EXaMINE

IST - 2000 26116

Deliverable D-3.6

DEPENDABILITY AND SECURITY ASPECTS

DRAFT v1.1 September 2003

September 29, 2003

DOCUMENT HISTORY AND VALIDATION SERIES

Version	Date	Written by	Checked by	Approved by
0.5	13/01/2003	A. PASQUINUCCI (UNIMI) C. BELLETTINI (UNIMI) E. ROSTI (UNIMI)		
0.8	11/02/2003			
0.9	18/02/2003			
1.0	24/08/2003			
1.1	29/09/2003			

Version	**Evolution history** (reference, date, Modification summary)

Deliverable Description

Objectives

Analyse the dependability and computer security aspects of the EXaMINE architecture, as specified in WP2 and WP3. The following aspects will be addressed:

- Dependability of communication infrastructures
- Security against external events and malicious attacks
- Confidentiality and integrity of information
- Communication performance.

Both Preventives and Emergency Security Control will be addressed.

Task Description

The task will include:

- Analysis of the communication flow among the nodes composing the EXaMINE system and among EXaMINE nodes and other System Operators hosts.
- Identification of the threat model from a computer security perspective and of the reliability, availability and safety critical factors in the architecture from the computer and communication system point of view, with respect to both the system components and the communication flow.
- Identification of performance indices whose value must be guaranteed for system safety and availability and reliability constraints; analysis of the performance of the communication protocol.

Index

Executive Summary

In this Deliverable some aspects of the communications between the nodes of the EXaMINE architecture will be considered together with an analysis of some security issues. Various a priori remarks must be made:

- costs of the implementation must be somehow taken at least in perspective even if they will not be considered explicitly in this Deliverable; the final solutions proposed seem to be cost effective, even if no detailed costs analysis has been done; in the body of the Deliverable, other solutions will be discussed for which not even preliminary considerations of costs have been done;
- the requirements of fast phenomena and almost real-time communications will be the most stringent and difficult to satisfy and guarantee, and will require a very careful deployment of the solution taking in full consideration all possible issues;
- fulfillment of the security requirements conflicts with the previous requirements of almost real-time communications; thus a balance must be found between the needed performances and the security impediments.

This Deliverable is divided in 4 PARTS.

- PART 1 deals with the network design to satisfy all the communication needs of the EXaMINE project. Starting from a classification of the requirements, possible solutions will be presented.
- In the second PART the issue of dependability of the communications will be considered. PART 2 will be divided in two sections, the first one on high-availability and the second one on security with respects to external attacks. Within these two sections all aspects of dependability will be considered.
- In PART 3 the suggested solution will be described.
- In PART 4 an analysis of the Dependability of the communication network will be done according to some results of the DSoS project [46].

1 Communications Infrastructure

1.1 Network Classification and Requirements

Different network communications are requested between different parts of the EXaMINE project. From a geographical point of view there are two classes of communications:

1. long distance, which for this Deliverable will be interpreted as a maximum distance of 10,000 kilometers;
2. regional distance, which is limited to a maximum of 500 kilometers.

The communications can be divided in four classes depending on their type and contents:

1. inter-regional communications used by the Preventive Mode; these communications are long-distance;
2. data exchange for the Transient Stability phenomenon in the Emergency mode; these communications are regional-distance;
3. data exchange for the Voltage Stability phenomenon in the Emergency mode; these communications are regional-distance;
4. network management communications, common to all networks.

We will now discuss the requirements for these four classes of communications.

1.1.1 Inter-regional communications

Data exchange for the protocols of the Preventive mode is bursty, that is at various moments during the day there will be an interaction between two regional Area Centers which requires the sudden exchange of a quantity of data. The amount of data to be exchanged in the worst case is of about 100KBytes, and the full process should take no longer than 5 minutes. Data exchange is done in 2 phases. In the first phase the ICCP protocol is used to transfer general information about each regional Area borders. By an analysis of these data, it could be requested to start the second protocol which requires the exchange of more detailed information in many iterations. Thus communication is in bursts and requires to transfer packets within reasonable time between the locations. In a worst case scenario it will be assumed that each burst consists of transferring 1KByte of data within 1 second.

Requirements: transfer 1KByte of data within 1 second.

1.1.2 Transient Stability communications

The topological setup is the following: in some locations there are the PMUs which must send information to the regional Area Server.[1] In this project two PMU models have been considered, one with a generation frequency of 50 measurements per seconds and one of 20 measurements per second. In the following analysis the PMU with a

[1] For what concerns the issues discussed in this Deliverable, a PMU can be generically considered to be a single device located at a remote site which takes measures from a generator and sends data to the regional Area Center via a computer network.

frequency of 50 measurements per second will be considered. In PART 3 it will be described what will change if the other PMU model will be adopted instead. We will assume for the purposes of this analysis that the distance between the locations is of the order of few hundred kilometers, never exceeding 500 kilometers. The regional Area Server Computational Unit must elaborate the information and then possibly send a remedial action command back to the appropriate nodes under its control. There are different requirements on the total delay within which the full procedure must be completed depending on the type of phenomena. Most of the phenomena require that the full procedure, from the start of the physical phenomenon to the moment in which the remedial action is effective, is completed within 800ms. For a few rare phenomena the procedure must instead be completed within 500ms. In this Deliverable it will discussed the possibility of satisfy this requirement for all phenomena, so setting our maximum total delay to 500ms. In Part 3 it will be discussed if this is possible.

The time needed for the procedure can be detailed as follows:

1. the PMUs take a measurement every 20ms and send it in a single packet; the regional Area Server Computational Unit needs at most 180ms from the beginning of the phenomenon to recognize a pattern which requires an action. Considering always a worst case scenario, it will be assumed that from the start of the physical phenomenon to the moment when the PMU sends the last packet needed for the detection there is a delay of 200ms;
2. the information sent by the PMU reaches the regional Area Server Computational Unit traveling on the network; the maximum delay admissible for this travel must be assured in any circumstance;
3. the regional Area Server Computational Unit receives and elaborates the information, then it prepares a remedial command and sends it; this computation must be done within a fixed maximum delay;
4. the remedial commands reach the remote nodes where they must be put in action; again the maximum delay for this transmission must be assured;
5. at the remote node, an action should be taken and completed; it will be assumed that from the arrival of the packet to the completion of the action there will be a delay of 70ms at most, including the time the device takes to upload the packet from the network.

The aim of this part is to design a network and provide specifications for the hardware and software of the hosts so to be able to guarantee that it takes a fixed maximum time strictly less than 500ms from the beginning of the phenomenon to the enacting of the remedial action. The difference between 500ms and the fixed maximum time allowed is a Safety Factor, which is considered to be necessary due to the possibility of lost measurements, lost packets on the network, need of longer time to recognize the phenomenon or a remedial action which takes more than 70ms to complete. The reason and the use of this Safety Factor will be described in detail in Part 2.

Moreover, the amount of information exchanged is not too big, the typical higher-layer packet containing the data is at most 400Bytes. Indeed a PMU can send for each measurement 66 single-float plus a time-stamp, this amounts to almost 300Bytes; adding some extra Bytes for the application level protocol headers, the total data sent is between 300 and 400Bytes. It is estimated in this project that a PMU will have a maximum packet generation frequency of 50 packets per second, or one packet every 20ms. This gives a data traffic of approximately 160Kbps, not considering overhead due to lower layer encapsulation, nor encryption and other security overhead.

The topology of the network is a typical *Star*, with one center, the regional Area Server

Computational Unit, and many satellites, the PMU and the remote nodes where remedial actions are taken. No direct communication between the satellites is requested. This implies that there are different requirements between the satellites nodes and the regional Area node for what concerns the internal network. Indeed at the satellite nodes the internal network is very simple since only one device is connected to it. Instead at the regional Area node many external lines arrive and more devices will be present which will require the presence of a full Local Area Network (LAN).

A slightly different configuration is possible, and has been considered in this project. At each power plant there can be more than one PMU, and from the point of view of the algorithms all of them are consolidated in a virtual PMU-plant. It is then possible to have all PMUs send their data to the regional Area Center independently, or to have a device at each remote location which does the consolidation of the data before sending it to the regional Area Center. This device could also run the Artificial Neural Network (ANN). In this Deliverable it will be considered the case in which each PMU sends independently its data to the regional Area Center. Modifications and other possibilities will be described where needed.

Requirements: transfer packets with 400Bytes of data every 20ms so that a remedial action command is put in action within 500ms from the starting of the phenomenon.

1.1.3 Voltage Stability Communications

The setup is very similar to the one for Transient Stability and some satellite nodes could be used for both measurements. The kind of data exchanged is the same, what changes is the time requirement. Indeed to detect a Voltage Stability problem it is required to analyze measurements for a few seconds and the delay from the beginning of the phenomenon to when the remedial action has to be enacted is of the order of at least a few seconds. For these reasons, network solutions for the Transient Stability communications can be adopted also for the Voltage Stability communications. Thus, in the following discussion of the networking for the Voltage Stability communications, we will restrict ourselves to indicate possible modifications with respect to the solutions described for the Transient Stability communications.

Requirements: transfer packets with 400Bytes of data every 20ms so that a remedial action command is put in action within 2sec from the starting of the phenomenon.

1.1.4 Network Management Communications

All the equipment at remote locations, for the Transient and Voltage Stability cases, and network links in all cases, must be monitored and some hosts must be accessed remotely for maintenance. Maintenance communications do not need particular networks since data is small and delays do not need to be minimized in the order of the milliseconds. Often maintenance is done *in-band*, that is using the same network as the one for the data. This solution could be adopted here, except that for the Transient Stability networks, but it is not suggested in general for reasons which will be discussed in Part 2.

Requirements: allow communication with all remote hosts for maintenance and surveillance.

1.2 Network Infrastructure

1.2.1 General Considerations

In the next sections various technological solutions for the network connectivity of the EXaMINE nodes will be presented. Not all existing technological solutions will be discussed in details, but only the ones which present themselves as the most promising candidates. In particular, technologies which are not enough dependable or lack in security will be only mentioned.[2] In particular radio links using high orbit satellites will introduce too large delays, whereas low orbit satellites are too new and it is not clear yet if their characteristics will be able to match the requirements of the EXaMINE communications. Ground level wireless communications are at the moment limited to relatively short distances, which requires the implementations of many antennas to relay the signal with added extra delays. The dependability and security of wireless communication must also be considered and compared with wired communications, and are in favor of the latter ones. Moreover for the EXaMINE project it has been deemed best to present solutions which are technically deployable today, if at all possible, leaving aside new technologies which as of today cannot be implemented as they do not exist yet on the market.

Due to the different infrastructures of the energy companies that could implement the EXaMINE system, it has been decided to present solutions which can be implemented both by those that own and manage directly the data communication networks between their nodes, and those who instead rent circuits from Communication Service Providers. A detailed analysis of the problems and strengths of both approaches is outside the possibilities of this Deliverable. It should anyway be mentioned that creating network infrastructures reserved for the use of public systems like EXaMINE could be the best approach to guarantee the dependability required by these systems.

The technologies and solutions which will be described, will, at the end, be standard, well-established and proven. It is considered to be a success if it is possible to satisfy the requirements of the EXaMINE communication infrastructure adopting market technologies which are well-established, based on open and verified standards, adopted and well tested by many users around the world. It has to be noted that the technologies which will be described here, were not so easily available four years ago. Indeed four years ago it would have been much more difficult, if not impossible, to satisfy the requirements of the Transient Stability Communications by leasing circuits from a Communication Service Provider.

Moreover in designing the network to connect the EXaMINE nodes, it will be of the utmost importance to consider timing properties that the communication infrastructure should provide. For this reason a **Worst Case Execution Time** (WCET) analysis will be carried out all through this Deliverable. This is necessary since for most of the EXaMINE connections it is not important that in *average* the communication will guarantee some maximum delay, or that the infrastructure is able to deliver a large

[2] See also Section 2.1.8 for a brief discussion of security and dependability problems of other network technologies.

quantity of data, but instead it is very important that the information will be delivered always within real-time constraints.

1.2.2 Inter-regional Infrastructure

The amount of data to transfer is relatively small, indeed 100KBytes in 5 minutes makes an average of 3Kbps, whereas 1KByte per second means 8Kbps. Adding to these numbers the headers due to the lower protocols and assuming that the data is transferred in small packets so that the headers will be as much as the data, circuits of 20Kbps or 30Kbps could in principle satisfy the requirements. Even if the requirements are such, it is suggested to adopt much faster circuits since these give better assurance for service and higher stability. A dedicated 256Kbps leased circuit with, for example, Frame-Relay protocol could be adopted as a WAN link. Alternatively if the site has a 2Mbps connection with ETSO-Electronic Highway, this could be used also for this traffic, under the strict requirement that either some bandwidth is reserved for this traffic, or that the circuit is never over 75% of its capacity, otherwise there will be bottlenecks and the requirements for the Inter-regional traffic will not be satisfied.

It is suggested to adopt an internal LAN, to which the servers and the local routers are connected, with standard full-duplex 100Mbps Ethernet connections. Again the only precaution is to avoid bottlenecks and if possible reserve bandwidth for this traffic.

Suggestions: adopt a dedicated 256Kbps leased circuit with, for example, Frame-Relay, or use a 2Mbps connection with ETSO-Electronic Highway.

1.2.3 Transient Stability Infrastructure

The connection between the PMU and the regional Area Server Computational Unit is considered here. Identical considerations can be done for the connection between the regional Area Server Computational Unit and the nodes to which it should send information and in case a remedial action command. The starting configuration for the analysis is indicated in Figure 1. This configuration is possibly over-simplified, but it is taken as the starting point of the analysis.

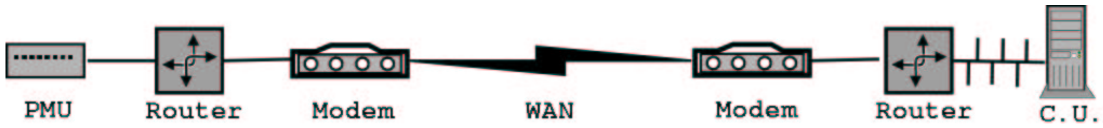

Figure 1: Starting Network Configuration

The PMU is connected to a router through a simple internal network, the router is connected to the long distance carrier service through a *modem* or equivalent device (CSU/DSU, DCE/DTE etc.). The data travels through the long distance carrier service network (data WAN) to the regional Area Center where another modem or equivalent device is connected to a router. This router is connected to a LAN to which the regional Area Server Computational Unit is also connected.

The timing composition is as follows:

- PMU handling time at the transmitter
- transmission delay time on the LAN
- time the router needs to receive, elaborate the packet and send the packet out to the modem
- modem, or equivalent device, delay
- transmission delay time on the WAN network
- modem delay on the receiving side
- router delay on the receiving side
- network delay on the receiving LAN
- regional Area Server Computational Unit handling time at the receiving side

To understand how to interpret the delays, it is necessary to describe how the packets travel along the physical network. Each packet is comprised of a set of bits, each one of them is sent as a signal on the physical medium in sequence, one after the other. The usual unit adopted for this is the number of bits per second that an interface sends on a physical medium. If an interface runs at 8Kbps, in one second it sends on the physical medium a full packet of 1KByte (1 Byte = 8 bits). This implies that the delay at the arrival of a full 1KByte packet, that is when the receiver has the full packet, is given by 1 second, the time the sender takes to send the full packet, plus the travelling time of the signals on the physical medium.[3] Routers usually receive a full packet before examine it, act on it if necessary, and then send it to the outgoing interface. This behaviour of routers introduces large delays, and for this reason national and international network provider are introducing alternative techniques which allow switching packets through routers (using for example Multi-Protocol Label Switching, MPLS [13]) reducing the delays for the transit of packets across their backbone in some cases even by an order of magnitude.

The speed in bps of a telecommunication link is usually taken as a measure of the amount of information that can be transferred through the link in one second. In the case of the PMU the amount of data is modest, on average just 160Kbps. What is more important is the delay it takes to transfer the data and in order to minimize this it is necessary to increase the speed of the communication channel.

1.2.3.1 The LAN Segment

On the PMU segment it has been proposed to use an Ethernet [6,21-23] connection between the PMU and the router. In this case there can be a direct physical connection with a short cable between the router and the PMU. In case other hosts had to be connected to the router, it is suggested that the other hosts not be connected to the same Ethernet interface as the PMU using a hub or switch. Thus, in this case, the router should have at least 2 Ethernet interfaces of which one reserved for the PMU.

MAC frames transit on an Ethernet cable. The shortest possible MAC frame is 72Bytes, the longest 1526Bytes. 26Bytes are MAC headers and the remaining 46

[3] Actually the delay of the receiving interface is not exactly identical to the one introduced by the sending interface but this can be ignored for the current purposes.

to 1500 Bytes are data. It has been suggested to use IP as the protocol at the network (second) level of the OSI stack. Thus 20Bytes of the MAC frame data are IP headers. Moreover it will be suggested to use UDP [16] at the transport (third) level of the OSI stack, which adds another 8Bytes of headers. Thus, without any application level data, a MAC frame has 54Bytes of headers. Adding approximately 400 Bytes of data, the typical MAC frame is of 454Bytes, which for purposes of estimates will be approximated to 500Bytes.

The PMU models which have been considered for this project have half-duplex 10BaseT Ethernet interfaces. A half-duplex 10BaseT Ethernet connection (with cables of Cat V) transmission is approximately 3Mbps (this estimate is conservative).[4] This implies that to transmit a packet the interface takes 1.33ms. The speed of the signal in a Cat V cable is 231,000Km/sec and for a distance of 20mt the signal takes 0.00008ms to propagate. Using instead a full-duplex 100BaseT Ethernet connection, the transmission speed is approximately 60Mbps and the interface takes 0.066ms to transmit a 500Bytes frame. Thus at a remote location where is located only a PMU, a half-duplex 10BaseT Ethernet direct connection could be sufficient to guarantee an acceptable delay. Otherwise it would be suggested to always to adopt at least full-duplex 100BaseT Ethernet connections to guarantee delays less than one millisecond.

At the regional Area Center, the topology of the LAN is more complicated and it could not be possible to make a direct Ethernet connection between the router and the regional Area Server Computational Unit (see §1.2.2.9). Thus there will be a reasonable high level switch (not an hub) with guaranteed fast switching characteristics. It should be possible for example to use the *cut-through switching method* in which the LAN switch copies on the internal buffer only the destination address, looks it up in the destination switching table to find the outgoing interface, and then forwards the frame out even before all the frame has arrived. Using this method, contrary to the *store-and-forward switching method*, no CRC [29] (error) check of each frame is performed, so no error is detected, but the lowest latency is achieved.[5] Some switches allow to set user-defined error-threshold so that if the error threshold is reached, the switch will pass to the store-and-forward method, and when the error rate falls below the threshold the cut-through method is applied again. The router(s) and the local computers will be connected to this switch. From the previous consideration it is strongly suggested to use a switch dedicated only to this traffic, and to use only full-duplex FastEthernet links. Doing so would guarantee that the total delay on the transmitting and receiving LANs, including the handling time of the network cards, will be at most of 2ms.

To further increase the speed of transmission at the regional Area Center, it could be considered to deploy a full GigabitEthernet LAN at 1,000Mbps instead of a FastEthernet network. In this case the transmission speed is approximately 600Mbps and the interface takes 0.006ms to transmit a 500Bytes frame. Consequently, the total delay on regional Area Center LAN, including the handling time of the network cards, will be much less than a millisecond.

[4] For what concerns transmission speed, only worst case scenarios will be considered. Indeed for small packets and ignoring other traffic (like ARP), a 10BaseT Ethernet could run up to 3 times faster. More correctly, a 10Mbps Ethernet runs at 10Mhz.

[5] A discussion of error detection will be done in Part 2.

Moreover it should be considered the number of PMUs connected to the regional Area Center. For example if 100 PMUs are connected to the regional Area Center and each one sends every 20ms 400Bytes of data, 500Bytes packets, a 100BaseT FastEthernet LAN will take at least 7ms to deliver them to the Computational Unit. In case each PMU sends larger packets, the delay can become of the order of the tenth of milliseconds and it will be necessary to deploy a full GigabitEthernet LAN at 1.000Mbps.

Suggestions: adopt at least full-duplex 100BaseT Fast-Ethernet; for direct connections to PMU (or equivalent devices) half-duplex 10BaseT Ethernet could be acceptable.

