NEAT

Nordic Enterprise Architecture Team

NMEG

Nordic Market Expert Group

Oslo, January 22nd, 2020

Position regarding asynchronous communications in Nordic area

1 Executive summary

The four TSOs in the Nordic area are currently managing a number of deeply interrelated projects, which are making profound changes to the information flows in the wholesale market. This makes a golden opportunity to reap the benefits of establishing a harmonized way of communication in the market.

It is the recommendation to adopt the MADES standard on a Nordic level. The Nordic TSO should insure a strong influence on the governance of the implementation at ENTSO-E level. We recommend describing EDX functionality in an IEC Technical Specification.

The recommendation is based on an analytic reasoning that we will harmonize with European standards, to fully be able to adopt to ongoing and future centralization of services.

This brief provides a recommendation to the Nordic TSOs on optimal use of the MADES and EDX technologies to support planned new business processes in the Nordic and European wholesale electricity market in a 5-10-year horizon.

We believe that by adopting an industry standard as a communication foundation for TSO's, TSO shared services and TSO connected parties, we will achieve an optimal time-to-market and cost for new services.

We will know if we are successful when we see new products and services enrolling on this platform on a minimum of overhead and no need for extra security controls to comply with regulations and requirements.

Implementing the basic security controls in a platform/foundation will ensure a higher level of function and security.

Total capital investment and operation costs will decrease with the IT supported function, but we need to be aware of the OPEX and APEX associated with establishing and operating the shared resource. In this sense, it can be argued that we are converting product APEX to OPEX.

This brief is addressing multiple recipients so not all chapters are equally relevant to all. Business executives should focus on chapters 1, 4, 5, 8 and 10. Whereas IT professionals and other stakeholders need to read the whole document to understand the possibilities and impact of the decision.

2 Table of contents

1 Executive summary 1
2 Table of contents 2
3 Editors 3
4 List of terms and acronyms 4
5 Background information 6
6 Drivers 7
6.1 Key IT consideration drivers 7
6.2 Key business drivers 9
7 Description of principal components 11
7.1 MADES 11
7.2 EDX 12
8 Listing of issues 14
8.1 Physical Hosting: 14
8.2 Administration (Component Directory / Service Catalogue) 14
8.3 Service Level Agreements 15
9 Design/topology - 3 layers of communication 16
9.1 Overview 16
The three different characteristics, written in prosaic language is: 16
9.2 TSO and connected parties 18
9.3 Nordic messaging network on "Dark fibre" 18
9.4 Pan European communication network 20
10 Organizational resources, deployment and operations 21
10.1 Organizational resources 21
10.2 TSO Operations 22
10.3 Nordic Operations 23
11 Resource overview 24
11.1 Resource requirements 24
11.2 Central infrastructure 24
11.3 Participant infrastructure 25
12 Evaluation of options 26
13 Conclusion 27

3 Editors

This document represents a joint position of NEAT & NMEG. The members are:

NEAT:

- Ove Morten Stalheim, Statnett
- Tage Søndergaard Larsen, Energinet
- Veli-Jukka Pyötsiä, Fingrid
- Åke Svilling, Svenska kraftnät

NMEG:

- Anne Stine Hop, Elhub
- Christian Odgaard, Energinet
- Fedder Skovgaard, Energinet
- Jan Owe, Svenska kraftnät
- Jari Hirvonen, Fingrid
- Jon-Egil Nordvik, Statnett
- Teemu Hiekka, Fingrid

Contributing editors:

- Alexander Lindén, Svenska kraftnät
- Ove Nesvik, Edisys (Secretary, NMEG)

4 List of terms and acronyms

AMICA	Client-server based IT System used by TSCNET and in its member TSOs
Amprion	A Transmission System Operator located near Cologne, Germany
AMQP	Advanced Message Queue Protocol, ISO 19464 (The primary data exchange protocol of MADES)
AMQPS	Shorthand for AMQP data exchange in a TLS tunnel
ATOM	All TSO operation and Market data network (A pan European network intended to carry the information for the OPDE system)
CAPEX	Capital expense
CGMM	Common Grid Model Methodology (A document establishing a guideline on electricity transmission system operation in accordance with Commission Regulation (EU) 2017/1485)
Coreso	A regional security coordinator based in Brussels, covering Western Europe and the UK
CWE	Central Western Europe (Belgium, France, Germany and the Netherlands)
DER	Distributed Energy Resources
ECP	Energy Communication Platform (An implementation of the MADES standard owned by ENTSO-E. Developed by Unicorn AS)
ENTSO-E	European Network Transmission System Operators for Electricity (Regulation (EC) No 714/2009)
FTE	Full Time Equivalent
HA	High Availability (A characteristic of a system, which aims to ensure an agreed level of operational performance, usually uptime, for a higher than normal period)
JMS	Java Message Service
IEC	International Electrotechnical Commission
MADES	Market Data Exchange Standard (The definition of the communication protocol and surrounding business processes for operating a network. Published as international standard IEC 62325-503)
MPLS	Multi-Protocol Label Switching (A way to logically separate network traffic on the same hardware)
MSG	Market Steering Group
OPDE	Operational Planning Data Environment (Definition 74 of SO-GL)
OPEX	Operational expense
PCN	Physical Connectivity Network (A Pan-European MPLS based network primarily on TSO controlled fibre links to host Electronic Highway, ATOM as well as other services. A delivery of the ENTSO-E CGM Program)
RSC	Regional Security Coordinator
SO-GL	System Operator Guide Line (Commission regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation)
TC57/WG15	IEC working specializing in “Data and communication security”

TC57/WG16	IEC working specializing in “Deregulated energy market communications”
TLS	Transport Layer Security (RFC 5246)
TSCNET	A regional security coordinator based in Munich, covering central and eastern Europe
VPN	Virtual Private Network
XBID	Cross Border Intraday

5 Background information

The European power sector is currently undergoing drastic changes coming from several factors, including:

- Unbundling of sector increases number of actors
- Introduction of renewable energy increases number of DER resources
- Depletion of central power plants increases importance of communication platform for balancing the grid
- Nation state sponsored cyber terrorism increases security requirements to platform

In combination, these factors incur an exponential increase in the requirements and thus complexity of the communication platform, which can only be effectively addressed by applying standards throughout the market. Further on, we as TSOs need to present a homogeneous interface towards market actors.

The Nordic TSO's are looking into a future with ever-increasing requirements for data exchange, both in number of business processes, and in criticality. This has led ENTSO-E to drive the design and development of a communication system specifically targeting the requirements of the European Transmission System Operators, MADES.

The Nordics will have to comply with future requirements in Pan-European services, for instance balancing services.

