TECHNICAL ARTICLE

System Availability for SCADA Systems

By Jason Little, Regional Municipality of Peel
and Graham Nasby, City of Guelph Water Services

Industrial Control Automation Systems are responsible for the safe and reliable operations of a wide range of public and private infrastructure and business. These systems are both responsible for safe operations and economic output of the business. Within numerous industries, including the municipal water/wastewater sector, the term SCADA (supervisory control and data acquisition) is commonly used to describe these systems.

In the scope of critical infrastructure, SCADA systems are responsible for providing water and or electricity to the public. In these types of systems, failure of the control system needs to be avoided at all costs.

When designing and operating a control system the following guidelines should be reviewed and implemented based on your specific use case. As engineers, all designs need to ensure safety. This is the top priority. To ensure this safety, the Industrial Control System Engineer needs to ensure that three key aspects to the design are met at all times, namely:

1.) **Availability**
Design the system to ensure that the system and their components are available to complete their intended job continuously and when required.

2.) **Integrity**
Have checks and balances that ensure that the information that is being acted upon is correct and unalterable.

3.) **Confidentiality**
Access to the control system as well as data in and out of the control system is secured and provided/accessed by those people or devices with the authentication privileges to do so.

This is illustrated in the below figure:

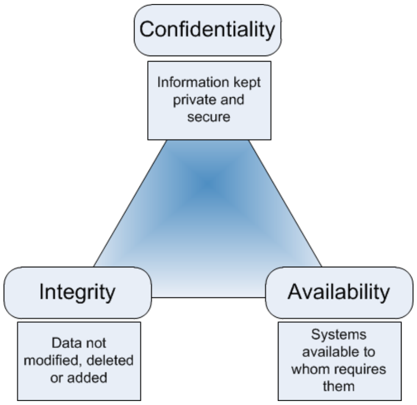

Confidentiality
Information kept private and secure
Integrity
Data not modified, deleted or added
Availability
Systems available to whom requires them

Figure 1 - Three major aspects of automatic control systems design

The ISA 62443 series of standards provides a solid framework for managing the cyber security aspects of the industrial automation control systems, including areas such as overall design goals, policies, procedures, systems and components.

An overview of the ISA-62443 series of cybersecurity standards can be seen in the following figure:

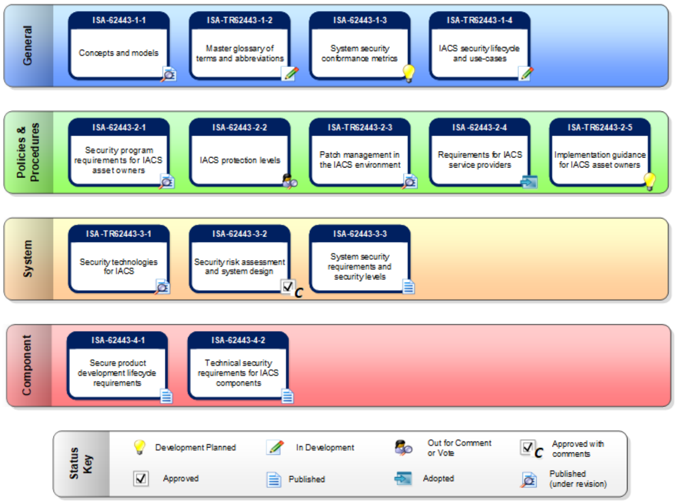

General
ISA-62443-1-1
Concepts and models
ISA-TR62443-1-2
Master glossary of terms and abbreviations
ISA-62443-1-3
System security conformance metrics
ISA-TR62443-1-4
IACS security lifecycle and use-cases
Policies & Procedures
ISA-62443-2-1
Security program requirements for IACS asset owners
ISA-62443-2-2
IACS protection levels
ISA-TR62443-2-3
Patch management in the IACS environment
ISA-62443-2-4
Requirements for IACS service providers
ISA-TR62443-2-5
Implementation guidance for IACS asset owners
System
ISA-TR62443-3-1
Security technologies for IACS
ISA-62443-3-2
Security risk assessment and system design
ISA-62443-3-3
System security requirements and security levels
Component
ISA-62443-4-1
Secure product development lifecycle requirements
ISA-62443-4-2
Technical security requirements for IACS components
Status Key
Development Planned
In Development
Out for Comment or Vote
Approved with comments
Approved
Published
Adopted
Published (under revision)

Figure 2 - ISA 62443 series of standards (source: www.isa.org)

How to Measure System Availability: MTBF

A commonly used term for system availability is the MTBF, which stands for Mean Time Before Failure. The word "mean" in this context is the statistical average. The MTBF is the amount of time that a system is expected to operate before a component fails that causes it to no longer function. This a good measure of a system's robustness.

