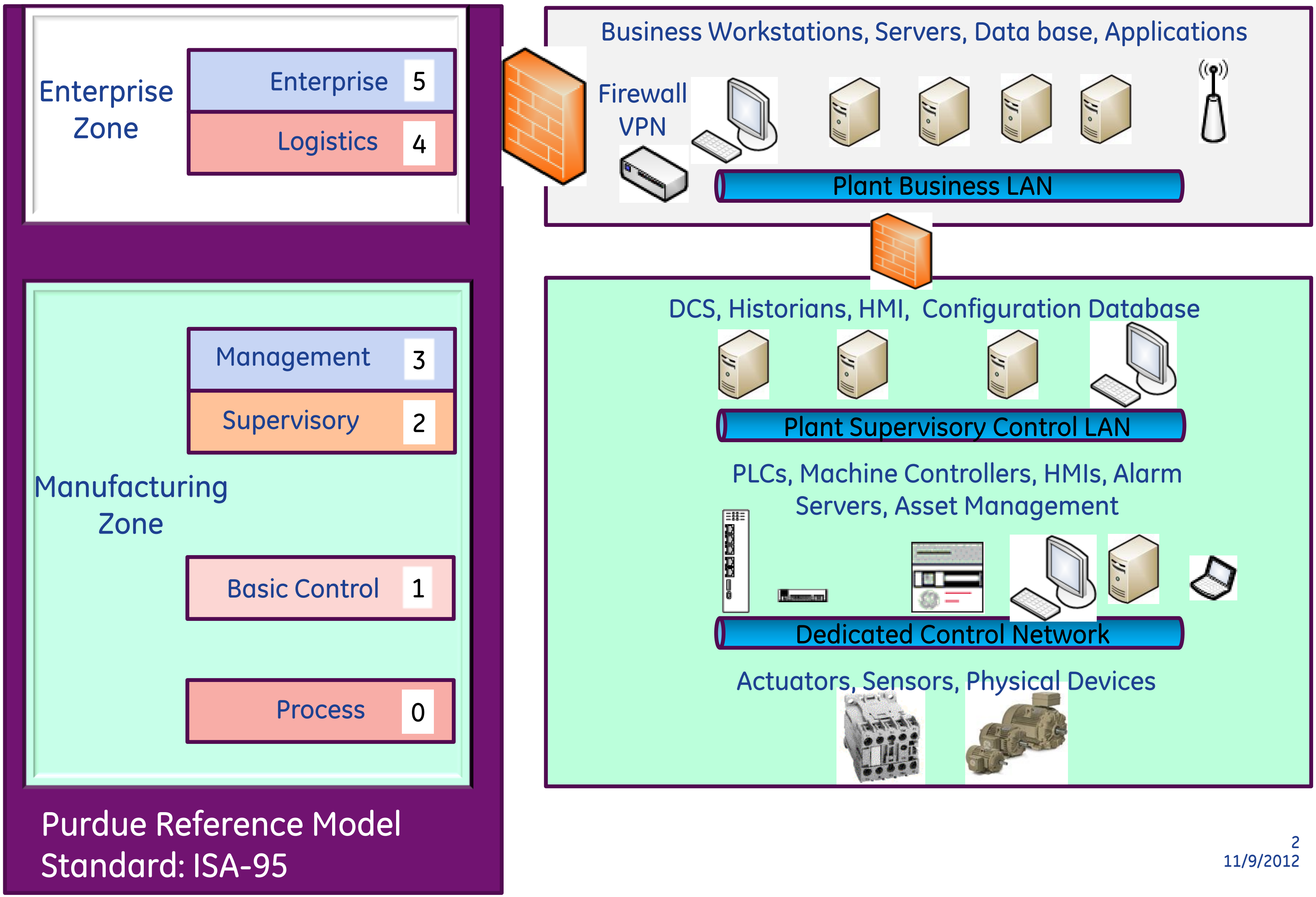
Ethernet for Converged Applications

Daniel Sexton
GE Global Research
Niskayuna, NY
sextonda@ge.com

imagination at work

Typical Plant Control Model



Why Converge the Networks?

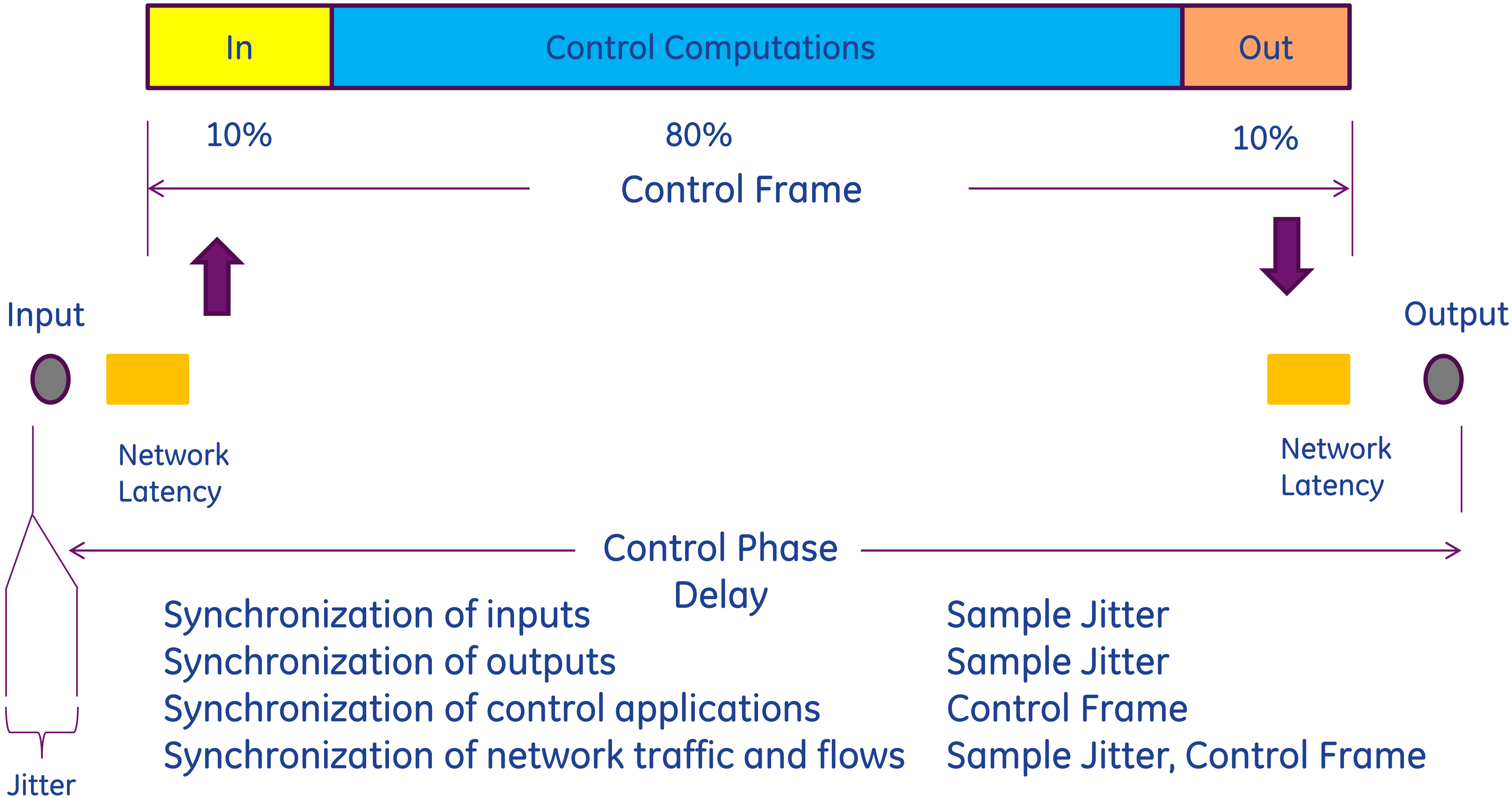
- Security concerns – we can no longer rely on the perimeter for security.
- Simplicity - Maintenance and management.
- Connectivity
- Personnel
- Flexibility
- Future proofing (faster upgrades and retrofits)
- Standards convergence, Open Systems

