POLICY 6

COMMUNICATION INFRASTRUCTURE

P6 – Policy 6: Communication Infrastructure [E]

Chapters

Introduction

UCTE has established a communication network that provides the necessary infrastructure to support 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 UCTE Operation Handbook. All relevant data exchanges between TSOs shall be communicated using the application services of the EH. If additional application services are required, UCTE will decide how to build, operate and maintain these services.

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

The engineering and technically sensitive information are consolidated in a separate document entitled “Electronic Highway Technical Reference Manual”, maintained by pNOC. The Electronic Highway Technical Reference Manual is marked as a UCTE confidential document and is strictly distributed to the participating TSOs.

History of changes

v.0.9 final policy, approved by the UCTE Steering Committee on 03.05.2006

Current status

This document summarises current UCTE recommendations related to architecture, operation, maintenance, extension and use of the Electronic Highway for data communication. Please refer to the glossary of terms of the UCTE Operation Handbook (see G) for the detailed definitions of terms used within this Policy.

This Policy is based on the EH documents produced by the ETSO Task Force 6 and SGEH as UCTE Document. This document consolidates all the previous UCTE documents regarding communication infrastructure. This version of the document (version 0.9, level E, dated 03.05.2006) has "final policy" status.

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 the data exchange between TSOs, and operates under the responsibility of the TSOs and management by the two UCTE Network Operation Centers – NOCs.

The primary scope of the EH is 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.

Criteria

C1. **EH availability**. The percentage of time the EH was in operation. Its calculation is based on the MTBF/(MTBF+MTTR) of each component between two EH gateways including also the backup links, and it is recommended to be higher than 99.8%. EH is considered to be of the same availability as SCADA, and it is expected to be in operation under any condition.

C2. **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. Incorrect data received (not corrected at the network level), lost data or duplicated data to the recipient decrease the reliability. Data corruption is not acceptable.

C3. **EH performance**. Under normal conditions, the transmission delay on the EH, for a given data volume of mutually agreed real-time data exchange, between gateways should not exceed 2 seconds. The system has to have sufficient bandwidth for a given data volume to meet the required performance. Recommended bandwidth is given in a later section.

C4. **Redundancy.** The EH has to be redundant in order to remain in operation in case of a single failure. This includes network and transmission components.

C5. **Maintenance**. The EH failures should be treated in the same way as the TSO's SCADA. The troubleshooting procedure is given in the Technical Reference Manual.

C6. **Line** is a physical connection between two locations of the TSOs using a dedicated communication infrastructure.

C7. **Link** is a logical connection between two TSOs using one or more lines. These lines may or may not directly connect the two TSOs.

Requirements

R1. **Private network.** The Electronic Highway:

R1.1. Is dedicated to the electricity sector to be used by TSOs only.

R1.2. Transfers only UCTE-approved operational and electricity market data between TSOs. Only approved data exchanges between TSOs and NOCs are transferred over the EH.

R1.3. Shall use only protocols and formats approved by the responsible body of UCTE.

R1.4. Has no direct connection to the Internet.

R2. **Dedicated network for data exchange**. The EH is the communication media for TSOs' data exchanges related to network operation and the market.

R3. **Network Operating Centers.** The two UCTE Network Operating Centers that operate in the respective UCTE Co-ordination Center. NOCs perform the monitoring of the operation of the EH and provide technical support to the TSOs. Both NOCs are represented in the UCTE organizational structure.

R4. **EH interconnections.**

R4.1. **TSO connections.** At least two independent point-to-point physical connections with two other TSOs must be implemented in such a way that EH backbone redundancy is ensured. To increase the level of redundancy and performance, it is recommended that each TSO has additional physical lines to neighbouring TSOs.

If due to the geographical location of the TSO it is unfeasible or excessively expensive to have two independent physical connections to two different TSOs, a suitable backup line must be implemented. Such a backup line has to be discussed and agreed with neighbours, and approved by UCTE.

R4.2. **EH backbone.** The EH backbone consists of all the interconnections that are crossing TSO boundaries.

R4.3. **Connection bandwidth.** A speed of 2 Mbps is recommended for all the lines of the network, a minimum speed of 64 kbps is obligatory. A lower speed than 2 Mbps should only be used as an interim solution.

R4.4. **Network extensions.** Any network construction or modification and the minimum technical standard of components have to be agreed by responsible UCTE bodies.

R5. **EH connections in countries with more than one TSO.**

R5.1. In countries where more than one TSO are active, these TSOs have to develop a solution in accordance with this document within their country.

