AVnu™ Alliance White Paper

Networking for Power Generation

Version 1.0 - 12/2014

Author

Dan Sexton, General Electric

Executive Summary

Power plants are not isolated control islands; they must exist within the broader context of the power grid. Wide area communications is essential to their operation. This drives complexity into the networks both outside the plant as well as inside the plant. Operators seek to optimize plant operations and manage multiple plants as an optimized fleet, equipment suppliers offer more cloud based services to assist their customers, this drives the market to higher levels of network complexity as well as the need for the networks to reach equipment deep within the plant as well as across plants. AVnu Alliance is pulling together the industrial ecosystem to assure that new networking technologies will provide benefits to the industrial markets. This paper explores one application which can benefit from a simplification of networking architecture with the added functionality to support the Industrial Internet.

About AVnu Alliance

The AVnu Alliance is a community creating an interoperable ecosystem of low-latency, time-synchronized, highly reliable networked devices using open standards. AVnu creates comprehensive certification programs to ensure interoperability of networked devices. The foundational technology enables deterministic synchronized networking based on IEEE Audio Video Bridging (AVB) / Time Sensitive Networking (TSN) base standards. The Alliance, in conjunction with other complimentary standards bodies and alliances, develops complete solutions in professional AV, automotive, industrial control and consumer segments.

THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, EXPRESS, IMPLIED, OR STATUTORY. AVnu Alliance MAKES NO GUARANTEES, CONDITIONS OR REPRESENTATIONS AS TO THE ACCURACY OR

CONTAINED HEREIN. AVnu Alliance disclaims all liability, including liability for infringement, of any proprietary or intellectual property rights, relating to use of information in this document. No license, express or implied, by estoppel or otherwise, to any proprietary or intellectual property rights is granted herein.

Introduction

This whitepaper outlines the need for new networking technologies to meet the needs of the ever increasing complexity of industrial applications such as power generation.

Large power plants consist of a collection of control and protection systems that must operate in harmony. This requires a complex array of isolated communications systems to achieve the types of performance and reliability guarantees required to support real time control. A large plant can have six or more network levels in the hierarchy with multiple networks at each level.

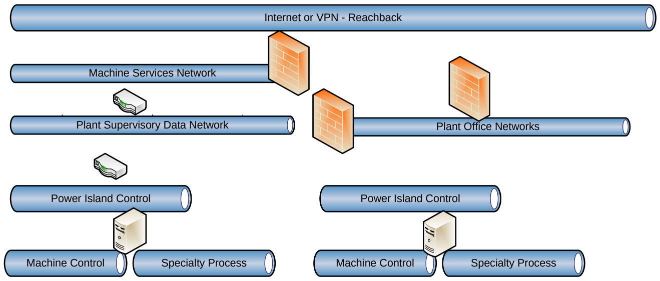

Figure 1: Industrial Applications-Complex Hierarchy

Figure 1 shows just a small portion of the networks that can be within a power generation plant. Within each power plant there is:

- Business and operations center or back office.
- Supervisory control for the plant itself.
- Power generation unit control for each power island which includes the control of each of the auxiliary systems required to operate the machine.
- High speed control for the turbines and generators.
- Specialty I/O networks that handle unique sensors and actuators.
- Electrical protection and power distribution systems that protect the equipment and integrate power delivery with the grid.
- Machine maintenance and diagnostics.
- In addition, new applications are being added to the plant infrastructure all the time.

This makes for a very complex and dynamic network infrastructure where the maintenance needs are high and reliability is critical. What is described is a simple single cycle plant but in today's world many large plants are combined cycle meaning that not only is power being generated using gas turbines, but also steam turbines are used to recover the heat from the gas turbines to further increase the thermal efficiency of the plants. The system then grows in complexity adding more and more networks and applications. Lastly, consider the case where power generation is combined with another process application such as a petrochemical refinery or desalination plant and the system grows even larger. The number of networks to manage and the various skill levels required to maintain those network becomes very large.

Today network complexity is managed through application isolation, each application is given its own private network. In the cases where control is not critical, VLAN technology can be used to reduce the number of physical networks. Network architecture loosely follows the ISA95 reference model (Figure 2) although typically we see more layers.

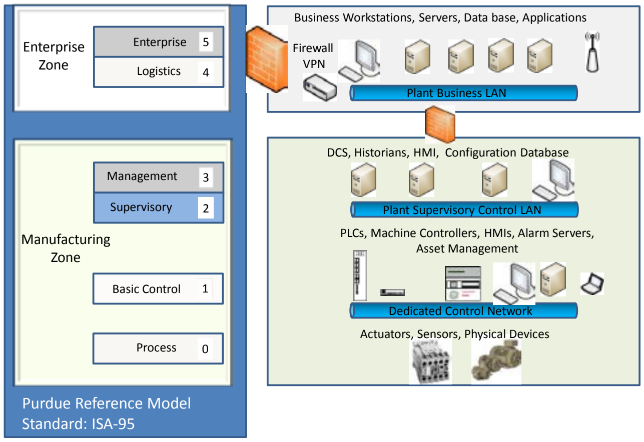
Enterprise Zone
Enterprise 5
Logistics 4
Management 3
Supervisory 2
Manufacturing Zone
Basic Control 1
Process 0
Purdue Reference Model
Standard: ISA-95
Business Workstations, Servers, Data base, Applications
Firewall
VPN
Plant Business LAN
DCS, Historians, HMI, Configuration Database
Plant Supervisory Control LAN
PLCs, Machine Controllers, HMIs, Alarm Servers, Asset Management
Dedicated Control Network
Actuators, Sensors, Physical Devices