Lastly, according to the utility directive[1], international standards or European norms have precedence over national regulation, which makes it challenging to write public tender requirements that do not adopt existing standards.

System operation is notoriously legacy bound and implementing such fundamental changes as consolidating the messaging protocols is necessarily a result of a centrally dedicated and coordinated effort. Thus, the current proposal is in line with a strategy endorsed by ENTSO-E at committee level and by MSG decision of May 5th, 2014 of choosing MADES as the preferred means of communication for asynchronous communication. The first projects utilizing MADES have seen multiple years of production usage[2] and it is now the time to do a coordinated effort to execute the full consolidation.

[1] DIRECTIVE 2014/25/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, Article 60 "Technical Specifications" §3

[2] AMICA, XBID, Transparency platform, CWE Market coupling.

6 Drivers

IT capabilities, architecture and infrastructure itself is no primary goal for any organization.
There are however characteristics of IT capabilities and foundational elements that form a foundation for "business-value" delivered.
These characteristics is our goal target - to enable business to exploit current opportunities and explore future possibilities in a rapid and cost-efficient manner.

6.1 Key IT consideration drivers

Handling data communication between the different key roles in the energy market is a complex exercise, it requires expert skills and solid communications skills to handle the interests of all parties. One key, and ever returning, issue is the handling of security controls, to satisfy the requirements to confidentiality, integrity and availability.

6.1.1 Innovation

By applying a foundation for communication, we will decrease the amount of effort required to be able to exploit new ideas and explore new business cases/products. Which in turn generates socioeconomic benefit.

In this time of radical change to the way we do business in the Nordics, a shift towards higher regional control and new balancing concepts, we need to optimize the IT product development.

Since the assumptions we make when getting into a project are rarely fully correct, we need to optimize for the times when we are wrong. In order to lower the threshold for exploring and exploiting new products, it is vital that an innovation process has enough momentum and speed.

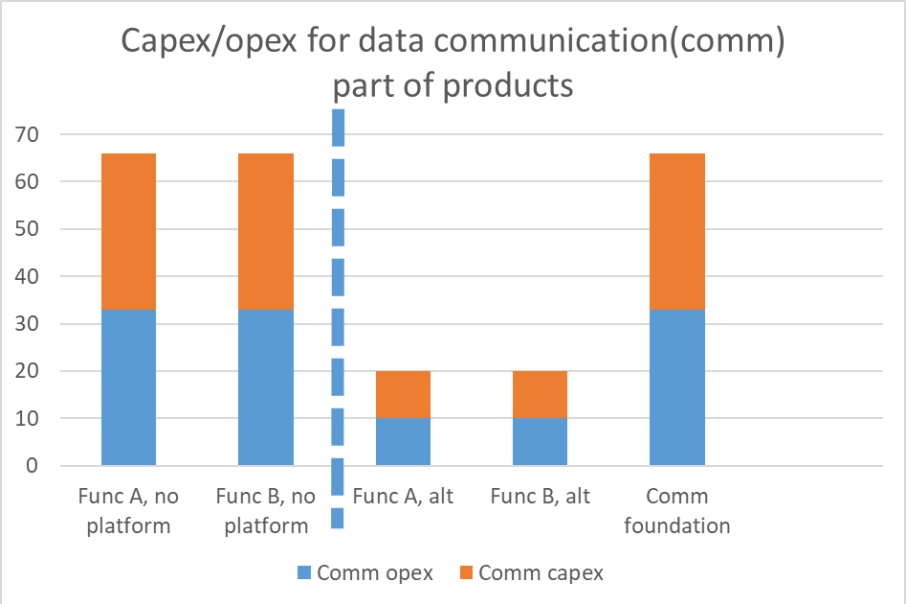
From Daniele Gerundino (From foreword to ISO-CERN Standardization and innovation conference[3]):

- Contributing to technical evolution by applying, at the right time, critical design constraints (i.e. avoiding re-inventing the wheel). Standards can help to reduce wasteful, redundant product development, allowing to free up resources that can instead be dedicated to fresh, inventive work
- Facilitating the development of new markets and trade, by helping to establish and exploit network effects, increasing consumer confidence and allowing to reach critical mass
- Permitting the sharing of investments and risks associated with the development of new technologies and applications (fostering innovation through collaboration)
- Helping the commercial exploitation of innovative ideas, providing a basis for the dissemination of information and an accepted framework within which patents can be drawn up, removing undue proprietary interests and barriers to trade

6.1.2 CAPEX/OPEX

Whilst building the foundation for data-communication, we also reduce the amount of CAPEX and OPEX needed in every function that utilizes this foundation. The underlying argument for this is that the marginal costs per integration is very low, once the communication platform has been established.

[3] Source: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/standardization_and_innovation.pdf



6.1.3 Time to market

By standardizing the interface between TSO connected parties, TSO's and shared regional services – we will contribute to evolve the market for system vendors to compete in this market. It enables IT vendors from any region to compete in all regions of Europe.

By providing an abstraction of the infrastructure, the only thing projects need to agree on are the names of the services.

6.1.4 Built-in security controls

One of the main arguments for choosing/developing the MADES standard was the in-built security controls.

A MADES compliant application provides:

- Encryption on two levels, payload and transport (addresses Confidentiality and Integrity)
- Non-repudiation, the guarantee of transparency of "who sent what" (addresses Integrity)
- Message delivery guarantee (addresses Availability)

To address this security controls without a platform that delivers this, is a huge load on both CAPEX and OPEX to any new product. This is amongst the reasons that we see a lot of breaches to these security controls in our existing systems and products today.

Since these issues seldom are amongst the key metrics that projects are measured upon, we will continue to fight these security controls unless we make them an in-built feature.

Another benefit of using standardized solutions is the attention to detail and “thousand eyes” that are available during the formalized process of getting the standard approved. For the MADES standard, these external reviewers included members from IEC TC57/WG15, which are among the world’s most knowledgeable persons within cyber security for the electricity sector.

6.2 Key business drivers

6.2.1 RSC

Being a Regional Security coordinator, the Nordic-RSC is a key stakeholder in realising the OPDE vision, which is described in the CGMM, as a service provider. The very reason for a RSC is to collect, analyse and publish data. To do this, it must be well connected to its peers, which is exactly what OPDE vision aims to establish.

In the spring of 2016 ENTSO-E initiated design sessions for the "ATOM" network, which at that time was expected to be realised through several regional networks, which were interconnected through a common backbone. It was decided to take a lead in this strategy, which led to the creation of the Nordic-RPN (Regional Private Network), which is built using SDH connections of TSO controlled fibre networks. Once the backbone and the OPDE service provider environments hosted by Coreso and TSCNET were up, a trace redundant connection from Energinet to Amprion were created to allow selective routing of traffic to these environments, thereby fulfilling connectivity requirements for all Nordic TSOs and the Nordic RSC in one go.