Traffic types in converged networks

- Business transactions/Internet Access
- Physical Security, Plant Maintenance
  - Video, Voice
- Business Communications
  - VOIP
- Asset management/Inventory tracking
  - Blob transfers, database access
- Control
  - Supervisory, Discrete, Process, Coordinated, Safety Critical
  - High speed, periodic & aperiodic, alarms and alerts
  - High reliability, availability

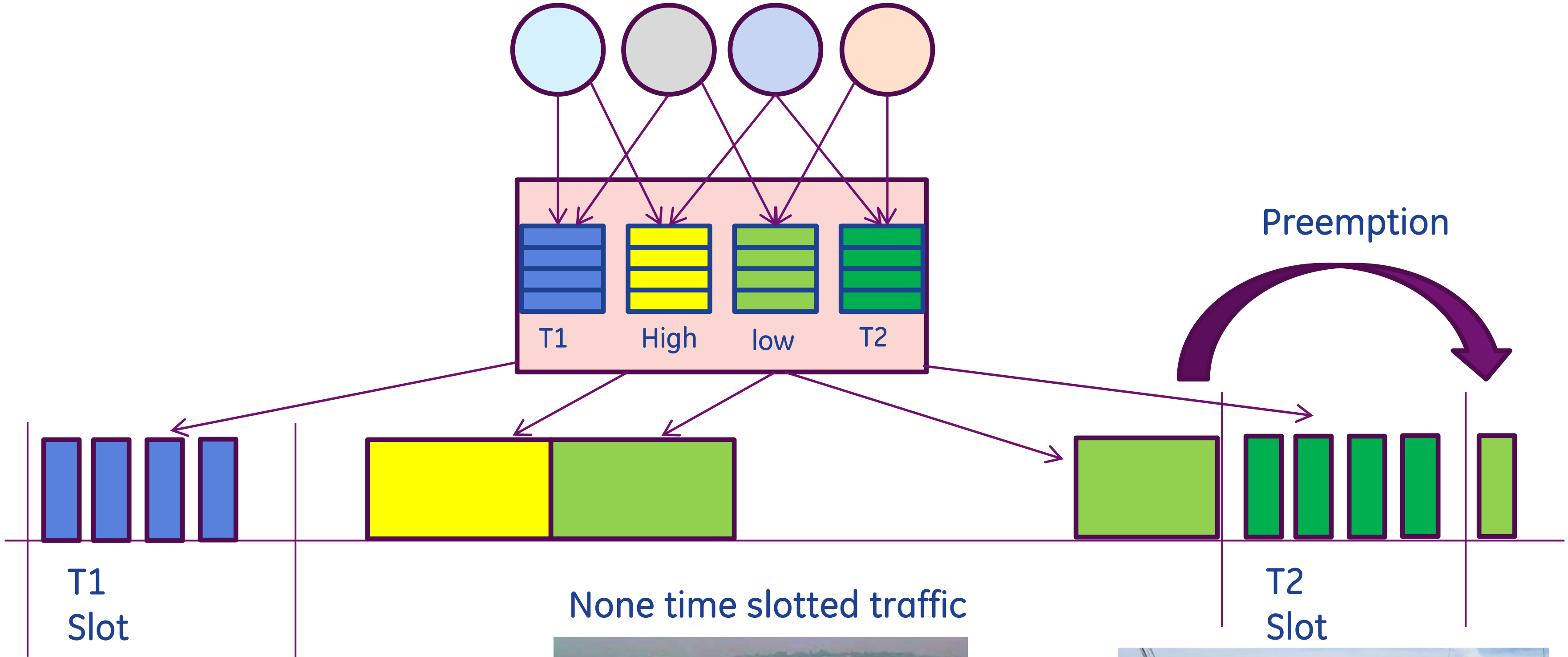
Controls – a diverse set of markets

The Basic Control Cycle



Overall Phase Delay Drives System Controllability/Stability

Traffic Controlled Networks



Time Cyclic
Control Traffic

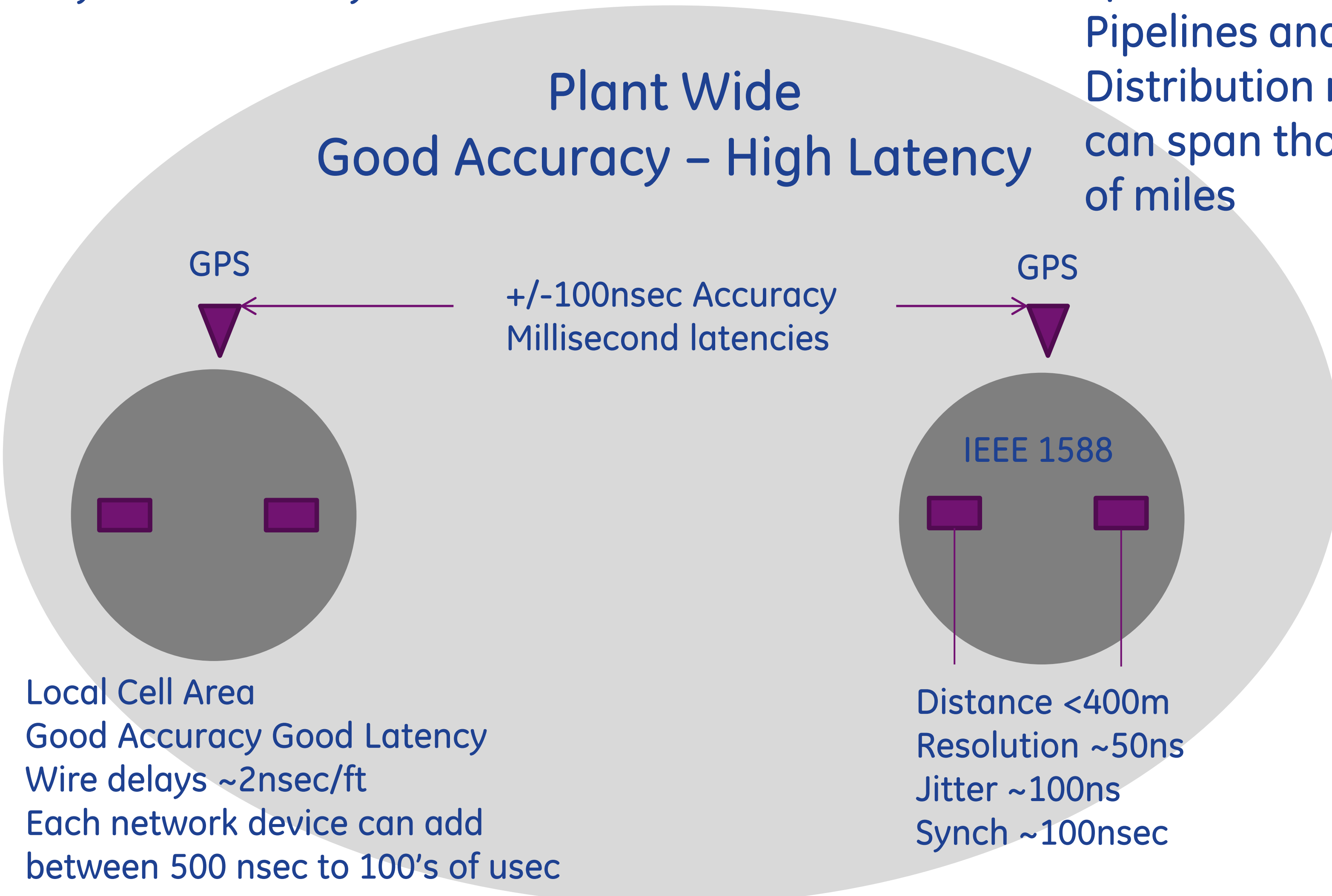
None Real time Traffic
- Logging
- Alerting

Real time – non cyclic Traffic
- Critical Alarms
- Discrete/event control

Time Synchronization

Accuracy versus Latency/Plant versus Cell

Physical plant can span miles
Pipelines and Distribution networks can span thousands of miles



imagination at work

Let Physics Dictate Latency

Requirements – End User Perspective

Provide access to the data sources within the underlying control systems to allow asset management and perform system wide optimizations that and maximize customer value.

Accommodate a wide array of vendor products that would participate in plant equipment control where access from higher layers within the plant hierarchy will be required.

- Minimize the customer impact and effort when applying products from various application segments; improve the interoperability and integration.
- Provide a more homogeneous experience for the customer.

Accommodate the addition and integration of multi-vendor products based on industry accepted standards.

Provide network security.

- Device authentication
- Network availability
- Access Control
- Confidentiality
- Integrity, traceability

imagination at work

Requirements

Scalable from small systems to large systems.

Flexible – Once installed, can grow as the needs of the system grow.

Easy to implement – does not require a great deal of user configuration or intervention. Customers who are not network traffic engineers can use it.

A single device can have various applications, applications within a device have different QOS needs but may share the same protocol.

Redundancy must be scalable at the network level as well as the application level. Future high reliability systems will contain both wired and wireless to prevent common mode failures. Best effort traffic can be sacrificed when failures occur. Failure detection/reporting is as important as failover protection.

Physical clock level point to point synchronization (Use 1588 for time/phase lock and use physical clock for frequency lock of local clocks: ITU-T G.8261, ITU-T G.8262 ITU-T G.8264)

Able to integrate legacy equipment (NICs, bridges and switches) without sacrificing AVBG2 features.

Allow traffic convergence with a wide variety of application protocols including proprietary protocols.