1.2.3.2 The WAN Segment

Analogous considerations to the previous case can be done for the delays of the router and WAN transit. First of all, the velocity of signal in an optical fiber is 205,000Km/sec. On distances of 500Km this implies a signal travel time of 2.5ms. Usually a Telecom service provider would not have a single unique fiber going from one customer location to another, but the signals will pass through routers, repeaters, modems etc. which will add delays. A European commercial standard for rented telcom lines which recently has started to be quite commercially spread, is of circuits at a speed of 2Mbps (E1). A packet of 500Bytes takes 2ms to be transmitted by an interface at 2Mbps. The total dimension of the packet is given by the IP [17,44] packet to which are added the headers of the Data Link Layer protocol whose length depends on the protocol chosen. Usually the extra Data Link Layer headers can go from 5Bytes to 50Bytes and since the UDP/IP packets are of 428Bytes the full transmitted packets should always be at most of 500Bytes. Thus, theoretically, the data under consideration could be transported in approximately 5ms from the sending to the receiving router.

It is not easy to give an a priori estimate of the delays for a leased 2Mbps circuit from a commercial Telecom operator. Current industry standard results indicate that average delays, as measured with icmp echo-request/echo-reply IP packets (also known as *ping*) [18] between routers on the European backbone of leading operators, are of the order of 20ms (one-way),[6] up to 40ms (one-way) for routers belonging to networks of different operators [2,7,8,10,11,14,41,43]. It is to be noticed that the standard dimension of an icmp echo-request/echo-reply IP packet used for these tests is between 84 and 100Bytes. Tests with larger packets show that the delay does not change appreciably, just one or two more millisecond for 500Bytes packet, if the network is with a very light load. On regional, and not European, scale the average delays are of the order of 10ms.

The time the signal takes to reach the customer premises on the 2Mbps leased line (the so called *last mile*) must be added to this delay. Different technologies exist for this connection, at the physical level it can be copper or optical fiber, and the signaling protocol can be SONET/SDH, HDSL or other variants of the DSL family, Direct Numerical Connection (CDN) etc. The exact solution to be chosen depends on many local factors like the distance of the customer premises to the closest Point of Presence (POP) of the Telecom provider, the possibility of

[6] All the estimates presented are conservative.

deploying optical fibers between the POP and the node, the length and quality of the copper lines etc. For each node a detailed study of the solutions must be done, which guarantees a delay of no more than 5ms in the last mile, including CSU/DSU or DCE/DTE terminals (improperly generically called modems) latency.

In conclusion, industry standard 2Mbps leased circuits of a single provider can offer customer router-to-router one-way transfer time of small packets (full packets of 500Bytes) of about 25ms on regional distances.

To achieve this result, and obtain guaranteed service [27,32], besides the physical layer it is important to use a correct Data Link Layer protocol. The choice of this protocol can be common to all nodes or not. The current industry standard is to adopt the Asynchronous Transfer Mode (ATM) switching protocol [1]. This protocol has been developed for real-time, like voice and video, packet switching and it lends itself very well to the current situation. ATM is a cell switching and multiplexing technology with guaranteed capacity and constant transmission delay in circuits from a few Mbps to many Gbps. Each cell is of 53Bytes of which 5 are headers and 48 are data to be transported.[7] Thus the IP packet in consideration should fit in 9 ATM cells. Telecom service providers offer ATM leased permanent virtual circuits (PVC) between two customer endpoint routers with guaranteed bandwidth and maximum latency.

It must be noticed that not every provider could be able to offer an ATM circuit in all locations, and alternative circuits, like CDN, can be adopted as far as they satisfy the requirements described in this document.

Suggestions: adopt 2Mbps dedicated ATM WAN circuit with guaranteed delay, it is suggested to request guaranteed one-way average delay of the order of 20ms and maximum delay less than 60ms.

1.2.3.3 More Considerations on the WAN and LAN networks

A few more points must be considered. In the previous sections it has been proposed to use a 2Mbps ATM leased circuit to connect a PMU node to the regional Area Center, but the bandwidth used at the IP level (headers included) would be only of approximately 160Kbps. It could be considered to use this circuit for transmitting also other data since only 1/10 of the capacity of the circuit is used. (To have a fully reliable circuit on average no more than half of its capacity should be used.) If other data besides the packets sent by the PMU, is sent on this circuit it is possible that the previous estimates for the transmission time will not hold. Indeed if other data is transmitted on the circuit, the PMU packet will have to wait in the router queue until all previous packets have been sent on the circuit. This will add a delay which is difficult to estimate and that invalidates the previous estimates. It is possible to divide the traffic in the router assigning the packets coming from the PMU to a real-time, maximum precedence queue, all other traffic to low precedence queues. When a PMU packet arrives in the router it will be put in the maximum precedence queue and it will be the next packet to be sent on the circuit ahead of any other packet coming from other sources already waiting in the router queues. This solution is

[7] This does not mean that one 48Bytes packet fits exactly in one ATM frame, since more headers are added in the data portion of the cell by the ATM Adaptation Layer protocol (AAL).

still not good enough because the PMU packet cannot pass ahead of the packet that is currently sent by the router. In the worst case in which a PMU packet arrives just when the router has started sending on the circuit a 1500Bytes packet, the PMU packet will have to wait that the full 1500Bytes packet is sent, which will add a waiting time of 6ms at 2Mbps. Since the PMU packets are approximately 500Bytes, one solution to this problem is to reduce the MTU of all router interfaces and of all hosts connected or which can send packets to the router, to e.g. 600Bytes from the standard 1500Bytes of Ethernet. On the other side, this could introduce problems for the communication between hosts on the LAN.

Another possible solution[8] to this situation is to use a fundamental feature of ATM, that is the possibility of creating Virtual Channels within a Permanent Channel. In other words, it is possible to divide the 2Mbps link in sub-links and it is possible to specify for each sub-link the guaranteed capacity, delay etc. It could then be possibile to divide, for example, the 2Mbps link in two links of 1Mbps each. Being ATM a multiplexing protocol, it will send on the wire alternatively the frames belonging to each Virtual Channel. Thus if one VC is used by the small packets coming from a PMU, the other VC can be used by other data, even with large packets. Indeed the small packets will not have to wait since they will be immediately sent down the wire multiplexed with the large packets. Moreover the speed of the interface is still the same, 2Mbps. What changes is that not all consecutive frames belong to the same flow, so that if a packet does not fit into one frame the next frames carrying the rest of the packet will not be consecutive to the first one. Effectively, in our example we are halving the speed of the interface so that the packets coming from a PMU will be sent at 1Mbps. This gives for a 500Bytes packet a delay of 4ms. Thus it is not suggested to use the PMU data WAN circuit also for other traffic. If it is really necessary to adopt such a solution, extremely careful evaluation must be done.

Analogous considerations should be done for the Ethernet LAN. If on the LAN there are connected also other hosts besides the router and the PMU, and at the regional Area Center the router and the Server Computational Unit, delays can be added in the transmission of the PMU packet if other traffic is running on the wire, in particular if packets are arriving to the router or broadcast (i.e. ARP) packets are sent to all hosts on the LAN. In these cases the PMU packet will be held in queue for example in the PMU interface card, adding usually minimal but in worst case scenario not tolerable, delays.

Analogous considerations should be done for the router itself. The delay added by a router in receiving and forwarding a packet depends not only on the speed of the interfaces, but also on the speed with which the router reads and if needed acts on the packet. This depends on the speed of the CPU and in reduced form on the amount of RAM memory of the router. Moreover, high level routers usually offer fast forwarding (almost switching) capabilities, where after a first packet is examined by the CPU and its routing is found, all future packets of the same type are directly sent from the arriving interface to the sending interface, thus reducing the delay. An example of this is Cisco Express Forwarding (CEF) present in recent IOS versions on high level Cisco routers. Thus in considering a

[8] Other solutions exist, like Link Interleaving on ppp-multilink [30], but are not suggested in this case.

router, due care should be taken in the speed of its CPU and forwarding capabilities.
All these considerations point to have LAN and WAN circuits, routers and switches (almost) completely reserved for the transit of the PMU packets and the regional Area Server Unit remedial action packets. Even if this will under-utilize the hardware from the point of view of capacity, it will guarantee the requested latency.

Finally, if at a PMU location there is also a unit to which the regional Area Center Computational Unit should send informational or remedial action packets, and if these packets are of exactly the same type and generate exactly the same kind of traffic as the ones of the PMU but in the opposite direction, then the same WAN circuit and router can be used for this traffic also. Alternatively a different ATM VC can be created to transfer these packets, as discussed before. Again the host which should receive these packets must be connected on a different (Fast) Ethernet interface of the router than the one to which is connected the PMU.

Suggestions: reserve WAN and LAN circuits only for communications between PMUs and regional Area Center, with the only possible exception being traffic going in the opposite direction for remedial action commands.

1.2.3.4 Transport Layer Protocol

Having chosen to use IP as the Network Layer Protocol, it remains to choose the Transport Layer Protocol. There are two possibilities for the Transient Stability case. The first is to use UDP. UDP adds an 8Bytes header to the data packet and offers a connectionless protocol in which the sender of the packet does not expect to receive an acknowledgment of the arrival of the packet. Acknowledgments, checks and all other connection oriented features must be implemented at a higher application layer. In the case at hand, this is the requested behavior. If TCP [19,20] were to be used instead, before sending some data, 3 packets should have been exchanged between the two peers to establish the connection, and all delay estimates considered before would not apply. It could be considered to establish a single TCP session to transfer all packets for an indefinite amount of time. In this case the overhead of the establishment of the TCP session will be only for the first packet at the beginning of the connection, and this probably is not a problem. In any case, TCP acknowledges the arrival of the packets, sending ACK control packets back. Moreover, if a packet is lost for any reason, TCP adopts a *sliding window* approach, that is the sender keeps sending a few other packets even if it has not received the ACK for the missing packet, in case the lost packet will arrive out of order. The receiver will get these new packets, but since it misses one, it will hold them in a buffer. If the packet is really lost, then it will be resent and when the receiver gets it, it will pass to the application all the packets held in the buffer at once. This behavior will introduce large and variable delays and it is not acceptable. The use of UDP is the suggested solution.
If for some reason the use of UDP is not possible, the alternative would be for the applications to send and receive directly IP packets skipping altogether the

Transport Layer protocol. In this case appropriate drivers should be engineered for creating, sending and receiving the packets on the PMU, the regional Area Center Computational Unit and the units which receive from it informational or remedial action packets.

Suggestions: adopt UDP as Transport Layer Protocol since the sliding window property of TCP will introduce unacceptable delays when a packet is lost during transmission.

1.2.3.5 A Small Test

To verify if the previous considerations hold to a final practical application, some preliminary tests have been done. For the first test an existing network of a private company has been considered. The setup was much below the previously recommended specifications. Two routers were physically located at different premises of the company at a physical distance of approximately 100 kilometers. The routers were entry level 1721 Cisco with operating system IOS-12.2 with VPN 3-DES feature. At both premises there was an internal LAN connected to an Ethernet interface of the router. The routers were connected to the public internet backbone of a Telecom service provider through a 2Mbps Frame-Relay on HDSL link. It should be noted that Frame-Relay was used, which has lower quality and higher latency than ATM. No guarantees of service were offered by the Telecom service provider. Moreover the Frame-Relay links did not connect directly the two customer routers with a single virtual circuit, but instead each router was connected directly to the public internet backbone of the Telecom service provider. Thus a packet from one router would cross the public Internet, even if just within the same Telecom service provider, before reaching the other router.

As mentioned in §1.2.2.2, various ping tests with 100Bytes packets were done from one router to the other. The tests were done when no other traffic was passing through the routers and at a time when the traffic on the Telecom service provider backbone could be considered normal. The result for the round-trip time of the 100Bytes ping packets were: minimum 28ms, average 29ms, maximum 36ms. Usually the first packet in a series (1 packet per second) would be the slowest. This denotes that at least some routers in the path would fully route the first packet, whereas the subsequent packets would be fast-forwarded. This behavior would not appear with a direct permanent ATM virtual circuit. Thus the average transit time, router to router, for a small packet was of 14.5ms, the worst of 18ms. No difference has been measured when sending a ping packet from a router to a host in the LAN of the other router, which implies that the LAN delay was below 1ms. Thus in this small test it would have been possible to transfer a packet of 100Bytes from a host on one LAN to a host on the LAN in the other premise in less than 20ms.

Another test has been done on a similar network of a different private company. The routers used were again some Cisco 1721, the distance between the locations, more than two, this time were between 50 and 100 kilometers, there was also a firewall (Cisco PIX) and the tests were done from server to server, not from router to server. 500Bytes packets were used for the ping tests and the maximum one-way delay has been 16ms.

The setup for this test should be considered only indicative and must not be adopted for the situation under consideration. Indeed no guarantee of service was provided and it is not suggested in any case to adopt Frame-Relay instead of ATM due to the lack of guarantee on latency for Frame-Relay.

1.2.3.6 Advanced Network Solutions

The architecture indicated in the previous section can be upgraded in case the final analysis will require higher standards to be fulfilled. A physical limit which cannot be modified is the signal travel time in optical fibers, which for distances of 500Km is 2.5ms. If stronger guarantees and higher speed must be achieved than those achievable with the solution described earlier, the best solution would be to realize a direct connection on optical fibers. Indeed increasing the speed of the link to 34Mbps or 155Mbps will not change much the delays of the configuration previously described, since these delays are given by the transit of the packets through the network of the telecom service provider. Eliminating all routers and WAN switches on the path should reduce the principal cause of the 10-20ms delays. The simplest solution would be to pose an optical fiber from each node to the regional Area Center and to directly connect the optical fiber to the PMU on one side and the regional Area Center Computational Unit on the other side. Apart from the extremely high operational costs of posing optical fibers which could be not an issue in many cases since at the locations of many nodes interested by the EXaMINE project there could be already optical fibers, this would require to find or develop suitable hardware interfaces to connect directly the optical fibers to the hosts. The use of fibers is suggested because fibers dissipate the signal less than copper, for example, and can carry the signal for longer distances and require a lower number of repeater or amplifiers. This solution would avoid the use of any router, switch, LAN etc. and the time a packet would take to travel could reduce to 4-5ms on distances of 500 kilometers.

In case an optical fiber is not already present at a node, a less extreme solution could be of using direct copper connection from the customer premises with high speed signaling protocols like HDSL, or faster, to the POP of the service provider where the signal would be directly transferred to optical fiber, or a leased Lambda Frequency of a fiber or of a SONET/SDH channel. Thus the use of a fiber, or multiple pieces of fibers, would be rented from the Telecom service provider whereas the last mile link would be on copper. As before, the line would be directly connected to the hosts, avoiding the use of routers, switches, LAN etc. but there will be still need of transceivers and modems to transfer the signal from one means to the other. Depending on exactly how such a solution would be implemented, traveling time of a packet could be similar to the previous one or two times larger. On the other side, costs would be significantly lower. It is to be noted anyway that such a solution, besides the absence of routers etc., technically does not differ too much from what a telecom service provider could offer as a full service.

1.2.3.7 An Alternative Network at the PMUs Locations

A possible problem is if the PMUs do not filter the data which they send, and thus send many data which are not of interest for the Transient Stability phenomenon or the format in which the data is sent is not appropriate for network delivery. There are obviously two possibilities if a PMU sends more data than needed.

1. The extra data is small and its transit on the network does not modify the previous estimates. In this case the extra data can be dropped by the Computational Unit.
2. If the extra data is not small, it might interfere with the estimates just discussed, and in this case it could even generate an overload at the Regional Area Center Computational Unit when adding the data from many PMUs. It is then necessary to filter the output of the PMU before sending it on the WAN circuits.

Also if the PMU data is not appropriate for network delivery, it must be transformed just as it is sent out by the PMU. If the PMU sends the data using a protocol not acceptable for the previous requests, like TCP, this host could receive the data from the PMU using TCP, but send it to the regional Area Center using UDP. In this case, TCP would be used only on a direct Ethernet connection where the possibilities of lost or corrupted packets are extremely small, thus reducing the problem described before.

If any of these two problems happen, a computer should be directly connected to the PMU. Extreme care must be taken to guarantee that this host will not add intolerable delays. For this, the hardware must be chosen appropriately with low latency in interface cards, busses and timers, and the Operating System should be preferably a Real-Time one. In any case, such a host will add a delay of a few milliseconds, which could require modifying the previous network setup. If the delay added by this host turns out to be large, one possibility to reduce the delay is to eliminate the router at the PMU premises and add an ATM WAN interface card directly to the host. This solution has anyway many potential problems: for example it is possible that the hardware which guarantees the requested performance can not manage the needed ATM WAN interface card, moreover in PART 2 more jobs will be given to the routers for various aspects of security, from routing on backup circuits to encryption, and all of these should also be supplied in case by this host.

Moreover, as already mentioned, at a remote location there can be more than one generator and more than one PMU. An alternative network architecture has been suggested where the ANN (see §1.2.2.9) are at the remote locations on the host just mentioned. The ANN would receive all data from all PMUs present at the location and elaborate it, sending to the regional Area Center only the elaborated data already consolidated. There is anyway one problem, the ANN must receive some data from a reference PMU before being able to do any elaboration. This means that every 20ms the ANN must wait for this data before starting the elaboration. This data must arrive through the network from a remote PMU. Since all PMU are synchronized the ANN will have to wait after it has received the data from its PMUs to get the one from the remote PMU. This will introduce delays of at least 20ms and it is not suggested.

If more than one PMU are at a remote location, two possibility can be devised for the network connection.

1. Each PMU has its own network connection to the regional Area Center

2. there is only one network connection to the regional Area Center common to all PMUs

In the second case it is necessary that a host is placed in front of the PMUs and before the network connection. This host should

1. receive the data from the local PMUs
2. strip all not necessary data
3. consolidate data from different PMUs
4. compress if possible the data
5. send to regional Area Center as UDP packet.

As mentioned before the host must be fast and the hardware must be chosen appropriately. Direct connection to the WAN network should be considered if delays introduced by this machine are relevant. It will be assumed that this machine will add a delay of no more than 10ms to the transmission of the data. This requires careful examination of the compression algorithm since to have higher compression more computational time is needed. Of course a detailed analysis must be done and a balance must be reached between the amount of compression, the delay introduced by the compression and the time gained on the network transfer due to the smaller packets.

An important consideration to be done is about the amount of data to be transferred if more than one PMU has to use the same WAN circuit. For example if the consolidated and compressed data amounts to 900Bytes, the delay at the 2Mbps ATM interface for sending the packet (in 19 ATM cells) is 4ms (this is equivalent to a 400Kbps traffic). With 1850Bytes (in 39 ATM cells) the delay is 8ms (equivalent to 800Kbps). This last is very close to half utilization of the circuit, level never to be passed, and thus is not suggested. Moreover it should be recall that the PMUs have a 20ms frequency for sending the measures. It should also be recalled that the maximum dimension of a Ethernet packet is 1500Bytes and that usual UDP packets are 512Bytes. So if the data is large, more than one UDP packet could be needed to send it. This introduces more problems some of which will be discussed in Part 2. In any case sending more than one packet is less efficient than sending a single packet, thus more delays can be added.

If consolidation and compression lead to packets larger than 900Bytes, higher speed links must be adopted, like 34Mbps ATM circuits. For example, 8500Bytes at 34Mbps take theoretically 2ms to be sent. An intermediate alternative is to adopt 8Mbps ATM-IMA circuits; these are four 2Mbps ATM circuit multiplexed so to become a single virtual circuit of approximately 7Mbps total capacity. The speed of the four interfaces is still 2Mbps but in case of 2000Bytes data divided in 4 packets of 500Bytes each, this circuit will transfer almost in parallel at 2Mbps the 4 packets.

Suggestions: if needed, add a host at each remote location to transform, consolidate, compress the data from the PMUs. This host must add a delay less than 10ms to the transmission of the data. If consolidation and compression lead to packets larger than 900Bytes, higher speed links must be adopted, like 34Mbps ATM circuits (or 8Mbps ATM-IMA circuits).