The second metric is the MTTR, which is the Mean Time To Repair, which a measure of how well an organization can support a system when it fails. If good work procedures, staff capabilities, spares and support contracts are in place a quicker MTTR is possible – without proper planning and resourcing, the MTTR can be excessively long.

The MTBF is a key metric that needs to be evaluated for each component in the system. Placing components in series or placing components in parallel will change the system MTBF. Series placing will decrease reliability or increase the probability of failure, while parallel placement will increase reliability and decrease the probability of failure.

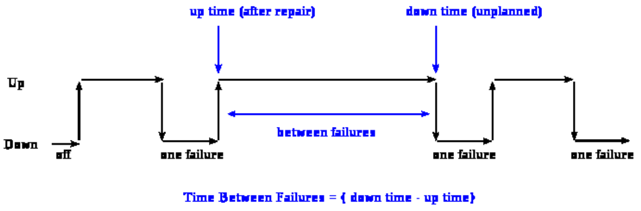


Figure 3 – MTBF: Mean Time Between Failures

ISA112 SCADA Systems Architecture Model

When looking at system availability, a systems approach is a helpful way to look at how the different components of a SCADA system interact with each other For this article, we will use the ISA112 SCADA System Architecture model as the framework to look at – See Figure 4.

The ISA112 SCADA System Architecture model provides a method to break SCADA systems into a series of layers. Availability has to be looked at on a layer by layer approach.

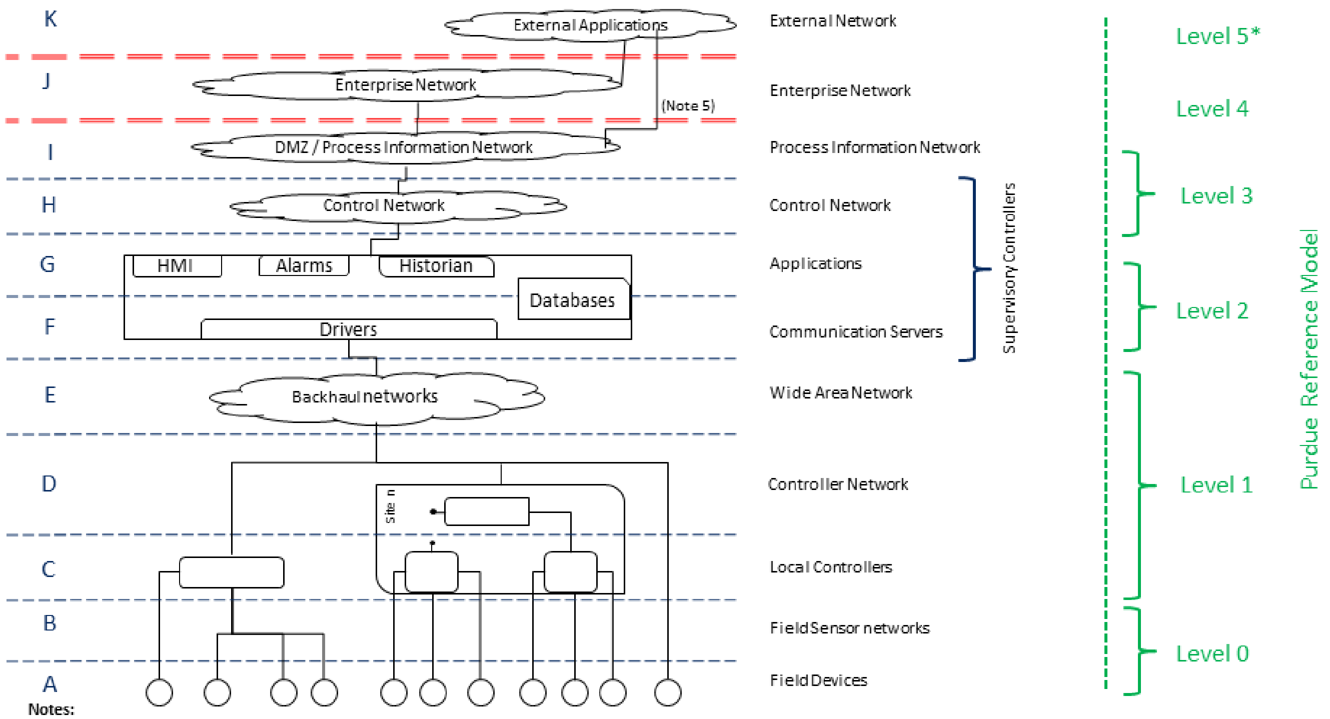
Factors affecting SCADA Systems Availability

Electric Power

Since most of the devices that form the SCADA system are power dependent, careful design considerations need to be applied to ensure the availability of power. Controls System Engineers need to engage with other engineering disciplines to ensure that the overall design meets the needs of the system. Where emergency backup power is available, all control equipment should be powered from circuits that are automatically restored by the backup power by means of automatic transfers switches and or depending on size automated switchgear. Control equipment should also be feed from uninterruptable power supplies with automatic bypasses, along with manual bypasses that can be used for maintenance purposes. Finally, key control equipment should have two independent parallel power supplies with independent fuses/breakers.