Figure 2: ISA 95 Reference Model

This design methodology has worked well in the past but is now quickly nearing the end of its useful life. Figure 3 illustrates the progression of network complexity and system complexity versus time. With the addition of new applications to support the ever expanding need for new cloud based services to support plant and equipment optimization and the increasing need for critical infrastructure security within the plant, current networking technologies don't scale well.

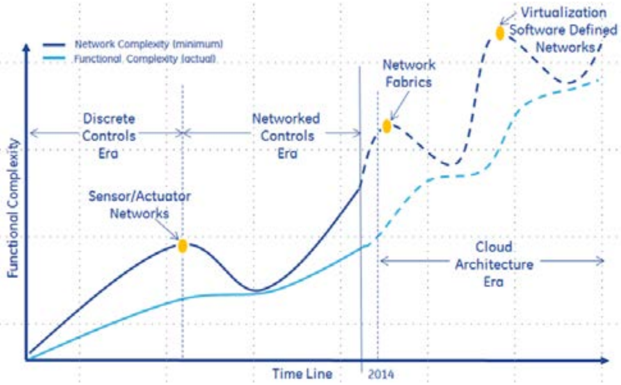

Figure 3: Growing Network Complexity

Today's operating plants have fewer and fewer maintenance engineers. It is not surprising to walk into a large operating power plant with multiple power islands and only find two operators and two maintenance engineers. The need to automate the equipment maintenance processes and provide the day to day optimization schemes is an area where modern plant operators are demanding more from their suppliers.

Attributes of a Control Network

In this new environment control networks must be reliable. They must be able to deliver information within a guaranteed amount of time under all loading conditions (guaranteed latency). They must be resilient and maintainable, they must be able to survive one or more failures and still operate as if a failure never occurred. They must be flexible and adapt to changes in plant configurations adding new applications (scalable) and they must be secure. In the age of the Industrial Internet reliance on physical security at the perimeter is not enough, the emerging cloud based services as well as global asset management require that there be connectivity everywhere and this places more stringent security requirements on the network.

It is rare today that a single supplier will provide all the equipment and applications within a plant. Interoperability and coexistence between applications operating on the same network is critical.

Combining critical control applications on a single network today and guaranteeing Quality of Service (QoS) can only be done by isolating traffic and substantial testing. Switched Ethernet can suffer from congestion losses if traffic flows are not controlled and the traffic itself is not engineered. Updates to standard Ethernet such as TSN provide mechanisms for mathematically provable latency and delivery guarantees without the need to do exhaustive testing. This can greatly reduce system requisition engineering and network testing and qualification time. Network hot standby redundancy is a feature which provides reliability and availability. Traffic scheduling along with Virtual Local area Network (VLAN) technology provides traffic isolation on a fine grained basis. This allows the plant operator to add new applications at any to the network and be assured that currently running applications will not see any degradation in performance time as long as sufficient resources exist. He will also know beforehand if there is a chance that his network will become overloaded. If a new application needs specific QoS guarantees and they are not available the operator will be informed immediately and not find out later after the application fails on deployment.

Cloud Based Services & the Industrial Internet

Large scale Industrial Equipment Providers are now able to offer more plant and asset management and optimization services given the amount of computational power that exists within the cloud. To allow this to occur, the security barrier needs to extend much further down into the plant equipment than it has historically. Virtualization at the controller level, hypervisors, and multicore processors provide the avenue for a whole new generation of control architectures which can be remotely managed in in a secure way. Asset management in the power plant will be much more highly automated, product updates and upgrades will be faster and more transparent. TSN can provide the secure traffic isolation needed to allow cloud based services to communicate directly to the edge on the plant floor in this new generation of control platforms.

The Role of AVnu

Many industrial application protocols have already been adapted to standard Ethernet. This does not mean they can coexist on the same network. For the network to enforce coexistence then all network devices must be compatible. This level of compatibility requires interoperability specifications and certification testing much as the WiFi alliance has done for 802.11 and all its variants. AVnu as an organization can provide not only the labeling to give end users confidence, but also provide the specifications that are required to pull together the family of standards that will assure that networks can meet the demands of the various applications. To this end AVnu provides the following benefits:

1. Filling the gap between the standards and the specifications for network functionality that meets the needs of industrial applications
2. Certification of conformance to the standards and specifications
3. Driving industrial application needs into the standards process
4. Coordination of the various standards bodies
5. End user education and outreach
6. Education of regulatory agencies which affect compliance of critical infrastructure applications.
7. Open interoperable technology with multiple suppliers