1.2.3.8 WAN Network at the Regional Area Center

A few more considerations on the network and setup of the regional Area Center must be discussed. In the previously considered setup, at the regional Area Center there is one or more routers to which the WAN circuits are connected. More than one WAN circuit can be connected to one router. Besides the particular hardware chosen for the router, the number of WAN circuits connected to one router actually depends on the LAN connection to the Computational Unit. It is important not to introduce delays by having packets from/to different PMU waiting in queue to transit on the LAN. Given the timing discussed before, with 10 WAN circuits on the same router and a half-duplex 10BaseT Ethernet LAN, in the worst case packets could experience a 14ms delay before being transmitted on the LAN. It is then suggested to have at least a full-duplex 100BaseT FastEthernet LAN and no more than 20 WAN circuits per router.[9] As it will be the case due to security restrictions, more than one router will be present. In this case each one will be connected to a switch and the switch to the Computational Unit all at 100Mbps.

1.2.3.9 Computational Unit at the Regional Area Center

For what concerns the regional Area Center Computational Unit, it too has to guarantee to be able to receive, elaborate and send data within a very short delay. First of all, the regional Area Center Computational Unit is connected to other systems, for example to the SC-PM SCADA or to remote managing stations, and these connections must be through a different LAN, switches, WAN and routers and different physical interfaces on the Computational Unit hosts, than the ones used to connect to the nodes/satellites.

The Computational Unit can be composed by one or more hosts. In particular two different kinds of transformations and analysis are done on the data arriving from the PMUs:[10]

- first the Artificial Neural Networks (ANN) calculate machine angles, speed and accelerations from the data arriving from each PMU;[11]
- then a central unit receives the data from all PMUs and ANN, decides if a remedial action is necessary and in this case prepares the remedial action.

There can be different hardware setup:

1. for each PMU or remote site, there is one host for the ANN, plus one host for the final elaboration, thus N+1 hosts;
2. there is one host for all ANN and one host for the final elaboration, thus 2 hosts in total;
3. there is only one host for all elaboration.

The problem with the first two solutions is that it takes time for a computer to receive/send a packet from/to the network, loading it in memory and activating the process which has to handle it, and depending on the hardware and operating system this can be even of the order of 40ms or more[12]. Thus having a different

[9] For more than 10 WAN circuits it could be convenient to have a 34Mbps interface on the router and aggregate the 2Mbps circuits in a 34Mbps one.

[10] All data arriving from PMUs have a time-stamp of the measure. PMUs are globally synchronized with GPS signal.

[11] In the alternative configuration the ANN are located at the PMU location. Centralization of all ANN at the regional Area Center can reduce network traffic and simplifies maintenance.

[12] This for example depends on how interrupts, page hits, cache, scheduler etc. are managed by the hardware and Operating System.

host for the ANN can add a delay up to 40ms, even if the computational time of the ANN is extremely small. Also, the data arriving from a PMU will have to transit twice on the LAN, first from the router to the host of the ANN and then from this to the final host. Moreover if for each PMU there is a host which runs the ANN, this will add more stations on the LAN and then more traffic, like ARP packets etc., on the switch.

It is possible to drastically reduce the delays inside a host by choosing appropriate hardware and software. For example a high/middle range server with real-time OS (or a particular version of a Unix/Unix-like OS) could give performances such to practically cancel the delays just described. The higher level of hardware should guarantee:

- faster hardware I/O both on internal busses and interfaces
- faster IP stack and driver with very low or customizable latencies and timers
- better management of hardware resources
- lower possibility of errors or faults

In all cases, large RAM memories are required to guarantee that all programs and data are always kept in RAM and saved on disk only for archiving purposes. Obviously fast disks should be employed too.

The final host which receives all data and prepares the remedial command, has to perform two different computations. The first is a constant analysis of the arriving data to detect if it is necessary to prepare a remedial command, the second is the preparation of the remedial command. These two tasks must not interfere with each other, and for this reason 2 CPU could be needed. It would be better still if in the future the first task could be done by a specially designed acquisition (and network) card.

Thus various solutions for the hosts of the Computational Unit can be proposed:

- if an extra delay of 40ms or more is deemed acceptable, normal hardware and Operating Systems can be adopted, and solution 1. above can be chosen;
- otherwise solution 3. above is preferable to solution 2. from the point of view of performances. Solution 3. implies choosing a high-level server with many CPU and large RAM. It has to be considered that all PMU are synchronised and send their measurements approximately at the same instant. Thus the server will receive the data from the PMUs in bursts, one packet just after the other, and will have to process the ANN almost at the same moment. Having an adequate number of CPUs guarantees that no delays are introduced.

Suggestions: have a single host to perform all computation at the regional Area Center; this host should guarantee to be able to perform all cyclical activities well under 20ms, preferable under 10ms, included the time for receiving all packets from the network (hardware interfaces and drivers included), and to prepare and send on the network (hardware interfaces and drivers included) a remedial action command in less than 50ms from the moment in which the packets which trigger this command arrive at the network interface of the host.

1.2.4 Voltage Stability Infrastructure

As already stated, the kind of data exchanged for the Voltage Stability phenomenon is the same as for the Transient Stability one, just the timing requirements are less severe. Anyway it is suggested to adopt the same overall network structure. Due to the lower requirements, in case instead of an ATM circuit a less expensive Frame-Relay 2Mbps circuit[13] can be adopted at a node which has to send measurement only for the Voltage Stability phenomenon.

It is also suggested that at the regional Area Center the WAN circuit for the Voltage Stability arrive on a different router than the one for the Transient Stability and use a different internal LAN to reach their Computational Unit.

Suggestions: adopt a Frame-Relay 2Mbps circuit and independent LAN from the one used for the Transient Stability.

1.2.5 Network Management Infrastructure

All three previous communication networks require to have a network management infrastructure.

For the inter-regional communications, due to the simple requirements, network management can be done in-band. Since the two connected Centers in this case belong to different entities, each one will have its own management system which monitors its own hosts and network. The two system can exchange information about the status of the respective hosts and networks, if this is considered useful and appropriate. If this is not adopted, the reasons for a failure in communication could remain unknown to one of the partners, making more difficult also the management of the internal resources of the site which is not affected by the failure.

For the Transient and Voltage Stability, network management is done at the regional Area Center. Due to the requirements of Transient Stability and the security requirements discussed later, in this case network management should be done off-band, which means that independent WAN circuits and LAN connection must be provided for the management. The use of a Virtual Circuit on the same WAN link is possible but it is not suggested since in case of failure of the link also all reporting and management will fail. The speed of the WAN circuit is not particularly important, in some cases even a 64Kbps line would suffice, but it is important that it is a permanent circuit, not a dial-up connection. At the regional Area Center there must be an independent LAN with the management stations, and if the management WAN circuits are more than a few, it is suggested to dedicate a router to their connection.

Suggestions: adopt permanent independent circuits for management communications.

[13] Even circuits at 512Kbps or 1Mbps could be sufficient.

2 Dependability of Communications

It is well known that introducing security measures in a project reduces usability and makes implementation more difficult. In the present case there is a strong constraint due to the almost real-time requirements for the Transient Stability data exchange previously discussed, which will make more difficult to implement security measures without introducing delays that would invalidate the timing requirements. The analysis will be divided in two sections, first the fault-tolerance aspects and then the security with respects to malicious attacks. In both cases the threats and risks first, and then the measures to adopt to prevent them will be described.

Physical security, meaning access of unauthorized persons to the premises, hosts, machines, hardware of any kind, will not be considered in details. It is assumed that physical security is fully guaranteed. Indeed all the hosts and network equipment will be in dedicated areas which should be already secured. In any case, if an unauthorized person has physical access to a machine, he/she could change the configuration, read the data, turn it off or unplug the network. No guarantees of services or security can be given if an unauthorized person has physical access to a machine. All standard high-security controls on personal access must be implemented to guarantee that only authorized personnel can access the machines and networks.

The analysis will be carried out by imposing a **single failure fault-tolerance**[14] model on all network, communication and hardware components. Moreover the model will have a **multiple layered security structure** (also called *defense in depth*) in which, whenever possible, various and different layers of security measures will mitigate each threat. In particular two layers of security are considered:

1. the communication layer
2. the application layer.

The aim of the analysis is that the communication infrastructure will be able to dependably transfer information between the nodes in a way such that the dependability is realized as much as possible without depending of the content of the information transferred. On the other side, the nodes, provided that some communication, even if fragmented, is possible, should be able to obtain dependable data by having information encoded and structured in such a way to be able to verify the correctness of the data received even reconstructing missing data whenever possible. This requires that the algorithms and protocols adopted are specifically designed.

A first formal analysis of the results of the final model will be done in PART 4.

2.1 Fault Tolerance

A very important aspect of Dependability is to plan a network infrastructure so that even in case of failure of some equipment, temporary or final, or errors in the communication channels, the communication is not interrupted and at most suffers minor delays which are deemed acceptable for the service. Thus based on the requirements of each service, it will be discussed various network infrastructures which give the maximum guarantee of service with minimum acceptable interruptions or delays.

[14] I.e. the system should address all single, independent failures of each component of the infrastructure.

2.1.1 *Threats and Risks of Leased Circuits*

In this Deliverable it has been suggested to lease commercial circuits to connect the various locations which comprise the EXaMINE network. There are some risks inherent in the fact that the circuits are not under direct control of those who use the network itself. For example, by leasing direct point-to-point ATM circuits from a Telecom provider, it has to be recognized that these circuits will run on the same cables and ATM switches as the ones of many other customers of the Telecom provider. The Telecom provider has to assure its customers that the configuration of its network is such that guarantees the offered bandwidth and delay assurance to each customer. It should be noted that an ATM circuit does not provide an exact multiplexing, i.e. each cell (or time slot) is assigned to a fixed circuit, but it multiplexes in an asyncronous way all circuits on a particular link.

Let consider an ATM link between two switches on the backbone of a Telecom provider. On this link there will flow many ATM circuits (PVC) of many different customers, some circuits could even be transferring public Internet traffic on the backbone of the provider. An ATM switch will multiplex all the circuits, but not in a fixed timed way, instead for example, if on a circuit there is no traffic, its cells can be used by another circuit that at that moment has a lot of traffic. In this way it is possible to obtain a better use of the full ATM link. One problem is that in some situations it is possible to assign to a link more circuits than its maximum capacity: in normal conditions everything will work fine, but if exceptionally all circuits will be at maximum capacity the full link will not be able to carry all of them, and some data could be dropped.

This and similar risks associated to the fact of sharing with other customers the hardware resources of the Telecom provider, are usually deemed remote, but in extreme cases degradation of service could happen and even the full service could be in jeopardy. For example on January 25th 2003 the W32/SQLSlammer worm attacked Internet. There have been various cases where other connections like point-to-point ATM circuits, which are not Internet related, suffered from the fact that the internet backbones of the Telecom operators were overwhelmed by the traffic generated by the worm.

2.1.2 Threats and Risks for Inter-regional Communications

Even if in the Preventive Mode there is not a request for the network communications between Area Centers to be guaranteed at the millisecond, the communication must be done when requested with at most a few seconds delay. The points of failure are

- the hosts at the Area Centers
- the network equipment, LAN, switches, routers etc., at the Area Centers
- the WAN circuit.

Possible threats are:

- failure in each one of these components
- corruption of data during the communication

In the event of the total failure of communication, the Preventive Mode algorithm will not be run between the two Areas.

In the event of corrupted or wrong information exchanged between the two Area Centers, the algorithm could obtain wrong evaluation for the next day provisions.

2.1.3 Threats and Risks for Transient Stability

As network delay is important in achieving the stated goals of this project, so is the fact that the service must work without interruption. The system which will be considered here is formed by the PMU, the network which connects it to the regional Area Center Computational Unit, the regional Area Center Computational Unit itself, the network which connects it to a remote active node, and the remote host to which a remedial command is sent.

The list of points of failure is:

- PMU
- network connecting the PMU to the router
- router
- WAN connection
- router at the regional Area Center
- network connecting the router to the Area Center Computational Unit
- Area Center Computational Unit
- and a similar list of objects back to the host to which the remedial command is sent

Various threats are possible:

1. PMU will not function
2. data sent from a PMU will not arrive at the regional Area Center Computational Unit
3. data sent from a PMU will arrive late (different scales of delays are possible) at the regional Area Center Computational Unit
4. data sent from a PMU will arrive corrupted at the regional Area Center Computational Unit
5. Computational Unit will not prepare a remedial command in time
6. Computational Unit will be unavailable
7. remedial command will not arrive at the remote node
8. remedial command will arrive late (different scales of delays are possible) at the remote node
9. remedial command will arrive corrupted at the remote node
10. remote node will not be able to process the remedial command

It is important to notice that the remedial commands sent to the remote nodes are all of the same kind, with which is intended that they are all of the (symbolic) kind DOWN and that never is sent an UP command. Moreover commands are atomic, with which it is intended that if the remedial action consists of sending a remedial command to 3 remote nodes and only one, or two or all three commands are executed, independently of which one and how many are executed, the final situation is always better than if no command was executed at all.

Another possibility is if a PMU takes a wrong measurement so that the initial data is not correct. In this case even if transmission is perfect, at the regional Area Center false information will arrive. The problem of avoiding the occurrence of a wrong measurement at the moment is very difficult to address.

In the event of the total failure of communication, the regional Area center will not receive information that a phenomenon has started, or remote nodes will not receive the remedial command.

In the event of corrupted or wrong information arriving at the regional Area Center Computational Unit, the algorithm could send a not needed remedial command, or not send a command when instead it would have been necessary.

2.1.4 Threats and Risks for Voltage Stability

The analysis for Voltage Stability is quite similar to the one of Transient Stability. The only difference is that in the case of Voltage Stability commands can be of opposite type, that is for example both UP or DOWN are acceptable commands. This introduces an extra risk, that is that by mistake the opposite command than the needed one is performed. Moreover there is the possibility that opposite commands are sent one after the other, possibly introducing an instability.

2.1.5 Threats and Risks for Management Communications

Management communications allow to control the status of all hosts and networks, thus giving fundamental informations to prevent or correct problems. If management communications fail, data could be lost which helps to diagnose problems and find solutions in short time, but also accounting data could be lost and the possibility of remotely control and act on hosts. Analogously if wrong or modified data arrives on the management console, wrong actions could be taken, or the necessary action could be not adopted. Thus it is important that management communications are reliable, to guarantee the gathering of data and the possibility of remotely connecting to the hosts.

2.1.6 Mitigation of Threats and Risks of Leased Circuits

The simplest possibility to mitigate the risks of leasing circuits from Telecom providers, is to have two different Telecoms to provide the two redundant connections. Obviously, the two providers must be truly independent for the services given, that is for example that one must not be a sub-contractor of the other, or that both must not use a third provider so that eventually both circuits will pass on the same link.

A higher assurance can be obtained if instead of leasing ATM or similar circuits, it is leased the use of a fiber or of a Clear Channel on a fiber, that is of light frequency or of a time slot in a Dense Wavelength Division Multiplexing (DWDM) link or a SONET/SDH link. By having a fixed time slot or the direct use of the fiber and not asyncronous multiplexing, it is possible to mitigate these risks.

On the other side, these solutions are quite expensive both for the equipment and for the management needed. Moreover, as already discussed, the communications of the EXaMINE project do not need such technical solutions to satisfy the delay and bandwidth requirements. A possible future solution is if there would be created networks reserved for communications of infrastructural services, like the one considered in this project. By sharing the same infrastructure and having all similar requirements on dependability it could be obtain to have at the same time a higher level of assurance and a lower cost.

2.1.7 Fault-tolerance solutions for Inter-regional Communications

It is necessary to have a backup connection, and this could be another 256Kbps line, or a satellite connection since the delay in this case is not too important, or again even a dialup isdn connection at 128Kbps. If a 2Mbps circuit with ETSO-Electronic Highway is chosen, to avoid bottlenecks it is suggested that there is a reserved backup circuit only for this traffic, or that the backup circuit would be at least 1Mbps. To guarantee fast backup, double routers are needed, and it is important to have constant monitoring and hardware contracts with supplier for hardware replacement within 4 hours. Internal LAN and hosts should be doubled or redundant. On-site and Off-site backup of all data and configurations is needed.

2.1.7.1 Dependability of Algorithms

When an error is detected the algorithm does not update the information in the frontier (as in case there is a communication failure and the channel is lost). All the values exchanged have to verify strong numerical relations (complex Ohm's law) with values that are locally available, so internal checks can be done before accepting information coming from a neighbourhood EXaMINE machine.

2.1.8 Fault-tolerance Solutions for Transient Stability

In this section the 10 threats listed for the Transient Stability will be considered. For each one possible solutions to mitigate the risk will be described. Solutions can be different depending on different physical settings and different requirements in different locations. For each Regional Area a careful study should be done to find the overall solution which gives the maximum protection against the risks.

1 the PMU will not function

An hardware failure of a PMU can be mitigated by having a hot-stand-by PMU fully active. That is, another PMU fully functional which sends its data to the regional Area Center, but its data is not used by the regional Area Center. This requires that the regional Area Center has a means of discarding duplicated data. A more cost effective possibility is to distribute the PMU so that not all data is necessary for the Computational Unit to function, but if all data is present, all data is used. In this case the distribution of the PMU can be such that out of N, the data of N-1 (or N-2 etc.) PMUs is sufficient for the regional Area Computational Unit, this will be called a N-p model. Hardware failure of the PMU are very rare, even if they are guaranteed not to happen they can (and do) and it is not possible to rely on the assurance that PMU never fail. Since the possibility of failure is very low, the N-1 model can be adopted. Indeed, since the frequency of failure of a PMU is very low, and the number of PMU installed in a regional area is at most of a few dozen, the risk of a failure of a PMU during the time that a failed PMU is repaired is still very low. Otherwise a N-2 model should be chosen. With a N-2 model, the argument would be that in case of a failure of a PMU, since the repairing time could be long, the model will drop to be N-1 and thus the risk of failure of another PMU would still be mitigated. Anyway, for what concerns this analysis it will be assumed that this risk is very low, and that the N-1 model can be adopted.

The dependability of the PMUs has been widely discussed since failures or mis-functioning of some models did happen. As with any new technology, a few years are needed to obtain the level of assurance required of these instruments. Recent tests and deployments in production are showing consistent dependable behavior of the most recent models of PMUs, see for example refs. [53] and [54], and in various countries, like for example in China, large deployments have already started.

In this analysis it has been considered that all PMUs will be installed in different geographical locations, but if two or more PMUs would be at the same geographical location, they must be considered as totally independent. The main analysis will be done considering each PMU having its own connection to the regional Area Center even if at the same location.

2 data sent from a PMU will not arrive at the regional Area Center Computational Unit
3 data sent from a PMU will arrive late (different scales of delays are possible) at the regional Area Center Computational Unit
4 data sent from a PMU will arrive corrupted at the regional Area Center Computational Unit

Case 2 and 4 are equivalent since if some data arrives at the regional Area Center Computational Unit corrupted and it has not been discarded already at the network level, the applications should discard it without even considering it. Thus case 4 becomes equivalent to case 2. This implies that consistency checks on the data transmitted must be built into the high level protocol adopted by the applications, besides the ones present at the network level.[15]

If a packet sent from a PMU does not arrive at the regional Area Center Computational Unit, it must be possible for the Computational Unit to operate correctly anyway. Adopting the model discussed in 1 of N-1 redundancy, in normal situation it is possible to loose 1 packet of the same measure, i.e. sent at the same time, without having a failure of the algorithm. On the other side, this is not the correct way of assessing the risk management since it should be considered as independent the risk of a hardware failure and of loosing one packet as a pseudo-random phenomenon. It is important to distinguish different kind of failures with respect to the time for which the failure lasts:

- single packets could be lost on perfectly functioning circuits, but all subsequent packets will transit correctly;
- a circuit failure could last a few seconds until a backup circuit is

[15] We recall that all network protocols like Ethernet, IP, UDP etc., add to each packet a checksum CRC field which gives a reasonable level of guarantee that if a bit in the packet is modified, it is detected by the corresponding network driver and the packet is discarded. No error correction is built directly in these low level networking protocols. This issue will be discussed again in the section about Prevention of Malicious Attacks.

activated;

- an hardware failure could last a few hours until a (fast) repairing is operated;
- an hardware failure could last days until a (slow) repairing is operated.

The last 3 cases will be generically denoted as hardware failures and in case of one of them no packets will arrive from that PMU until a (physical) repairing of the unit is done. Due to the request on fast time delivery of the data of the Transient Stability, all hardware failure risks should be mitigated by redundancy in the distribution of the PMUs, that is adopting a N-p model with p sufficiently large. On the other side, N-p models with p equal or larger than 2 are not cost effective due to the large number of PMU needed. It should then be decided if the risks associated with a N-1 model are considered acceptable, even if the only one hardware failure at the time is protected out of different and independent kinds of failures.

