ISA112 SCADA STANDARDS COMMITTEE NEWS

The Importance of having a strong SCADA Governance policy framework and work process for SCADA Systems

By Graham Nasby, ISA112 committee co-chair

One of the topics currently being discussed by the ISA112 SCADA systems management committee is how we can more effectively manage SCADA systems in terms of not just funding/staffing, but also in terms of ensuring that decision-making processes associated with the design, building and maintenance of SCADA system continue to meet the functional and business needs of the organization. Thus, the topic of effective SCADA governance is something that is built into the ISA112 SCADA systems standard.

Any SCADA system, to be effective, must have a clearly defined purpose, owner, and ongoing resources assigned to the system to be able to maintain its functionality, availability, and effectiveness over time. Thus, it is imperative for any SCADA system that a strong governance structure be put in place by the end user who owns the system. To do otherwise, can create significant problems when it comes to maintaining functionality, ensuring the system meets business needs, and achieving the required system availability.

SCADA governance is a conceptual structure and set of rules that outline how an end-user's SCADA program is to be managed and controlled. The structure of an effective SCADA governance program will be defined in a written policy document that has been endorsed by executives at the organization.

SCADA Governance Policy Document

As a minimum, a SCADA Governance Policy document needs to be developed by the system owner that clearly defines key governance characteristics of the system, As a high-level steering document, the governance policy provides a framework of how the SCADA system will be developed, built, and maintained over time, and a work process for how decisions regarding the SCADA system will be made over time. Also, as a steering document, it requires executive endorsement and support in the organization so the role of SCADA is clearly defined in terms of what it needs to do and the resources to be allocated to it.

Required SCAD Governance Policy Document Topics

As a minimum, a SCADA Governance Policy document needs to clearly define the following characteristics of the system:

1. The purpose of the SCADA system
2. The scope and boundaries of the SCADA system (e.g., who owns IEDs vs. SCADA system)
3. The business functions/needs of the SCADA system must meet or exceed
4. The business criticality of the SCADA system and the required overall uptime/availability
5. Known regulatory/compliance requirements the SCADA system must meet or exceed
6. Known technical standards that the SCADA system must meet or exceed (e.g., ISA112)
7. The primary users of the SCADA system and their high-level requirements
8. Who in the organization (or department) is the owner of the system, and if there are if there specific components that are to be owned by specific departments/groups in the organization
9. Who in the organization is responsible for providing the funding to operate and maintain the system in a state of good repair
10. How is the annual budget for operating and maintaining the system determined, approved and administered
11. Who in the organization is responsible for the upkeep and maintenance of the system
12. Who carries out system maintenance and upgrade work to keep it in a state of good repair
13. Who provides support as needed to the users of the system
14. Who is responsible for providing emergency support/repairs for the system
15. Who must be consulted, in terms of being informed, consulted and for approvals, before changes are made to the system
16. For major changes to the system, what change management procedures must be used
17. For changes to the system, what criteria are to be used for classifying very minor, minor and major changes to the system
18. For proposed major upgrades, what is the process to be used for approving major upgrades, determining who pays for them, and then carrying them out
19. Any known business risks if the SCADA system is not available for use or does not work properly, and if there are any agreed-upon mitigations or controls
20. An agreed set of high-level overall SCADA system performance metrics for measuring system performance on at least an annual basis
21. Policy on what the expected lifespan of SCADA system components should be, to guide the design, procurement, and maintenance of system components.

Recommended Additional Policy Document Topics

The following topics are also recommended for inclusion in the SCADA Governance Policy document:

1. Any other high-level requirements specific to the end-user/industry that the SCADA system must meet
2. Any secondary users of the SCADA system and their high-level requirements
3. Other stakeholders impacted by the SCADA system and their high-level requirements
4. What staffing is required for the ongoing of the system and who is responsible for providing that staffing.
5. Who classifies the SCADA systems data and ensures its security and confidentiality
6. Policy and procedures for testing SCADA system changes before they are put into production.
7. For highly regulated industries, who is responsible for carrying out SCADA system validation and compliance testing activities.
8. Who provides (and decides which) minor feature requests from users are to be implemented
9. What is the change control process/workflow for making minor changes to the system?
10. Minimum requirements for periodic system backup/restore, ongoing revision control, and capabilities for disaster recovery
11. In the event of a catastrophic failure, the agreed expected minimum time for a return to system availability
12. High-level plans of how the organization has agreed to respond to SCADA outages.
13. What type of vendor and service provider support must be in place for the SCADA system
14. Policy on how SCADA system component warranties and support agreements should be managed.
15. Policy on the use of open-systems (can be modified by end-user or any integrator) versus closed-systems (can only be modified by the original vendor) for both in-warranty and out-of-warranty support
16. Policy on procurement of SCADA equipment when there are unique requirements. This should include a framework defining when/if the use of pre-approved, pre-qualified, single-source, and/or sole-source providers are appropriate.
17. Policy on procurement of SCADA system integration work when there are unique requirements. Should include a framework for defining when/if the use of pre-approved, pre-qualified, single source and/or sole source providers are appropriate.

Additional Policy Document Guidance

Depending on the organization type, industry, and role of the specific SCADA system, there may be additional characteristics or details that may need to be outlined in the SCADA Governance Policy Document. This will be up to the end-user to determine as needed.

The SCADA Governance Policy document should be written at a very high level and contain no more than one to four short paragraphs in each section. It is meant to act as a high-level steering document only. Further details about how various aspects of the SCADA system are to be designed, implemented and operated/maintained are to be detailed in the SCADA Systems Standards documents.

The SCADA Governance Policy Document shall be reviewed periodically to ensure that it continues to meet the organization's needs. To be effective, the document should be endorsed by a sponsor at the executive level of the end-user organization each time it is reviewed (for example, at the board of directors, CEO or COO level in a traditional corporation).

Note: It is recommended that the SCADA Governance Policy Document be reviewed, edited, and approved annually.

SCADA Strategy Documents

For large systems, it is sometimes advisable to develop a set of strategic documents that outlines a high-level road map in terms of how the SCADA system will be funded, staffed, and developed over time to meet long-term business needs. These high-level strategy documents can be used in conjunction with the more technical "SCADA Long Term Planning" documents to develop a comprehensive long-term plan for capital investment and upgrades to the SCADA system over time. If used, any SCADA strategy documents should be reviewed and updated on a regular basis. Depending on the type of organization, these documents may be treated as confidential to the end user.

Additional SCADA Governance Policy Documents

Depending on the size and complexity of the SCADA system and/or the organization that it serves, some organizations may decide to have additional high-level policy documents to supplement the overall SCADA Governance Policy document. This is, of course, keeping in mind that the intent is that the specific technical requirements, policies, procedures, guidelines and templates or the end user are meant to reside within the SCADA Standards package as outlined in this standard. Two examples of this are developing RACI tables and SCADA Risk registers.

Using RACI Tables

The use of a RACI (responsible, accountable, consulted, informed) tables can often be an effective visual tool to use in a SCADA Governance Policy document to further illustrate the

content of the policy document's statements. An example is shown in Table 1.

Table 1 - Example of a RACI Matrix Table

	Senior Management	SCADA Team	Operations	Compliance	Accounting
SCADA Governance Document	A	R,A	C	C	I
SCADA Cybersecurity Program	C	R	I	I	--
SCADA backup systems	I	A,R	I	I	--

SCADA Risks Register

It is recommended that a risk assessment for the SCADA system is undertaken on a regular interval to document potential risks to the SCADA systems and what controls can be applied to mitigate risks. Many organizations do this on an annual or semi-annual basis. Risks should be classified as mitigated, transferred, or accepted. The SCADA risk register document should be periodically reviewed at a set interval.

A mitigated risk is a risk for which compensating measures have been put in place to reduce the chance of the risk occurring (e.g., having periodic automatic backups and maintaining a hardware spares inventory reduces the risk of downtime resulting for a significant hardware failure.). An example of transferred risk is using a third party to reduce the likelihood of a risk's impact or occurrence (e.g., having a 4-hour response vendor support contract in place to replace hardware if it fails). An accepted risk is a risk that cannot be mitigated, but the system has clearly defined what the risk is, documented it, and accepted it as part of normal operations (e.g., the risk has been identified and documented, and the organization knows what to do if it occurs).