R5.2. At least the UCTE control block operator should be connected directly to the EH.

R6. **TSO infrastructure.** Each TSO has to build, operate and maintain the part of the EH network located in its control area, and bear the related expenses for investment operation, maintenance and improvement.

R7. **TSOs permitted for connection to the EH**

R7.1. Each UCTE member shall be connected to the EH. TSOs planning to join UCTE should contact pNOC for procedures to connect to the Electronic Highway.

R7.2. Non-UCTE TSOs connected to the synchronous UCTE grid and all members of ETSO can be connected to the EH after UCTE approval;

R7.3. Companies which fulfill TSO tasks on behalf of one TSO or a group of TSOs as described in R5.1 and R5.2 and which are owned by one or more TSOs can be connected to the EH after UCTE approval.

R8. **TSOs responsibilities. TSOs have to:**

R8.1. Ensure the security of operation of the EH.

R8.2. Take appropriate measures to protect the Electronic Highway and each connected TSO against the following two main risks:

8.2.1.1.1. operation disruption or data corruption

8.2.1.1.2. disclosure of confidential data as defined by law, by regulatory bodies or by bilateral conventions.

R8.3. Protect against any unauthorized access to the EH.

R8.4. Perform virus / worm checks. It is the primary responsibility of each TSO to take care of its own input files to ensure that only valid, virus-scanned files are sent to other TSOs.

R8.5. Monitor and ensure the availability and reliability of EH components in their domain.

R8.6. Ensure that its own local EH network concept complies with the EH requirements which is subject to approval of NOCs.

R9. TSOs shall check redundancy of their physical lines and SCADA connection by testing and reporting the actions and the results to responsible UCTE bodies and NOCs. This should be coordinated among neighbours.

Standards

S1. **EH Wide Area Network**. The wide area networking in EH is based on TCP/IP. The IP addressing scheme is defined in the Electronic Highway Technical Reference Manual.

S2. **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.

S3. **Multipurpose use.** The purpose of the Electronic Highway is to exchange:

- telecontrol real-time information (TASE2 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 (SMTP).

Procedures

P1. **Network management**. The network management is implemented by the primary (pNOC) and the secondary (sNOC) Network Operation Center.

P2. **TSOs management activities:** Each company manages its own parts of the network (routers, gateways, etc). Traps are not used in the network.

P2.1. **SNMP.** Everyone has to allow the SNMP read access to its own routers from both Network Operation Centers.

P2.2. **Reports.** All link failures for more than 60 minutes should be reported to the NOCs. In addition, link availability of less than 99.5 % excluding planned outage in a reporting period (one year) should also be reported.

P2.3. **Response time to failures:** Analysis for all link failures should start within 60 minutes. At least one line should be restored to make the link operational. The redundant line should be restored as soon as possible.

P2.4. **Link/Line monitoring:** All TSOs are responsible for monitoring and maintaining the EH links/lines to their neighbours.

P2.5. **Passwords.** Full access password is only known to the router owner. Router passwords (Login / Enable) are local issues and will not be distributed to any of the partners.

P2.6. **Features.** All the routers have to implement Management Information Base (MIB) II, Remote monitoring (RMON) will not be used. Internet control message protocol ICMP (PING) must be open to everyone. There will be no MIB implemented in the gateways.

P3. **Network Operation Centers activities:** The Network Operation Centers have to fulfill at least the following activities and requirements:

P3.1. Distribute the network addresses (pNOC);

P3.2. Create and maintain the primary DNS (pNOC);

P3.3. Be operational 7 days a week and 24 hours a day;

P3.4. React on failure in less than 1 hour;

P3.5. Supervise the consistency of the network (pNOC);

P3.6. Be responsible of the numbering of the serial (physical) line of the network (pNOC);

P3.7. Coordinate the realization and the modification of the network structure;

P3.8. Implement the solutions defined by the responsible UCTE body following the users' requirements;

P3.9. Maintain the documents describing the network (addresses, names, speed and topology) (pNOC) and make them available to all users of the EH;

P3.10. Make a status and activity report to UCTE responsible bodies;

P3.11. Give technical assistance to other TSOs if required concerning the local configuration;

P3.12. Keep statistics of disturbance;

P3.13. Monitor the link state;

P3.14. Collect and distribute the necessary information about persons to be contacted in case of malfunctions, maintenance and changes;

P3.15. Be responsible for the documentation of the EH addressing and naming scheme (pNOC);

P3.16. Issue IP-addresses for the communication lines (pNOC);

P3.17. Integrate new participants;

P3.18. Supervise that new members are integrated in accordance with all rules and guidelines of the EH including mail addresses and IP-addresses.