Layer A - Fields Devices

These devices should be chosen in such a manner that their process application and installation location are supported by the device. The failure of a unit device should be easily detectable by both operations and maintenance. Critical control devices used for loop control should be hardwired to the controller. Upon loss of power, these devices should fail to safe state. Field devices of the same parallel function should be connected to different Input/Output cards. Field devices of the same process should be connected to the same processor, so their operation is not impacted by failures of processor-to-process communications. Under most circumstances, field devices should not start in a faulted state after a power outage. Automation systems that connect to field devices should also be intelligent enough to realize that field devices often need time start-up/boot after a power outage, and be programmed to avoid triggering nuisance alarms and/or false interlocks during initial power up.



Notes:
1 Letters are used to avoid potential conflict with ISA-95 and other "Layer" models.
2 Routers and Firewalls between layers are not shown.
3 Other system-specific servers, applications ,and workstations are not shown.
4 Communications for any remote-hosted external applications (Cloud) with lower levels must be done using extreme care.
5 The use of direct-connections for remote applications is strongly discouraged. Refer to ISA/IEC-62443 for guidance on an appropriate zone/conduit implementation.
* We show a Purdue Level 5. The true Purdue Model only has levels 0-4 because it did not anticipate external applications.

Revision Oct 25, 2019

Figure 4 – ISA112 SCADA Systems Architecture Mode (source; ISA112 committee)

Layer B - Field Sensor Networks

These networks should be independent of other automation networks. The failure of an end device should not impact the network as a whole. In critical applications, these networks should be used for monitoring and additional troubling shooting information and or back up integrity checks.

Layer C - Local Controllers

Programming should deal with normal operations, however just as much time should be allocated for the development of fault response to upper and lower level devices as well as to other local controllers. Controllers should be developed for process areas. More local controllers doesn't always equate to better reliability. Most times, more local controllers lead to high complexity and edge case fault response that can lead to significant downtime. Thus there often a sweet spot for the number of controllers to use, as a balance between distributed vs. centralized controllers.

Depending on process requirements, critical controllers can be specified with redundancy in processing, and communications. I/O to the control should be segmented based on device type in the field. I/O should be limited to the specific process area. All controller failures should be easily detected, programming be place for the system to automatically respond appropriately, and operations personnel be notified immediately. The ISA technical report TR91 provides helpful guidance in how to determine field device and controller criticality.

Layer D - Controller Network

The controller network should be localized so it is used only for controller-to-controller and communications servers only. Using this network for other purposes or users is not recommended, as having multiple conflicting uses increases rick of outage and would mean outages impact larger parts of the system. Broadcast traffic should be limited or eliminated all-together. It goes without out saying that field sensor communications should be on their own network, and not part of the controller network.

For large facilities, an approach of using zone network panels with redundant switches forming ring topologies can a high degree of robustness with minimal cost, while still allowing for straight-forward troubleshooting.

Unless there is a very specific use care for it, proprietary networking protocols from switch manufacturers should be avoided and instead fault tolerant open protocols should be employed such as Rapid Spanning Tree for layer two networks.

For smaller facilities, redundant media star topologies could be employed, where the top level of the network is located in the server room or control room.

All controller network failures should be easily detectable by automatic means, and operations notified immediately.

Layer E - Wide Area Network (WAN)

Redundant media or physical redundant path should be in areas where high availability is required. Open, fault tolerant, automatic-healing protocols such as OSPF and BGP should be utilized. Focus should be given as to not saturate the bandwidth of the WAN network and QoS (Quality of Service) should be utilized, if guaranteed controller-to-controller communications is required. If multiple types of data are being passed over a WAN, an approach of using multiple VLANS (virtual local area networks) couple with QoS can provide a robust implementation. As with other networks, any wide area network failures should be easily detected – ideally by automatic means, have automatic routing to re-route the traffic, and a mechanism provided to notify both operations and SCADA staff immediately.

Layer F - Communication Servers/Hosts

The amount of availability needed for a SCADA system will guide the selection of appropriate server hardware to use. For most SCADA systems, the system designer should be using server grade hardware with dual processors, dual network cards, dual power supplies and redundant storage controllers. Disc mirroring or RAID level 5 (which can accommodate one disc failure in an array) should be utilized at minimum. Depending on the application, RAID 6 (which can sustain two disc failures in an array) may be an appropriate choice. . RAID 0, which stripes disks with the sole goal of increasing performance, should be avoided.