6.2.2 NBM

The Nordic balancing initiative NBM has extensive needs for data communication on several layers. Following is a non-exhaustive list of examples:

1. Real time communication for exchange of measurements and FRR demands
2. Transactional communications for orders and other processes that need high availability and low latency
3. Data shifting for analytical and other needs that don't need low latency
4. Portal like communications for access to exposed functions in shared applications

The specific needs are gathered below, with respect to no. 2 transactional communication

1. aFRR bid handling
   Needs communication to BSP's and TSO's for collecting bids
2. aFRR TSO-TSO market results
   Needs communication to BSP's, transparency NUCS and TSO's to distribute the result of market
3. mFRR capacity market bid handling
   Same as 1
4. mFRR TSO-TSO market results
   Same as 2

<u>mFRR activation market</u>
Needs communication to TSO's for receiving mFRR demand and MOL.
Needs communication to BSP's for activation of mFRR bids.

<u>NBM Settlement</u>
Needs communication with eSett for handling balance settlement.

6.2.3 NUCS

The Nordic Unavailability Collection System (NUCS) has implemented MADES/EDX as the primary channel for receiving and publishing unavailability documents.

Following decision by the ENTSO-E Market Committee, all data exchanges of newly created market related platforms must support MADES.

In the ICT review of balancing project, it is identified that MADES and ECP are the recommended goals for PICASSO, MARI and TERRE(RR)[4].

OPDE

MADES and EDX are the principal components of the ENTSO-E OPDE platform, as described in the SO-GL.

PICASSO

Procurement documentation clearly states that for some communication, for instance MOL, ECP is the future target.

It is identified in the Picasso RFP that ECP is identified as communication product.

> The MOLs are available in the ERRP format, see also [R10]. MOL files are provided via the TransnetBW BIS (data hub). In future it is intended to use the Energy Communication Platform (ECP), see also [R11].

MARI

Formal ENTSO-E ICT review recommends the use of MADES/ECP as communication platform for MARI.

Transparency platform

ENTSO-E WG TPC has approved a transition from ECP v3 to ECP v4 (the recommended version for the Nordics) on the Transparency platform. This is scheduled to be completed in Q3-2019.

eSett

The BASSE system of eSett is currently supporting several legacy interfaces for B2B communications. eSett has a goal to consolidate these on the MADES standard in the future.

[4] https://extra.entsoe.eu/Board/DC/BP%20ICT%20Review/Balancing%20ICT%20Review%20-%20final.docx

7 Description of principal components

7.1 MADES

MADES is a profile of existing Internet standards for establishing a solution for secure exchange of asynchronous data between organisations in the European electricity sector. It achieves this by leveraging a common trust anchor, the component directory, which facilitates trust between the parties in the MADES network.

MADES is a published International Standard and EU Norm[5]

7.1.1 Component Directory:

The component directory is the centre of trust in the MADES network. It contains a list of all trusted components (Brokers & Endpoints), as well as a list of Message Paths in the network.

The component directory contains no confidential data beyond the private key of the intermediary CA Certificate.

7.1.2 Broker:

A broker is an optional component in a MADES network, which acts as a gateway between two endpoints. This facilitates non-repudiation of messages in the network, by introducing a third party in the message exchange and further enables deployment in segregated networks. In ECP4 the Broker is implemented by using the Apache ActiveMQ library with a custom authentication plugin.

7.1.3 Endpoint:

An endpoint is the component, which is the entry point to a MADES network for the business applications in the participants IT landscapes. It provides an abstraction of the services required for addressing, routing and secure exchange of messages. It achieves this by signing and encrypting the payload for the intended recipient and ensuring that delivery is (eventually) possible.

7.1.4 Message Type

To enable usage of one endpoint for multiple independent business processes, the concept of Message Type is introduced. This, essentially, works like the subject field on an e-mail and lets business applications on the receiving side select for which business process they want to retrieve messages.

[5] IEC IS 62325-503

7.1.5 Message Path

The MADES interface provides a complete abstraction of the underlying infrastructure, but to provide routing capabilities between endpoints, the concept of Message Path defines the route a given message shall take between its source endpoint, and an optional broker before reaching its destination endpoint.

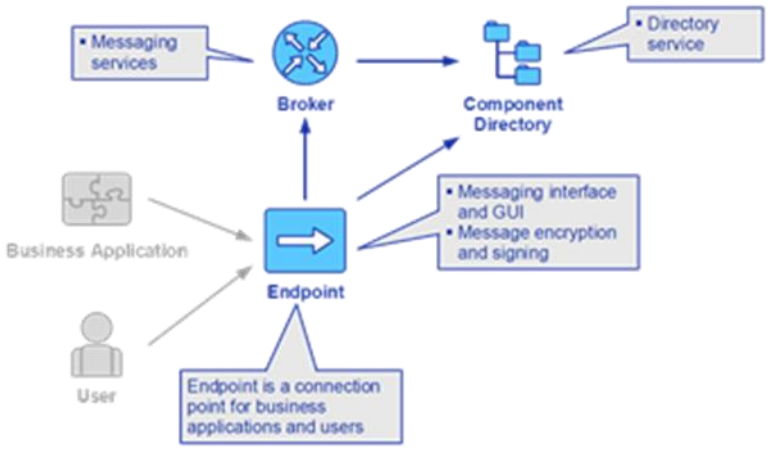
In this way Message Paths enables separation of traffic as well as transparent migration from one broker to another to facilitate high availability.

A message path is selected based on recipient and Message Type and is stored in and distributed via the Component Directory.

7.2 EDX

To facilitate the requirements of publication and subscription of data in the CGMM[6] a business application was developed, to provide an additional layer of abstraction on top of a MADES endpoint.

