit frequency responses, data throughput, latency or jitter. The audit must confirm:

- What systems and equipment are connected?
- What protocols are in use?
- How is the network performing?
- Is the network topology as expected?
- What is the connectivity type? e.g. copper, fibre, microwave radio, scanning radio etc.

TXO are well positioned to provide remote audits of your current system.

4. Solution design

Now you have a fully formed specification it needs to be formed into the final design. The next step is to select and size the equipment that will be deployed at each node across the network to deliver the specified performance. Equipment may be from multiple manufacturers and it is essential that it all interoperates so care in selection is a must.

Detailed low-level designs are required for each node type in the network. This is down to rack layouts and wiring regimes. Particular care is necessary where network equipment is to be co-located in existing operational racks. Final designs should be socialised with all stakeholders to demonstrate that the specification has been met in the final design.

Keep up to date with all our latest projects on our case studies page on our website.

During a previous project that we had with a major DNO, we identified there were 15 node types. Where a type was defined by the connectivity medium(s), the node capacity, the protocols from RTUs etc. This type of grouping determines the equipment required for each node type allowing a relatively standardised approach across the network. Again, this reduces risk and cost, and reduces timescales on deployment. Feel free to check out our case studies for more information.

5. Proof of concept

A critical phase is establishing that the new design will work as expected and fits into the overall OT network. This phase once again reduces project risk and costs. A two-stage proof of concept (POC) phase is recommended: lab-based and field-based.

The phase one lab-based POC system will be technically identical to the field based deployment. During this phase you should establish that all systems interoperate correctly, and iron out any final issues and confirm configuration and performance. At the POC you should check compliance with your cyber security requirements.

Phase two embeds the POC equipment in the wild and integrates with live RTUs and management centre.

A full risk assessment based upon IEC-62443 can be made by our team.

6. Roll out

Now it's time to roll out the new network. Initially the core should be established and integrated with existing systems where possible. The roll out of non-core nodes is best done in geographical groups and may follow other asset replacement programmes.

Our expertise in IP network design and build

We have many years of experience in the design and implementation of complex, modern and secure IP networks for our customers. We take great care in ensuring each network is tailored for interoperability with new equipment and with existing operational technologies. What's more, a huge benefit of choosing us as your system integration partner is that we're not restricted to using just one OEM. This allows us to choose the most appropriate vendor's equipment according to the specific needs of your project. Equipment manufacturers in our portfolio include Cisco, ECI, NEC, Racom and Siemens.

Our project team is made up of engineers and managers, with specific skill sets, who will go above and beyond to ensure that every project is a success. Please contact us to discuss your requirements, our team is here to help.

Phone:
EMEA: +44 (0)1291 623 813 | USA: +1 410 766 4540
APAC: +61 (0) 2 9513 8818 | BRAZIL: +55 43 3253 4695
Email: hello@txo.com

TXO.com