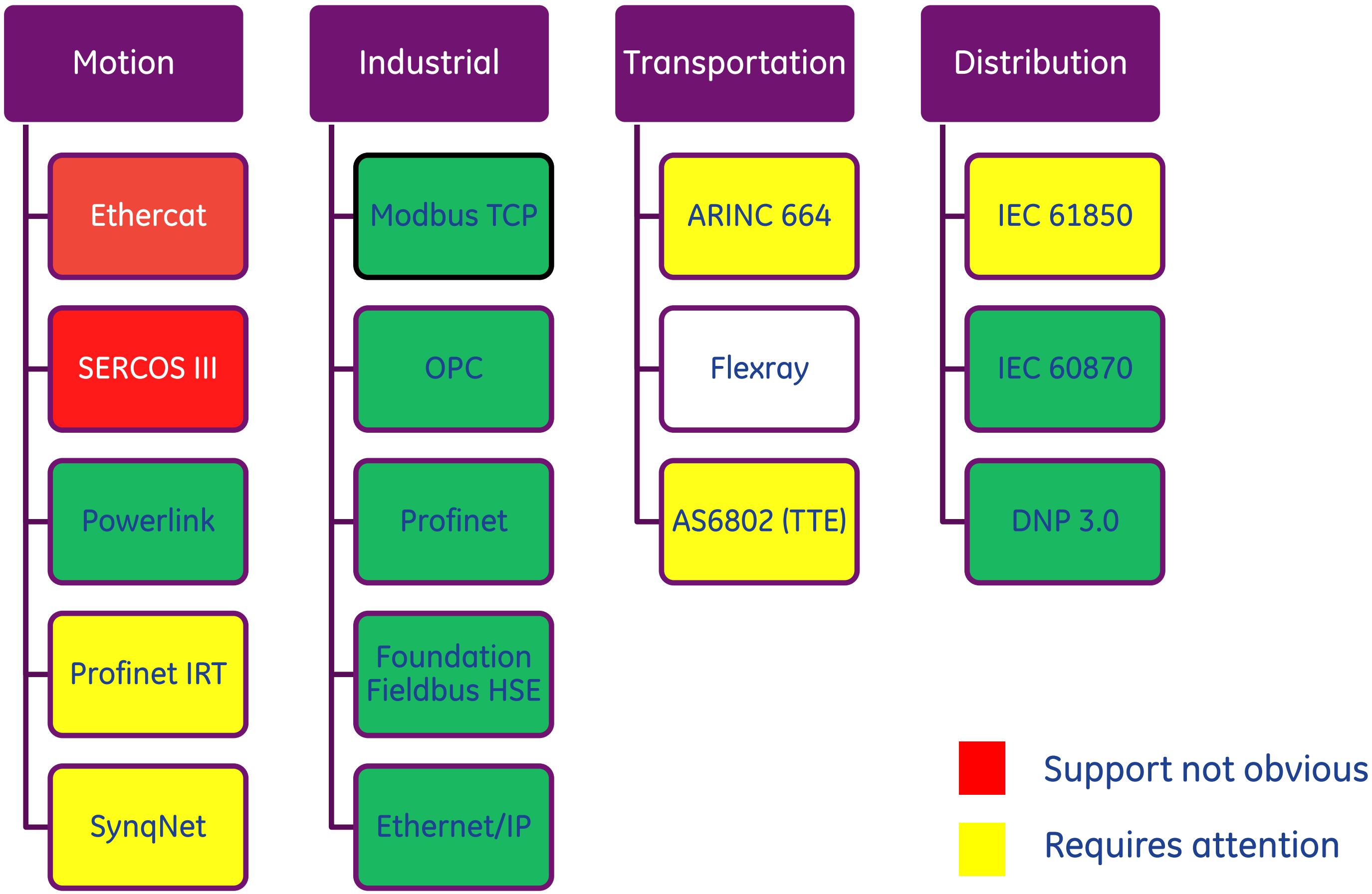
Security

- Relying on physical security (within the fence) is no longer enough. Devices are mobile, wireless or wired.
- Converged networks with mixed traffic increase the threats from multiple users both malicious as well as accidental.
- Denial of service, flooding, babbling devices, viruses, snooping, cloning, etc. all become issues.
- The control mission cannot be compromised.
- Authentication for devices as well as users. Access control & authentication for resource allocations.
- The bridge is the first line of defense for attacks.
- Security attacks and threats must be logged and reported.
- Trust must be established between all devices.

Configuration – Use cases