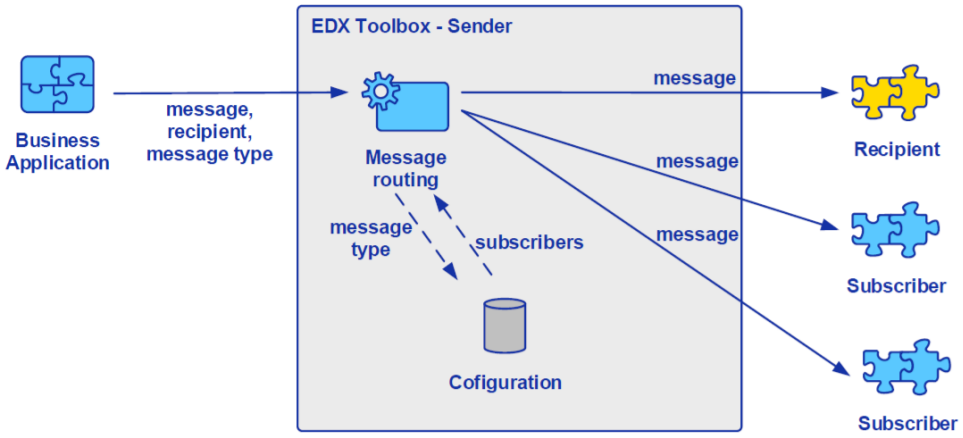
The reasoning for this split is the fact that MADES was already subject to standardization in IEC, and its scope was frozen.



7.2.1 Service Catalogue:

Complementary to the Component Directory, the Service Catalogue is a shared component, which provides a central source of truth for all subscriptions and publications in the network. The Service Catalogue is implemented as an application, which uses an Endpoint to communicate on the network.

[6] Common Grid Model Methodology



7.2.2 Toolbox:

A Toolbox is essentially a business application, which itself provides the same interfaces as an Endpoint, to its business applications, but adds a set of addressing capabilities to the system. These concerns the ability to publish messages to and receiving from services, as defined in the service catalogue. All actual exchange of data is still handled by the Endpoints and is getting all the promises from the MADES standard, such as non-repudiation, guarantee of delivery and encryption.

Toolbox's also supports an optional feature supporting exchange of large files using the claim-based message transfer pattern. Implementing this is however out of scope of this text, as no use-cases have been identified that requires it.

7.2.3 Overview of scope

MADES/EDX is applicable in a set of business contexts defined by projects. These include, amongst others:

- NBM Nordic Balancing Model
- MNA Multi NEMO Agreement
- HVDC Scheduling process for HVDC interconnectors
- eSett Data exchange with eSett
- N-RSC Nordic Regional Security Coordinator
- ENTSO-E Operational Planning Data Environment, OPDE

8 Listing of issues

This chapter provides a non-exhaustive listing of issues that must be taken in to account when deciding how to deploy MADES/EDX based communication networks in the Nordics.

8.1 Physical Hosting:

As all components of MADES and EDX are loosely coupled, there are many options for deployment.

- All components placed at one location or split?
- Responsibility, one host or multiple?
- Is public cloud an option?
- Which business services can be consolidated on the same components?

In the end, these questions are implementation details, which are project deliverables, under the guidance and oversight of NEAT vis a vis the Enterprise Architecture functions at each TSO.

8.2 Administration (Component Directory / Service Catalogue)

In the context of the domain covered by this text, common projects between Nordic TSOs, the following options come into play:

1. One central installation
2. Local at each TSO, but federated
3. Stand-alone local installs

8.2.1 One central installation

From a technical perspective, this is a viable solution. Participants will only need to install one endpoint and communication is potential between all parties.

This solution is, not advised, as governance of this single entity will need to be centralized, which is expected to be problematic from a regulatory perspective.

All components must be kept at the same major version number and upgrades from one major version to another requires careful planning.

8.2.2 Federated national installations

Component Directories can be federated, that is, periodically import of a read-only copy of other trusted directories. Thus, a participant in one directory will be able to exchange messages with any participant in another directory, while the individual directory is still under local governance. This introduces some extra complexity when establishing the trust between directories and requires clearly defined interfaces between the administrators of each directory. Participants need only one endpoint to communicate with all other parties.

Message Paths must be defined in the receiving directory, which means that every directory is ultimately in control of which (foreign) endpoints can connect to the local endpoints.

All components must be kept at the same major version number and upgrades from one major version to another requires careful planning.

8.2.3 Isolated installations

In a zero-trust environment all instances are built in isolation. Participants will need to install one endpoint per business context. There is also the overhead of managing multiple independent directories, which must all be maintained.

8.3 Service Level Agreements

How to adopt for various projects and their service level agreements?

- Should all go on one setup (Like XBID / CWE node)
- Should we have one environment per “major business process”, thus having multiple instances of each component