It is important that any SCADA risks be evaluated from both a management/operational level and a technical level. This includes looking at risks from a perspective of an operational impact but also by looking at impacts on the technical integrity of the SCADA system itself. Both perspectives are needed in order to properly assess potential risks and associated mitigations for the SCADA system.

SCADA Long-Term Planning

To be effective, a strong SCADA governance program also needs to be accompanied by an equally effective long-term planning process for any SCADA system. Well-managed SCADA systems will have a long-term operational and capital plan that outlines the expected investments and operational improvements to the system from the perspective of the next 5, 10, 15, 20 and 25 years and beyond. Part of effective long-term planning is by looking at system components and engineering investments from a lifecycle approach, realizing that all parts of the system will need ongoing investments and upgrades in order to continue to meet business needs and be maintainable in the long term.

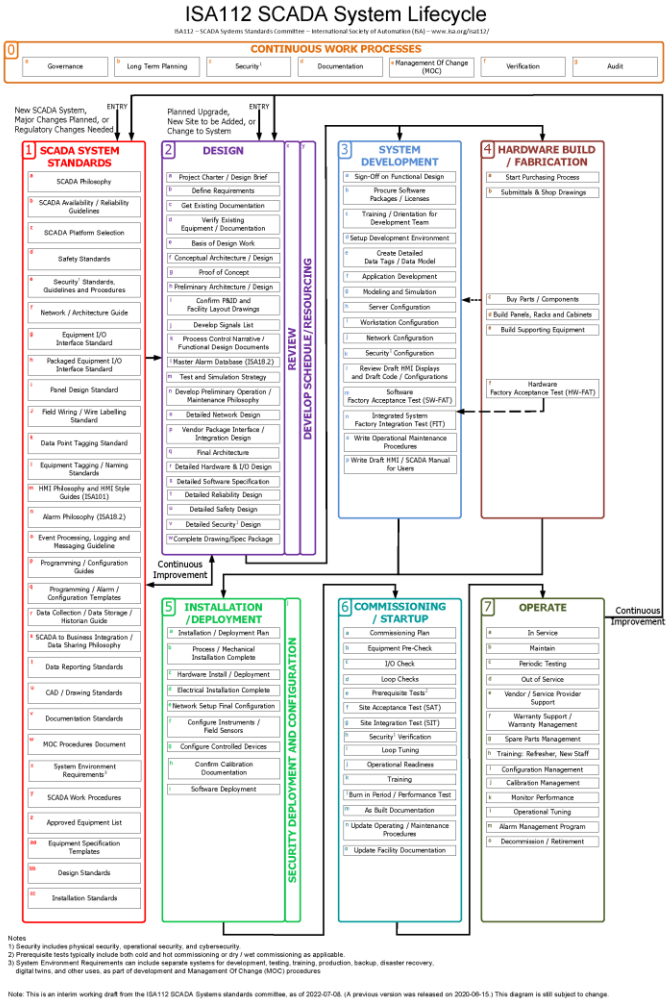

Figure 1- ISA112 SCADA System Lifecycle (source: www.isa.org/isa112)

Summary

Governance is an area where SCADA systems have traditionally struggled. To be able to build and maintain a well-functioning SCADA system that continues to meet business needs, a strong written policy framework must be established, endorsed and maintained by the owner of the system. This includes defining who is responsible for staffing/funding the system, how decisions are made and keeping it safe from threats such as cybersecurity and obsolescence. It is time we up our SCADA game to include effective governance, just like enterprise IT and CSIO professions have begun doing in recent years. The upcoming ISA112 SCADA systems management standard emphasizes the need for effective governance of SCADA systems

About the Author

Graham Nasby, P.Eng, PMP, CAP, CISM, CISSP is a licensed professional engineer with more than 15 years with automatic control systems. Located in Guelph, Ontario, Canada he holds a B.Sc.(Eng.) from the University of Guelph a certificate in Project Management from the University of Waterloo. He is senior member of the International Society of Automation (ISA) and co-chair of the ISA112 SCADA System Standards Committee. Contact: graham.nasby@grahamnasby.com