1. Fixed Systems (autos, aviation), rarely change, fixed capacity. Configured once at point of manufacture. System manager not a requirement.
2. Large Flexible Systems (Manufacturing plant), change occurs slowly. Various subsystems and applications can be added. System can be reconfigured or re-engineered, upgraded overtime. System management required, resource planning tools may be needed.
3. Small Systems (Small custom machines), cost and complexity really matters. User must perceive no additional effort or cost.

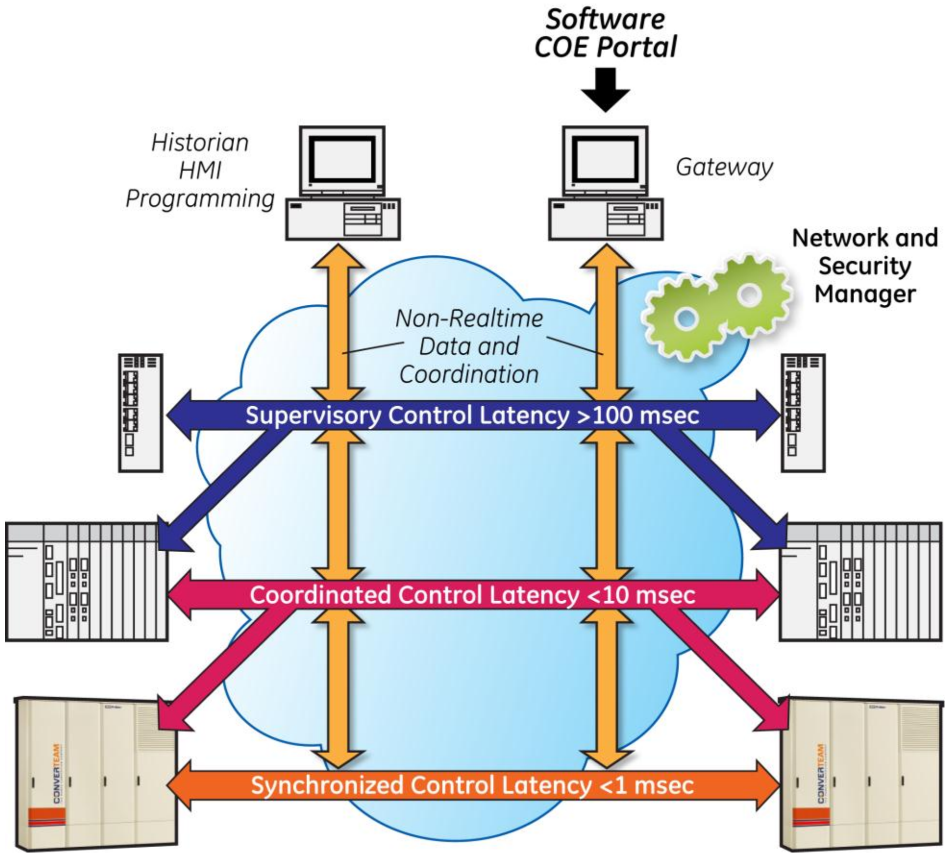
Application Protocols for Control



Not a complete List

Note: There are many proprietary protocols not on this list

Vision: Converged Networks on the plant floor



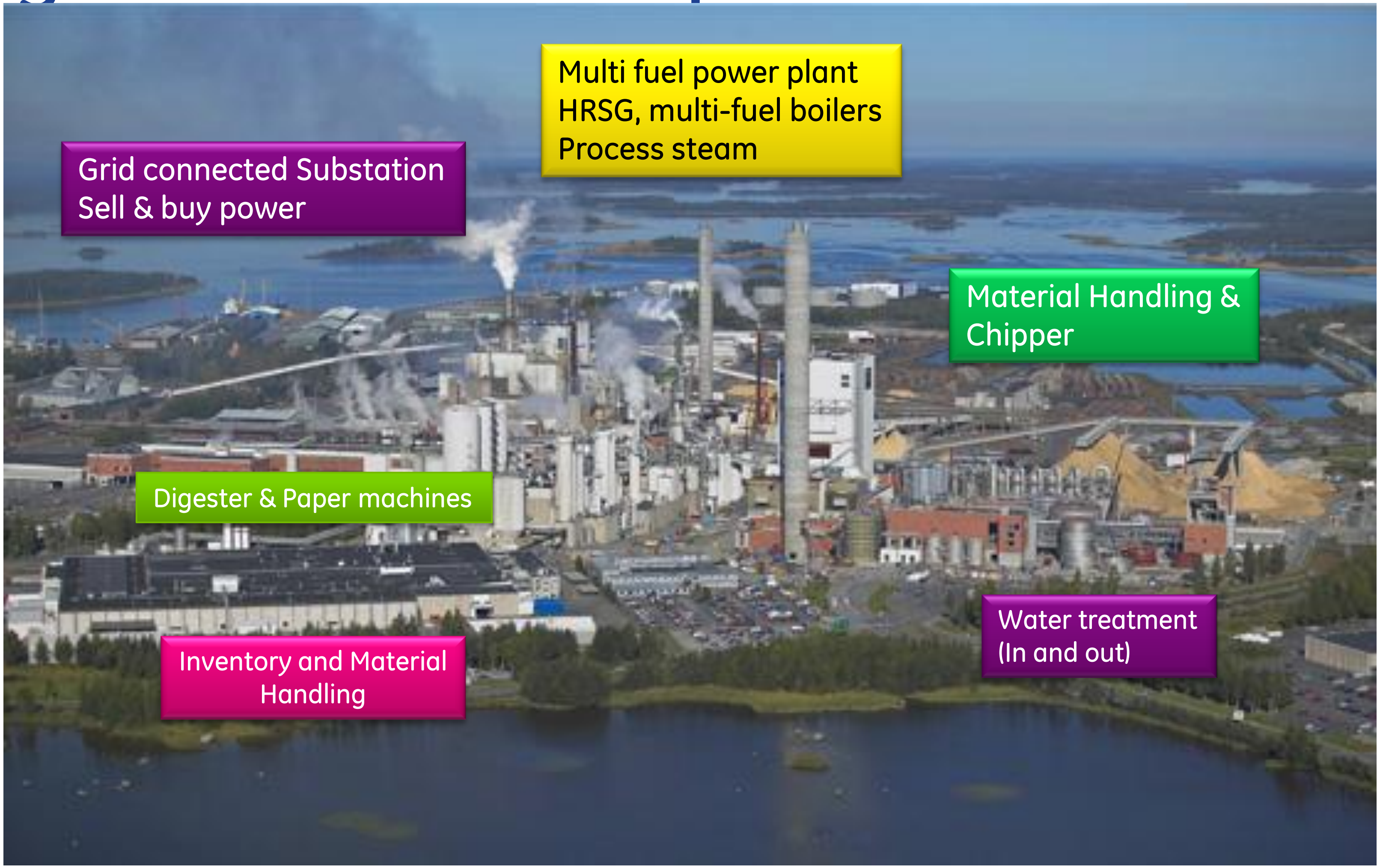
Control Fabric:

- 802.3 physical connection
- 802.3 MAC protocol
- Ethernet protocol suite
- Managed QOS – various levels
- Redundancy
- Security
- Market specific application protocols
- Third party device support
- Single network
- Scalable from very small to very large systems
- Built on standards based switch technology
- Optional network manager eliminates manual configuration
- Optional security manager controls access

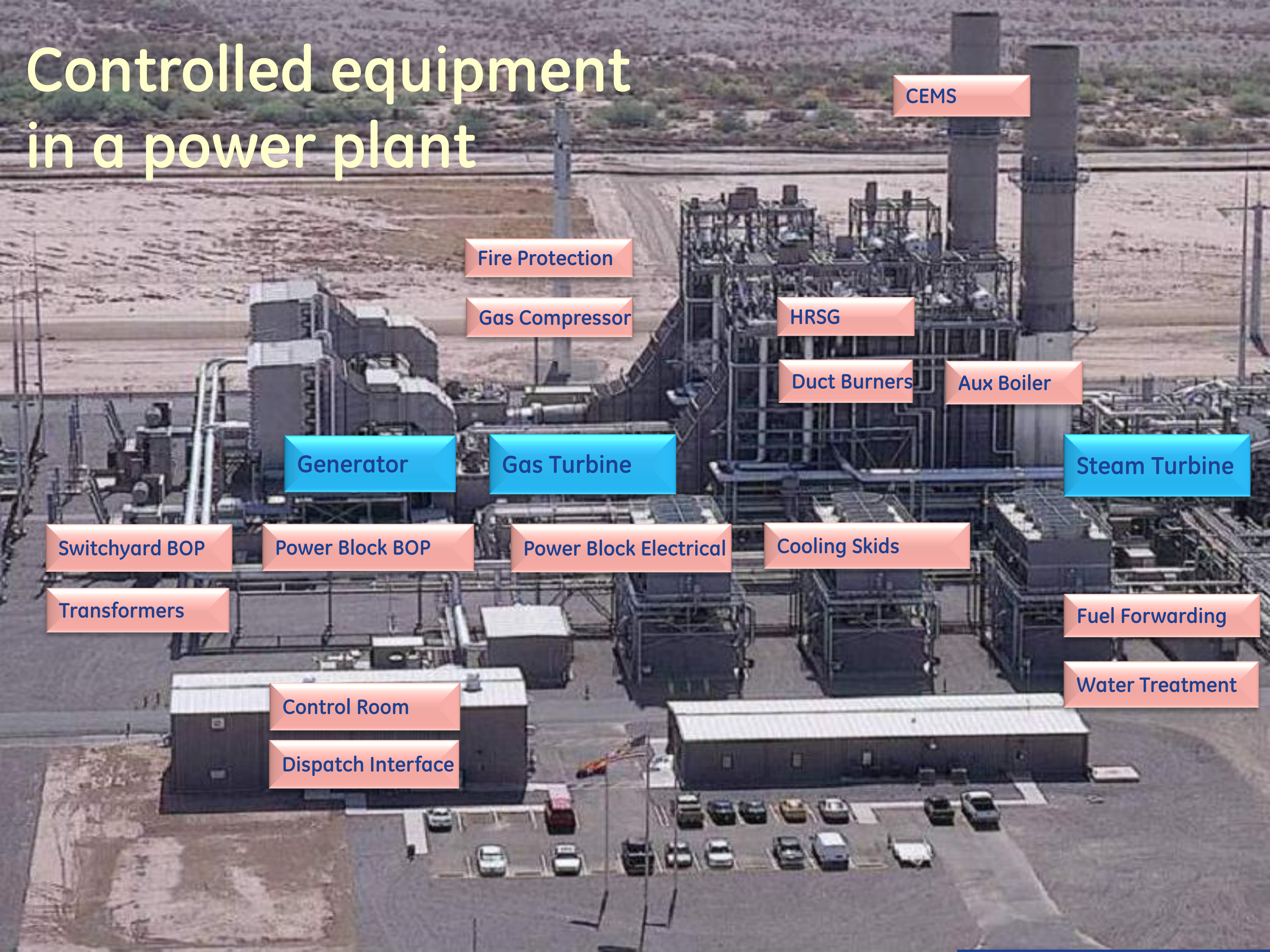
Bonus Material

Level	Name	Description
Enterprise Zone		
Level 5	Enterprise	Corporate level applications (for example, ERP, CRM, document management) and services (Internet access, VPN entry point) exist in this level.
Level 4	Site business (planning and Logistics)	Manufacturing facility IT services exist in this level and may include scheduling systems, material flow applications, manufacturing execution systems (MES), and local IT services (phone, E-mail, printing, security/monitoring).
DMZ		Provides a buffer zone where services and data can be shared between the Manufacturing and Enterprise zones. In addition, the DMZ allows for easy segmentation of organizational control.
Manufacturing Zone		
Level 3	Site manufacturing operations and control	Includes the functions involved in managing the work flows to produce the desired end products. Examples include detailed production scheduling, reliability assurance, site-wide control optimization, security management, network management, and potentially other required IT services such as DHCP, LDAP, DNS, and file servers.
Cell/Local Area Zone		
Level 2	**Area supervisory control**	**Control room, controller status, control network/application administration, and other control-related applications (supervisory control, historian)**
Level 1	**Basic Control**	**Multidiscipline controllers, dedicated HMIs, and other applications may talk to each other to run a part or whole control system.**
Level 0	Process	Where devices (sensors, actuators) and machines (drives, motors, robots) communicate with the controller or multiple controllers.
Safety Zone		
	Safety Critical Functions	Devices, sensors, and other equipment used to manage the safety functions