9 Design/topology - 3 layers of communication

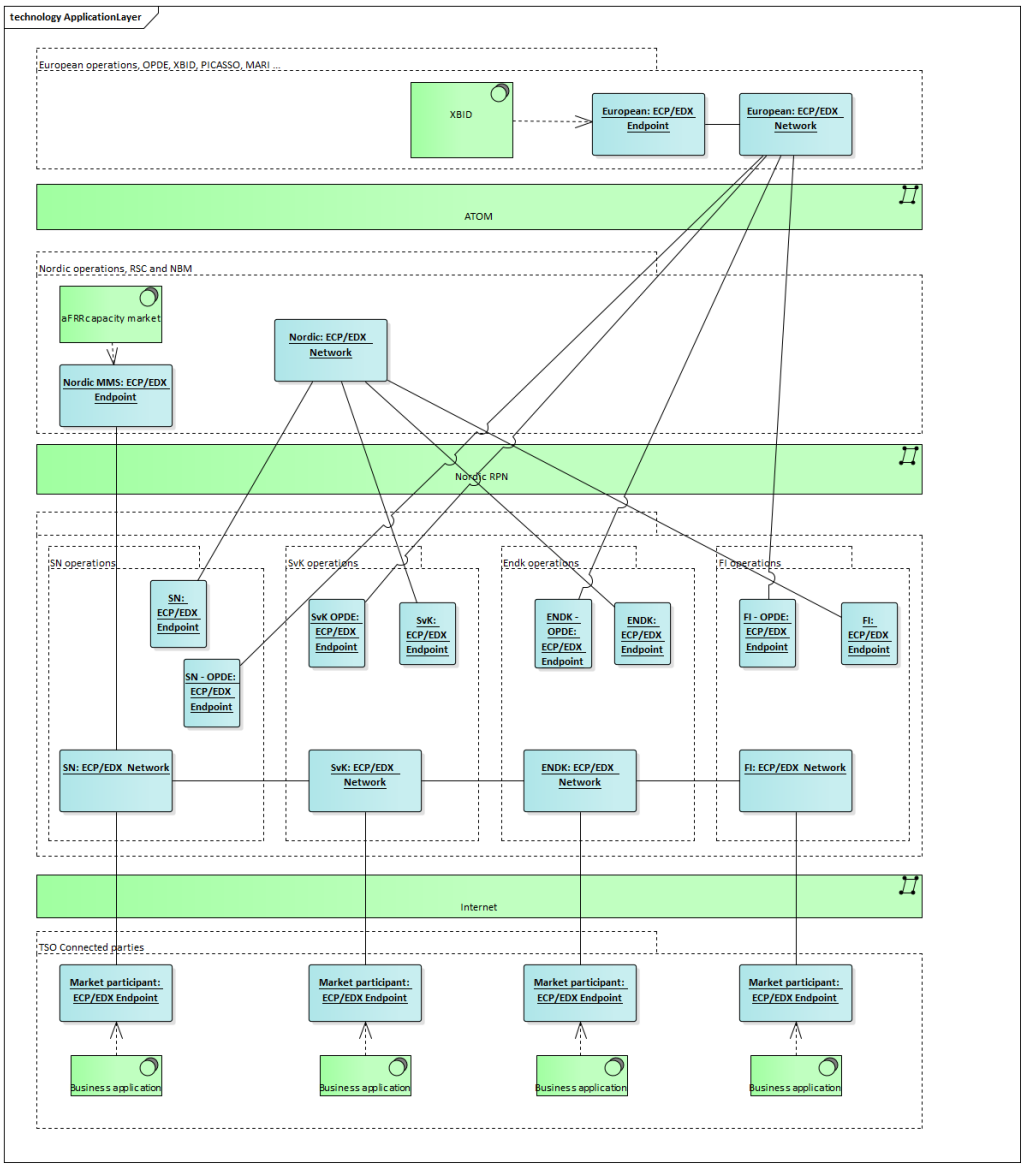
9.1 Overview

According to our analysis and knowledge about current and soon-to-be realized business needs, we need three different messaging networks that has distinctive different characteristics. Underlying technology, architecture and standards are the same, to enable fast adoption of use and effective use and technical know-how.

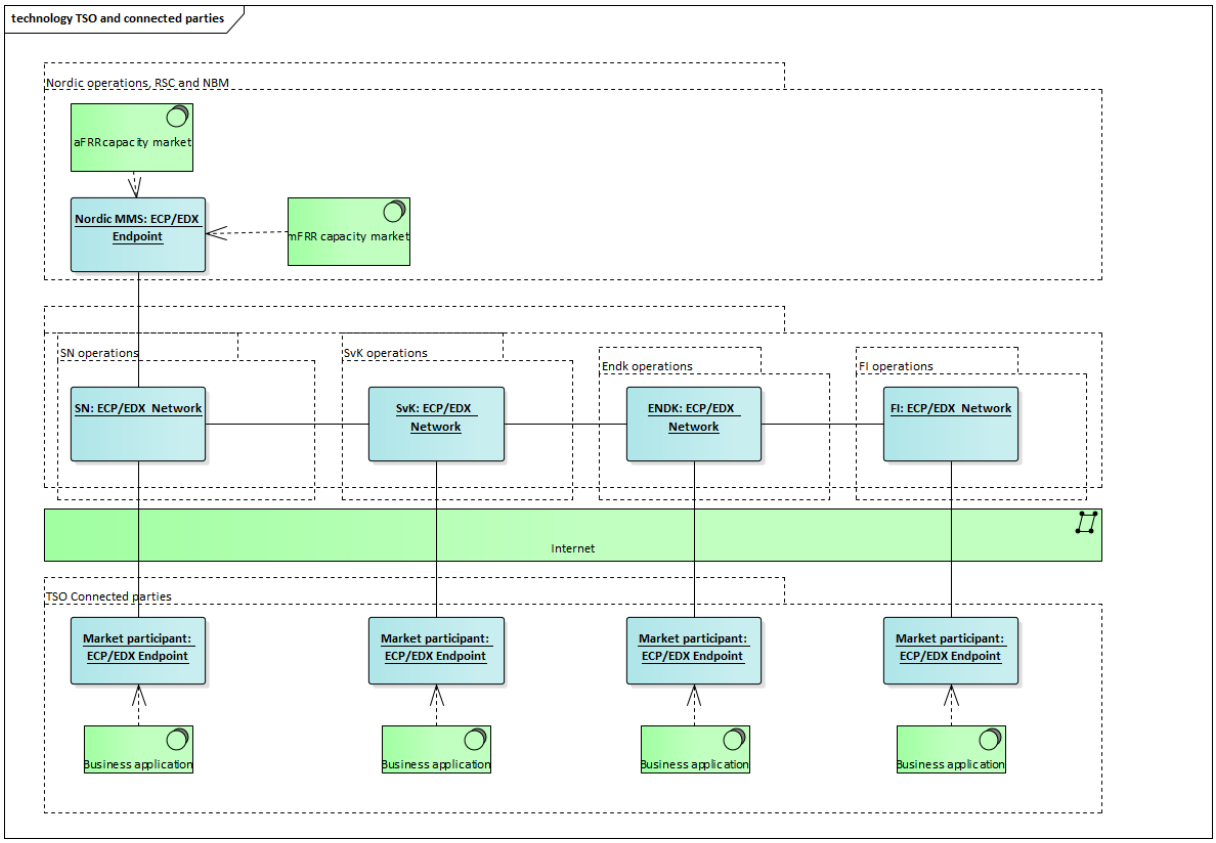
The three different characteristics, written in prosaic language is:

1. Interconnected Europe, to enable sharing of common services and data.
   Need for High-Availability and focus on Confidentiality and Integrity.
2. Interconnected Nordic region, to enable sharing of common services and data.
   Need for High-Availability, for instance closed loop regulation loops for mFRR and aFRR.
   Secret level of Confidentiality and Integrity, due to regulations that is stricter than the rest of Europe (Svenska kraftnät and Statnett, are unique in this matter)
3. Interconnected Nordic region, to enable TSO connected parties to utilize common Nordic services.
   The risk for breach of availability is higher, due to the need for exposure to physical networks we do not have full network control over. Trust to some extent is federated to our connected parties' abilities to secure their access to network components.