P4. **Publishing.** Changes and maintenance in the network including the management equipment shall be published because in this way it is easier to detect the reasons of malfunctions. Experience shows that many malfunctions occur by uncoordinated changes or mistakes during changes. Publishing can be done via the web-site (see next procedure) or using the FTP site on the EH.

P5. **Reporting.** A web site / FTP will be implemented on the EH for the admin persons. Every participant should report malfunctions to this site. Experience reports will also be published on this FTP/ web-site. This will include the behavior of the equipment as well as measurement of the network traffic and the detection of bottlenecks.

P6. **Information exchange.** All necessary information will be sent to the administrators via email if possible. The information can be sent to the admin mailbox of the EH or in case of trouble to the Internet e-mail address published in the list of the technical contact persons.

Measures

M1. Monitoring of EH operation:

M1.1 **NOCs** will monitor the link state by one hour polling of the links, and report the statistics to the UCTE responsible body.

M1.2 **NOCs** will communicate any non-satisfactory link performance to the TSOs concerned.

M1.3 NOCs should monitor the EH for :

M1.3.1 Detection of faults

M1.3.2 Coordination of malfunction's correction

M1.3.3 Detection of bottlenecks

M1.4 pNOC shall maintain and update the EH drawing according to the information communicated by TSOs. The drawing should show not only the EH configuration but also the addressees, the names of the interfaces and the bandwidth of the communication lines.

M1.5 pNOC shall maintain and update the telephone numbers and e-mail addresses of the people responsible for operation of the EH in a separate document called „Technical contact person“.

M1.6 Concerning the use of the EH itself, the IT responsible person can be reached by e-mail using the email-address admin@TSO_Abbreviation.etso. The IT responsible person of the Network Operation Center can be reached by using the e-mail address „admin@noc1.etso“.

M1.7 All TSOs are responsible for monitoring and maintaining the EH links and lines to their neighbours.

M2. The responsible UCTE body shall evaluate the EH performance and all link losses of more than 60 minutes collected and reported to the NOCs.

M3. The responsible UCTE body shall report all the links which have less than 99.5 % availability, excluding planned outage. The reporting period shall be one year or less.

M4. Dialed ISDN connections to EH are allowed temporarily. These should be moved to fixed lines as soon as possible. In this case caller line identification is applied for security reasons.

M5. Rules of conduct in case of failures.

M5.1 Each local TSO is responsible for its own equipment while the Network Operation Centers (NOCs) are responsible for all overlapping tasks. In case of overlapping failures like line dropping, the responsibility lies first with the two TSOs being connected by this line.

M5.2 As far as possible, all faults have to be cleared at the local TSO site.

M5.3 It has to be guaranteed that the IT responsible person of every control centre and of the Network Operation Centre can be informed immediately.

M6. **Detection of malfunctions.** A malfunction occurs if one or more TSOs cannot be reached on the EH with one of the functions. This means that one or more functions are out of order. It can be detected in several different ways, by any of the users or technical experts working on the EH.

M7. Reporting and actions in case of malfunctions.

M7.1 The operator at the TSO control center informs the IT responsible person at its own control centre.

M7.2 The IT responsible person at the TSO control centre tries to locate the error and to correct it. If necessary, he informs the IT responsible person at the other end of the link affected to help him correct the malfunction. The Network Operation Centre will be informed additionally if it is necessary to correct an overlapping malfunction.

B. Real-Time Data Exchange

Introduction

For real-time data exchange on the EH, the IEC standards TASE.2 protocol is recommended. The ELCOM-90 protocol may also be temporarily used if mutually agreed by two TSOs.

The type and the amount of data to be exchanged in real time has to be mutually agreed upon between involved TSOs within the framework of the UCTE policies. The EH is meant for data exchange which helps the TSOs in monitoring and coordinating system operation. It is recommended not to use the exchanged data through EH for real-time control applications. The aim of this part 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.

Requirements

R1. Operation security-Related data. These data concern high-voltage lines, transformers, breakers, disconnectors of the transmission networks. They are important for the security of the transmission network, for Energy Management System applications (EMS) and for load-flow calculation of Power Application Software (PAS) and includes:

Transmission network:

- Switch status (on, off, in between)
- Active (MW) and reactive power (MVar)
- Voltage (kV)
- 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).

The data exchange has to be agreed among the involved TSOs.

R2. Outside the scope of the Electronic Highway

R2.1. Load-frequency control. The Electronic Highway cannot guarantee delays less than 2 seconds from the substation to the remote SCADA system, therefore load-frequency control is considered to be outside its scope.