The risk of the first case can be addressed by having some extra time for this left free. This is exactly what it was proposed at the beginning when out of the maximum 500ms it was kept a Safety Factor of some milliseconds. For example, having a Safety Factor of more than 20ms would guarantee that if one packet from a PMU is lost, but not the following one, still the remedial command can be prepared and put in action in time.

For 3 if a packet arrives late to be used for the computation to which it should have contributed, the packet must be discarded for the computation and in case kept for slower computation or for archiving purposes. This requires that the higher level protocol keeps a time-stamp of the generation time of the packet so that when received, the application would check the time-stamp and decide if to use or discard the packet. Thus all end-points (PMU, Computational Unit etc.) should globally synchronised with a reference clock by means for example of a GPS antenna. This introduces another hardware element, the antenna and its interface card, and its software driver. Failure in the hardware or software in a PMU implies that all data from that PMU will be discarded, failure in the GPS synchronization of the regional Area Computational Unit will have the final consequence of discarding all packets thus stopping altogether the system.

Some consideration must be done in case more than one PMU are at a remote location and there is a host which consolidates and compresses the data from the PMUs before sending it to the regional Area Center. If the data is large and does not fit into one UDP packet, then the entire data is divided in smaller packets. Each packet should contain independent data and be compressed independently so that the loss of one packet does not compromises the others. Viceversa independent division of the data in packets and compression of only part of the data is less efficient.

It is necessary now to study each point of failure listed above.

- Hardware maintenance For all hardware components it is necessary to have all spare parts in place or contracts with suppliers for the substitution of failed components within guaranteed time, usually 4 hours, at the location of the hardware.
- Power supply It is suggested that each hardware component is powered by a (redundant in case) Uninterruptible Power Source

(UPS), i.e. a battery powered backup. Purpose of this power backup is to allow the hosts to shut down cleanly to prevent hardware and software damages in case of power failure, and to permit to some hosts and network devices to continue to function for a short time after the failure has happened to allow them to report the failure itself.

- Network connecting a PMU to a router An Ethernet CAT V cabling is proven to be quite stable, if correctly installed, safe physical threats of course. Usual practice indicates to change all cables every approximately 10 years. Since between a PMU and a router there is a direct connection which should be inside a safe and protected area, it does not seem necessary to have double network.
- Interface cards Also interface cards are quite stable but not as long lived, it is best practice to substitute all of them every 3 years. Cards older than 3 years have a higher possibility of hardware failure. This holds for routers, switches, and hosts in general.
- Routers The main failure points of high level routers are interface cards, power supplies, controllers, fans. As for the interface cards in general, it is suggested to substitute the full hardware every 3 years. At a PMU location only one router is present, due to the analysis done up to now and the requirements set, this seems sufficient. As will be shown in the next points, at the regional Area Center all hardware will be doubled.
- WAN connection Due to the length of the cabling, the handling of the service in out-sourcing and the inherent problems with managing long distance connections, this is one of the weakest points. It is far more easier to have a *hardware* failure or just loss of some packets in the WAN circuits. For this reason a double (or triple) redundancy on the WAN circuits is suggested. Unfortunately, due to the restrictions on the latency, diversity on the hardware circuits is not possible. Transmission through satellite links can be used as an extreme backup to receive anyway the data at the regional Area Center for archiving or post-elaboration. Indeed in practice round-trip time from ground to orbit of a packet takes not less than 400ms, for an order of magnitude computation it is enough to consider orbits at 36000 kilometers and speed of light. In the future low orbit (500-1000 Km) satellites will provide IP transit service which could satisfy the latency requirements. Discussion of this possibility is postponed due to lack of reliable data. Dialup connections (isdn etc.) are too slow and will not satisfy the latency requirements. Another alternative could be a WLAN (Wireless-LAN) implementation, that is the realization of a ground level radio circuit. Current technologies can do this, the only problem is that the maximum distance between repeaters (antennas in sight of view) is only of a few kilometers. This would require to install and maintain (on top of the physical security threats) many antennas and will add very large delay due to the time for each antenna to relay the signal. Maintenance of so many antennas and delay due to relaying make also this solution not practicable. Thus the only practicable solution seems to be to double

the WAN 2Mbps ATM circuit having in case a satellite circuit (or isdn) as an extreme backup only for archiving the data. To improve reliability the 2 WAN circuits should be physically distinct, for example one cable leaving the premises towards east and the other towards west. Moreover, all along the path the 2 circuit should not use the same physical locations, but always run at least a few kilometers apart since one of the greatest risks is an accidental cut of the cable. Higher guarantees could be obtained if the two circuits are managed by different Telecom operators, otherwise if leased by the same operator there should be the absolute guarantee that the 2 circuits never pass in the same physical locations. At the regional Area Center, the 2 circuits should terminate on two different routers for maximum reliability. The common setup of such networks is to have one link active and the second in hot stand-by. In case of failure of the primary link, the router at the PMU detects it, for example by using very frequent *keep-alive,* and activates the second circuit. It is to be noted that if the routers use very frequent *keep-alive* packets to immediately detect if a link has failed, more traffic is added on the line, and this could add other delays to the PMU data (even if the *keep-aliv*e packets are very small). Due to the latency restrictions and the time the router at the PMU location takes to detect and switch the circuits, it is probably not enough to keep one circuit active and the second in hot stand-by, indeed considering the time it takes to switch between one circuit and the backup, a circuit failure will lead to the final loss of a few packets. If the problem is due to the last mile connection of one router at the regional Area Center, this would imply that a few packets could be lost for all PMUs in one region. A more reliable solution is to double each packet and send it through both circuits. At the arrival the application in the Computational Unit will discard the packet which arrives second. Doubling the packet can be done directly by the PMU, by the router or by the optional host at the remote location. The PMU could send a packet to a multicast address and the router at the PMU location should do multicast routing and send a copy of the packet on each circuit. This of course could add some minor delay due to the multicast routing. The difference between the two solutions is that having a stand-by circuit the time needed to switch from one circuit to the other must be covered by the redundancy in the distribution of the PMU (the N-p model chosen) or the Safety Factor, instead doubling the traffic addresses directly the risk.

An alternative less valid solution could be adopted if at the regional Area Center only one router is installed. It is then possible to use Inverse Multiplexing for ATM (IMA) which is a technique for bundling ATM physical channels into a logical circuit.[16] This technique requires that there is a single router for both circuits at the end. In this way a packet will travel alternatively only on one physical circuit but both circuit are in use simultaneously. If one circuit fails, the other carries the traffic and there is very little delay

[16] Similar techniques exist for other protocols.

in the transition. The problems with this solution are: if a circuit fails while it is carrying a packet, that packet could be lost; overhead is added for managing the IMA protocol; the speed of the interfaces is still 2Mbps, even if the bandwidth of the logical circuit is 4Mbps; only one router is at the regional Area Center.

- Routers at the regional Area Center As previously discussed, at the regional Area Center all routers should be doubled. Each PMU will have a circuit connected to one router and the other circuit to another router. Hardware reliability and physical security of routers have been already discussed.
- LAN at the regional Area Center Having two (or more) routers implies that as a minimal security feature the two routers are connected with two completely independent LAN, double cabling, two switches etc., to the Computational Unit. Since it is very important that internal communications at the regional Area Center will not fail, since otherwise all data would be lost, it is suggested to double the Ethernet connections from the routers to the Computational Unit, using independent FastEthernet cards and connecting each router to both switches. In this way failure of one router and of one switch at the same time will not impair the service.
- Computational Unit at the regional Area Center For maximum guarantee of service, two identical Computational Units must be installed at the regional Area Center and connected with both switches with 2 FastEthernet cards. Depending on the application software, both hosts could be active at the same time, or one could be in hot-stand-by of the other. Direct communication between the two hosts must be done through independent FastEthernet or other fast connecting interface. It is suggested that data does not reside on any of the hosts, on which only the Operating System, configuration files and temporary data should reside. Instead all data should be on a common highly redundant, fast disk array, for example. In this kind of solutions all redundancy is built into the data host, with double power supplies, spare hot-disks, hot-swappable disks and redundant configurations so that failure of any disk unit will not impair the service. If high level server hardware is chosen, it could be not needed to have 2 identical units since these hosts usually have built in very highly redundant features. Moreover these hosts usually come with highly redundant disk farm.

  If the Computational Unit is made by more than one host, for example having different hardware for the ANN, the same considerations apply also to all other hosts.
- Data Backup It is important that for all data there are various backups both for future analysis and, more important for the present discussion, for fast reconstruction. In particular, all Operating System configurations must have a backup on-site and off-site, and these backups must be kept updated. In case of hardware failure this will allow a fast configuration of new hardware. The same considerations must be applied to any kind of data or software program that is needed to restart all services.

Moreover, it is strongly suggested to keep all PMU data and remedial command prepared by the Computational Unit in a safe backup for at least a few months. Later off-line analysis of this data could always be useful both for scientific understanding and for security reasons. For example, data which led to the preparation of remedial commands, the remedial command itself and the measurements for a brief period of time after the activation of the remedial command, must always be kept in safe backups for longer time.

- Hosts at remote locations It could be necessary to have a host at a remote location of a PMU for treating the data before is sent on the WAN circuit. In this case the host should have a stand-by machine which should automatically be activated in case of failure of the primary host. Since the time of take-over could be of a few seconds, this risk cannot be mitigated by the Safety Factor, but must be included among the hardware failures and thus mitigated by the N-p distribution model for the PMUs. On the other side, since the failure will last only a few seconds, it is assumed that this risk is reasonably low.

  In case of presence of this host, the simplest solution for sending the double packets on the WAN circuits is that the host itself sends two UDP packets addressed in such a way that each will be routed on a different WAN circuit.

5 the Computational Unit will not prepare a remedial command in time

In this case it is still suggested that the Computational Unit will send the remedial command to its final destination. Even if the command will arrive late, due to the kind of phenomena of the Transient Stability, the delayed action could still be useful. To mitigate this risk, it will be added another delay time to the Safety Factor.

6 the Computational Unit will be unavailable

This risk is mitigated by the redundancy of the Computational Unit, for the rest is as 5.

7 the remedial command will not arrive at the remote node

8 the remedial command will arrive late (different scales of delays are possible) at the remote node

9 the remedial command will arrive corrupted at the remote node

These risks are mitigated by the same arguments as for the connection between the PMU and the regional Area Center. In particular, to mitigate this risk, it will be added another delay time to the Safety Factor. Moreover it could be devised a system such that in case of failure of one of these devices, a remedial action can be carried out by another device, similar to the N-p model for the PMU. It is suggested that the remote device will send back to the regional Area Center a confirmation of having received the remedial command, and in case the regional Area Center does not receive this confirmation within a reasonable time-out it should assume that the command has been lost. The remote node would be connected to the regional Area Center with a double WAN circuit configured as for the connection with the PMU, that is both circuits will be always active. The

regional Area Center Computational Unit will then send two copies of the command each through one circuit, and could also send more than one (double) copy of the command within a very short time to minimize the risk of the loss of a single packet.
It could be also needed to have a host at such a remote location to transform the remedial command received by the network in a command that the device can understand. In this case the host will receive two packets from the regional Area Center Computational Unit which would have arrived through the two WAN links, and it will discard the second packet. This host could then send back a packet, again through both WAN links, containing the message that it has received the remedial command packet.

10 the remote node will not be able to process the remedial command

Same as 7. To mitigate this risk, it will be added another delay time to the Safety Factor. It is suggested that the remote device will send back to the regional Area Center a confirmation of having carried out the remedial command. Of course the effects of the remedial command will be seen by the future measurements of the PMUs, but if the information gained by the receipt of this confirmation could be useful at the application level.

2.1.8.1 Dependability of Algorithms

The ANN modules use phasor measurement inputs of several past samples obtained by the PMU device to provide the power plant state estimation. These inputs are partly redundant but also to some extent noisy. ANNs are intrinsically able to exploit redundant and/or noisy inputs, provided that they are trained in appropriate conditions.
Although these aspects have not yet been verified in the context of the simulations so far carried out, we therefore strongly believe that by proper training the ANN modules can be made robust with respect to the following type of conditions

- Occasionally missing PMU outputs.
- Small timing errors (small with respect to the sampling period).
- Measurement errors and background noise.

Suggestions: adopt N-1 PMU distribution model; have doubled WAN 2Mbps circuits fully active sending double packets; current assurance of channel availability offered by providers are of 99.99% (allowed downtime of 53 minutes per year) or 99.95% (allowed downtime of 4.4 hour per year), higher assurance (like 99.999%, allowed downtime of 5 minutes per year) would be better but probably not possible to obtain; assured packet loss < 0.3% or similar on the WAN circuits; have fully doubled network at the regional Area Center; have a single, very high level, fully redundant Computational Unit; adopt full data and configuration Backup strategies; have hosts at remote locations with hot-stand-by unit; have hardware maintenance and fast replacement contracts.

2.1.9 Fault-tolerance Solutions for Voltage Stability

As before, the analysis is very similar to the case of Transient Stability. One difference is that there is not anymore such a stringent constraint of latency for the communications. This allows to have diversity in the communication circuits. For example backup satellite links are in this case a viable possibility, since a 400ms travel time on one leg could still give the possibility of a remedial command arriving in time. Even a isdn dialup connection at 384Kbps can deliver a 500Byte packet in 10.5ms (to which all overheads and the latency of circuits should be added), so that a total travelling time on one leg of the order of a 200ms could be achieved. In any case a backup line must be provided at the remote location, which should be activated automatically by the router in case of failure of the principal line. As before, it takes some time to activate the backup line and in this time packets could be lost, or get too much delayed to be useful. In particular the activation time of a dialup connection could be too long, so dialup connection is not suggested also in this case. Thus it would be better to adopt a backup permanent circuit, either satellite or ground.

Consistency checks are built into the low level network protocols, and further checks will be added when considering Prevention of Malicious Attacks, thus the possibility that a corrupted packet arrives at the regional Area Center or at a remote node where a remedial command should be enacted, are very small. Packets corrupted during the network transit are usually discarded. Another problem is if the data contained in the packet is wrong from the beginning, as for example in the case of a wrong measurement from a PMU. In this case the algorithms at higher level must be able to detect and act or discard wrong data. This is particularly important in the case of Voltage Stability since commands of opposite kind can be given.

2.1.9.1 Dependability of Algorithms

Generally speaking, on considering about algorithm dependability we should account for the choices made about system observability; in other words, if state estimation is focused, including N-p security criterion applied against branch or device losses, missing data can be substituted by calculation of pseudo quantities deduced via Kirchhoff and Ohm laws basic application. The same numerical checks, obviously time consuming, are commonly used in conventional state estimation programs to perform bad data assessment.

To consider the worst case, full dependability forces to adopt PMUs placement strategies in a fashion very similar to the one usually adopted in nuclear power stations for safety reasons.

With specific concern to voltage stability algorithm, missing and or bad data assessment is therefore guaranteed by data redundancy and validation, whereas the mere algorithm could only check against abnormal values (out of the range 0.5 -1.5 times the rated value), being very cautious along faulted and perturbed conditions, where indicators should not be considered immediately, but delayed after fault removal.

If then we focus on the efficiency of the algorithm itself, it happens that voltage magnitude time first and second derivatives proves reliable whenever resembling critical and informative local state variable, which for example occurs when monitoring load nodes with automatically regulated tap changers in grid radial configuration, causing a good de-coupling between network dynamic aperiodic modes. Coupling effects between local modes is obviously present, and may cause the algorithm to produce ineffective results, but this occurs where the grid proves more strong and consequently less bound to voltage stability problems.

Suggestions: similar to Transient Stability; in this case the backup WAN circuit could be in hot stand-by if its activation takes no more than 1 second; the backup WAN circuit can be of a different type from the default one, even satellite could be appropriate.

2.1.10 Fault-tolerance Solutions for Management Communications

Part of the fault tolerance solution is also the management of hosts and networks. It is very important to have an overall system which constantly controls the status of hosts and networks. This system usually gathers informations from all hosts and networks continuously and reports all data to one or more central stations. In case of a problem, alerts are given on real-time to operators and in some cases actions are taken automatically. Moreover all data is archived for future analysis. A high level, fully redundant management solution must be installed. Personnel must be present 24 hours a day, 365 days a year. Care should be taken to plan this infrastructure. The usual solution adopted is to have all hosts, routers etc. report informations to the central management stations using the SNMP protocol [26,28,33-40]. At a regional Area Center, the best solution is to introduce a dedicated LAN for the management. Each host, router, switch etc. is connected to this LAN and only this LAN is used to gather data and to connect to the hosts, routers etc. for management purposes. Thus for example, remote logins on the hosts or routers would be allowed only through this dedicated interface and snmp queries would also be allowed only through this interface. Besides the obvious security requirements, this solution would also guarantee that the management traffic does not interfere with the fast traffic between PMU and Computational Unit. For the remote locations, for example where PMUs are, the best solution would be again to have an independent WAN circuit which connects the remote router to the regional Area Center and that it is used only for management purposes. Due to the type of traffic this circuit can be much slower, even 64Kbps or 128Kbps could suffice. If other hosts inside the remote location should be monitored, and independent LAN should be devoted to this purpose. In-band management, that is using the existing data WAN connections also for management, can be adopted for inter-regional management communications, but it is not optimal for the following reasons:

- the management traffic could interfere with fast or heavy traffic as discussed in details previously
- having independent circuits for management and data improve the reliability of the solution
- having independent circuits for management and data improve the security of the solution.

Suggestions: have a fully dedicate network, WAN and LAN, and around the clock monitoring.

2.2 Security Against External Events and Malicious Attacks

Malicious attacks against networks and hosts are always possible. The first line of defense must be the physical security of the hardware, the procedures to guarantee this and the training of the personnel. Malicious attacks are a threats because they can

- disclose private/secret information;
- reduce or halt the services;
- obtain the control of the services.

For a service of such an importance as the one considered in this project, none of these risks is tolerable. Moreover, it is important that no kind of information, and with information here it is intended all kind of data present in hosts and networks, is left unprotected. Experience shows that even information that at first sight could look meaningless, can become crucial for a malicious attacker. A malicious attacker could discover patterns in a, at first sight, random stream of data left not protected, and be able to inject in the stream totally meaningless but formally correct data with the consequence of reducing, changing the behaviour, completely stopping or even taking control of the services. Thus it should be practically impossible for a malicious attacker or anyone who is not correctly identified and authorized to do so, to

- obtain information from the hosts and the networks
- inject information in the hosts and the networks.

For access to all information there should be appropriate levels of

- authentication
- authorization
- accounting
- confidentiality.

2.2.1 Threats and Risks for Inter-regional Communications

Communication between regional Area Centers suffers the general threats and risks just described.

2.2.2 Threats and Risks for Transient Stability Communications

Communication for Transient Stability suffers the general threats and risks just described.

2.2.3 Threats and Risks for Voltage Stability Communications

Communication for Voltage Stability suffers the general threats and risks just described.

2.2.4 Threats and Risks for Management Communications

It is particularly important that management connections are protected, since an unauthorized access to management resources can give to an attacker direct access and control to all hosts and networks.

2.2.5 Mitigation of Malicious Attacks

First of all, comprehensive security policy and procedures must be prepared, adopted and enforced for personnel, network, hosts and software adoption and maintenance.

It is assumed that physical security of all hosts and networks within all premises is guaranteed. Since all networks within all premises are cabled and physical security is guaranteed, no attacks from within the premises are considered.[17] It must be noted that if a malicious attacker gains access to a premise and obtains direct control of a host, she or he will be able to remotely influence or even control the full regional Area System and all remote hosts connected to it. For this reason all hosts, including routers, switches etc. must be configured with the highest possible security that they provide even for physical access at the console, at least by the use of username and passwords wherever possible. Console access with smart tokens or similar identification devices would be better, since an attacker should first obtain a device and then discover username, password etc. Unfortunately this kind of protection is not yet incorporated in network devices and seldom in servers. Of course this kind of protection would not make it impossible for an attacker who has physical access to do what she or he wants, but it will make it more difficult. At the end, an attacker with physical access could just replace the hosts with her own new hardware.

The WAN transit is the most exposed to a malicious attack. Even if only leased lines, direct circuits are considered, and packets will never transit on public (internet) circuits, still it is not possible to guarantee the physical security of the cables against accidental or intentional attacks and damages, even less in case of wireless or satellite transmissions. Thus the WAN transit must be considered not secure and backup lines, as discussed in section §2.1, must be adopted in case of intentional damage to a line, moreover encryption [12,42] must be adopted on all links to prevent non-destructive direct malicious attacks.