In a near future one can foresee the merge of the European and Nordic closed network on PCN.


technology ApplicationLayer
European operations, OPDE, XBID, PICASSO, MARI
XBID
European: ECP/EDX Endpoint
European: ECP/EDX Network
ATOM
Nordic operations, RSC and NBM
aFRR capacity market
Nordic MMS: ECP/EDX Endpoint
Nordic: ECP/EDX Network
Nordic RPN
SN operations
SvK operations
Endk operations
FI operations
SN: ECP/EDX Endpoint
SN - OPDE: ECP/EDX Endpoint
SvK OPDE: ECP/EDX Endpoint
SvK: ECP/EDX Endpoint
ENDK - OPDE: ECP/EDX Endpoint
ENDK: ECP/EDX Endpoint
FI - OPDE: ECP/EDX Endpoint
FI: ECP/EDX Endpoint
SN: ECP/EDX Network
SvK: ECP/EDX Network
ENDK: ECP/EDX Network
FI: ECP/EDX Network
Internet
TSO Connected parties
Market participant: ECP/EDX Endpoint
Market participant: ECP/EDX Endpoint
Market participant: ECP/EDX Endpoint
Market participant: ECP/EDX Endpoint
Business application
Business application
Business application
Business application

9.2 TSO and connected parties



- An interconnected messaging network
  - Facilitating connected parties ability to use shared Nordic services
  - Local TSO responsibility for support to its connected parties
  - Local TSO has control over exposed services on its network

9.3 Nordic messaging network on "Dark fibre"

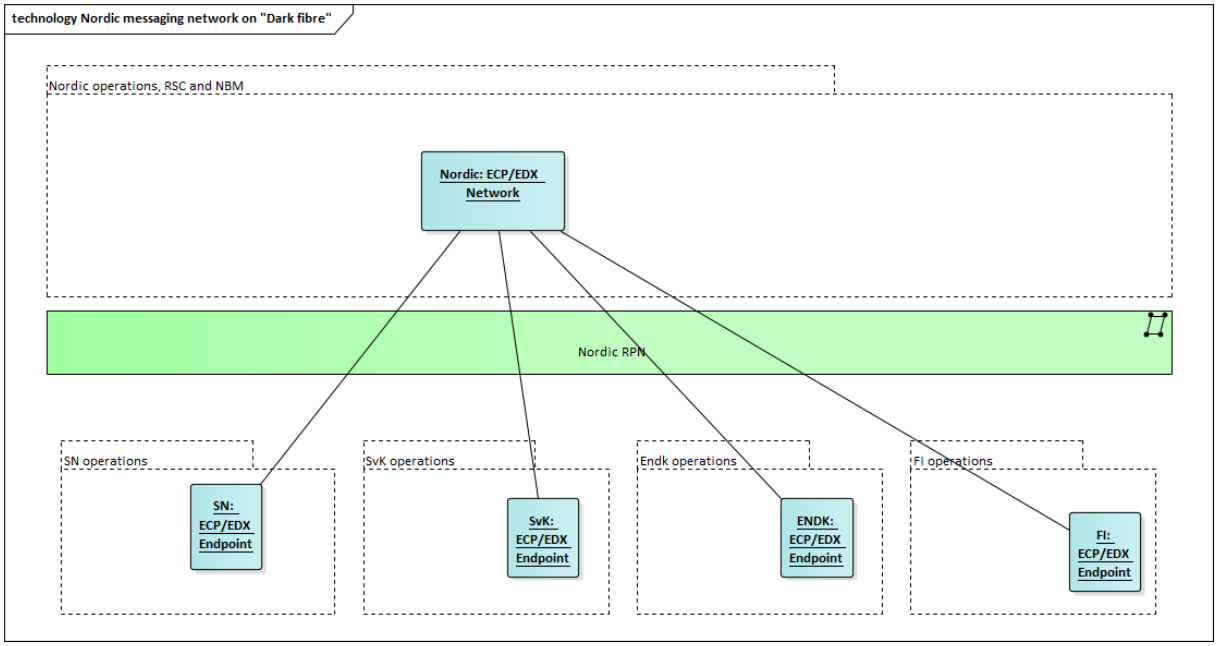
The Nordic TSOs have a vast network based on optical fibres co-routed with the transmission power lines, which are principally used for substation control and real-time data acquisition. There is generally ample spare capacity in these fibres and using SDH technology this can be used to carry other data, which can be considered physically separated from each other[7].

In the initial phase of establishing the Nordic-RSC, the requirement for establishing a separate and highly reliable network became evident. Especially as the outlook for delivery of the OPDE vision from ENTSO-E turned into a far vision.

As the data for performing flow-based capacity calculations in the Nordic area bears a strict classification, this can only be effectively exchanged on a network[8], which is separated from other networks. This is perceived to be the only viable solution for the foreseeable future. When, and if, the central OPDE platform, as delivered by the ENTSO-E CGM Program is fulfilling the requirements set forth by the OPDE Secret level in the MVS agreement, this decision should be revisited.

[7] While the data is transmitted through the same optical fiber, this is completely transparent to the logical network.

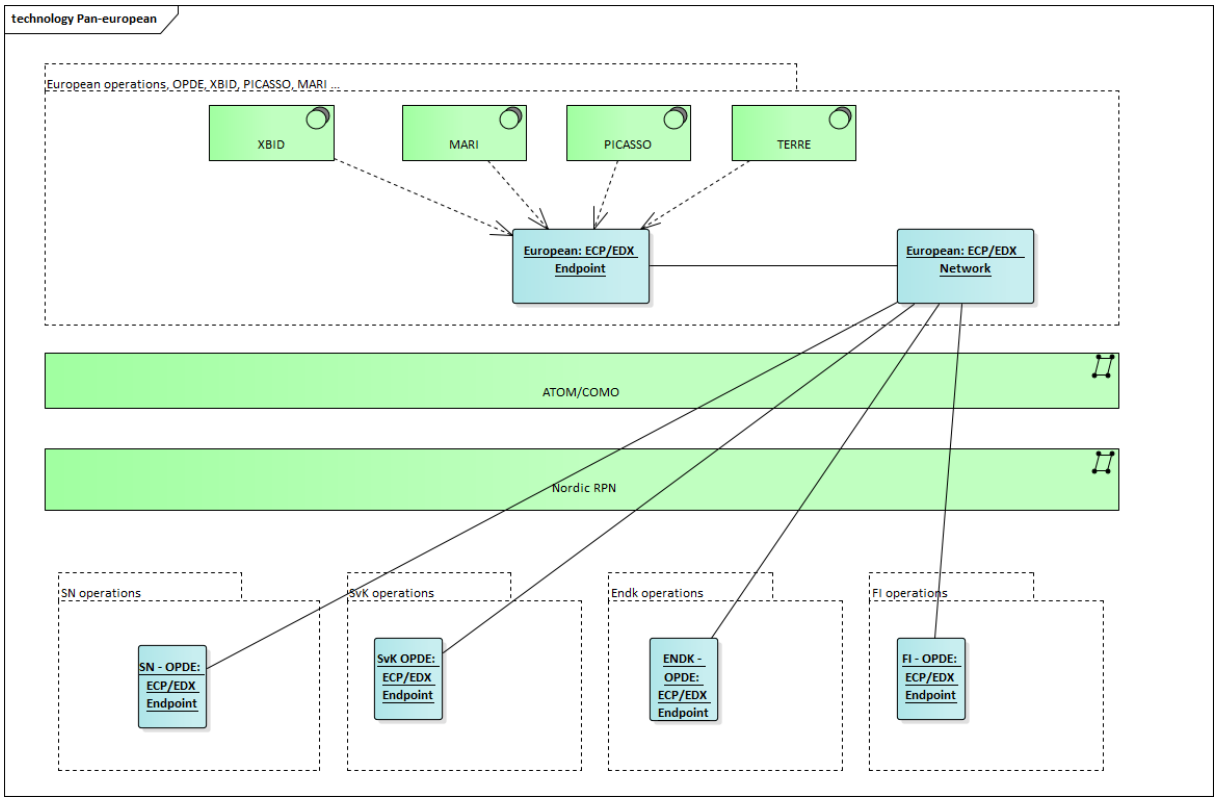
[8] Both in context of IP level as well as application level.



