

Significant Information Security / Vulnerability in Substations

RAVI SANKAR,KOMMU

Ravisankar_kommu@maytasinfra.com

Power Sector Maytas Infra Ltd., Hyd, 23rd Sept 2008

MAYTAS INFRA



Need For Info Security

- **Critical Infrastructure whose incapacity or destruction would have a debilitating impact on the defence or economic security of a nation, include :**
 - **Telecommunications,**
 - **Electrical power systems,**
 - **Gas and Oil,**
 - **Banking and Finance,**
 - **Transportation,**
 - **Water Supply Systems,**
 - **Government Services &**
 - **Emergency Services**
- **Over years EPS is considered as Brain for Human Body since the Universe is living on the same need**

EPS STRUCTURE / SECURITY

- **Structure of Electric Power Systems**
- EPS is described using the word “security”. The ability of the bulk power electric system to withstand sudden disturbances such as electric short circuits or unanticipated loss of system components.
- Also EPS is highly technologically advanced systems consists of many different companies involved : electric power generation, bulk transmission of electricity from power stations to load centres and its distribution to customers
- EPS is implemented through high technology systems and assets, such as telecommunications, computers/software, the Internet, satellites, fibre optics, using TCP/IP protocols, MODBUS communications etc. and on interconnected computers and networks and the services through Powerful Data Highway

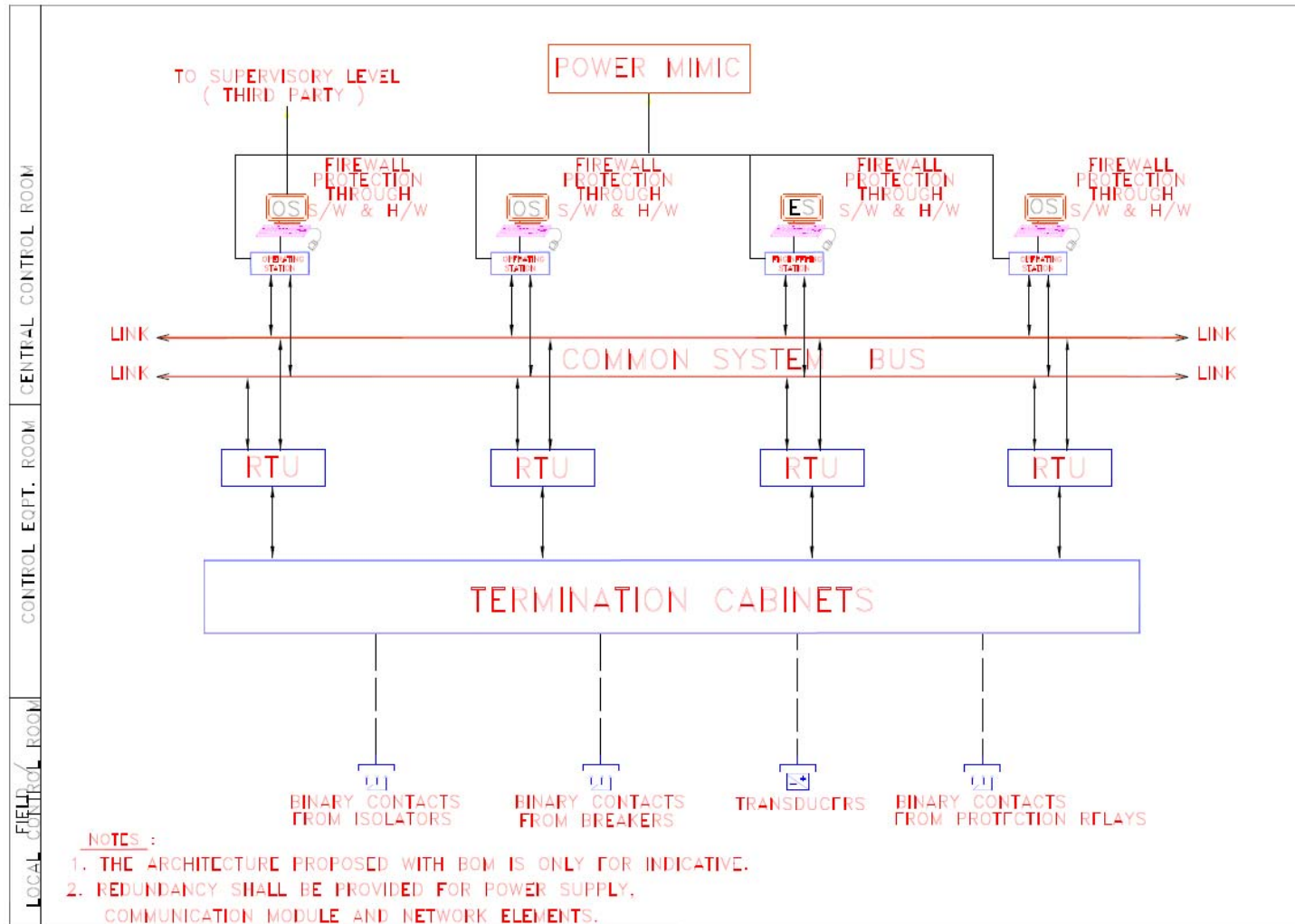
POSSIBLE CONSEQUENCES FOR SAFETY / THREAT

