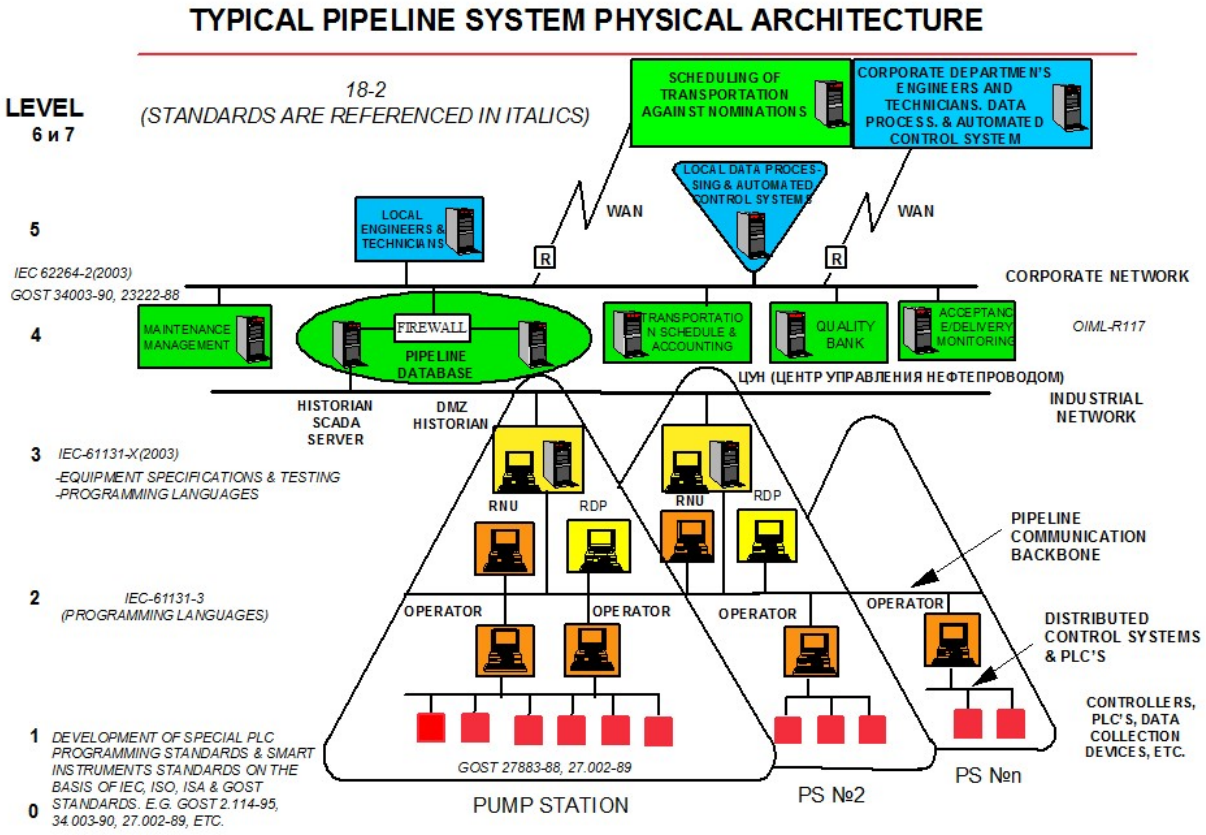
PERA Enterprise Network Design Principles

~~PERA physical architecture diagrams~~ show networks as horizontal connecting lines. Control and Information System devices are shown between and connected to these. Networks connecting these devices are shown at the same "Level" as the most demanding device that they are connected to (without an isolating router, gateway, firewall, etc.). The number of Levels shown in a given plant architecture depends on the nature of the enterprise. Typically Levels 1 to 3 are below the plant firewall (called IACS, or Industrial Automation and Control Systems). Levels 4 to 6 are IT systems in the plant and corporate business areas.

The following is a Physical Architecture Diagram for an Oil & Gas Industry Pipeline that demonstrates Use of PERA Levels.



In this example, IACS systems at Levels 0, 1, 2, and 3 are the responsibility of Control Engineers and Industrial Network designers. Level 4 is designed by IT and Industrial Network Designers, and Levels 5 and above are the responsibility of IT specialists and Commercial Network designers,

Physical Network Diagrams are designed progressively beginning with simple block diagrams during Conceptual Engineering Phase, and are developed and updated through to Construction Phase.