- Enabling a messaging network for TSO-TSO-RSC communication
- Full control over all endpoints and connected networks
- Enabling HA and secret level of communication
- Built on trace-redundant TSO controlled fibre
- Black out resilient infrastructure

9.4 Pan European communication network

This is essentially the ATOM network, which is a key deliverable from the ENTSO-E CGM Program. However, there are no confirmed milestone plan for the realisation of this at the time of writing.



- Access to central European services; XBID, OPDE …
- Hybrid network consisting of TSO Fibre, commercial MPLS and VPN.
- Centrally managed infrastructure under governance and operation of ENTSO-E[9]

[9] Network Operation Centre (NOC) will be handled by Swissgrid & Amprion. Network Security Center (NSC) will be handled by RTE

10 Organizational resources, deployment and operations

This section describes which functions, resources and roles that need to be established to adopt, develop, deploy and maintain MADES/EDX based communication networks on national, Nordic and European level.

10.1 Organizational resources

The administrator of a MADES network is responsible for providing reliable, secure and performant services to its connected parties. It is therefore important that the Service Provider (SP) of a MADES network has an organization in place to ensure technical operation and administration, but also to govern architectural and design principles for future development of its services. The daily workload will be volatile, but the organization is going to need at least two main roles; an application manager and an architect.

Consumers of the MADES network services are going to need a technical role to deploy and configure ECP/EDX platform components. These components could then be included in the daily technical operations. An agreement, between the Service Provider, i.e. a TSO and the Service Recipient, i.e. a BSP, should be in place, to assure that each party in the network is responsible for securing and monitoring its deployed components.

10.1.1 Application manager

The application manager has a technical profile and is used to work with Java based systems and application servers, using message protocols such as JMS and HTTP over secure transport protocols, deployed in clustered environments. The overall responsibility for the application manager is to ensure the technical operation of the application to handle incidents. Additional work assignments need to be handled on certain occasions:

- Administrate new users in the network
- Administrate/ensure certification renewal
- Deploy new versions of software components used by the platform

As an indication of effort required for this role, Statnett currently has one FTE allocated as Application manager.

10.1.2 Architect

The architect needs to design the initial platform, ensure that the network is implemented according to the MADES standard and in symbiosis with the current organizational eco-system. Integrations and services need to be established for business applications to exchange messages in the MADES network. Additional work assignments need to be handled on certain occasions:

- Create/connect to new MADES networks
- Integrate new business applications
- Provide new services
- Scale current architecture

There is a significant overlap between the Application Manager and the Architect roles, which depends primarily to the organizational setup at the organization.

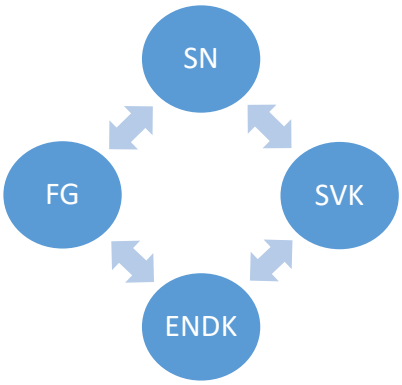
Additionally, there is a need for a coordinated effort to keep the strategic development of the applications and underlying standards coherent with the business requirements. This work is

currently taking place in the “Communications standards” subgroup of the CIM Expert Group in ENTSO-E.

Role	Activity	Dev	Ops
Architect	Design server architecture	X	
	Realize network architecture	X	
	Establish CA	X	
	Compose EDX services	X	X
	Application integration design	X	X
Application Manager	Application deployment	X	X
	Application integration development	X	X
	Application monitoring	X	X
	Incident/change management		X
	Administrate new users / certificates		X
	ECP/EDX project contact		X

10.2 TSO Operations

At a national level, each Nordic TSO is responsible for setting up an organization/project to operate, administrate and develop ECP/EDX services. The project could be another vertical in existing technical operations, but it is up to the TSO to determine where the project should be in the current organization. However, it is important that the project can function together with operations and application development at the national TSO organization, meet SLAs towards BSPs and other TSO connected parties, and collaborate with the other Nordic TSOs for development of TSO shared services.



10.2.1 Deployment

Each Nordic TSO is responsible for deployment of their ECP/EDX network components and decides which hardware to use, how deployment and availability are set up, how security issues are mitigated, etc. The TSO network is self-organized and there are no hard dependencies between each network. However, the Nordic TSO’s are recommended to interconnect their Component Directories, enabling BSPs to implicitly integrate with multiple national markets, while only physically connected

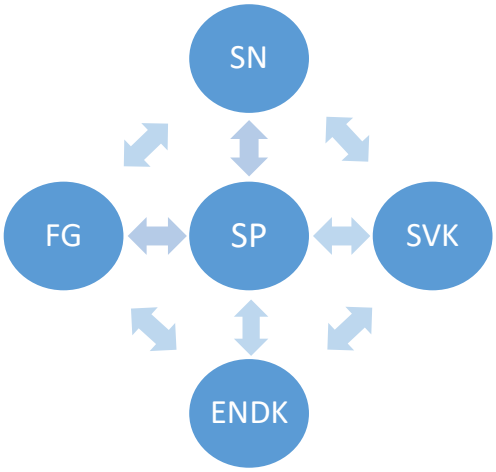
to their national TSO. This approach requires component directories to run the same major version of software and provide services to be duplicated through multiple national TSO networks.

10.2.2 Operations

Each TSO needs to have 24/7 operations in place for 1st and 2nd level support, including infrastructure and software monitoring with 99.9% availability on provided services to its business applications and connected BSPs. The TSO is responsible for delivery of messages in the network. A transaction is complete when a message is sent, and an acknowledgement is received. The TSO cannot take any further responsibility than assured messages delivery into the network. Level 3 support, handled by the platform supplier, Unicorn, must be consulted for specific requests related to the software platform. No tactical decisions, involving other networks, projects or services, should be solved locally by the TSO. Operations also include architectural design for integration of new business applications and re-design/development of new MADES networks.