When virtualizing hardware, which is recommend to improve availability, a strategy should be implemented for clustering of servers and storage to increase availability. When possible, use redundant communications hosts that act as a middle layer between the local controllers and the application hosts. An automated backup strategy should be developed for offsite backups on a scheduled basis. All virtual servers should be monitored for load on the key physical aspects of the server, including CPU, Disk, Memory and Network loads. In a well-designed system, there will be multiple layers of redundancy built in along with automatic fail-over as needed.

Layer G - Application Servers/Hosts

The same hardware considerations that apply to Communication Servers/Hosts, also apply when looking at the Application Server level. Care needs to be taken to adequately resource the amount of CPU, memory, disk and other resources for the specific applications that are being run. Some SCADA applications may have very specific hardware or network requirements in order to be run reliably.

Layer H - Control Network

In larger systems, the control network is physically separate from the site specific controller networks. For smaller systems, sometimes these two networks are combined. It is on the Control network that SCADA view terminals, operator terminals and other user-facing devices usually reside. Good network design for reliability is tied to the availability needs for these aspects of the system. Depending on requirements, part of this network may be built using redundant components. The Control Network is also the way that higher levels of the SCADA system reach down, by way of firewalls, routers and proxies, to pull data put into higher up applications.

Layers I, J, K and beyond

Reliability for the Process Information Network, Enterprise Network, and networks to external applications is a function of the system uptime needed for these systems. At these higher levels, reliability is less about process control and instead more about data availability, connectivity, and supporting business/maintenance management systems. Availability in these systems is usually a combination of power availability, network connectivity, hardware redundancy, and application design. Often an IT-based approach, rather than using OT-based design, is used to build in reliability for these systems. Guidance for keeping these systems secure can be found in both the ISA-62443 series of standards and also in the IT-focused ISO 27000 series of system reliability standards.

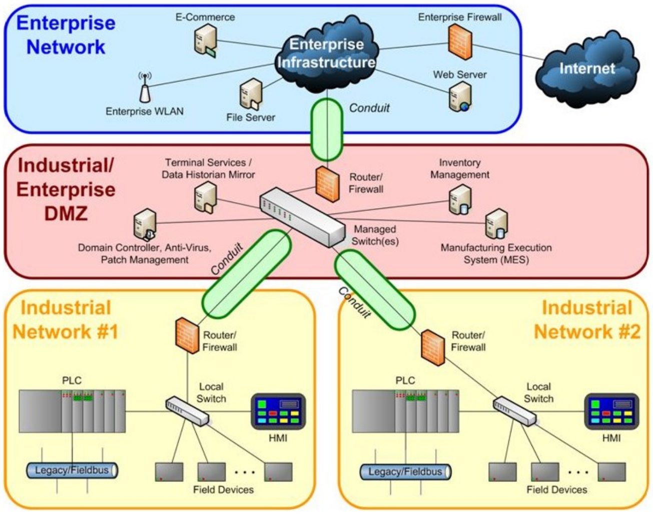


Figure 5 - The ISA-62443 zones/conduits model provides cybersecurity robustness as well as compartmentalizing risks within the various levels of a SCADA system (Source: ISA99 committee)

Summary

There are many aspects and layers that contribute to the overall system availably metric. This is a key performance indicator for an industrial automation control system. This availability or uptime should be used as a guide for decision making during the design and implementation of a control system. The higher the availability an owner or engineer wants to achieve the greater the capital investment. Tracking MTTR can be used as an effective measure to see if capital investments in SCADA systems are meeting expectations. Designing for system availability is one of the great design and operational challengesof the modern SCADA system.

About the Authors:

Jason Little is an Automation Professional with over 15 years of experience in the Water/Wastewater industry. He studied electrical engineering at McMaster University and currently works for the Regional Municipality of Peel as an advisor in the SCADA division of the Public Works Department. Jason is an active member of the automation community, most recently holding the chair position in the OWWA Automation Committee. Jason is a contributing member to ISA with his most recent contributions to ISA 112. Jason also develops open source SCADA applications through his company Triple Point Solutions Inc. Contact: jason@triplepoint.solutions

Graham Nasby, P.Eng, PMP, CAP holds the position of Water SCADA & Security Specialist at City of Guelph Water Services, a publicly-owned/operated water utility located in Guelph, Ontario, Canada. Prior to joining Guelph Water, he spent 10 years in the engineering consulting community after completing his B.Sc.(Eng.) at the University of Guelph. He is senior member of the International Society of Automation (ISA) and co-chair of the ISA112 SCADA System Standards Committee. Contact: graham.nasby@guelph.ca