Conceptual Engineering Phase

The approximate bandwidth (Mbps) of each network link is indicated at the Conceptual Engineering stage. These systems and networks may be represented in a simple block diagram, or a more graphic "Control and Information Network Diagram" or CIND.

In order to represent the resilience to cyber attack, ISA 62443 has introduced the concepts of "Zones and Conduits". These are also defined at Conceptual Engineering Phase. A distinction is made by ISA 62443 between the simple probability of failure (MTBF) of software or hardware, and the probability of a cyber attack, multiplied by the likelihood of successful penetration. In both cases, the annual cost of a probable failure is multiplied by the MTBF/year

Considerable effort is required by ISA 62443 to quantify the risk resulting from cybersecurity incidents. However, the suggested calculations vary widely, and may prove unreliable. Ultimately, the probability of a cyber incident times the magnitude of expected loss must be compared to other risks according to the accepted risk calculations and risk tolerance of the corporation.

It is not clear that the extra cost and complexity of proposed risk determination is justified (compared to a simple "estimated reliability".

Preliminary Engineering Phase

At this design phase, the physical network architecture is shown as a schematic diagram with Control and Information System devices, gateways and routers, HMIs and system software.

"PERA 4Rs" (Response, Resolution, Reliability, and Repairability) are considered in the design of the physical architecture. These 4Rs are all time-based parameters used to determine the requirements of devices and networks at a each "PERA Level."

- **Reliability** is the classical MTBF (Mean Time Between Failure often in months or years). Hal was suggesting that we might "fake" a cybersecurity "Resilience" by changing this to include the combined MTBF for device failure (e.g. for an SIS/SIL safety system) and cyber penetration. This won't work because the likelihood of cyber penetration is the statistical sum of the likelihood of attack and the likelihood of successful penetration.
- **Repairability** is the time to repair a failed device or to swing over to a backup unit or redundant subsystem (which could be days to repair or milliseconds to switch over). This can be as simple as an installed spare that the operator "swings over", or a triply-redundant Triconix system with multiple processors on multiple busses reading replicated sensors and applying 2-of-3 or 3-of-3 logic.
- **Response** is the time it takes to get the answer (e.g. seconds for an update from a field device). In a process plant, this would be the update rate on the DCS screen and might be a few times per second, but on a pipeline SCADA system could be many seconds or even minutes.

- **Resolution** is the sample rate of the device or network (from microseconds for a high-resolution breaker log, to seconds for a temperature scanner). In the old days, analog sensors were instantaneous. In fact, the operator would "tap the gauge" to see it "wiggle" in order to be sure that it was not stuck. With modern digital transmitters, the scan rate of the A/D converter determines the "standard deviation of the noise" which can actually be remotely read for some vendors' sensors.

It is important to note that in a process industry plant, the 4Rs defined by a control engineer generally correspond to the design parameters used by a network engineer in the same industry.

Control Engineer	Network Engineer	Typical Value
Reliability	MTBF (Mean time between failure)	Months to years
Repairability	MTTR (Mean time to repair)	Seconds to hours
Response	Latency	Milliseconds to seconds
Resolution	Scan rate	Milliseconds to seconds

These parameters are generally consistent for each PERA architectural level for a certain process industry.

PERA Levels (with their corresponding parameters) are used during the Preliminary Engineering Phase to design the industrial automation networks and during the Procurement Phase to specify devices.

These sets of parameters are traditionally specified by the control systems and IT designers (above and below the plant firewall). Any of these 4 Rs may be the most critical parameter for a given device, network, or system.

These parameters also tend to be consistent across a given industry. For example, the Response and Resolution for control systems in process Industries tend to be of the order of fractions of a second to a few seconds. By comparison, however, in aerospace industries, Reliability, Response, Resolution, and Repairability may be hundreds of times more demanding.

Detailed Engineering, Procurement and Construction Phase

During this phase, the 3D layout of cableways, rack rooms, fencing, and other physical designs are completed, and devices and network components are specified. This typically takes the form of "bid specifications" that are responded to by vendors. Vendors clarify exceptions and options and Purchasing or Contracts group return "purchase specifications" to the vendors.

These Functional specifications and "specification sheets" should be modified to add cybersecurity requirements.