P6 – Policy 6: Communication Infrastructure

Policy Subsections

A. The EH Network, Architecture and Operation
B. Real Time Data Collection and Exchange
C. File Transfer Data Exchange
D. E-mail on the EH
E. Information Publication in Hypertext on EH
F. Non-EH communication among TSOs

Introduction

ENTSO-E has established a communication network that provides the necessary infrastructure to support all data exchanges among TSOs. The minimum requirements, the rules for the implementation, extension, operation and maintenance of the Communication Network of European Transmission System Operators (Electronic Highway-EH) and the main application services are explained in this document.

The applications themselves, along with the specification of the application data for exchange, are described in the appropriate policies of the ENTSO-E RG CE Handbook. All relevant data exchanges between TSOs shall be communicated using the application services of the EH. If additional application services are required, ENTSO-E will decide how to build, operate and maintain these services.

The EH is a private network dedicated to data exchange among TSOs, that operates under the responsibility of the member TSOs and the network management by the two ENTSO-E RG CE Network Operation Centres (NOCs), primary (pNOC) and secondary (sNOC). The EH extension to additional TSOs is also considered.

Engineering and technically sensitive information are consolidated in a separate Electronic Highway Technical Reference Manual (TRM), maintained by pNOC. The Electronic Highway Technical Reference Manual is marked as a confidential document and it is distributed only to the participating TSOs.

A. The EH Network and Architecture

[Policy Subsection A6–A: The EH Network and Architecture]

Introduction

A meshed private communication network between TSOs provides the necessary infrastructure that facilitates and supports data exchanges among TSOs. This part of the policy describes the necessary framework for the implementation, operation, extension and maintenance of the Communication Network of European Transmission System Operators (Electronic Highway-EH).

The EH is a private network dedicated to data exchange between electricity sector TSOs and operates under the responsibility of the TSOs and the management of the two ENTSO-E RG CE Network Operation Centres (NOCs).

The primary scope of the EH is the real-time data exchange, that enhances the security of operation.

As a result of this, real-time data traffic has the highest priority amongst all the other data communicated.

Definitions

A-D1. Multipurpose Use: The purpose of the Electronic Highway is to exchange:

- telecontrol real-time information (TASE.2 or ELCOM90);
- non-real-time services such as file transfer for exchange of transmission schedules, network model, planning data or statistics (FTP);
- E-mail for special applications Simple Mail Transfer Protocol (SMTP).

A-D2. EH Availability: The EH must be a high availability system. Availability is the percentage of time the EH is in operation. Its calculation is based on the Mean Time Between Failure (MTBF) and Mean Time Between Repair (MTBF), MTBF/(MTBF+MTTR) of each component between two EH gateways including the backup links.

A-D3. Line is a physical point-to-point telecommunication connection between two locations of the TSOs using a dedicated communication infrastructure.

A-D4. Link is a logical connection between two TSOs using one or more lines. These lines may or may not directly connect the two TSOs

A-D5. Direct Connection is a connection between two TSOs using only physical lines.

A-D6. Network Operating Centres: The two ENTSO-E RG CE EH Network Operating Centers (NOCs) perform the monitoring of the operation of the EH and provide technical support to the TSOs. NOC duties are performed by TSOs within ENTSO-E RG CE organizational structure.

A-D7. .

A-D8. EH Backbone: EH backbone consists of all the lines that are crossing TSO boundaries and lines connecting EH backbone routers within the TSO premises.

A-D9. TRM: Electronic Highway Technical reference Manual (TRM) is the document which specifies technical details for the EH. All connected TSOs must follow the technical specification as described in TRM.

Standards

A-S1. TSO connection to the EH

A-S1.1. Every TSO member of the ENTSO-E RG CE ENTSO-E has to be connected to the EH.

A-S1.2. All other ENTSO-E TSO members are allowed to be connected to the EH.

A-S1.3. ENTSO-E Any TSO which is not ENTSO-E member may be connected to the EH if the following requirements are fulfilled:

A-S1.3.1. There is a formal approval of the ENTSO-E SOC for the new connection.

A-S1.3.2. The applicant TSO maintains the confidentiality of information and complies with the Policy 6 and the EH TRM.