For this last the technically simplest solution is to realize *router-to-router*, as opposed to *end-to-end* or *host-to-host*, IPSEC [9] Virtual Private Networks (VPN). In this scenario on each WAN circuit only encrypted packets will transit. IPSEC VPN guarantees:

- authentication: since only the two routers which are peers know the secret keys used to encrypt the packets
- authorization: since only authenticated packets with some specific sources and destination addresses are admitted, thus for example a VPN tunnel cannot be used to send packets to a destination which is not explicitly configured in the tunnel itself
- accounting: since the routers can (partially) keep track of the packets which transit through the VPN tunnels
- confidentiality: since all traffic within the tunnel is encrypted.

Today, to satisfy these requirements the IPSEC VPN tunnel must use ESP (Encapsulation Security Payload) and not AH (Authentication Headers) mode, and should adopt 3DES (Triple Data Encryption Standard) or AES (Advanced Encryption Standard) encryption with at least group 2 DH (Diffie-Hellman) and SHA1 (Secure Hash Algorithm version 1) or MD5 (Message Digest version 5) checksum algorithm. An attacker will not be able to decipher the packets in transit, nor he/she will be able to

[17] Anyway through the use of *social engineering* (i.e. the use of human communication, impersonation or bribes and similar *social* strategies), this kind of attack will be the most likely to be attempted and to succeed.

inject packets in the tunnel since he/she does not know the secret encryption key and cannot deduce it from the traffic. The protocol is also resistant with respect to man-in-the-middle attacks, that is the establishment of VPN tunnels with a router owned by the attacker.

Moreover the protocol adds strong consistency checks on the packet itself, which guarantees that no modifications of the packet, accidental or intentional, can go undetected. Malformed packets, as with other network protocols, are discarded.

In this configuration, the routers become the weakest points since an attacker could try to inject traffic in the circuit to gain access to a router. Current routers have firewall [3,5,45] and limited Network Intrusion Detection (NIDS) [15] features. Thus one possibility is to configure all routers with these features and control directly on the router the traffic which tries to access the internal network and the router itself, and viceversa the traffic that from the internal network tries to enter the VPN tunnel or go on the WAN circuit. If well configured these features will not add particular delay to packets in transit on a reasonable high level router.

One risk that should be considered is if a malicious attacker gains control of a remote location, for example a site with a PMU, and is then able to send data through the encrypted tunnel. In this case the data which will arrive at the regional Area Center through the VPN will be correctly authorized and very little can be done about this. The presence of a firewall and a NIDS examining the traffic after it has exited the encrypted tunnel, will anyway be able to detect and possibly stop the attacker. Indeed the attacker will try to access services or hosts which will not be usually accessed by the PMU, and this kind of traffic should be detected by a well-configured NIDS and possibly automatically stopped by a firewall.

Thus a more complete solution would require to install at each location one or more firewalls and NIDS. A possible more general solution is indicated in Figure 2.

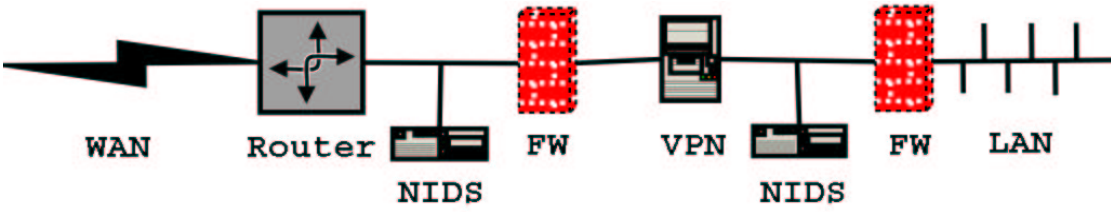

Figure 2. General positioning of Firewall, VPN concentrators and NIDS.

One firewall is located behind the router and the VPN will end on a VPN concentrator just behind it. After the VPN concentrator another firewall will filter the packets which have come out of the encrypted tunnel. Indeed the two firewalls have two different purposes, the first to permit only the encrypted tunnel to reach the VPN concentrator, the second to filter the contents of the encrypted tunnel in case a malicious attacker has taken control of the remote site and tries to inject packets in the encrypted tunnel. As with any security setup, it is better if the two firewalls are by different vendors. Coupled to each firewall there is a Network Intrusion Detection System which has the duty of detecting and reporting anomalous traffic and, in case, of activating automatically counter-measures when under attack.

In this configuration, the router will have to protect itself from attackers who aim to take control of the router, but will not have neither to terminate the VPN tunnel nor to

examine the traffic from/to the internal network. Thus having less to do, it will be faster. The VPN concentrator indeed helps the router by terminating all encrypted tunnels.
It is to be noted that the introduction of extra components like firewalls and NIDS gives more complication at the management level and at the same time more points of failure. It should be stressed here that management of firewalls and NIDS is a delicate task and require highly specialized personnel. Since this kind of expertise is difficult to find and expensive, this service can be obtained in out-sourcing from specialized companies.

Various simpler solutions can be designed. One which could be of interest for this project is to assign to the router the duties of the first firewall and of the VPN concentrator, as in Figure 3.

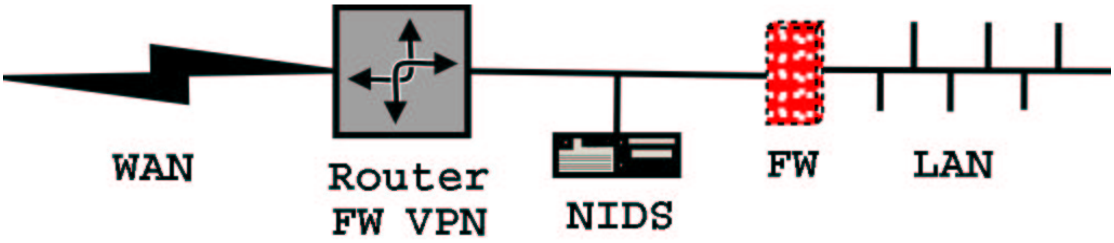

Figure 3. A simpler positioning of Firewall, VPN concentrator and NIDS.

In this configuration the router can apply NIDS and firewall functions to the external WAN interface. The VPN tunnel would then be terminated on an virtual internal interface which would play the role of the VPN concentrator. Still the remaining firewall and NIDS will protect the hosts in the internal network.

A final simplification consists in eliminating also the remaining firewall and NIDS and assign their functions to the internal interface of the router.

As general comments on the simplified solutions, it has to be considered that a router with firewall and NIDS features is not completely equivalent to have dedicated hardware built on purpose. Moreover, if in the final simplest configuration the router falls in the hands of an attacker, all is lost, whereas in the first solution the attacker will still have to gain access to 2 firewalls and one VPN concentrator and, if all is well configured, the chances that the NIDS will detect these attacks are extremely high. A similar argument holds for the middle configuration. Thus great care should be taken before choosing one of the simplified solutions.

The choice of the type of firewall is also a critical point in the setup. Depending on their internal logic, it can be generically considered that there are 3 kinds of firewalls:

1. Access Control List (ACL): the simplest kind of firewall is based on a list of checks with respects to the network and transport headers of the packets; every packet is checked against this list in order and at the first match a command usually of accept or deny, is applied
2. Stateful Inspection: an extension to the previous case, once a packet is accepted all following packets belonging to the same connection are accepted without the need to be checked against the List
3. Application Level: the firewall in this case works at the higher levels of the OSI pile, by proxying all connections between clients and servers; in

practice it behaves as if it was the final server for a client, and as if it was a client for the real server; in between it can check the content of all passing packets.

Obviously current firewalls do often have features belonging to all 3 kinds, even if pure Application Level firewalls are usually quite different from the other two kinds.

For the applications of this project and the kind of data transferred between the different location, the choice is between a ACL or a Stateful Inspection firewall. Indeed the traffic coming from the outside network is encrypted and in this case very simple ACL rules are enough for the external firewall. More difficult can be the job of the internal firewall and this will be discussed in turn in each case.

For what concerns the high-availability of these security devices, all the considerations done in section §**2.1** must be applied. In particular Firewall, NIDS, VPN concentrators must be redundant or doubled, depending on the LAN on which they are.

An alternative solution for the security of the data is to adopt end-to-end encryption. In this solution, data is encrypted before leaving the source host and is decrypted only by the arrival host, for example the data is encrypted by a PMU and decrypted by the regional Area Center Computational Unit. This solution guarantees the end-to-end security of the data, whereas with router-to-router VPN, all traffic on the internal LANs is not protected by encryption. If physical security of the premises is guaranteed, the security added by this solution would not be particularly relevant. In any case, the rules of defense in depth state that more layers of barriers must be deployed to obtain more effective security systems. This solution offers the following advantages:

- end-to-end encryption
- less work for routers and not necessity of VPN concentrators, which implies lower delays on the network.

On the other side there are the following disadvantages

- encryption/decryption must be done in all hosts, for example if at the regional Area Center more than one host is present for the ANN, the communications between all these hosts should be encrypted too
- for connections which require minimum latency, encryption/decryption cannot be done in software because precious resources of the hosts will be used for this, but must be done in hardware, thus all hosts must be supplied with encryption/decryption hardware; if at a regional Area Center there is more than one host, the extra encryption/decryption of the communications between the hosts in any case add extra delays
- new hardware (and software) means more points of failure, and more devices to manage
- changes in security protocols will require hardware changes in all hosts with encryption cards
- possibility of controlling the incoming data after it has exited the encrypted tunnel are very limited since the data will already be in the destination host, thus if a malicious attacker will take control of a remote site, he/she will be able to send packets directly to an host at the regional Area Center and even if it still possible, depending on the Operating System of the host, to apply some filters and checks to the incoming packets, not the full extensive checks

provided by firewall and NIDS are possible.
Safe these changes, all considerations done before apply also to this solution.

An important issue, unfortunately too often overlooked, is the maintenance of software releases for all platforms, from hosts to routers etc. Within the management duties there must be devoted personnel to this maintenance, and procedures must be in place to guarantee that security patches are applied as soon as technically possible. This means that patches and upgrades must be applied to all devices as soon as it has been tested and verified that the patch or upgrade does not interfere with the normal operation of the devices. Again, maximum priority must be given to this activity.
It must be also verified, for example once a year, if the protocols adopted for the security of the communications, like IPSEC, 3DES etc., can still be considered secure for this particular application. In case there have been particular advances in crypto-analysis, it could be required to upgrade or change all or part of the security protocols adopted.

2.2.6 Mitigation of Malicious Attacks for Inter-regional Communications

In the case of inter-regional connections between regional Area Centers, it seems appropriate to adopt the first more general security setup previously illustrated (see Figure 2.), using router-to-router IPSEC VPN. The filters and controls should be applied both at the outside traffic arriving at the external router, and at the traffic just exited from the VPN tunnel, as described before. In case maintenance and costs will make this solution difficult to implement, the second solution (see Figure 3.) could be implemented. It is not suggested to adopt the simplest, router only, configuration.
Since the connections established between the regional Area Centers are of different type using both TCP and UDP, and in same cases also complicated protocols like RPC [24] can be adopted, a Stateful Inspection internal firewall is suggested in this case. Indeed this type of firewall will be able to understand many, if not all, kind of connections and automatically open and close the needed and authorized ports.

Suggestions: adopt security policy for personnel, network, hosts and software maintenance, local physical security, encrypted tunnel on WAN circuits with IPSEC VPN (3DES or AES, ESP, group 2 DH, SHA1 or MD5), firewall, NIDS and VPN concentrator as in Figure 2 (preferred) or 3; all hardware must be redundant.

2.2.7 Mitigation of Malicious Attacks for Transient Stability

In principle, for the highest performance requested by this service, host-to-host encryption with dedicated hardware cards could provide the fastest solution. In this solution the regional Area Computational Unit is not protected by malicious traffic injected in the tunnel at the remote location. From this point of view it could be considered to install Host Intrusion Detection System on the Computational Units. Again the problem is to evaluate the benefits of such software with respect to the amount of resources that they will use on the Computational Unit hosts. In any case, connection of the Computational Units towards other networks, for example to the SC-PM SCADA or to remote managing stations, must be protected by firewalls and NIDS, obviously different hardware with respect to the ones in case adopted for the WAN connections considered before.

The most common solution, easier to implement and maintain, is to adopt router-to-router encryption. Probably the best compromise between security and efficiency is to adopt an unbalanced solution.

At a remote location of a PMU, the simplest solution where all duties of firewall, VPN and NIDS are done by the router, can be adopted. The reasons for this choice are that the internal network at these premises is very simple and little data has to be transmitted. The management of the remote hardware will be simplified and the delays will be minimized by having a high level router do everything. The major risk is if an attacker gets control of the router itself, in this case he/she will be able to inject traffic towards the regional Area Center, and to send data on the internal network. This second is the highest threat since the attacker could try to send fake remedial commands with the intent of perturbing the normal operation of the electrical network. This risk should be mitigated by the management network of the router which should be configured in such a way to notify the operator if changes in the router configuration take place.

At remote locations where remedial commands are sent, it is suggested to adopt the solution described in Figure 3., that is with a firewall after the router that will filter the data arriving out of the VPN from regional Area Center. The reason for this extra security with respect to the case of the PMU's locations is because an attacker could try to inject some fake remedial commands and if the attacker is able to enter the router, without a firewall no other defense would remain. It is also suggested from a security point of view, to have after the firewall and before the final device an host which could receive the command from the regional Area Center, apply some strong consistency checks, and only after this it should pass the command to the device. In presence of this host, an intermediate solution could be adopted where the host has an integrated firewall and thus it is not needed to have an independent firewall appliance. This solution would be less secure than the previous one, but it could reduce delays and be easier to maintain.

At the regional Area Center the solution described in Figure 2. or, if deemed not possible, at most the one described in Figure 3. must be adopted. For what concerns the type of firewall, it should either be configured as a ACL or Stateful Inspection depending on the performances of the firewall itself. Different firewall from different vendors adopt different internal logic to filter the packets, and it is difficult to estimate a priori if with the kind of traffic that will flow through them, it will be more performant to use short and well written ACL or simple Stateful rules. It has to be remembered that the traffic which will pass is of simple UDP packets, so that good ACL rules could still give the best performance.

At a remote location the router will have to do more work to encrypt and decrypt packets, and this amounts to some extra delay. To quantify this, the tests of section §1.2.2.5 have been repeated establishing between the two routers an ESP IPSEC tunnel with 3DES, SHA1 and group2 DH. The same measurements as in §1.2.2.5 have been repeated now transmitting the packets through the VPN tunnel. The delay in the one-way transit has increased by 5ms, to 19ms for 100Bytes packets, and by 6ms to 22ms for 500Bytes packets. It should be considered that the router is a very low level model, and that for higher level models there exist hardware cards which make the encryption/decryption reducing the delay. Moreover, without encryption card, the delay is also proportional to the amount of traffic that must be encrypted/decrypted and the speed of the CPU.

At the regional Area Center the presence of firewall and VPN concentrators will add delays, just by the fact that each packet has to be loaded and unloaded by each device. Depending on the solution chosen and the kind of hardware employed, delays of a few milliseconds will be added by these devices.

Suggestions: adopt security policy for personnel, network, hosts and software maintenance, local physical security, encrypted tunnel on WAN circuits with IPSEC VPN (3DES or AES, ESP, group 2 DH, SHA1 or MD5), firewall, NIDS and VPN concentrator as in Figure 2 (preferred) or 3 for the regional Area Center, the all-in-the-router solution at the remote locations with PMU, and solution as in Figure 3. at remote locations where remedial commands are sent; all hardware must be redundant at the regional Area Center.

2.2.8 Mitigation of Malicious Attacks for Voltage Stability

The discussion for the Transient Stability applies also to this case.

Suggestions: the solution for the Transient Stability applies also to this case.

2.2.9 Mitigation of Malicious Attacks for Management Communications

An issue that should not be overlooked is the security of the management of the devices. As previously discussed, a full management solution, preferable using different networks from the data ones, must be in place. An attacker must not be allowed to attack any management host or communication channel. Besides the information that an attacker could gather from listening to the communications between the devices, he/she could be able to inject commands, reduce or completely halt the services, or even get full access to the devices. Again all management communications between all devices must be encrypted. In this case it is not suggested to use an encrypted tunnel, but to adopt protocols which are intrinsically secure, that is adopt end-to-end cryptography. For example direct remote console access to hosts and routers should be allowed only using the Secure-Shell SSH (or similar) protocol and not TELNET, analogously SNMPv3 (Simple Network Management Protocol version 3) with encryption must be adopted and not previous versions of SNMP. Moreover, all communications should be one way that is the central management should be allowed to connect to the remote host but not viceversa, to prevent the risk of a remote host falling in the control of an attacker who could then easily have access to the central management station and from there to all network. Security against attacks of all management hosts and networks must be at least at the same level of the security procedure adopted for the data, and the general considerations done previously apply also in this case. For example the adoption of firewalls and NIDS should be considered also for the management network.

Suggestions: adopt security policy for personnel, network, hosts and software maintenance, local physical security, host-to-host encryption and secure protocols, firewall and NIDS.

3 Suggested Solutions

In this section the different solutions will be summarized. Moreover at the end some test configurations will be indicated.

3.1 Inter-regional solution

3.1.1 *WAN Network*

Adopt a dedicated 256Kbps leased circuit with, for example, Frame-Relay, or use a 2Mbps connection with ETSO-Electronic Highway.

3.1.2 *LAN Network*

A full-duplex 100Mbps FastEthernet network is suggested.

3.1.3 *Dependability*

It is necessary to have a backup connection, and this could be another 256Kbps line, or a satellite connection since the delay in this case is not too important, or again even a dialup isdn connection at 128Kbps. If a 2Mbps circuit with ETSO-Electronic Highway is chosen, to avoid bottlenecks it is suggested that there is a reserved backup circuit only for this traffic, or that the backup circuit would be at least 1Mbps. To guarantee fast backup, double routers are needed, and it is important to have constant monitoring and hardware contracts with supplier for hardware replacement within 4 hours. Internal LAN and hosts should be doubled or redundant. On-site and Off-site backup of all data and configurations is needed.

For security router-to-router encryption and a firewall, NIDS, VPN concentrator solution like the one in Figure 2. or Figure 3.

Comprehensive security policy and procedures must be prepared, adopted and enforced for personnel, network, hosts and software adoption and maintenance.

3.2 Transient Stability

Figure 4. is a diagram of the proposed general network solution, dashed lines indicate management connections. In the Figure only PMU are indicated, but the same network structure can be adopted for remote devices which should receive remedial commands.