- **Most potential threats in EPS are similar to those in other infrastructures, like:**
- Accidental physical damage;
- Terrorism and sabotage;
- Vandalism;
- Disgruntled employees and ex-employees;
- Malicious code and viruses;
- Insiders and associates;
- Labour conflicts;
- Economic conditions;
- Curiosity and ignorance, fraud and theft.
- An example of safety-related function in thermal power stations can be starting the oil burners upon disappearing of flame in the boiler combustion chamber in order to prevent the damping of flame because a very dangerous explosion could take place in case of a repeated ignition of coal dust burned under the boiler to produce vapour

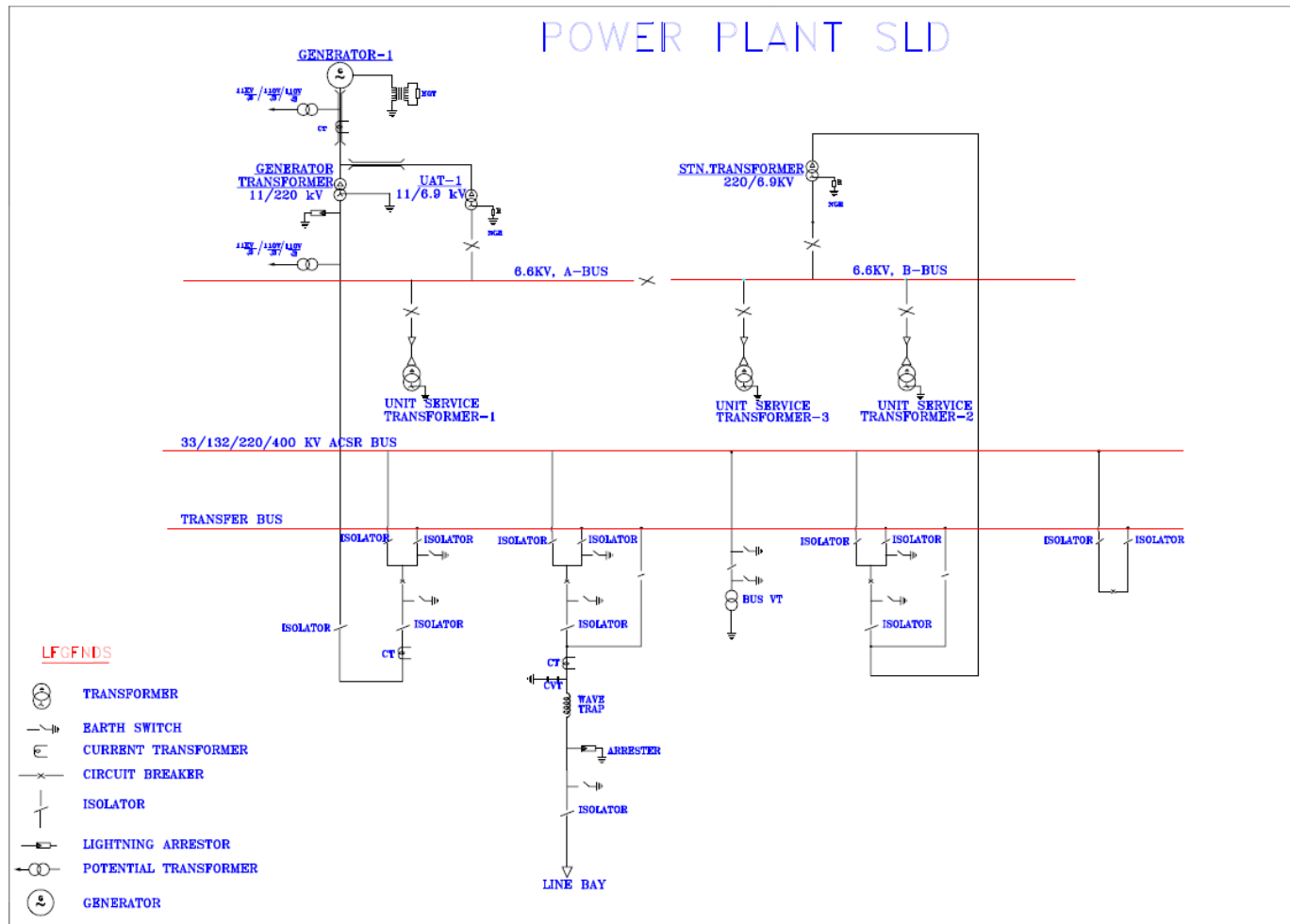
IMPLEMENTATION OF SECURITY THRU AUTOMATION

- Recently all, EPS telecontrol systems used for communication and transmission of data between power generating stations, substations and control centres for remote operation and remote real-time signaling, metering, control and fault protection on real-time State of Art of **SCADA Systems**
- A remote terminal unit (**RTU**) transmits needed information from each substation to the area control centre. This information is used to draw a complete picture of the supervised network. In the reverse direction RTU transmits commands from the area control centre to the substations
- In a large network, with several area control centres, a load dispatching centre manages and monitors the procurement of energy and the optimal arrangement of the power transmission network. A load dispatching center in turn gets the information from power plants, area control centres, etc.