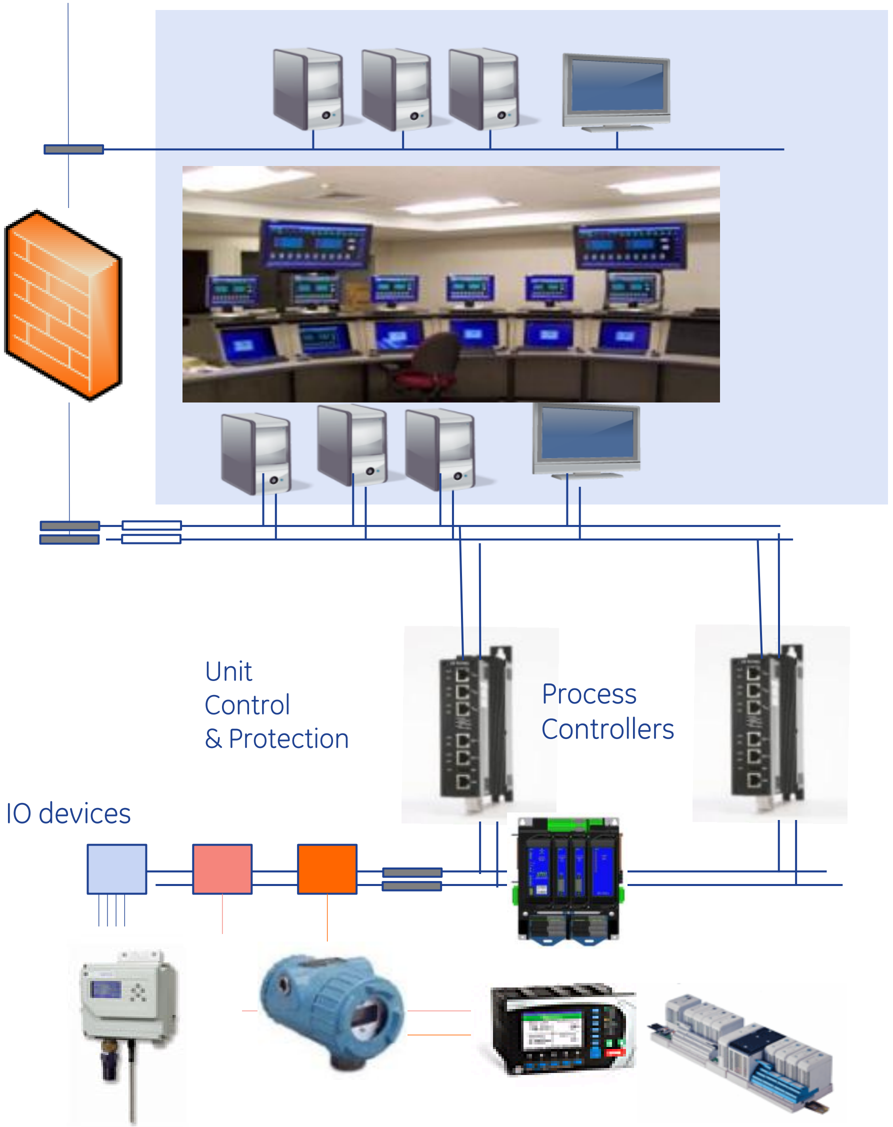
System Complexity – Industrial Plant Cogeneration Example



Controlled equipment in a power plant



Power Plant Network

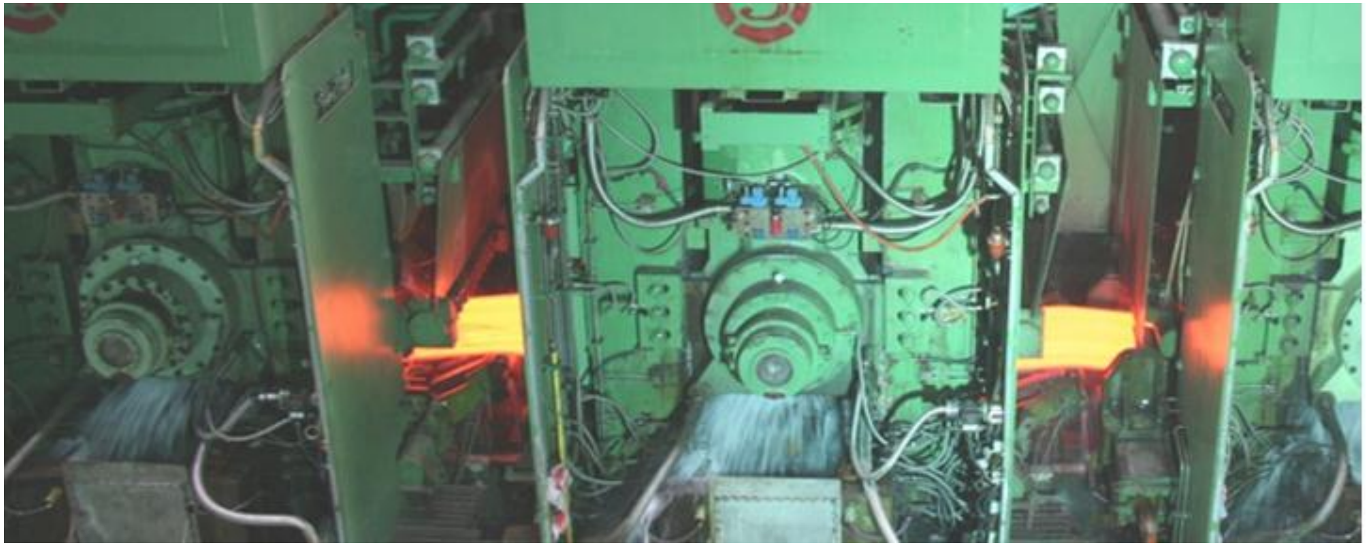


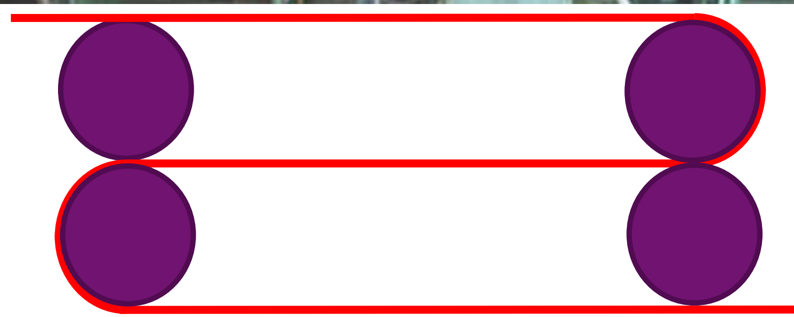
- Historians
- Asset Monitoring
- Cyber Security
- Plant Level Analytics
  - Plant Performance
  - Asset Management
  - Visualization