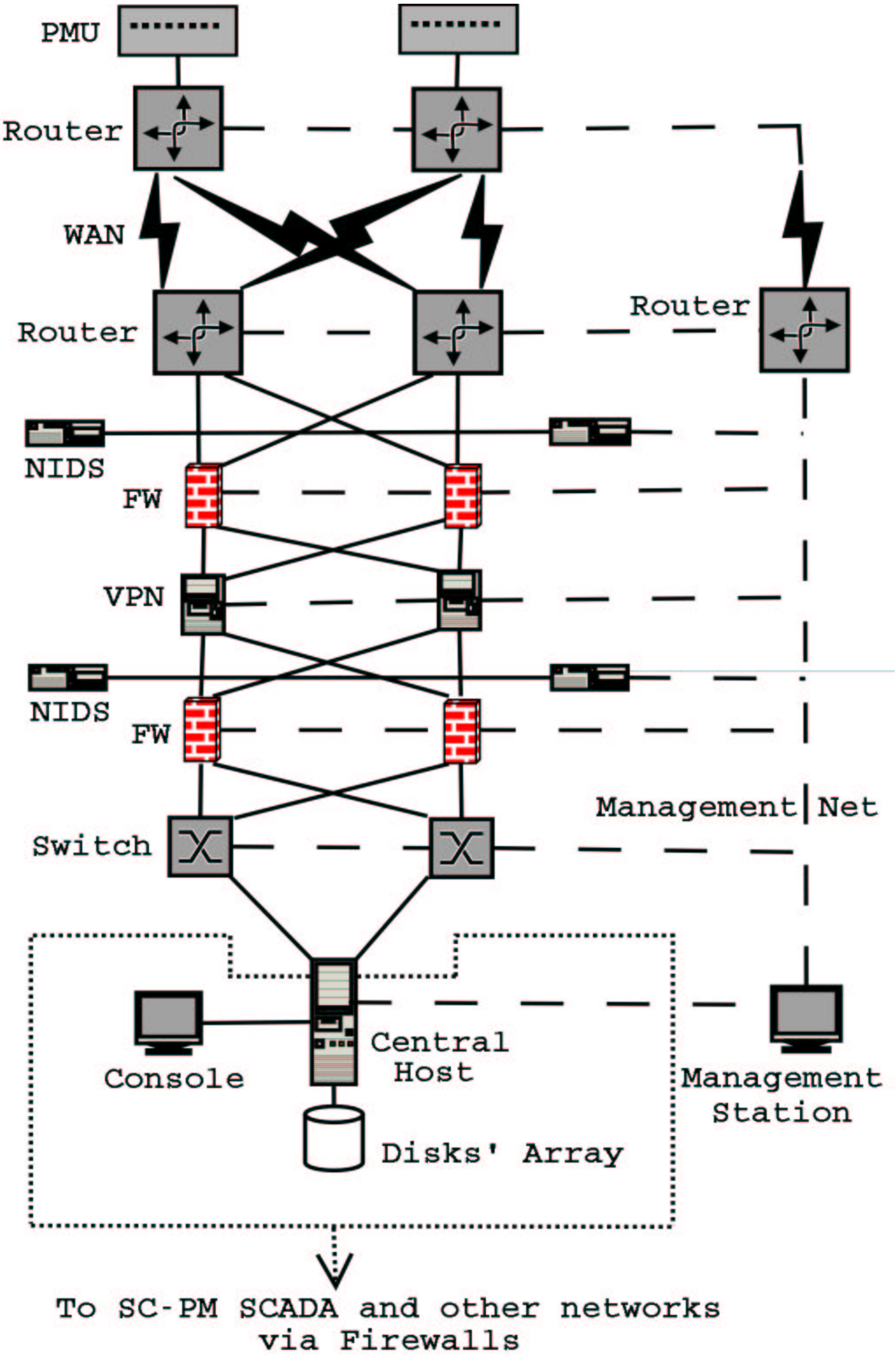

Figure 4. A diagram of the proposed general network solution, dashed lines indicate management connections.

3.2.1 *Delays Assessment*

As already stated, the full procedure, from the starting of the physical phenomenon to the moment in which the remedial action is effective, must complete within 500ms. After the discussion in the previous sections, the time needed for the procedure can be detailed as follows:

10ms for the PMU to prepare the data (**input data**)

200ms for a PMU to send all data needed to recognize a phenomenon (**input data**)

10ms for the host at the remote location to prepare the data to be sent on the network (**requirement on implementation**);

100ms of transmission delay time for the data (maximum 400Bytes per measure) sent by a PMU on the LAN and WAN networks included encryption/decryption and firewall filters to reach the regional Area Center Computational Unit (**estimated**)

50ms for all hosts at the regional Area Center to receive, upload, analyze the data sent by the PMUs and prepare, download, send a remedial command, included the time needed for communications between the hosts at the regional Area Center, if more than one host is present (**requirement on implementation**)

80ms of transmission delay time for the data (less than 70Bytes) sent by the regional Area Center Computational Unit on the LAN and WAN networks included encryption/decryption and firewall filters to reach the remote remedial action device (**estimated**)

70ms for the device to realize the remedial action (**input data**);

520ms SUM

All timings here considered are in the worst case, *estimated* timings must be verified in the implementation. A different estimate can be done considering delays in normal conditions:

<10ms for the PMU to prepare the data (**input data**)

200ms for a PMU to send all data needed to recognize a phenomenon (**input data**)

<10ms for the host at the remote location to prepare the data to be sent on the network (**requirement on implementation**);

<40ms of transmission delay time for the data (maximum 400Bytes

per measure) sent by a PMU on the LAN and WAN networks included encryption/decryption and firewall filters to reach the regional Area Center Computational Unit (**estimated**)

<30ms for all hosts at the regional Area Center to receive, upload, analyze the data sent by the PMUs and prepare, download, send a remedial command, included the time needed for communications between the hosts at the regional Area Center, if more than one host is present (**requirement on implementation**)

<30ms of transmission delay time for the data (less than 70Bytes) sent by the regional Area Center Computational Unit on the LAN and WAN networks included encryption/decryption and firewall filters to reach the remote remedial action device (**estimated**)

<70ms for the device to realize the remedial action (**input data**);

<390ms SUM

Moreover in this document it has been stated that to mitigate various risks (for example: lost measurements, lost packets on the network, need of more time to recognize the phenomenon, switching of WAN links or a remedial action which takes more than 70ms to complete) it is necessary to introduce a Safety Factor which should be at least

120ms Safety Factor.

Thus, including the Safety Factor the total delays become[18]

640ms worst case

<510ms normal condition.

Based on these results, the following conclusions can be taken:

- in normal conditions every phenomenon can be successfully addressed (in normal conditions the Safety Factor is not needed) since the total delay is less than 390ms;

- if, for example, what are usually considered normal network oscillation in the transit delay happen, it is not possible to give any assurance that the phenomena which require maximum delays of 500ms, can be addressed in time;

- there is no possible risk mitigation for the phenomena which require maximum delays of 500ms;

[18] A condition which could lead to the *normal condition + Safety Factor* situation is when a packet is lost but all others just before and after it on the same circuit, are delivered with average normal delay.

- worst case network and host conditions, and risk mitigation as discussed in this Deliverable are assured for phenomena which have time scale larger than 640ms.

In conclusion, in normal network and host conditions, fast phenomena requiring maximum delays of 500ms, can be addressed, but no risk mitigation or assurance can be given that this will happen in every circumstance. Phenomena which have time scale larger than 640ms can be fully addressed with the approach and technologies discussed in this Deliverable.

It should be stressed that further analysis, different technologies or implementations, direct tests in laboratory and on field, could improve (or disprove) the results here presented.

It should be also considered here what are the changes to these time scheduling if the PMU model with a frequency of the measurements of 20 per second, that is one every 50ms, would be chosen instead. The only change to the previous estimates would be that the time needed to recognized a phenomenon would be 230ms instead of 200ms. There will be then an increase by 30ms of all previous estimates. On one side this makes it more difficult to assure that the 500ms phenomena are always addressed within the maximum delay, since now in the Worst Case Scenario the maximum delay is 670ms. On the other hand, most of the phenomena require a maximum delay of 800ms, which is still easily assured. At the same time with this second model of PMU the measurements arrive at the Computational Unit every 50ms, leaving 30ms more to analyze all data and detect a fault before a new set of data arrives.

3.2.2 *WAN Network*

Adopt 2Mbps dedicated ATM WAN circuit with guaranteed delay, it is suggested to request guaranteed one-way average delay of the order of 20ms and maximum delay less than 60ms. Assured packet loss < 0.3% or similar on the WAN circuits. High level routers are requested to end these circuits. Reserve WAN and LAN circuits only for communications between PMUs and regional Area Center, with the only possible exception being traffic going in the opposite direction for remedial action commands.

3.2.3 *LAN Network*

A full-duplex 100Mbps FastEthernet network at the regional Area Center, and at least a half-duplex 10Mbps Ethernet network at the remote locations. Fast switch are requested at the regional Area Center whereas PMU and devices should be directly connected to the routers at the remote locations. Data should be transmitted using UDP protocol. Have a high quality, fully redundant host as computational unit with many CPU, large RAM and fast disk array. Adopt if possible a Real Time Operating System.

3.2.4 *Dependability*

Adopt N-1 PMU distribution model; have doubled WAN 2Mbps circuits fully active sending double packets; current assurance of channel availability offered by provider are of 99.99% (allowed downtime of 53 minutes per year) or 99.95% (allowed downtime of 4.4 hour per year); have fully doubled network at the regional Area Center; have a single, very high level, fully redundant Computational Unit; adopt full data and configuration Backup strategies; have hosts at remote locations with hot-stand-by unit; have hardware maintenance and fast replacement contracts.

For security router-to-router encryption should be adopted and, at the regional Area Center a firewall, NIDS, VPN concentrator solution like the one in Figure 2. or Figure 3. At the remote locations with PMUs should be adopted instead the simple solution where everything is done by the high level router, and solution as in Figure 3. at remote locations where remedial commands are sent.

Comprehensive security policy and procedures must be prepared, adopted and enforced for personnel, network, hosts and software adoption and maintenance.

3.3 Voltage Stability

The solution for the Voltage Stability is similar to the one for the Transient Stability, but due to the lower requirements on network delays, slower or less guaranteed WAN circuits can be adopted. For example Frame Relay [4] circuits from 512Kbps to 2Mbps can be adopted, and backup circuits can be also via satellite links. Analogously less requirements are on the quality of the hardware and Operating Systems chosen. All other features are the same as for the solution proposed for the Transient Stability.

3.4 Management Network

3.4.1 *WAN Network*

The optimal solution is to have independent (not too fast) permanent circuits dedicated to this task with dedicated routers. For the inter-regional networks also in-band communication is possible.

3.4.2 *LAN Network*

An independent LAN is suggested.

3.4.3 *Dependability*

All hardware must have contract with supplier for hardware replacement within 4 hours. There should be on-site and off-site backup of all data and configurations. All communications should be encrypted adopting host-to-host secure protocols like SSH or SNMP-v3. Wherever possible all communications should be one-way, that is only from the management server to the clients and not viceversa.

3.5 Test Configuration

The main configuration needed to be tested is the one for the Transient Stability, to explicitly verify that all time constraints are satisfied by the proposed solution. To conduct reliable tests, the Transient Stability solution can be simplified as follows:

- the WAN circuit can be chosen to be a 2Mbps point-to-point Frame-Relay link without explicit strict guarantees
- routers and network devices can be of not so high quality and without guaranteed performances
- the LAN at the regional Area Center can be single instead of double
- the simplest security solution can be adopted where firewall, VPN and NIDS activities are all done by the routers
- the hardware and Operating System of the hosts can be of lower quality from the point of view of guarantees on speed for real-time analysis of data
- no redundancy on the distribution of the PMUs can be adopted
- management can be done in-band

In any case, careful considerations must be done to verify that the test setup will give reliable indications for the true configuration. For example, by choosing lower quality hardware and software for the hosts, more delays can be introduced than in the true solution. On the other side, by simplifying the network and omitting for example the firewalls, the delays introduced by these other network devices are not taken in consideration. A detailed analysis must be done considering the precise performances of all networks and hosts both in the test and real setup.

4 Dependability Analysis

In this fourth Part, further formal dependability analysis of the EXaMINE infrastructure described in the previous parts of this Deliverable, will be addressed. Most of the analysis will be done based on the recent work of the DSoS project [46].

4.1 Conceptual Dependability Analysis

To start a dependability analysis it is necessary to have a formal description of the EXaMINE system. For this reason it is necessary to reformulate the entire structure of the EXaMINE system in a form suitable for this analysis.[19]

The EXaMINE project has been divided in two modes, the Emergency and Preventive Mode. The Emergency Mode can be sub-divided again in two modes, one for the Transient and the other the Voltage Stability phenomena. Actually all two (three) modes address different aspects of the same basic problem: provide a more dependable system for the provision of electricity. The fundamental differences between the two main modes are[20]

1. the Preventive Mode adopts a *pro-active* point of view
2. the Emergency Mode adopts a *re-active* point of view;

moreover

1. the Preventive Mode addresses *large* time scale issues
2. the Emergency Mode addresses *short* time scale issues;

and finally

1. the Preventive Mode requires *long* distance interactions
2. the Emergency Mode requires *short* distance interactions.

4.1.1 *Metalevel description of fundamental features of the Preventive Mode*

The main goal of the Preventive Mode is to plan more precisely the production of electrical power so to be able to better satisfy the requests in the following hours/day. To obtain this it is first necessary to obtain more precise descriptions of the topological current status of the Electrical Power System network. The typical cycle of operations could be summarized by the following diagram (Figure 5):

[19] This section is mainly based on refs. [48], [49] and [52].

[20] All terms adopted in these definitions are relative to each other.

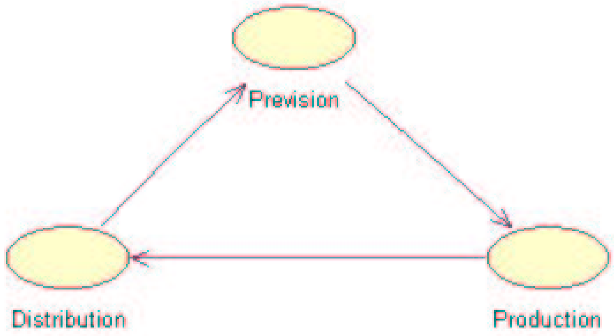

Figure 5. Preventive Mode Cycle

It is important to consider explicitly the administrative aspects of the problem. Lets start by assuming that a company produces and distributes energy for a geographical area, *without* outside links. In this case all three roles, Prevision, Production and Distribution are managed only internally. Nowadays this does not happen any more. The fundamental difference is that the main distribution lines are connected, which implies that the geographical (administrative) areas are connected: Energy is transferred from one area to another. This implies that to make the Prevision for the internal production, a company needs to take in consideration also the contribution of the neighbouring areas. The Figure 5 should then be modified as follows (Figure 6):

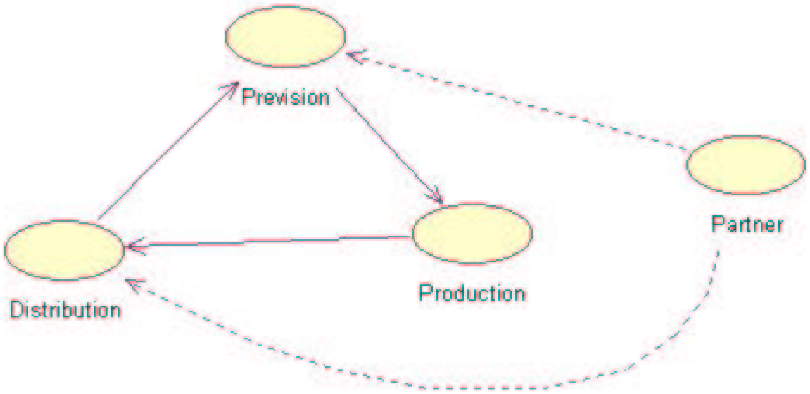

Figure 6. Extended Preventive Mode Cycle

It is quite important to be able to plan correctly the Production and Distribution, the two main reasons for this are:

1. an economical reason, since the flowing of electrical energy from one area to another, or better the domain of one company to another, is regulated by economical transactions
2. a technical reason, since over-production or under-production of electrical energy is likely to produce instability in the network and, most notable in the case of under-production, also problems for the consumers.

It should be stressed that the term *Geographical Area* is not completely proper, since two companies can operate in the same truly geographical zone, having anyway different *domains*, that is customers. Moreover also the interpretation of *Production* and *Distribution* should be interpreted in the most general way, since the free market approach of many European countries and of the EU, introduces different companies which produce and other which distribute energy. Moreover there can be a governing company or Authority responsible for the Prevision of the production and distribution of the energy in a geographical area, usually coinciding with national borders. The model just proposed can be applied both at the level of a geographical area in an overall approach, and within each company, where the Production and/or Distribution should be interpreted as relative to the company type of business. In other words, this model can be applied at two scale levels, the geographical/national level and a company level.

The main goal is then to obtain a system which runs in equilibrium, request and production match each other locally and globally. As it is obvious, this is anything but an easy task.

A critical point is the interaction between two different companies having common domain boundaries. The main issue is that each company needs information from the other to plan its internal production, but at the same time wants to make the most economical profit possible. Moreover, sensibly, neither company allows the other to have access or control over its own electrical network. Thus, in most cases even without been direct competitors, there is an economical interest in the information interchanged.

The Preventive Mode of the EXaMINE project has developed a protocol and application which addresses exactly this point: it provides and automatic way of exchanging information about the boundaries of each network so to be able to make a more precise planning of the production and distribution. This is achieved by having a more accurate way of determining the actual status of the electrical network including its boundaries, and a more accurate forecast of the network status. In practice a company should have EXaMINE connections with all companies with which it shares a border, geographical or administrative. When the company needs to make a Prevision it will request all Partners for updated informations about their boundaries. It should be noticed that it is not needed for a Partner to pass all information about its internal network, but only some informations about the network near its boundary. This application will be run manually by each company when needed, from every few minutes to a few hours.

In this way a company will be able to have a more accurate network actual status and to produce a more detailed and more accurate plan for the Production and Distribution of electrical power.

Following refs. [48] and [49] we now attempt a first classification of the Preventive Mode. For the Preventive Mode a *component* is an EXaMINE partner, that is a full company.

Attributes of Systems and Collection of Systems

1. The components have <u>independent existence</u> from the SoS considered by the EXaMINE project
2. The components have <u>independent operation</u>, i.e. independent management
3. The components have <u>independent evolution</u> but the interfaces between them

are stable as been fixed by EXaMINE

4. The components have no controllability or *intercession interfaces* on each other
5. The components have no observability or *introspection interfaces* on each other
6. A component has dependability provisions w.r.t. internal faults and has not dependability provisions w.r.t. external faults
7. The components are integrated at the electrical network level, at the transport ICT network level and at the application ICT level by sharing the EXaMINE Preventive Mode Application
8. The components interact for the ICT part in a event-triggered mode and with client-server type interaction style
9. The components have static name binding
10. The components have global time, that is they are globally synchronised
11. It is assumed that all mismatches are known a priori, that the components are dependable and that there are clear and fixed syntax, flow control, protocol, data representation, temporal accuracy and semantics for the ICT part
12. All components have single-failure fault tolerance model

To proceed it is needed to recall a few definitions.

Relationships between all components are based on their *roles*, *responsibilities* and *conversations*. The term conversation is used in the normative sense to describe a relationship between two roles. Viewed at the organizational level, conversations correspond to pre-defined contractual arrangements between systems. Each conversation is described by attributes such as: *significance*, *mutuality*, *capability* and *control*.

Significance indicates how the benefits of the relationship are being distributed and can either be symmetrical (equal benefits) or asymmetrical (unequal benefits). *Mutuality* indicates how responsibilities are being distributed. *Capability* shows if resources are shared by two systems in order to fulfil their responsibilities. *Control* indicates which agent in a network has the power to initiate or terminate a relationship.

In the Preventive Mode there are:

1. asymmetric significance for each EXaMINE transaction
2. zero mutuality
3. low capability since only little data is shared among two components
4. equally distributed control

Roles are holders of *responsibilities*. *Duties* represent the tasks that roles need to perform in order to fulfil their responsibilities. In the Preventive Mode each component has equal and reciprocal roles. It is possible to distinguish an active and a passive role. A component has an active role when it initiates a relation with another component starting the EXaMINE algorithm to produce new EPS state information. A component has a passive role when it is invoked by another component with which it shares a boundary. The interaction between components it is then of the client-server type.

A component has direct connection with one or more other components with which it shares a boundary. A component has connections only with other components with which it shares a boundary. Topologically this is a nearest neighbour interaction.

A typical problem of nearest neighbour interactions is to guarantee that the algorithm converges, in other words if there is a modification of the status in one component, this is communicated to the nearest components, which change their status too and communicate this to their nearest components and so on. The algorithm must be fast in converging to the new stable configuration if such a configuration exists in the electrical network, or to indicate that such new configuration is not possible in the electrical network. In both cases the algorithm converges to an final answer. The problem is if there is no answer and no stable point is reached.

Two components are connected through a *Linking Connection*, as described in the previous Parts of this Deliverable. Each component offers to a peer a *Serving or Linking Interface* (LIF) and optionally a restricted *Diagnostic and Management* (DM) interface. There is one such interface for each peer. It is suggested that each component offer to the peer a restricted DM interface through which the peer can obtain generic diagnostic information about the status of the EXaMINE machine and of the network connection. This would help each component to diagnose technical problems of the peers' LIF by adding more information for the human operators about the status of the EXaMINE machine and network than the information exchanged directly through the LIF.

4.1.2 *Metalevel description of fundamental features of the Emergency Mode*

We recall that the Preventive Mode has the purpose of being able to give the actual topology of the electrical network including the boundary connections and, based on this, the forecast status of the electrical network. Based on these two informations, two kinds of intervention are possible:

1. short time (minutes) human or automatic intervention to modify the status of the network
2. plan modifications of the network status in the near future (usually hours or days) to optimize its future behaviour.