10.3 Nordic Operations

Nordic Operations have the same obligations towards its connected parties, the Nordic TSOs, as the TSO operations have towards its connected BSPs. In addition, Nordic Operations also need to function as a common support organization for all the Nordic TSOs, acting as the service provider and support organization for common Nordic services.



10.3.1 Deployment

The Nordic Market Area network and its Service Provider are responsible for trust between all Nordic TSOs. Each TSO is a participant in the network and is responsible for setting up an ECP/EDX endpoint to exchange messages with other TSOs. The network is centralized around the Nordic Service Provider and it is forcing the Nordic TSOs to maintain software components in alignment with standards and services hosted by the provider. However, the network is federated since each Service Recipient is also a Service Provider of its own national MADES network.

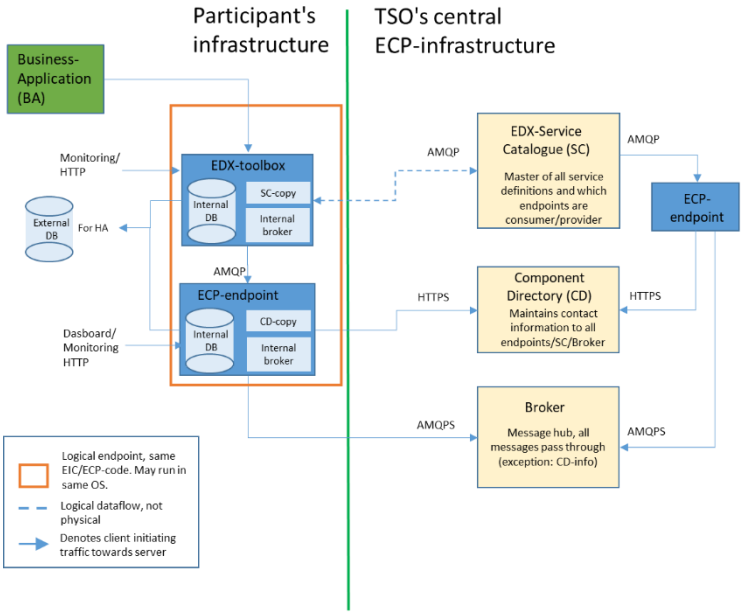
10.3.2 Operations

The Nordic Service Provider need to have 24/7 operations in place for 1st and 2nd level support, including infrastructure and software monitoring with 99.9% availability on provided services to its business applications and service recipients. Nordic operations (NIOPS) are going to be established in the Market Area, extending support operations further with Level 3 support from Unicorn. NIOPS will also handle common tactical decisions and functions in a shared operational forum between the Nordic TSOs, where regional market participants or Nordic projects can present inquiries or requests.

11 Resource overview

This chapter discusses recommendations for deployment of all services in the proposed networks, for different service levels. It does not specify technical details for infrastructure beyond HA / not-HA for availability and small / large for server capacity. This is done as every TSO have their own cost models and environments.

An overview of the logical components is shown below. It should be noted that the TSO itself is a Participant in the network.



11.1 Resource requirements

Statnett has established a MADES network with market participants and TSOs since 2015 and based on their experience, the following figures can be used as an indication of effort.

ROLLE	CAPEX	CAPEX RUNNING	OPEX
IT-ARCHITECT	½ Man year	1/12 Man year	¼ Man year
APPLICATION MANAGEMENT		½ Man year	½ Man year
PARTICIPANT SETUP	½ Day		24 Man hours

In addition to these roles, we propose to establish a shared “centre of excellence” between the Nordic TSOs. This should ideally be placed in relation to the existing collaboration forums under NIT, such as NEAT & NMEG.

11.2 Central infrastructure

All central components are expected to be highly available irrespectively of which logical network they are participating in.

An overview of instances for a typical setup can be expressed as follows:

No specific requirements for host operating systems or physical metrics provided, as these depends on local TSO preferences, but these numbers should make it easy to get an estimate of cost.

		HA cluster		Single instance	
		Basic	High perf	Basic	High perf
Shared Infrastructure					
	ECP Component Directory	1			
	ECP Broker		1		
	EDX Service Catalogue			2	
Participant Infrastructure					
	ECP Endpoint			1	
	EDX Toolbox			1	

11.2.1 Component Directory

As all information in the component directory is cached by all participating components, there is no formal need for deploying it in a HA setup. However, it is generally a requirement by TSOs that 24x7 systems need to be deployed in HA clusters. This also supports the criticality of the integrity of the data in the Component Directory.

The implementation for the Component Directory is not very resource intensive, why it can fit on shared infrastructure.

11.2.2 Broker

The broker is a high-performance component, whose availability is visible to all participants in a network. As this is a general-purpose standard application, with very limited customization, there are well established best practises on deploying this

11.2.3 EDX Service Catalogue

The Service Catalogue is a central registry of topics, and associated publishers and subscribers in the network. The service catalogue is also not imposing any specific requirements on availability as all data is cached in the individual EDX Toolbox.

11.3 Participant infrastructure

The SLA requirements for the participant infrastructure depends on criticality of the business processes that said participant is engaging in.

11.3.1 Endpoint

The individual endpoints are usually not bottlenecks and as long as there are efficient procedures for restoration after failure, the recommended practise is to build this on a single instance host. The most critical part is the configuration and integrity of the database.

11.3.2 EDX Toolbox

The individual toolboxes are usually not bottlenecks and as long as there are efficient procedures for restoration after failure, the recommended practise is to build this on a single instance host. The most critical part is the configuration and integrity of the database.

12 Evaluation of options

This paper provides a recommendation for adoption MADES/EDX in the Nordic. It is not a complete survey of all options, nor does it cover any alternatives.

It is advised that a set of principles are developed and that those are then used to qualify a recommended deployment option(s). This is regarded as an implementation detail, which can be a deliverable by projects following the intents of this paper.

The principles should, at least, cover:

- Consolidation
- Isolation
- Administration
- Service level agreements.

13 Conclusion

It is advised that a hybrid model is employed, where each member TSO hosts a component directory for their respective country and these are then federated to allow for seamless data exchange throughout the region.

In addition, we recommend that the component directory used by the Nordic-RSC for exchange of grid models on the Nordic-RPN network is kept completely isolated.

Yours sincerely,

Jon-Egil Nordvik
Convenor of NMEG
(Nordic Market Expert Group)

Ove Morten Stalheim
Convenor of NEAT
(Nordic Enterprise Architecture Team)