- Real time machine controllers
- Real time equipment protection
- Process Controllers

- Smart Field Device (Process, Electrical)
- Multi vendor general purpose IO
- Condition Monitoring Systems
- Integrated Safety Systems
- Various Field busses (Profinet Foundation Fieldbus)
- Power Distribution Networks - IEC 61850

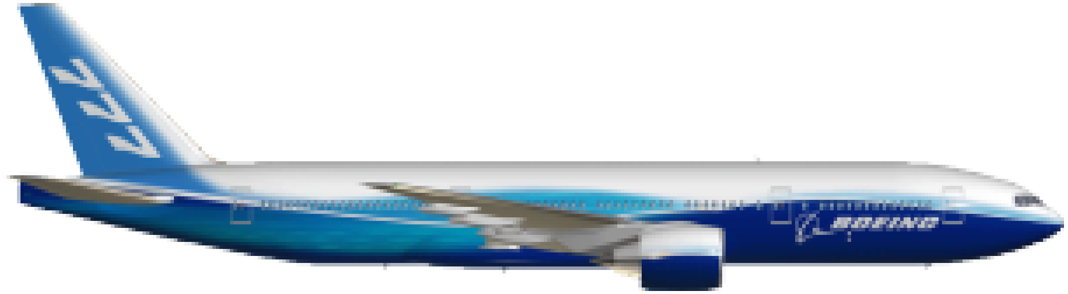
Coordinated Drives - Metals





- Each drum is driven by a separate high speed motor
- A rolling mill can have 45 synchronized motors, shaft rotation speed and position is tightly controlled.
- Material speeds can vary from 0 to 2km/min (75 mph) or more

Aviation



Low Data Rate, Interior Applications:
Sensors: Cabin Pressure -Smoke Detection -Fuel Tank/Line –ProximityTemperature -EMI Incident Detection -Structural Health Monitoring -Humidity/Corrosion Detection
Controls: Emergency Lighting -Cabin Functions

•Low Data Rate, Outside Applications:
Sensors: Ice Detection -Landing Gear Position Feedback -Brake Temperature -Tire Pressure -Wheel Speed -Steering Feedback -Flight Controls Position Feedback -Door Proximity -Engine Sensors -Cargo Compartment -Structural Sensors

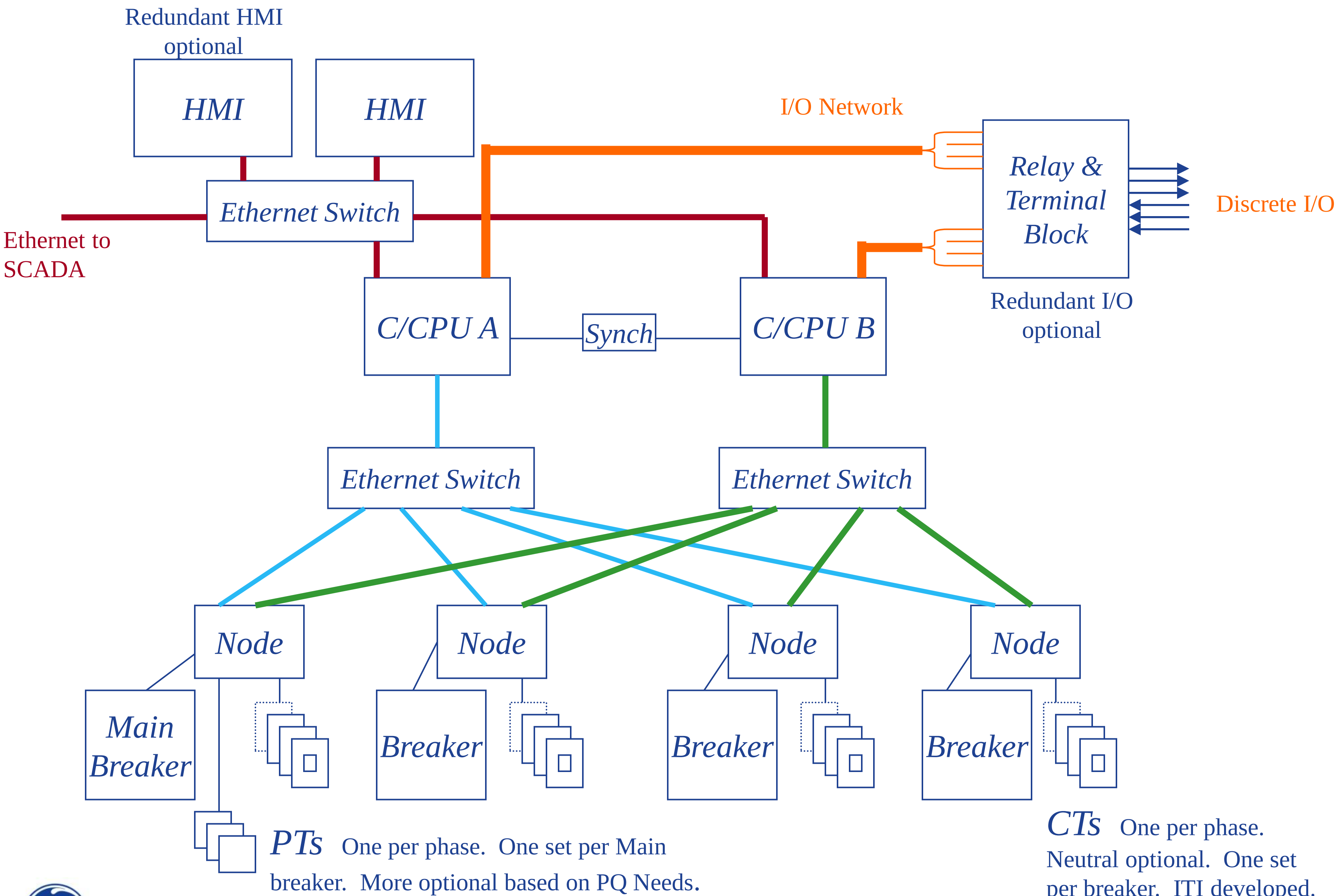
•High Data Rate, Interior Applications:
Sensors: Air Data -Engine Prognostic -Flight Deck/Cabin Crew Still Imagery / Video
Comm.: Avionics Communications Bus -FADEC Aircraft Interface -Flight Deck/Cabin Crew Audio / Video (safety-related) -Flight -Operations related Digital Data (e.g. EFOS…)
Audio / Video / Data Passenger entertainment