R2.2. Commands. It is not planned to exchange commands for switching operation such as breaker opening or closing as done over SCADA data links over the Electronic Highway. The available bandwidth, data volume and various time delays in data acquisition, data transmission and gateways response time may result in a non-acceptable level of performance required for the real-time control applications such as interlocking and load frequency control.

R3. Quality of data. It must be possible to assign to data values usual quality codes (sometimes named attributes), like:

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

- estimated or calculated

R4. **Maximum transmission delay.** Transmission delay between two Electronic Highway gateways is the time interval between:

- the time when data are available at the sender's gateway;
- the time when these data are available at the receiver's site.

A change in one data object often results in changes in several other data objects shortly thereafter. It is therefore useful to delay transfer of the data for a short interval (called buffer interval) to include several object changes within this interval, so reducing the network traffic.

Transmission delay should not exceed 2 seconds. The delay may arise in buffer interval and while processing data in gateways and transferring it through the network.

R5. **Redundant configurations.** Redundant configurations shall be designed to fulfill the availability and performance criterion. A switchover of local systems (e.g. SCADA, EMS) shall not have any impact on the data exchange with the partners. EH infrastructure shall be constructed as a redundant system where failure of a single component shall not affect the operation of TSO node within the EH.

Procedures

P1. **Procedure data transmission parameters.** The following transfer modes are required:

- Periodic;
- On receiver request;
- On sender initiative;
- Spontaneously (on change of value or quality).

When the spontaneous mode is used, the possibility should be provided to combine this mode with a slow periodic data transfer to increase data integrity.

A typical use of transfer modes would be:

- For status: to combine spontaneous data transfer (sending only the data which have changed) with a slow periodic data transfer, i.e. every 5 minutes.
- For measurements: a periodic data transfer or a spontaneous data transfer in case of a value variation greater than a defined boundary.

It is recommended that partners inform each other during the bilateral agreement phase what transfer modes and refreshment cycles they use. This will allow determining the most suitable transfer mode in all segments of the whole transmission chain.

P2. **Bilateral agreement.** The data exchange between communication partners is coordinated on a bilateral basis. Partners exchange the data as mutually agreed.

P3. **Independent associations.** The communication system can maintain many connections to remote systems. In order to limit the number of interruptions due to connection reconfigurations, the IT responsible person should be able to re-configure one connection without any interference with other ones.
The Electronic Highway should be able to integrate new connections with existing partners or new ones without any significant impact on existing communication links. Particularly, it should be possible to put a new connection into service without stopping and restarting existing ones.

Standards

S1. **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.

S2. **Conformance blocks and service objects required from 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.

C. File Transfer Exchange Using the FTP Server

Introduction

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

Criteria

C1. **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 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.

Requirements

R1. **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.

R2. **System maintenance.** Responsibility for system maintenance of the FTP servers belongs to the owner of the server.

Standards

S1. **Naming convention.** The File naming conventions shall be defined by the application groups planning to use the FTP on the EH for file transfer.

S2. **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. Typical use of this area will be to manage guidelines.

S3. **Data structure.** The data structure to be used on the FTP server is defined in detail in the Technical Reference Manual.

Procedures

P1. **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 UCTE bodies 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.

P2. **Access to the data.** The TSO which is the data source should inform the FTP administrator regarding the authorization for access of this data type. The data can be organized in folders and subfolders and authority can be customized to suit individual applications. The authorization matrix is defined in the Technical Reference Manual.

P3. **Security and user authorization.** User authorization will be organized by the system administrator based on the information provided by the users. The authorization of each user will be maintained in the Administration folder. The security and authorization details are defined in the Technical Reference Manual.

P4. **Service monitoring.** The FTP server owner / operator will check the use of the FTP Server and make statistics to allow better management of the services provided and of the main area of interaction.

P5. **Data storage capacity and cleanup.** The system will be designed to have data storage of at least 3 months.

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 the Electronic Highway. Each TSO using the service must implement mail client capability (ability to send and receive messages) using his own mail server (SMTP protocol) or a remote mail server (SMTP/POP3 protocols) at another TSO. Exchanged data format is agreed on an application or bilateral basis but should respect, if applicable, UCTE standards such as ESS based on an XML codification.

Requirements

R1. The e-mail addresses which are used on Electronic Highway are defined in the Technical Reference Manual. Appropriate security requirements such as authentication, isolation from Internet virus protection, etc. shall be used for SMTP server and for the clients.