A-S1.3.3. There are at least two ENTSO-E TSOs already connected to the EH who are willing to connect the applicant to their EH network equipment. These already connected TSOs have to ensure that there will be no negative impact on the existing parts of the EH concerning availability, quality of service, security and confidentiality due to the connection of the candidate TSO.

A-S1.3.4.

A-S1.3.5.

A-S1.4. Non-ENTSO-E RG CE members may be allowed non-real-time, partial access for an individual application if they participate in ENTSO-E RG CE processes respecting operational procedures.

ENTSO-E

A-S2. Non TSOs entities performing TSO operational process using the EH

The non TSO entities may interchange information trough the EH using the internal network of an already connected TSOs if fulfil the following requirements:

A-S2.1.1. There is a formal approval of the ENTSO-E SOC for the new interchange.

A-S2.1.2. The TSO whose connection to the EH is used to interchange the information has to ensure that there will be no negative impact on the existing parts of the EH concerning availability, quality of service, security and confidentiality due to the connection of the candidate TSO.

A-S3. Connection to Internet. There must not be any direct physical or logical connection between EH and Internet. Data exchange between EH and the outside world should be done under full security procedures. The separation of EH from insecure networks must be guaranteed by use of intermediate gateways. These gateways must be located in a Demilitarized Zone (DMZ) separated by different firewalls from both Internet and EH.

A-S4. Private Network. The electronic highway:

A-S4.1. Shall use only protocols and applications as specified in the TRM.

A-S4.2. Must not have a direct connection to the Internet.

A-S5. Dedicated network for data exchange. The EH is the main and preferred communication media for data exchanges among TSOs related to the operation. The

EH should also be used as communication media for data exchanges among TSOs related to the market.

A-S6. Incorporation of new protocols and applications: Procedure for requesting new protocols and applications is described in TRM.

A-S7. Requirement for EH interconnections

A-S7.1. **TSO connections:** At least two physically independent point-to-point lines with two other TSOs must be implemented in such a way that EH backbone redundancy is ensured.

A-S7.2. If, due to geographical location of TSO, it is difficult to have two independent physical connections to two different TSOs, a suitable second physical connection must be implemented. Such a solution has to be discussed and agreed with neighbours and approved by ENTSO-E.

A-S7.3. **Connection Bandwidth:** A speed of 2 Mbps or higher has to be established for all the lines of the network. Speeds lower than 2 Mbps may only be used after approval from ENTSO-E.

A-S7.4. **Network Extensions:** Any network construction or modification and the minimum technical standard of components have to comply with TRM.

A-S7.5. **EH Availability:** EH is considered to have the same availability as SCADA and should be in operation under any conditions. Each TSO-TSO link should not have lower availability than 99.9% excluding planned outages.

A-S7.6. **EH Reliability:** All data exchanged must be transmitted over the EH from the sender to the recipient uncorrupted, in sequence and in a timely manner. To achieve higher reliability, standard protocols as specified in TRM are used.

A-S7.7. **EH performance:** Under normal operating conditions, when the EH backbone is fully operational, or with an outage of any single EH Backbone component, the transmission delay for real-time data on the EH between any two end nodes should not exceed 2 seconds.

A-S8. TSO infrastructure. Each TSO has to build, operate and maintain the part of the EH network located in its control area, respecting the technical requirements, and to bear the related expenses for investment operation, maintenance and improvement.

A-S9. TSOs responsibilities.

TSOs have to ensure the security of operation of the EH.

A-S9.1. TSOs must take appropriate measures to protect the Electronic Highway and each connected TSO against any potential risks such as (a) operation disruption or data corruption and (b) disclosure of confidential data as defined by law, by regulatory bodies or by bilateral conventions.

A-S9.2. TSOs shall protect against any unauthorised access to the EH.

A-S9.3. TSOs shall perform malware checks. It is the responsibility of each TSO to take care that all files it sends over EH are valid and malware free.

A-S9.4. TSOs shall monitor and ensure the availability of EH components in their domain to reach the specified availability of EH.

A-S9.5. TSOs shall ensure that their own local EH network concept complies with the EH requirements as defined in TRM.

A-S9.6. TSOs shall check redundancy of their physical lines and SCADA connection as defined in TRM.

A-S9.7. The above items must be verified through self-assessment by each TSO. These assessments shall be done periodically as detailed in the TRM.