Still two main types of problem can appear

1. the planning is not successful due to changed conditions, i.e. different requests from the users, or different production or distribution capabilities than those assumed in the modelling
2. there are failures in the production and/or distribution.

In the first case usually the time schedules are such that the Preventive Mode and even human intervention are usually able to cope with the problem. For the second case there are physical phenomena for which the time scales are quite outside human capabilities, that is they require interventions in the order of seconds or less. The EXaMINE project has addressed in the Emergency Mode two of such problems, the Transient and Voltage Stability.

The Emergency Mode is enacted within an administrative and technical domain because:

1. the time schedule does not allow very long distance interactions
2. remedial actions must be put in action in an automatic way, without human intervention.

Thus the the Emergency mode must work within an administrative and technical domain. The activity of the Emergency Mode can be simply summarized by the following diagram (Figure 7)

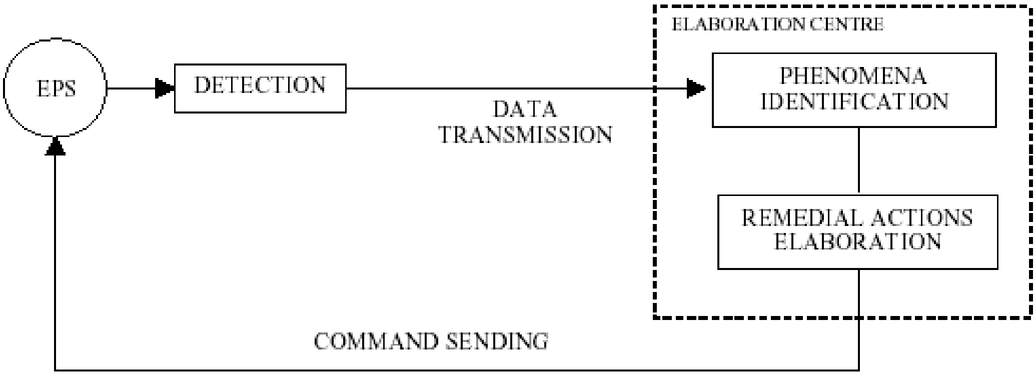

Figure 7. Emergency Mode

where EPS stands for the Electrical Power System, i.e. the electrical network.

Following refs. [48] and [49] we attempt a first classification of the Emergency Mode. For the Emergency Mode the *components* are the PMUs, the Regional Area Computational Unit and the remote devices for enacting the remedial commands, which will be called Actuators. The Regional Area Computational Unit is divided in two sub-components

1. a component which receives the data sent by the PMU and detect if there is a fault, called Detector
2. a component which prepares a remedial command and sends it to the remote Actuator, called Resolver

Attributes of Systems and Collection of Systems

1. The components have dependent existence from the SoS considered by th EXaMINE project
2. The components have dependent operation, i.e. the same management
3. The components have dependent evolution but the interfaces between them are stable as been fixed by ExaMINE
4. The Regional Area Computational Unit component has controllability or *intercession interfaces* on the other components
5. The components have observability or *introspection interfaces* on each other
6. A component has dependability provisions w.r.t. internal faults and has some dependability provisions w.r.t. external faults, in particular the Regional Area Computational Unit has dependability provisions w.r.t. the faults of the PMUs and of the Actuators, whereas these latter do not of the others
7. The components are integrated at the transport ICT network level and at the application ICT whereas the PMUs and the Actuators are also integrated at the electrical network level
8. The PMUs and the Regional Area Computational Unit interact in a time-

triggered mode and with temporal firewall type interaction style, whereas the Regional Area Computational Unit and the Actuators interact in a event-triggered mode and with client server type interaction style

9. The components have static name binding
10. The components have global time, that is they are globally synchronised
11. It is assumed that all mismatches are known a priori, that the components are dependable and that there are clear and fixed syntax, flow control, protocol, data representation, temporal accuracy and semantics for the ICT part
12. All components have single-failure fault tolerance model

This classification will be further explained and expanded in section §4.2.

Recalling the definitions introduced in the previous section, in the Emergency Mode there are:

1. asymmetric significance for each EXaMINE component
2. high mutuality since the responsibility of the benefits of the other components depends on each component to be able to deliver the requested informations in time
3. high capability for the PMUs and low capability for the other components
4. the Regional Area Computational Unit and the PMUs have high control since they send information and command to other components, whereas the Actuators have low control since they are activated by the Regional Area Computational Unit

The duties of each component are the following:

1. the PMUs must send every 20ms (50ms) a measurement of the electrical quantities to the Regional Area Computational Unit
2. the Detector must receive the data, validate it, analyse it and detect if there is an electrical fault, all within the required maximum delay for each cycle (measurement)
3. in case of a fault the Resolver must prepare a remedial command to send to the relevant Actuators
4. the Actuator must receive the command, validate it and put it in action within the required maximum delay.

Each component has the sole responsibility to carry out each duty, this being its role.

Two components are connected through a *Linking Connection*, as described in the previous Parts of this Deliverable. Each component offers to a peer a *Serving or Linking Interface* (LIF) and has a *Diagnostic and Management* (DM) interface accessible to the operators at the Regional Area Centre.

The connections between the components are further detailed by the following ADL/UML diagram prepared according to refs. [50] and [51] (Figure 8)[21]

[21] Following the work of DSoS presented in refs. [50] and [51] the Rational Rose tool has been adopted.

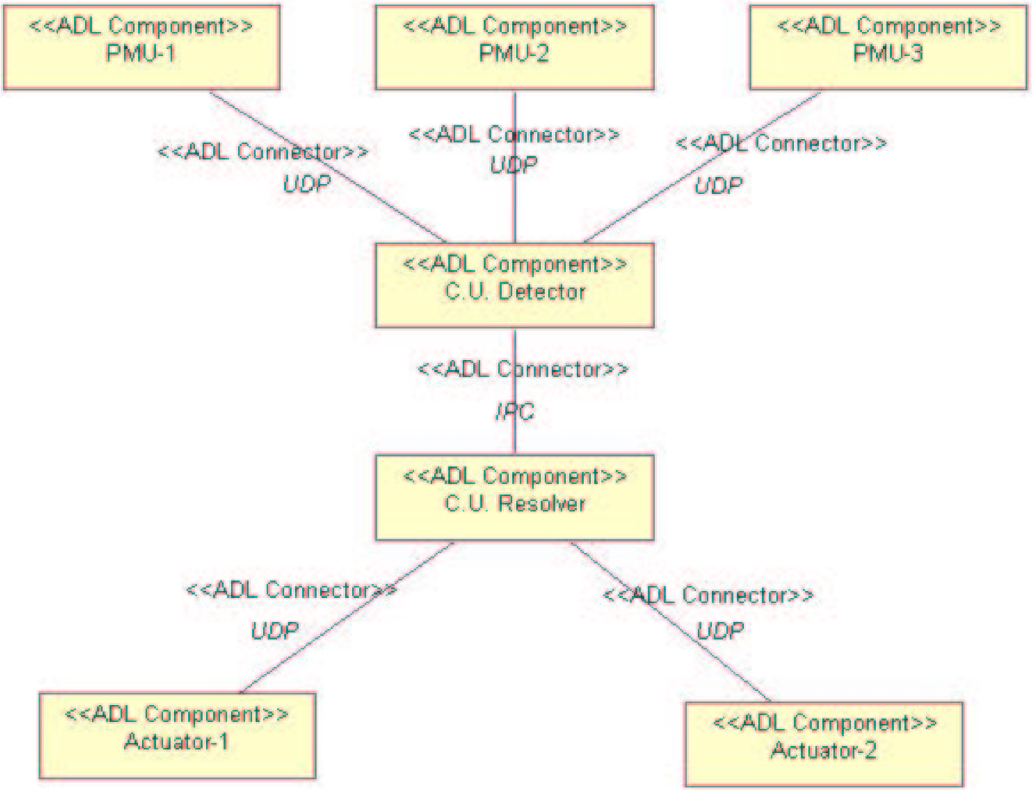

Figure 8. ADL/UML Architecture of the Emergency Mode

This diagram is reported here as a first step in a detailed dependability analysis of the Emergency Mode. Before starting this modelling, qualitative and quantitative study, it is necessary to go through a more detailed formal study and classification of the Emergency Mode; this is done in the next section following ref. [47]. A qualitative/quantitative study of the dependability of the Emergency Mode based on a ADL/UML formalization along the lines of refs. [50] and [51] including the adoption of tools like QNAP, ASSIST/SURE and SPIN, will not be done in this Deliverable.

4.2 Dependability of the Real-Time Infrastructure

Most of the analysis done in this section will follow the DSoS results of reference [47].
In this section the Transient and Voltage Stability Infrastructures will be mostly considered.
It is convenient to start by briefly recalling the relevant taxonomy.

4.2.1 *Taxonomy*

Sparse Time Base: In the sparse-time model the continuum of time is partitioned into an infinite sequence of alternating durations of *activity* and *silence*. The activity intervals form a synchronized system-wide action lattice; all events that occur within a duration of activity of the action lattice are considered to happen at the same time.

Component: In the context of a distributed real-time system, a complete node seems to be the best choice for a component, a component is thus considered to be a self-contained computer with its own hardware (processor, memory, communication interface, interface to the controlled object) and software (application programs, operating system), which interacts with its environment by exchanging messages across linking interfaces (LIFs).

LIF: Linking Interface, of which there exist four types

1. *Service Providing Linking Interface (SPLIF)*
2. *Service Requesting Linking Interface (SRLIF)*
3. *Diagnostic and Management (DM) Interface*
4. *Configuration Planning (CP) Interface*

A component consists of a communication controller (*CC*) and a host computer. The common boundary between the communication controller and the host computer within a component is called the communication network interface *CNI*

Closed Component: a component that interacts with its environment only via a single SPLIF and it is not time aware

Semi-closed Component: in addition to the LIF input messages has only one other type of (hidden) input message, a clock message, that is generated by a synchronized clock denoting the instant of the beginning of a sparse time-granule.

Open Component: a component that has one or more SRLIFs that accept input from the natural environment.

Semi-open Component: a component that can exchange data with the natural environment without delegating control to the natural environment. A sampling system that periodically looks at the natural environment under the control of the component's internal timer is an example of a semi-open component. An interrupt-driven component that accepts interrupts from the natural environment is an example of an open component.

Real-time Entities: entities that change their state as time progresses.

Observation: An observation is an atomic data structure Observation = <Name,Value, tobs> consisting of the name of the RT entity, the observed value of the RT entity, and the instant when the observation was made (tobs).

State Observation: A state observation records the state of a state variable at a particular instant, the point of observation. A state observation can be expressed by the atomic triple: <Name of the observed state variable, observed value, time of observation>

Event Information: Event information contains the difference between the state before the event and the state after the event. An event observation can be expressed by the atomic triple <Name of the observed state variable, value difference, time of event>

Composability: the act of combining parts or elements to form a whole, for an architecture to support composability, it must respect to the following four principles:

1. Independent development of components
2. Stability of prior services
3. Performability of the communication system
4. Replica determinism

Syntactic Specification of Messages: the specification of the data elements that cross the interface. The syntactic specification forms, out of the sequence of bits in a message, larger (information) chunks and assigns a name to each chunk.

Temporal Specification of Messages: the temporal specification of messages send and receive instants, e.g., at what instants the messages are sent and arrive, how the messages are ordered, and the rate of message arrival.

LIF Service Model Specification: a conceptual interface model that relates the names of the chunks to the user's conceptual world and thus assigns a deeper meaning to the chunks generated by the syntactic specification.

Operational Specification: the operational specification of an interface the syntactic specification and the temporal specification.

Metalevel Specifications: Consistency of the specifications of the LIF service models of the communicating partners which assures that the meaning of the information chunks in all involved components is in agreement with the user's intent.

State Message: A state message has the following characteristics:

1. Content: A state message contains state information
2. Flow control: A state message is sent and received periodically at a priori known instants that are common knowledge to the sender and the receiver. Flow control is implicit and unidirectional.
3. Delivery method: Every state message must be delivered at-least once.
4. Error detection: Error detection is performed by the receiver based on the a priori knowledge of the instant of message arrival.

State Message Interface or Temporal Firewalls: A temporal firewall is an operationally fully specified digital interface for the unidirectional exchange of periodic state messages between a sender/receiver over a time-triggered communication system.

Event Messages: An event message has the following characteristics:

1. Content: An event message contains event information
2. Flow control: An event message is sent as a consequence of the occurrence of a significant event. The receiver has no a priori knowledge at what instant an event message will arrive. Flow control is thus explicit and requires a bi-directional protocol.
3. Delivery method: Every event message must be delivered exactly once
4. Error detection: Error detection is performed by the sender based on a timeout for an acknowledgement message from the receiver.

Event Message Interface or Client-Server: an event message interface is an operationally fully specified digital interface for the exchange of event messages.

Stateless LIF: This is a LIF where a response to a service request depends on the parameters of the service request only and is independent of the time of the request.

Stateful LIF: This is a LIF where a response to the service request depends not only on the parameters of the service request but also on the instant when the service request is delivered.

4.2.2 *Principles of the analysis*

It is important to realize that the analysis of the Real-Time LIF model presented in [47] is goal oriented, while an algorithmic model is process oriented. In this context, a goal is a desirable state. A goal-oriented model specifies the intended state, while a algorithmic model specifies actions that must be taken in order to reach this intended state. The LIF service model of a component is different from the model that describes the algorithms that are implemented within a component. For the presentation of the LIF service model, the *means-end hierarchy* is relevant. A means-end hierarchy is goal oriented. The top-most level describes a goal in an abstract form. Subordinate levels specify more concrete sub-goals that contribute to the achievement of the top-most goal. Adjacent levels of a means-end hierarchy are related by an *achieved-by* relation.

In the real-time sparse-time base description, each component of a system at any fixed time is in a *state* which can be described by a *state observation*. But it is important to distinguish clearly between the state of a LIF and the state of the component that supports the LIF.

The DSoS Real-Time LIF model requires among other properties, that:

1. An interface should only serve a single purpose
2. The LIF conceptual model should be structured along a *means-end* hierarchy.

4.2.3 *Setup of the analysis of the Transient Stability Infrastructure*

The Transient Stability Infrastructure is the one with the most stringent requirements for real-time communications. The analysis done in this case can be easily adapted to the case of the Voltage Stability Infrastructure.

The first step of the analysis is to derive a model of the components of the infrastructure and of the associated sparse-time base. Then a first classification of the LIF will be done, on the basis of the goals of each component. The resulting description of the infrastructure will be compared with the results obtained in [47].

To proceed, it is necessary to fix a detailed model of implementation for the infrastructure. With respect to what described in the previous parts of this Deliverable, it will be assumed that:

1. all WAN network communication links are at 2Mbps
2. all WAN links are doubled and each packet is doubled and sent at the same time on both links
3. at the regional Area Centre there is only one Computational Unit which is a highly redundant, multi CPU host on which also all ANN run
4. all host are synchronized and all PMUs send a measurement at the same time

4.2.4 *Component model of the Transient Stability Infrastructure*

The Transient Stability Infrastructure is composed of three components:

1. PMU: these components send every 20ms (50ms) a measurement, which is a set of *state informations,* for this reason they are *semi-open* components with SPLIF interfaces of the type of Temporal Firewalls (i.e. State Message Interfaces), for this analysis it is assumed a maximum of 100 of these components in the system
2. Computational Unit: this single *semi-closed* component is in itself composed of sub-components, but at the highest level it is described as a component with a SRLIF which receives the communications from the PMU and a SPLIF which sends commands to the remote actuators.
3. Actuator: these components put in action remedial commands, it has a SRLIF interface and are (semi) *closed* components, it is assumed a maximum of 100 of these components in the system.

All these interfaces are stateful.

In this modelling of the infrastructure, the networking elements are not considered explicitly. They are modelled as *double cabling* connecting to the Computational Unit all other components. *Cable failure* is possible and summarizes all possible problems which can arise in the underlying complex network system, but the double cabling infrastructure guarantees the single failure fault-tolerance model protection. If one would introduce components also for all the networking elements (routers, firewalls etc.) the description would be quite simple in terms of SRLIF/SPLIF.

Besides the LIF mentioned above, each component should have its own DM and CP interface. This is so for the Computational Unit, but requires further comments for the

PMUs and Actuators. Moreover all networking elements not explicitly described, do have independent DM and CP interfaces and also an independent management network.

The PMU models considered in this project do not satisfy completely the requirements of this analysis. To adhere completely to the requirements they should

1. have two Fast-Ethernet interfaces to send the measurements
2. have independent DM and CP interfaces (some model do have an independent CP interface)
3. be able to send each measurement at the same time to more than one host using both Fast-Ethernet interfaces

Once such PMU models exist, the network configuration at the remote locations with PMUs can then be upgraded to have double Fast-Ethernet LAN with two routers connected to the two WAN circuits, so to have a fully single-failure hardware protection.

Analogous consideration can be done for the Actuators and the network at their locations.

In this way the requirement that an interface should only serve a single purpose is satisfied by the infrastructure proposed. Moreover the modelling as *double cable* of all network infrastructure satisfies the single-failure fault-tolerance protection model.

4.2.5 *Sparse-time base of the Transient Stability Infrastructure*

A possible definition of the sparse-time model from the PMU point of view is very simple: it is just as defining a period of 20ms (50ms) and a *duration of activity* of 1 ms and a *duration of silence* of 19ms (49ms). Since all PMUs are synchronized, they all send their measurements at the *same time*, that is within the duration of activity, and all concurrent state observations from different PMUs sent to the Computational Unit have the same timestamp (time of observation). It is to be noticed that this does not mean that the data are received by the Computational Unit all at the same time and within the duration of activity. Indeed in the Temporal Firewall mode, which is the one adopted by the PMU-Computational Unit communications, a PMU *pushes* the data to its CNI at the fixed time, and the Computational Unit *pulls* the data arrived at its CNI again at fixed times.

This definition of sparse-time model is not very convenient for the activity of the Computational Unit. Indeed in this way, the Computational Unit will wait 19ms (49ms) whereas in that time it could pull some data and start analysing it. Instead it is possible to define for example a *duration of activity* of 0.9 ms and a *duration of silence* of 0.1ms. With this definition each PMU sends a measurement every 20 (50) cycles or intervals, whereas the Computational Unit can pull the data arrived every interval, that is every millisecond. Moreover, this definition of sparse-time can be adopted also for the communications between the Computational Unit and the Actuators. Indeed in this case it is necessary to send the remedial action command to the Actuators as soon as possible, and thus it would not be good to pause up to 19ms (49ms) if the command is ready in the duration of silence interval.

4.2.6 *Composability*

One of the requirements of the model is that the full system be architecturally composable. In particular four principles must be respected:

1. *Independent Development of Components:* this requires a clear distinction between application architecture design and component design. In this Deliverable only the architecture design is considered and all components are described in terms of the properties of their LIF.
2. *Stability of Prior Services:* in the case here considered it means that new components, PMUs or Actuators, can be added to the system without violating its architecture.
3. *Performability of the Communication System:* this should guarantee that the performance of the system is maintained as new components are added to the system (within the maximum number allowed) and that even at a *critical instant*, i.e., when all components request the network resources at the same time, the specified timeliness of all communication requests can be satisfied. The detailed analysis done in the previous parts of this Deliverable gives this assurance.
4. *Replica Determinism:* when, as in the case of this Deliverable, fault-tolerance is achieved by the replication of components, they should be *replica determinated*. For what concerns the network infrastructure, which has not explicitly modelled by components, this is obvious by construction and the time interval of the replica is zero. Indeed redundant data is delivered at the same time through the network, and it is not necessary to reconstruct or retrieve lost or corrupted data from remote replicas. For the PMU fault-tolerance, the N-1 model has been adopted in which one PMU stands, in the language of this section, as a replica. If the Computational Unit receives all measurements of a given time, the data of the Nth PMU is the replica, otherwise if the data from one PMU is missing, then the data from the replica is used instead. Again in this case the time interval of the replica is zero. The case for the Actuators will be discussed below.

4.2.7 *Operational Goals*

The Goals of the Transient Stability Infrastructure are:

1. to be able to deliver to the regional Area Center Computational Unit within the specified maximum delay, at least N-1 out of N measurements of the N PMUs located at the remote measuring nodes
2. to have the Computational Unit elaborate the data so received within the specified maximum delay and if necessary to send to some remote nodes the remedial commands needed to correct the current problems
3. to be able to deliver, within the specified maximum delay, to the remote nodes the remedial commands that have to be put in action.