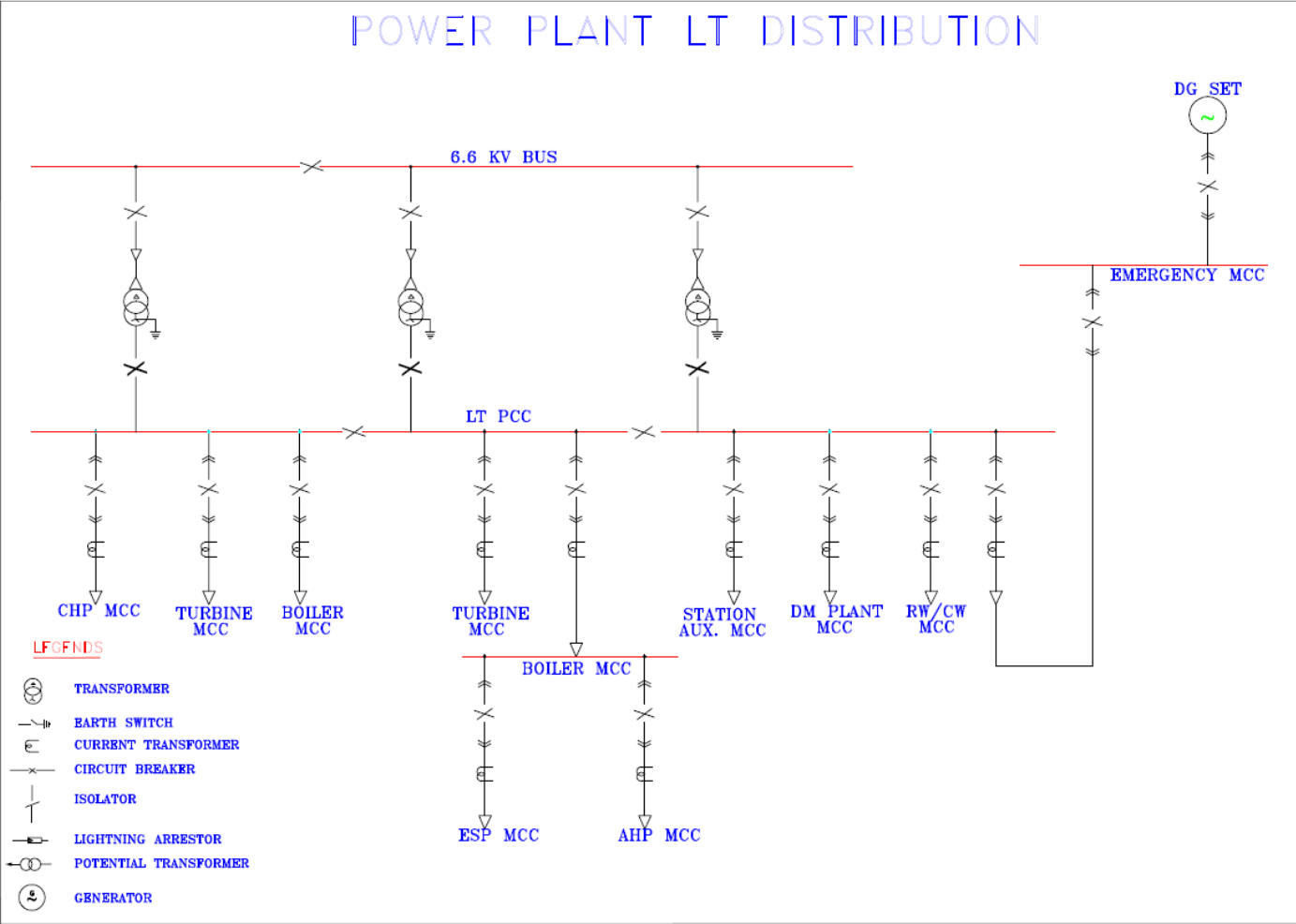
TYPICAL SCADA CONFIG IN EPS



TYPICAL POWER PLANT SLD



TYPICAL POWER PLANT LT DISTRIBUTION



GENERAL PRINCIPLES OF EQUIPMENT DESIGN

- The design of the new electrical facilities and systems will be based on the **following aspects**:
- **it is practically impossible to plan the way of electricity flow in power grid with the aim, for example, to maintain continuity of electricity supply. Electricity flows according to the physical laws not according to contracts.**
 - Safety to personnel during operation and maintenance of equipment
 - Reliability and continuity of service under all working conditions at site
 - Ease of inspection, maintenance and repairs
 - Full interchangeability of corresponding parts of similar equipment
 - Convenience of operation
 - Ease of future addition of loads / facilities
 - Compatibility of all power supply extensions to the existing systems

RISK ASSESSMENT

- According to the assessment of risks in some functions, performed by computer-based systems in **Extra High Voltage** substations, which vulnerabilities can produce a risk include but are not limited to the following functions:
- **Protection** (for the detection and the elimination of faults or of abnormal conditions on power systems and for the restoration of service)
- Control of **switching operations** which include:
 - **Programmable interlocking;**
 - **Synchronization;**
 - **Checking a continuity of control circuits of circuit breakers and disconnections**
 - **Measurement of analog quantities in an EPS**
 - **Voltage regulation (by changing a position of transformer tap-changer)**
 - **Warning signalling (e.g., reduced pressure in switchgear.)**

SOME OF PROTECTIONS USED IN EPS

Overhead Line Protection

- a. Distance protection
- b. Directional over current protection- 67
- c. Directional earth fault protection-67N
- d. Over voltage protection-59
- e. V.T. fuse failure protection-97
- f. over current protection-(50/51/50N/51N).
- g. Under voltage protection-27
- h. Local breaker back-up-50Z
- i. Forward & reverse power protection -32
- j. Phase balance protection- 46
- k. Over / under Frequency protection -81
- l. Phase sequence protection-47
- m. Low forward power protection- 37
- n. Auto reclose protection - 79

Generator Protection (One Settable Relay)