A-S9.8. The TSO shall respond to requests for proposed actions demanded by ENTSO-E.

A-S9.9. Each TSO shall manage its own components of the network (routers, gateways, physical lines etc).

A-S10. Maintenance: The EH operation shall be treated in the same way as the TSO's SCADA operation. TSOs shall maintain the EH service level and shall follow the troubleshooting procedure which is given in the TRM.

A-S11. EH Wide Area Network: The wide area networking in EH shall use TCP/IP Protocol suite.

A-S12. High Availability Configuration: Network components and gateways must be configured in such a way (e.g. hot standby or load-sharing configuration) that in case of failure of one component the functionality is automatically covered by the remaining components in the redundant system, within a minute.

A-S13. Network Management: The network management shall be implemented by the primary (pNOC) and the secondary (sNOC) Network Operation Centre.

A-S14. Network Operation Centre Activities: The NOCs help with monitoring, troubleshooting, coordination and reporting for the EH. NOCs and TSOs shall cooperate to maintain the agreed operation of the EH.

A-S15. TSO Cooperation with NOCs: Each TSO must cooperate with NOCs and allow access to their EH network interfaces in order to allow NOCs to fulfil their mission as defined in TRM.

A-S16. Change Notification: NOCs and neighbouring: TSOs must be informed of changes, maintenance and testing in the network and the network management equipment.

Guidelines

A-G1. Limitation on sampling rate: EH is neither designed nor suitable for data exchange requiring update rates faster than 2 seconds. Applications that need data interchange at a faster sampling rate than 2 seconds may not work properly on EH.

A-G2. Scanning of Received files: It is recommended that the receiver of the files checks them for malware.

A-G3. TSO connections: To increase the level of redundancy and performance it is recommended that each TSO has more than two obligatory physical lines to neighbouring TSOs.

A-G4. Backup Control Centres: Data exchange over EH will also be available at backup or emergency control centres.

A-G5. Publishing: The change and maintenance information should be sent via e-mail to NOCs and neighbouring TSOs. It may also be published on the web server on EH. Experience shows that many malfunctions occur through uncoordinated changes or mistakes during changes.

A-G6. Reporting. A website/FTP is maintained on the EH for the administrator. Experience reports and other documents of interest to EH users may also be published on this FTP/website. Such a report may include the behaviour of the equipment as well as measurement of the network traffic and the detection of bottlenecks. The details of reporting can be seen in TRM.

A-G7. Information exchange: All necessary and relevant information will be sent to the administrators via e-mail. The information can also be sent to the admin mailbox of the EH or, if necessary, to the Internet e-mail address published in the list of the technical contact persons.

A-G8. Use of Public Key Infrastructure (PKI): Guidelines for PKI use are given in TRM.

B. Real Time data exchange

[Policy Subsection A6–B: Real-time Data Exchange]

Introduction

Exchange of real-time data is the main focus of Electronic Highway. The measurements and switch positions from neighbouring TSOs are important for the secure operation of the transmission grid. The type and the amount of data to be exchanged in real time have to be mutually agreed upon between participating TSOs within the framework of the ENTSO-E RG CE policies. The EH is meant for data exchange which helps the TSOs in monitoring and coordinating operation of the system. It is recommended not to use the exchanged data through EH for real-time control applications. The aim of this section is to list the data types that can be exchanged in real time over the Electronic Highway. This list could be extended in the future.

Definitions

B-D1. Priority of Real-time Data Exchange: Real-time data exchange is the main function of the EH and therefore has highest priority.

B-D2. Scope of Real-Time Data Exchange: The operational security-related data concern high-voltage lines, transformers, breakers, and disconnectors of the transmission networks. They are important for the security of the transmission network, for Energy Management System (EMS) applications and for load flow calculation of Power Application Software (PAS). This may include:

Transmission network:

- Switch status (on, off, in between)
- Active (MW) and reactive power (MVAr)
- Voltage (kV) and frequency (Hz)
- Voltage presence (presence/absence)
- Tap changer position of transformers (step position)
- Alarms (if requested)

Generating Units:

- Unit status (in service/out of service)
- Active (MW) and reactive power (MVar).

B-D3. Bilateral Data Exchange: The data exchange between communication partners is coordinated on a bilateral basis. The data exchange has to be agreed among the participating TSOs.