R2. User data can be included in the body of the message and/or sent as an attachment. The content of the message standard fields (subject, sender, recipient etc…) shall not be used to encode user information.

Standards

S1. RFC 0821 Simple Mail Transfer Protocol is mandatory and related standards optional. MIME and S/MIME optional standards are recommended.

S2. RFC 1939 Post Office Protocol – Version 3 is mandatory and related standards optional.

Guidelines

G1. The e-mail may be used for applications such as day-ahead congestion forecast, auction results, operational planning, scheduling, green certificates, EH administration, etc.

E. Information Publication on EH Using Http Server

Introduction

Operational TSO information may be published 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 static or dynamically generated pages such as EH NOCs information or SCADA displays and also 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.

Requirements

R1. The http server shall be located in the Electronic Highway and shall be separated through firewalls from internal networks of TSOs.

Standards

S1. RFC 2616 Hypertext Transfer Protocol – HTTP/1.1. and optional related standards such as HTTPS RFC 2660.

S2. RFC 2854 The 'text/html' Media Type, which has replaced the RFC1866 "Hypertext Markup Language 2.0"

S3. **XML Definition.** www.w3.org

Guidelines

G1. Appropriate security requirements such as authentication shall be used.

G2. The EH should be used, if necessary, to transfer TSO information to be published on the server using FTP, mail or HTTP services.

F. Non-EH Communication

Introduction

It is important that in addition to the data exchange infrastructure using EH for dedicated application, 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 and subscribing information on the internet.

Requirements

R1. Requirements on voice communications. A dedicated telecommunication line for voice with all physical neighbours is required for normal and emergency situations.

R1.1. Independence from PABXs. These lines should be independent from the existing PABXs.

R1.2. Operation under emergency conditions. These lines and the related equipment should have provision to operate under extreme conditions of the system. (provision of UPS, redundant equipment etc).

R1.3. Back up of the lines. This line should be backed up with extension from the corporate PABX or separate line.

R1.4. Availability of mobile phone. A mobile or satellite phone should be also available to face emergency situation. The use of the mobile/ satellite phone is allowed only if all the other media are not functioning and the communication is authenticated (explaining the reason of its use) with written confirmation afterwards.

R1.5. Authentication for voice communication. Bilaterally agreed procedures, such as Caller Identification, shall be established to authenticate the identity of the calling or receiving parties.

R2. Requirements for FAX transmission

R2.1. Availability of FAX. Fax equipment should also be available 24 hours a day in the control room.

R2.2. Size of documents with FAX. At least A4 size paper should be supported.

R2.3. Signature on FAX. FAX should be properly stamped with senders name and senders name should be recognizable.

R3. Requirements on e-mail on internet. Internet e-mail should also be available for operators.

R3.1. Availability of e-mail. E-mail availability is not controllable by the parties exchanging the e-mails. However best effort shall be made to make it available 24 hours a day.

R3.2. Virus detection of e-mail. All incoming and outgoing mails shall be scanned for virus detection.

R3.3. Spam blocking and filtering. Each TSO should ensure that a filtering mechanism is in place in order to block unnecessary e-mails to the system operation.

R3.4. 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 modules, sound and video clips, are not allowed.

R3.5. Authentication requirements. The e-mail exchange should be subject to authentication and verification by other means.

Standards

S1. Voice transmission standards. The voice quality should conform at least to the CCITT standards G729.

S2. FAX transmission standard. For fax transmission, the standard usually adopted is the European Standard G3 (Group 3).

S3. Video-conferencing transmission standard. For Video conferencing ITU-T standards H.320 and H.323 are applicable.

Procedures

P1. List of authorized persons. The list of authorized people in the operation using the non-EH communication should be exchanged in order to minimize risks when the public network is used.

P2. 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.

P3. Recording of voice communication. All the communications among operators may be recorded and used according to individual TSO policies.

P3.1. Replay of the recorded communication. In case the other party or UCTE requires copies of these records these should be made available.

P3.2. Data privacy and personnel protection. All the communications among operators may be recorded and used according to applicable national and company legal framework.

P4. Troubleshooting in voice communication network. Any trouble in the lines should be communicated to the parties involved, and the restoration / down time should be handled in the same way as a disturbance in SCADA.

P5. Redirecting communication in case of breakdowns. In case of trouble to communicate with another TSO Control Centers, this can be done indirectly through a third TSO that will transfer information or orders.

Guidelines

G1. Digital signature and encryption. In general, digital signatures and encryption are not needed for TSO_TSO e-mail exchanges. However, on bilateral agreement these mechanisms are allowed for e-mails among TSOs.

G2. 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.