- a. Generator Differential protection
- b. Over voltage protection
- c. Stator earth fault protection
- d. Low forward power protection
- e. Reverse power protection
- f. Negative phase sequence protection
- g. Field failure protection
- h. Rotor earth fault protection
- i. Generator overload protection
- j. Generator under frequency protection (with df/dt stages)
- k. V.T. fuse failure protection
- l. Generator over current protection
- m. Under voltage protection
- n. Local breaker back-up
- o. Machine dead protection
- p. Pole slipping protection

Generator Transformer:

- a. Transformer Differential Protection
- b. Overfluxing Protection
- c. HV restricted earth fault protection
- d. HV backup overcurrent protection
- e. HV backup earth fault protection
- f. Buchholz protection
- g. Oil/winding temperature alarm/trip protection.
- h. Overall generator transformer differential protection

220 KV Switchyard

- a. Bus bar Differential Protection
- b. Local Breaker Backup protection

Station / Unit Auxiliary Transformer

- a. Transformer diff. protection
- b. HV high set instantaneous over current protection
- c. HV backup overcurrent protection
- d. HV instantaneous earth fault protection
- e. HV back up earth fault protection
- f. Buchholz, Winding & Oil Temperature alarm and trip protection
- g. LV restricted earth fault protection
- h. LV transformer neutral connected back up earth fault protection
- i. LV back up overcurrent protection
- j. LV backup earth fault protection

Motor Protection(ABOVE 90 KW)

- **Phase fault protection**
- **Instantaneous Earth Fault Protection**
- **Thermal Overload Protection by Thermal Replica protection trip and pre-trip alarm**
- **Negative sequence or current unbalance protection**
- **Long Starting time protection**
- **Stalled rotor protection during Starting and on-load**
- **Repeated-start protection**
- **Over voltage & under voltage protection**

For Small Motors (Below 90 KW)

- **Current limiting HRC fuses or current limiting MCCB offering type-2 Coordination**
- **Direct or CT operated bimetallic thermal overload relay with single phase operation features.**

SOME CRITICAL OBSERVATIONS / UNIQUE FEATURES OF EPS

- **Differently than any other infrastructure**, for example like telecommunication infrastructure, it is practically impossible to plan the way of electricity flow in power grid with the aim, for example, to maintain continuity of electricity supply. Electricity flows according to the physical laws not according to contracts.
- **If EPS is not carefully planned and operated**, it is very easy to trigger a cascading effect that leads to a great power system failure. For example tripping a line by protection devices can cause overload remaining line/lines in the grid, because of changing the way the electricity flows, and consequently tripping the overloaded line/lines by protection relays. This causes further change of the way the electricity flows with possible further tripping of an overloaded line/lines and cascading development big EPS failure or even totally collapse of the EPS
- In EPSs all lines, transformers, generators, etc. are protected by protection devices that operate within fraction of a second or - very rarely - a few seconds at the most. Therefore a very simple event that causes tripping an EPS element by protection devices can initiate very serious power system failure

PRECAUTIONS IMPLEMENTATION OF AUTOMATION

- The interlocking system must open disconnector when circuit breaker interlocked with the disconnector is closed, or closing an earthing switch
- When the circuit breaker interlocked with the earthing switch is closed, etc. All these requirements are described by the following basic safety-oriented interlocking rules:
- Load flows must not be switched on or off by disconnectors;
- Live nodes must not be grounded;
- When connecting live nodes the synchronisation conditions must be fulfilled

Normally such a software interlocking system consists of:

- Auxiliary contacts of disconnectors, circuit-breakers and earthing switches which transmit information about the status of main contacts to the computer system (closed or open);
- Auxiliary relays, used for the control of switch drives (coils of these relays are connected to the outputs of the computer system, whereas contacts are connected to control circuits of the switch drives);
- Wiring system,
- Intelligence of the software interlocking system implemented into the target system software

CONCLUSIONS

- Familiarity with electronic intrusion techniques and counter measures to be followed in , power generation and T&D utilities, can assess their vulnerabilities and take steps to mitigate their risks
- Isolate critical control systems from insecure networks by disconnection or adequate firewalls thru S/W and H/W
- Adopt best practices for password control and protection, or install modern authentication mechanisms
- Provide for individual accountability through protected action logs or the equivalent
- Controllers, and computer based SCADA and IT systems

THANK YOU