Standards

B-S1. Real-time Data Exchange: Every TSO must be capable of real-time data exchange on the EH using the TASE.2 protocol. Existing ELCOM90 on EH are permitted, however all new exchanges should be done using TASE.2.

B-S2. Use of TASE.2: At least TASE.2 conformance blocks 1 and 2 shall be used for real-time data exchange on TASE.2 on the Electronic Highway. Conformance to block 4 and 8 is optional.

B-S3. Redundant Configurations: Redundant configurations shall be designed to fulfil the availability criterion. TSO shall ensure that a switchover of local systems (e.g. SCADA, EMS) shall not have any impact on the data exchange with the partners.

B-S4. Quality of Data: Each TSO must be able to assign to data values the associated quality codes (sometimes named attributes), such as:

- valid/invalid
- held or not refreshed
- manually entered or substituted
- estimated or calculated

B-S5. Sign Convention: The convention about the sign of energy flow is: A negative sign refers to energy flowing into a node; a positive sign refers to energy flowing out of a node. Exceptions to this rule have to be agreed bilaterally between TSOs.

B-S6. Real-time Data Exchange Not Included on EH: The exchanges described in this chapter are related to the operational and security-related data of the transmission grid. This does not include data for telecontrol and load frequency control.

B-S7. Data Exchange for Synchronised Phasor Measurements: Since individual Phasor Measurement Unit (PMU) devices generate large amount of data traffic, it is not permissible to connect them directly to the EH. Wide Area Monitoring (WAM) data will be exchanged among TSOs solely through Process Data Concentrators (PDC) exchanging only a subset of the data. Details of protocols and the priority scheme are given in TRM.

Guidelines

B-G1. Independence of Connections: The communication system can maintain many TASE.2 connections to remote systems at the same time. The TSO should try to reduce the number of interruptions due to reconfigurations of existing connections or the introduction of new connections.

B-G2. Commands: It is not intended to exchange commands for switching operations such as breaker opening or closing, as done over SCADA data links, over the EH. The available bandwidth, data volume and various time delays in data acquisition, data transmission and gateways response time may result in an unacceptable level of performance required for the real-time control applications such as interlocking and load frequency control.

C. FILE TRANSFER Exchange using FTP server

[Policy Subsection A6–C. Data Exchange using FTP server]

Introduction

This part contains the document guidelines for file transfer over the EH and the implementation of the File Transfer Protocol (FTP) server. The FTP server is foreseen as the data exchange server for exchanging data and information among TSOs, which are connected on EH.

Definitions

C-D1. Use of the FTP-server: The server is explicitly defined as a data exchange server and will not be used as a data storage or archiving server.

The FTP server is used as a data exchange mechanism for current data requirements of the applications. Each TSO is responsible for archiving the data which he extracts or delivers to the FTP server.

C-D2. Location of the FTP-server: The FTP server(s) are located in a secure TSO environment and are maintained by one of the TSOs.

C-D3. FTP Clients: Each authorised user may access the FTP server using his FTP Client.

Standards

C-S1. Availability: To ensure higher availability, two FTP servers in main and standby mode will be used. If the main server is down, the standby server will be activated.

C-S2. System Maintenance: Responsibility for system maintenance of the FTP servers rests with the owner of the server.

C-S3. Naming Convention: The file naming conventions shall be defined by the authorised application groups (for example ENTSO-E working groups and task forces etc.) planning to use the FTP on EH for file transfer. TSOs using the application will comply with the naming convention.

C-S4. Data Structure: The data structure to be used on the FTP server is defined in detail in the TRM. TSOs will comply with the data structure defined by the application groups (for example ENTSO-E working groups and task forces etc.).

C-S5. Security and User Authorisation: User authorisation will be organised by the system administrator based on the information provided by the users. The authorisation of each user will be maintained in the administration folder. The security and authorisation details are defined in the TRM.

Guidelines

C-G1. Administrative files: The administrative information regarding FTP services is also stored on the FTP server. Only administrators will have access to these files.

In addition to the administration area, an open document area is defined. This area will be open to all the TSOs connected to the EH and will not require any password or access code to read these documents. The area will typically be used to manage guidelines.