As already stated, the full procedure, from the starting of the physical phenomenon to the moment in which the remedial action is effective, should complete within 500ms. From the analysis done in the previous Parts of this Deliverable, it has been shown that the EXaMINE Emergency Mode can assure that the full procedure takes at most 640ms for the PMUs with measurements every 20ms, and 670ms for the PMUs with measurements every 50ms. These maximum delays (640ms/670ms) will be then adopted in the following analysis as the real-time constraints.

The Metalevel Specifications of the LIFs follow easily from the goals just described. The consistency is guaranteed by the fact that the PMU LIF delivers, within the specified maximum delay, to the Computational Unit the data needed to detect a fault, in which case the Computational Unit prepares a remedial action command which is delivered to the relevant Actuators, each action always within its own specified maximum delay.

4.2.8 *Operational Specification of the PMU LIFs*

In this section the connection between the PMU and the Computational Unit will be studied in more details. As already seen, a PMU is a *semi-open* component which communicates only with the Computational Unit, which is a semi-closed component; indeed both components are time aware. The PMU sends to the Computational Unit state observations in state messages at fixed intervals, one every 20 intervals, i.e. 20ms (or every 50 intervals, i.e. 50ms). The PMU is a *sampling system* which, with the same periodicity, samples the *natural environment*, that is the electrical apparatus which is supposed to monitor, elaborates, prepares and sends the full measurement to the Computational Unit.

The SPLIF of the PMU is of the type of State Message Interface, also called Temporal Firewall. These interfaces satisfy the following four characteristics:

1. *Content:* A state message contains state information
2. *Flow control*: A state message is sent and received periodically at a priori known instants that are common knowledge to the sender and the receiver. Flow control is implicit and unidirectional.
3. *Delivery method*: Every state message must be delivered at-least once.
4. *Error detection*: Error detection is performed by the receiver based on the a priori knowledge of the instant of message arrival.

In the communication between a PMU and the Computational Unit all these properties are in practice satisfied: as just seen the content is a state information, messages are sent periodically using UDP, each message is delivered usually twice, and error detection is done by the Computational Unit based, for what concerns the real-time properties of the system, on the timestamp present in the state information and on the expected arrival time of the message.

The PMU component is in itself composed by sub-components, for example the clock is a semi-closed sub-component which generates periodic output messages.

4.2.9 *Operational Specification of the Computational Unit LIFs*

The Computational Unit is the most complex object and to understand better its structure and functionality so to be able to guarantee its dependability with respect to the real-time properties of the architecture, it will be necessary to split it in two sub-components.

The goals of the Computational Unit are

1. to receive the data sent periodically by the PMUs
2. to detect if there is a fault
3. to prepare a remedial command in case
4. to send the remedial command.

It is convenient to split the Computational Unit in

3. a component which receives the data sent by the PMU and detect if there is a fault, called Detector
4. a component which prepares a remedial command and sends it to the remote Actuator, called Resolver

The Detector has a CNI (Communication Network Interface), an hardware device which receives the data sent by the PMUs, and periodically pulls the information out of it. It is common knowledge of the sender (the PMU) and the receiver (the Detector) which is the *expected interval of time*[22] during which the data will be delivered to the CNI of the Detector by the communication network infrastructure (instead the *sending instants* are common knowledge of both). The reason for which it is known only an interval of time for the arrival time of the data, is due to many facts already described in details in the previous parts of this Deliverable. In particular, different PMU have different physical distances from the Computational Unit, so that their messages arrive at different times just because of the travel delays, moreover on so long WAN circuits and through so many devices, constancy of the jitters cannot be guaranteed.

The Detector must operate in a cyclic fashion, and must be able to end its work in less than 20ms.[23] The Detector comprises both the ANN and the real fault detection, plus all sanity checks of the data received by the PMUs. It also implements the PMU N-1 model. Moreover, in normal condition the Detector receives two copies of the same state message from each PMU, it should keep the first (if sane) and discard the second.

The Detector knows which is the current time, it is synchronized with the PMUs, and thus it knows that *sane* state messages have a timestamp between 0ms and 120ms ago. If the timestamp is older than 120ms ago, the data cannot be used anymore since the real-time property will be violated, but can anyway be archived for off-line analysis. If this happens, one full measurement is lost.

The Detector can adopt two principal strategies for elaborating the incoming data:

1. every 20ms (50ms) the Detector looks at all data received with a timestamp of 120ms ago and elaborates it
2. every activity interval, i.e. 1ms, the Detector looks if at least N-1 measurements with the oldest timestamp between 0 and 120ms ago are arrived, and if they are the data is elaborated, otherwise it waits until the next interval (obviously while elaborating the data the Detector does not look for the next bunch of data).

In normal conditions the first strategy, even if simpler to implement, adds an extra delay of at least 60ms, so the second strategy is to prefer specially if the computational time of the Detector is well under 20ms. Indeed if the computational time of the Detector is just under 20ms, after a maximum delay has been reached the Detector will not be able to regain time, the data that it will elaborate will always be of 120ms ago. On the other

[22] See also [48] section 5.3.2.1

[23] For the second type of PMU in principle this could be up to 50ms, but the analysis done in the previous Parts of this Deliverable requires a maximum delay of 20ms for the Detector for both PMUs models. If the second type of PMU is adopted, this requirement can be modified but keeping that the total maximum delay of one cycle of the Detector plus the maximum delay of the Resolver sum to up to 50ms.

hand, if the computational time of the Detector is well under 20ms, after a maximum delay of 120ms has been reached, in a few cycles the Detector will be able to again elaborate the data as soon as N-1 state messages arrive. This will practically always happen if the second model of PMU with a frequency of 20 measurements per second is adopted.

If the second and more performant strategy is chosen, it is quite important to speed up as much as possible the Detector. One easy choice is to parallelize all ANN and to execute each one of them independently as soon as the next (in time order) state message arrives.[24]

The Detector has a SRLIF interface which receives the state messages from the PMUs and a SPLIF interface which sends data to the Resolver. This second SPLIF interface is a Event Message Interface (or Client-Server) since a message is sent to the Resolver only if a fault is detected, and thus not a regular intervals. Moreover, after a fault is detected and a message sent to the Resolver, the Detector continues its cycle but it does not send any new fault messages to the Resolver for a minimum delay of 640ms (670ms), plus a possible extra estimated time for the effect of the remedial action to appear in the new measurements. This waiting time could be zeroed if the Resolver reports to the Detector that it has failed to prepared, send or put in action a remedial command. Notice that the fault message sent to the Resolver should contain all data necessary to the Resolver to prepare a remedial command, otherwise the Resolver should be given access at least to the last measurements sent by the PMUs and stored in an archive by the Detector.

Since the Detector and the Resolver are (collection of) processes running on the same host, the communications between them are through, for example, Inter-Process Communication (IPC), and satisfy all characteristics of an Event Message Interface. The Resolver, based on the a priori knowledge of the physical characteristics of the Electrical Network and the last measurements sent by the PMUs, should prepare one or more remedial commands to send to one or more remote Actuators within 30ms.[25] The Resolver has a SRLIF interface which receives the fault message from the Detector and a SPLIF interface which send the remedial command message to the remote Actuators.

4.2.10 *Operational Specification of the Actuators LIFs*

The interfaces between and Actuator and the Resolver sub-component of the Computational Unit are of the Event Message Interface type. For the remedial command to be delivered within 80ms, the data is transmitted using UDP, which is not a connectionful protocol and does not guarantee the delivery of the datagram. Thus no Flow Control is done by the network protocols and it should be done at the level of the application. Indeed Flow Control is one of the requested characteristics of a Event Message Interface. Moreover, two copies of the message are sent at the same time through the double network. Thus, in normal conditions the Actuator receives two copies of the same message, identified also by the timestamp put by the Resolver at the time of delivery, and, after having checked that at least one of the messages is *sane*, the

[24] Care should be taken for out-of-order state messages.

[25] This delay could be less if the second model of PMU is adopted, as discussed in the footnote in the previous page.

Actuator keeps the first sane message and deletes the second. At this point *exactly one* message has been delivered and the Actuator should send back to the Computational Unit a short message of acknowledgement. This message is again doubled and sent using UDP to the Computational Unit which should wait at least 160 ms from the moment in which it sent the remedial command for this acknowledgement to arrive. If no message arrives at the Computational Unit within 160ms from the moment it sent a remedial command message to an Actuator, the Computational Unit should assume that its remedial command message has gone lost.

Once an Actuator has received a remedial command, it should put it in action. After that it should send back to the Computational Unit a second message stating if the remedial action has been successfully implemented or not. This extra information could be useful to the Resolver for deciding future remedial command. This second message should reach the Resolver sub-component of the Computational Unit within 610ms (640ms) from the moment the remedial command has been first sent to the Actuator, that is before the Resolver will start to prepare, in case, a new remedial command.

Once the Actuator has received a remedial command, it should not accept new remedial commands for a minimum delay of 640ms (670ms), plus a possible extra estimated time for the effect of the remedial action to appear in the new measurements. If the Actuator fails to put in action the remedial command, it should zero this waiting time.

It remains to discuss the single failure fault-tolerance of the Actuators. First of all, the regional Area Computational Unit knows at any given time which PMUs are active, and reachable via the network, since every 20ms (50ms) it should receive a measurement from them. Thus it could be stipulated that if the Computational Unit does not receive M consecutive measurements (for example M=10) from a PMU, then it could declare the that PMU temporarily at fault/unreachable. Instead the interfaces in the communications between the Computational Unit and the Actuators are of the Event Message type, it is then suggested that keep-alive messages are exchanged between the Actuators and the Computational Unit so that the Computational Unit is aware of the status of all the Actuators at the moment of the preparation of a remedial command. It should be noted that this is different from the Diagnostic and Management (DM) Interface, which is not used in normal component operation, but is only an interface for the service engineers. Due to the real-time nature of the physical processes, it is not possible to have the information of a fault to be sent from the DM interface to the engineer who manually will reconfigure through the CP interface the Computational Unit. Thus the components should exchange the minimum necessary status information in real-time using their usual LIF interfaces. Finally, for what concerns the single failure fault-tolerance of the Actuators, the algorithm of the Resolver sub-component of the Computational Unit should adopt a N-1 model, that is be able to generate a set of remedial commands even if one of the Actuators is at fault or unreachable.

5 References

[1] ATM (ITU-T) standards are at the ATM Forum, http://www.atmforum.com/

[2] CAIDA, Bandwidth Estimation: Issues and Approaches, http://www.caida.org/analysis/performance/bandwidth/

[3] Cheswick, W.R. and Bellowing, S.M., Firewall and Internet Security: Repelling the Wily Hacker [Addison-Wesley, Reading, Mass. 1994]

[4] Frame Relay (ANSI) standards are at the Frame Relay Formu, http://www.frforum.com/

[5] Garfinkel, S. and Spafford, G., Practical Unix and Internet Security [O Reilly, Sebastopol, CA, 1996]

[6] IEEE-802.3, Standard for Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications-Media Access Control (MAC) Parameters

[7] INFN, Internet Performance Measurement, http://ipm.mib.infn.it/

[8] IPMA, Internet Performance Measurement and Analysis, http://www.merit.edu/ipma/

[9] IPSEC (IETF) standards are at http://www.ietf.org/html.charters/ipsec-charter.html

[10]Matrix NetSystem, Network Monitoring and Measurements, http://www.matrixnetsystems.com/

[11] Megabitex, Quality of Service Measurement, http://www.megabitex.it/

[12] Menezes, A., van Oorschot, P., and Vanstone, S., Handbook of Applied Cryptography [CRC Press, 1996]

[13] MPLS (IETF) standards are at the MPLS Forum, http://www.mplsforum.org/

[14] NLANR, Measurement and Network Analysis Group, http://moat.nlanr.net/

[15] Novak, J. and Northcutt, S., Network Intrusion Detection: An Analyst's Handbook [New Riders Publishing, 1999]

[16] RFC-0768, User Datagram Protocol, J. Postel [Aug-28-1980]

[17] RFC-0791, Internet Protocol, J. Postel [Sep-01-1981]

[18] RFC-0792, Internet Control Message Protocol, J. Postel [Sep-01-1981]

[19] RFC-0793, Transmission Control Protocol, J. Postel [Sep-01-1981]

[20] RFC-0813, Window and Acknowledgement Strategy in TCP, D.D. Clark [Jul-01-1982]

[21] RFC-0826, Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware, D.C. Plummer [Nov-01-1982]

[22] RFC-0894, Standard for the transmission of IP datagrams over Ethernet networks, C. Hornig [Apr-01-1984]

[23] RFC-1042, Standard for the transmission of IP datagrams over IEEE 802 networks, J. Postel, J.K. Reynolds [Feb-01-1988]

[24] RFC-1057, RPC: Remote Procedure Call Protocol specification, Sun Microsystems [Jun-01-1988]

[25] RFC-1122, Requirements for Internet Hosts - Communication Layers [October 1989]

[26] RFC-1157, Simple Network Management Protocol (SNMP), J.D. Case, M. Fedor, M.L. Schoffstall, C. Davin [May-01-1990]

[27] RFC-1349, Type of Service in the Internet Protocol Suite, P. Almquist [July 1992]

[28] RFC-1441, Introduction to version 2 of the Internet-standard Network Management Framework, J. Case, K. McCloghrie, M. Rose, S. Waldbusser [April 1993]

[29] RFC-1624, Computation of the Internet Checksum via Incremental Update, A. Rijsinghani, Ed. [May 1994]

[30] RFC-1661, The Point-to-Point Protocol (PPP), W. Simpson, Ed. [July 1994]

[31] RFC-1812, Requirements for IP Version 4 Routers, F. Baker, Ed. [June 1995]

[32] RFC-2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, K. Nichols, S. Blake, F. Baker, D. Black [December 1998]

[33] RFC-2570, Introduction to Version 3 of the Internet-standard Network Management, Framework J. Case, R. Mundy, D. Partain, B. Stewart [April 1999]

[34] RFC-2571, An Architecture for Describing SNMP Management Frameworks, B. Wijnen, D. Harrington, R. Presuhn [April 1999]

[35] RFC-2572, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), J. Case, D. Harrington, R. Presuhn, B. Wijnen [April 1999]

[36] RFC-2573, SNMP Applications, D. Levi, P. Meyer, B. Stewart [April 1999]

[37] RFC-2574, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), U. Blumenthal, B. Wijnen [April 1999]

[38] RFC-2575, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP), B. Wijnen, R. Presuhn, K. McCloghrie [April 1999]

[39] RFC-2576, Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework, R. Frye, D. Levi, S. Routhier, B. Wijnen [March 2000]

[40] RFC-2578, Structure of Management Information Version 2 (SMIv2), K. McCloghrie, D. Perkins, J. Schoenwaelder [April 1999]

[41] RIPE NCC, Test Traffic Measurements, http://www.ripe.net/ttm/

[42] Schneier, B., Applied Cryptography [John Wiley & Sons, New Yor, 1996]

[43] SLAC IEPM, Internet End-to-end Performance Monitoring, http://www-iepm.slac.stanford.edu/

[44] Stevens, R.W., TCP/IP Illustrated [Addison-Wesley, Reading, Mass. 1994]

[45] Zwicky, E.D., Cooper, S. and Chapman, D.B., Building Internet Firewall [O Reilly, Sebastopol, CA, 2000]

[46] Dependable Systems of Systems, IST Programme RTD Research Project IST-1999-11585, http://www.newcastle.research.ec.org/dsos/

[47] Kopetz, H., On the specification of lining interfaces in distributed real-time systems, Research report 8/2002, Technical University of Vienna, document DSoS-HK8, http://www.newcastle.research.ec.org/dsos/deliverables/index.html

[48] Gaudel, M.C. et al., Final Version of DSoS Conceptual Model (CSDA1), Report 54/2002, Technical University of Vienna, document DSoS-CSDA1, http://www.newcastle.research.ec.org/dsos/deliverables/index.html

[49]Periorellis, P., Addressing Dependability in Multiple Domains of Management, document DSoS-DCS3, http://www.newcastle.research.ec.org/dsos/deliverables/index.html

[50] Nguyen, V.K. Issarny, V., Demonstration of Support for Architectural Design for Dependable SoSs, document DsoS-CSDA2, http://www.newcastle.research.ec.org/dsos/deliverables/index.html

[51] Arlat, J. et al. , Initial Results on Architectures and Dependable Mechanisms for Dependable SoSs, document DSoS-IC2, http://www.newcastle.research.ec.org/dsos/deliverables/index.html

[52]Dobson, J. and Periorellis, P., Models of Organizational Failure, document DSoS-PCE4, http://www.newcastle.research.ec.org/dsos/deliverables/index.html

[53]Ballance, J.W. Bhargava, B. and Rodriguez, G.D., Monitoring Power System Dynamics using Phasor Measurement Technology for Power System Dynamic Security Assessment, Southern California Edison Co., Paper accepted for presentation at 2003 IEEE Bologna PowerTech Conference, June 23-26, Bologna, Italy

[54]Rasmussen, J. and Jørgensen,P., Synchronized Phasor Measurements of a Power System Event in

Eastern Denmark, Paper accepted for presentation at 2003 IEEE Bologna PowerTech Conference, June 23-26, Bologna, Italy

6 List of Acronyms

3DES	Triple Data Encryption Standard
AAL	ATM Adaptation Layer
AES	Advanced Encryption Standard
AH	Authentication Header, an IPSEC mode
ANN	Artificial Neural Networks
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode (a layer 2 network protocol)
bps	bit per second
CC	Communication Controller
CDN	Direct Numerical Circuit
CEF	Cisco Express Forwarding
CNI	Communication Network Interface
CP	Configuration Planning LIF
CPU	Central Processor Unit
CRC	Cyclic Redundancy Check (checksum)
CSU/DSU	Channel Service Unit/Data Service Unit
DCE/DTE	Data Communications Equipment/Data Terminal Equipment
DH	Diffie-Hellman key exchange algorithm
DM	Diagnostic and Management LIF
DSL	Digital Subscriber Line
DSoS	Dependable Systems of Systems
DWDM	Dense Wavelength Division Multiplexing (fiber-optic transmission technique that employs light wavelengths to transmit data parallel-by-bit or serial-by-character)
ETSO	European Transmission System Operators
ESP	Encapsulating Security Payload, an IPSEC mode
GPS	Global Positioning System
HDSL	High bit-rate Digital Subscriber Line
I/O	Input Output
ICCP	Inter Control Center Communications Protocol
ICMP	Internet Control Message Protocol
IMA	Inverse Multiplexing over ATM
IOS	Cisco IOS® Software is a feature-rich, network systems software for Cisco Routers that provides a common IP fabric, functionality and command-line interface (CLI) across a network
IP	Internet Protocol
IPC	Inter Process Communication
IPSEC	IP Security, a complex IETF protocol to secure IP communications
ISDN	Integrated Service Digital Network

Kbps	Kilo bit per second
LAN	Local Area Network
Lambda F.	A frequency on a multi frequency optical fiber
LIF	Linking InterFace
MD5	Message Digest version 5
MAC	Media Access Control (Ethernet) address
Mbps	Mega bit per second
MPLS	Multi-Protocol Label Switching (a layer 2 and 3 switching network protocol)
MTU	Maximum Transmission Unit (RFC 1191) usually 1500Bytes for Ethernet
NIDS	Network Intrusion Detection System
OS	Operating System
OSI	Open Systems Interconnection (ISO standard)
PIX	Cisco appliance firewall
POP	Point Of Presence
PMU	Phase Measurement Unit
PPP	Point-to-Point Protocol (multilink-ppp uses more than one physical channel to connect the two end-points; Link-Interleaving allows to multiplex packets on the same multilink-ppp connection so that small packets can pass ahead of big ones)
PVC	Permanent Virtual Circuit
RAM	Random Access Memory
RPC	Remote Procedure Call
RT	Real Time
SHA1	Secure Hash Algorithm version 1
SDH	Synchronous Digital Hierarchy (ETSI standard for transmission on optical fibers)
SNMP	Simple Network Management Protocol
SPLIF	Service Providing LIF
SRLIF	Service Requesting LIF
SSH	Secure Shell (secure replacement for Telnet)
SONET	Synchronous Optical NETwork (ANSI standard for transmission on optical fibers)
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VC	Virtual Circuit
VPN	Virtual Private Network
WAN	Wide Area Network
WCET	Worst Case Execution Time
WLAN	Wireless Local Area Network