•High Data Rate, Outside Applications:
Sensors:Structural Health Monitoring -Imaging Sensors (Still and Video)
Controls:Active Vibration Control
Comm.:Avionics Communications Bus, Engine controls

Rail

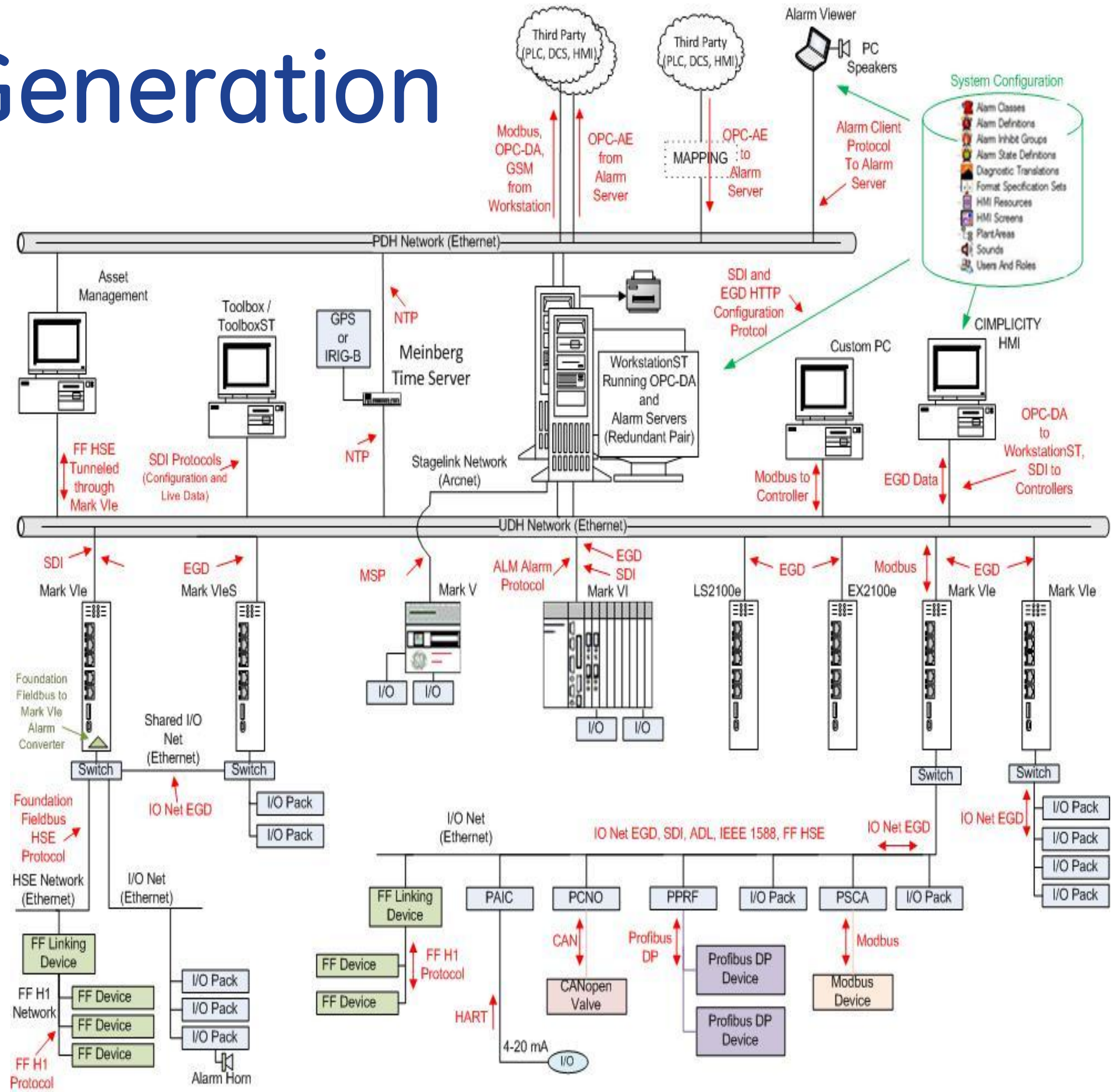
Operations
Asset
Operations Optimization
Railroads
Terminals & Ports
Shippers & 3PLs
Multiple Missions
Optimized for throughput
Command and Control
Freight Trains
Passenger Trains
Mission Execution
Safety Critical
Asset Optimization
Locomotives
Cars
Wayside & Crossing
Track
Crew
Command and Control
Available for a mission

Power Distribution -Substations & Switchgear



imagination at work

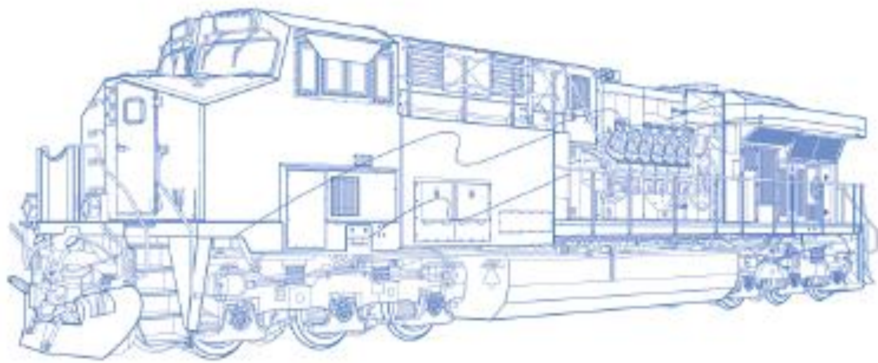
Energy Generation



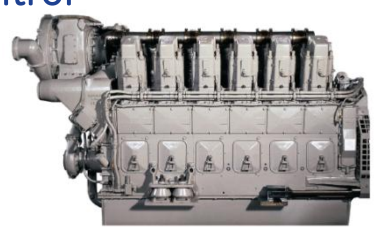
Typical Power Island 40K input 40K output points
Control Frame 5msec; Latency <1msec

imagination at work

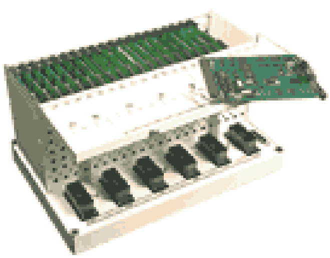
Rail



Network Traffic:
Automatic and Manual Train Control
Video
Voice
Diagnostics
Trip Recorder



Engine Controls



Traction Control

Video

Cab Control, SCADA & Comms

Braking Controls

Wayside Signaling

Voice/Radio