C-G2. Data types: Each TSO can upload its data in the defined structure and format. The structure and format of individual files will be decided and agreed upon by ENTSO-E working groups that are working in parallel on their individual topics. In addition to the individual TSO areas, some TSOs may also form a group to exchange information of mutual interest.

C-G3. Access to the data: The TSO which is the data source shall inform the FTP administrator regarding the authorisation for access of this data type. The data can be organised in folders and subfolders and authority can be customised to suit individual applications. The authorisation matrix is defined in the TRM.

C-G4. Used applications: The FTP server may be used for exchanges of non real-time information, such as Day Ahead Congestion Forecast (DACF), Intra-Day Congestion Forecast (IDCF), snapshots data, transmission schedules, network model, planning data or statistics etc.

C-G5. Service Monitoring: The FTP server owner or operator will supervise the use of the FTP server and prepare statistics to allow better management of the services provided and compile information on the main areas of interaction.

C-G6. Data storage capacity and cleanup: The system will be designed to have data storage for data transfer for at least one month.

D. E- mail on Electronic Highway

[Policy Subsection A6–D: E-mail on Electronic Highway]

Introduction

Electronic mail is a service that can be used for operational person-to-person and/or automated application-to-application asynchronous data exchanges between TSOs on Electronic Highway. Each TSO using the service must implement mail client capability (ability to send and receive messages) using its own mail server (SMTP/POP protocols). Exchanged data format is agreed on an application or bilateral basis but should respect, if applicable, ENTSO-E standards such as ESS based on an XML codification.

Definitions

D-D1. Mail-server and Clients: Mail-server and clients may be used on EH for TSO operational use.

Standards

D-S1. Installation of Mail Servers: Each TSO willing to use e-mail on EH shall install and maintain his own mail-server and client.

D-S2. Protocols: SMTP and POP3 standards are applicable for e-mails. The details are available in TRM.

D-S3. E-mail Addresses: The e-mail addresses which are used on EH are defined in the TRM. Appropriate security requirements such as authentication, isolation from Internet virus protection, etc. shall be used for SMTP servers and for clients.

D-S4. Message Body: User data shall be included in the body of the message and/or sent as an attachment. The content of the message standard fields (subject, sender, recipient and so on) shall not be used to encode user information.

Guidelines

D-G1. Used applications: E-mail may be used for applications such as auction results, operational planning, scheduling, green certificates, EH administration etc.

D-G2. Additional Standards: Multipurpose Internet Mail Extensions (MIME) standards are recommended.

E. Information Publication on EH using HTTP server

[Policy Subsection A6–E: Information Publication on EH using HTTP server]

Introduction

Operational TSO information may be exchanged on the EH in the rich hypertext format (HTML) or in the Extensible Markup Language (XML). The information is published on HTTP servers operated by one or several TSOs and may contain statically or dynamically generated pages such as EH NOCs information or SCADA displays as well as scheduling information for exchange of metering and energy transactions, for example . Each user TSO must use client HTTP/HTML (Web browsers) or B2B (business-to-business) HTTP/XML capabilities in order to read the HTML data.

Definitions

E-D1. Use of the HTTP server(s): The HTTP server(s) is explicitly defined for information exchange, and will not be used as a data-storage or an archiving server.

E-D2. Location of the HTTP server: The HTTP server(s) are located in a secure TSO environment and are maintained by one of the TSOs.

E-D3. HTTP Clients: Each authorised user may access the HTTP server using his HTTP client.

Standards

E-S1. Separation from TSO systems: The HTTP server shall be located in the EH and shall be separated through firewalls from the internal network of TSOs.

E-S2. Used Protocols: Hypertext Transfer Protocol – HTTP/1.1, and optional related standards such as HTTPS RFC 2660, RFC 2854. The 'text/html' media type and XML standards are applicable. The details are given in TRM.

Guidelines

E-G1. Appropriate security measures may be used, if required.

F. non-EH communication

[Policy Subsection A6–F: Non-EH communication]

Introduction

It is important that in addition to the data exchange infrastructure using EH for dedicated applications, communication over other media is also available. Other data exchange infrastructure may exist besides the EH network. Such communication between system operators may include voice communication, fax communication, video conferencing, e-mail, and publishing information on the Internet.

Standards

F-S1. Requirements on voice communications: A high availability telecommunication system for voice with all physical neighbours is required for normal and emergency situations.

F-S1.1. Independent telephone systems for operations: A reliable telephone system must be available for operational purposes. This system shall be independent from public telephone systems.

F-S1.2. Operation under emergency conditions: The telephone system shall have provision to operate under extreme conditions (provision of Uninterruptible Power Supply (UPS), redundant equipment etc).

F-S1.3. Backup of the telephone system: The telephone system line should be backed up with extension from the corporate Private Automatic Branch Exchange (PABX) or separate line through the public network.

F-S1.4. Availability of alternative phone: A satellite or mobile phone should be also available for emergency situations. The use of the satellite/mobile phone is allowed only if all the other media are not functioning or for test purposes after bilateral agreement. The procedures for authentication and confirmation have to be agreed among partners.

F-S1.5. Authentication for voice communication: Bilaterally agreed procedures, such as caller identification, shall be established to authenticate the identity of the calling or receiving parties.

F-S1.6. Availability at backup control centre: Voice communication should be available at both main and backup control centres.

F-S2. Requirement for fax transmission

F-S2.1. Availability of fax: Fax equipment should also be available 24 hours a day in the control room.

F-S2.2. Size of documents: At least A4 size paper should be supported.

F-S2.3. Signature on fax: Faxes should be properly stamped with sender's name, and sender's name should be recognisable.

F-S3. Requirements of e-mail on the Internet. Internet e-mail should also be available for operators.

F-S3.1. Availability of e-mail: E-mail availability is not controllable by the parties exchanging the e-mails. However, every effort shall be made to make it available 24 hours a day.

F-S3.2. Virus detection: All incoming and outgoing mails shall be scanned for virus detection.

F-S3.3. Spam blocking and filtering: Each TSO should ensure that a filtering mechanism is in place in order to block unnecessary e-mails.

F-S3.4. Allowed attachments with e-mail: The individual applications are allowed to define the type of attachment to be exchanged. Any attachment which might compromise the security and/or performance of communication infrastructure, such as executable files, sound and video clips, and macros, have to be handled according to TSO information security policies.

F-S3.5. Authentication requirements: The e-mail exchange should be subject to authentication and verification by other means.

F-S4. Voice transmission standards: Voice quality should conform to the CCITT standards G729 as a minimum.

F-S5. Fax transmission standards: The fax transmission should support at least ,the European Standard Group 3 (G3).

F-S6. Video and audio conferencing use and requirements: If needed, video conferencing may be used to discuss topics of mutual interest and help in system operation**.**

F-S7. Video conferencing transmission standard: For video conferencing should support ITU-T standards H.320 and H.323.

Guidelines

F-G1. List of authorised persons: The list of people in system operation authorised to use the non-EH communication should be available in order to minimise risks when the public network is used.

F-G2. List of available communication facilities: The list of all the communication facilities and any changes in the list should be exchanged between TSOs with all the information necessary to implement the communication.

F-G3. Recording of voice communication: All the communications among operators may be recorded and used according to individual TSO policies.

F-G3.1. Replay of the recorded communication: Where other parties or ENTSO-E requires copies, these records should be made available.

F-G3.2. Data privacy and personnel protection: All the communications among operators may be recorded and used according to applicable national and company legal frameworks.

F-G4. Troubleshooting in voice communication network: Any trouble with the lines should be communicated to the involved parties and the restoration should be handled in the same way as a disturbance in SCADA**.**

F-G5. Redirecting communication in case of breakdowns: In case of trouble communicating with another TSO Control Centre, this can be done indirectly through a third TSO that will transfer information or orders.

[Reference documents]

IEC 60870-6-601	Functional profile for providing the connection-oriented transport service in an end system connected via permanent access to a packet switched data network.
RFC 1918, 1597	Address allocation for private intranets
RCF 1122	Requirements for Internet hosts, communication layer
RFC 1006	ISO transport services on top of the TCP; Version 3
RFC 950	Internet standard subnetting procedure
RFC 1305, 1119	Network time protocol
RFC 1331	Point-to-point protocol
RFC 792, 777	ICMP Internet control message protocol
Xml	http://www.edition-w3c.de/TR/REC-xml

ESS ENTSO-E Scheduling System. Refer to www.entsoe.eu – resources – EDI library

ELCOM90

TASE.2