ISA

An Overview of the ISA112 SCADA Systems Management Lifecycle

Graham Nasby

ISA112 committee co-chair

Wednesday, March 29, 2023

ISA Hamilton Section – Members Meeting – Hamilton, Ontario, Canada

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

About the Speaker

Graham Nasby, P.Eng., FS Eng., PMP, CAP, CISM, CISSP

- 20+ years experience in operations, construction and automation sector
  - 1998-2005 IT Consultant – University of Guelph
  - 2005-2007 – controls specialist at various manufacturers
  - 2007-2010 Process Engineer – Cheme Engineering
  - 2010-2015 System Integrator & I/C Lead – Eramosa Engineering
  - 2015-2022 Water SCADA & Security Specialist – Guelph Water
  - 2022-present – Sr. Manager of OT Security Architecture – CN Rail

- Co-chair of ISA112 SCADA Systems standards committee
- Voting member of ISA101 HMI Design and ISA18 Alarm Management committees
- Past Section President, Division Director, Technical VP within ISA at local, regional and society levels
- Member of IEC/SCC TC65A "Industrial process measurement, control and automation"
- Member of CSA P125 "Operational Technology: Functional Safety and Security"
- Member of the OWWA Automation Committee since 2015, active in AWWA & WEF 2010-2022
- Holder of Ontario Drinking Water Treatment Operator & Wastewater Treatment Operator licenses

- Sessional instructor at McMaster University (Hamilton, ON) and Conestoga College (Cambridge, ON)
- Has published over 75 papers and articles on various OT, SCADA and industrial automation topics
- Received ISA's technical division leader of the year award in 2013
- Received "Mid-Career Achievement Award" from his *alma mater* University of Guelph in 2014
- Recipient of the ISA's society-level Standards Leader of the Year Award in 2021
- Contact: graham.nasby@grahamnasby.com

I wanna be a Water Guy when I grow up!
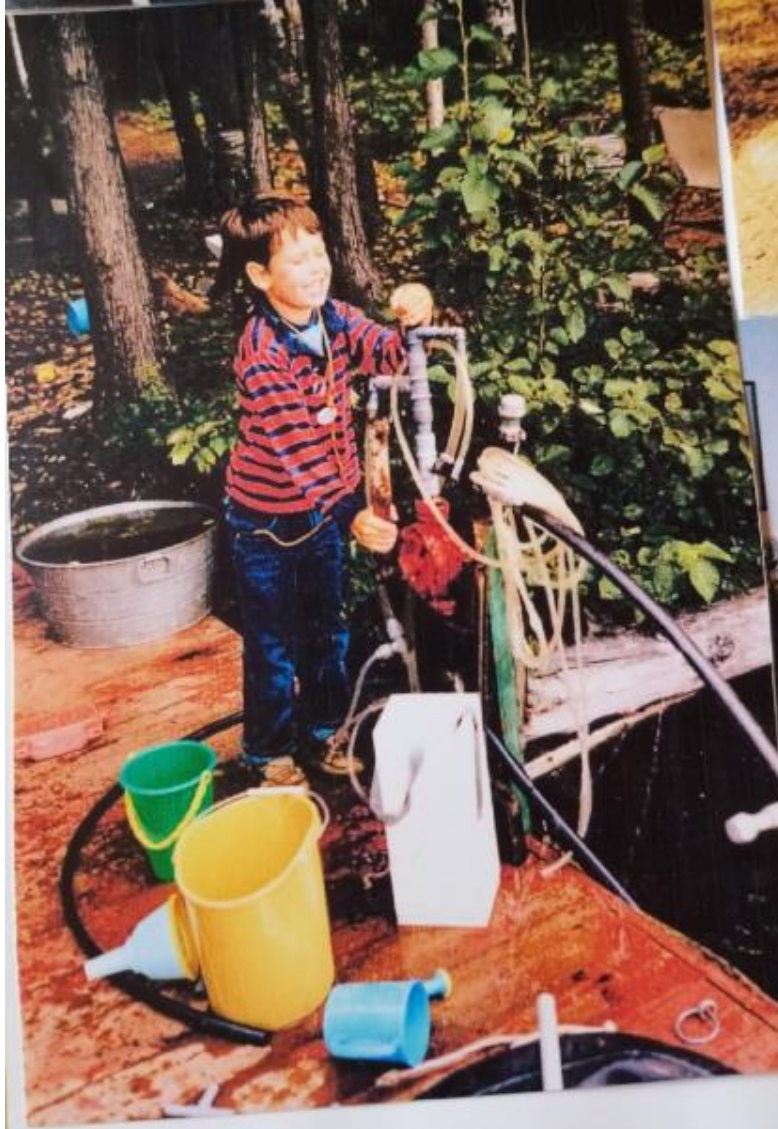
OK… Trains are cool too!

An Overview of ISA112

- **SCADA Refresher**
- **What is ISA112**
- **Goals of ISA112**

- **About the ISA112 Standards Committee**
- **Target Audience of ISA112**
- **How ISA112 defines "SCADA"**

- **Introduction to the ISA112 SCADA Management Lifecycle**
  - **Continuous Work Processes**
  - **(End-User) SCADA System Standards**
  - **Standardized Workflow for Projects**
    - **Design**
    - **Software Development**
    - **Hardware Build/Fabrication**
    - **Installation & Deployment**
    - **Commissioning**
  - **Operations & Maintenance**
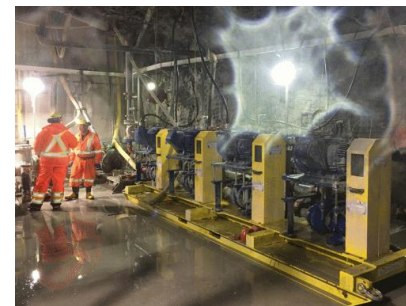
What is SCADA?

SCADA = Supervisory Control and Data Acquisition system
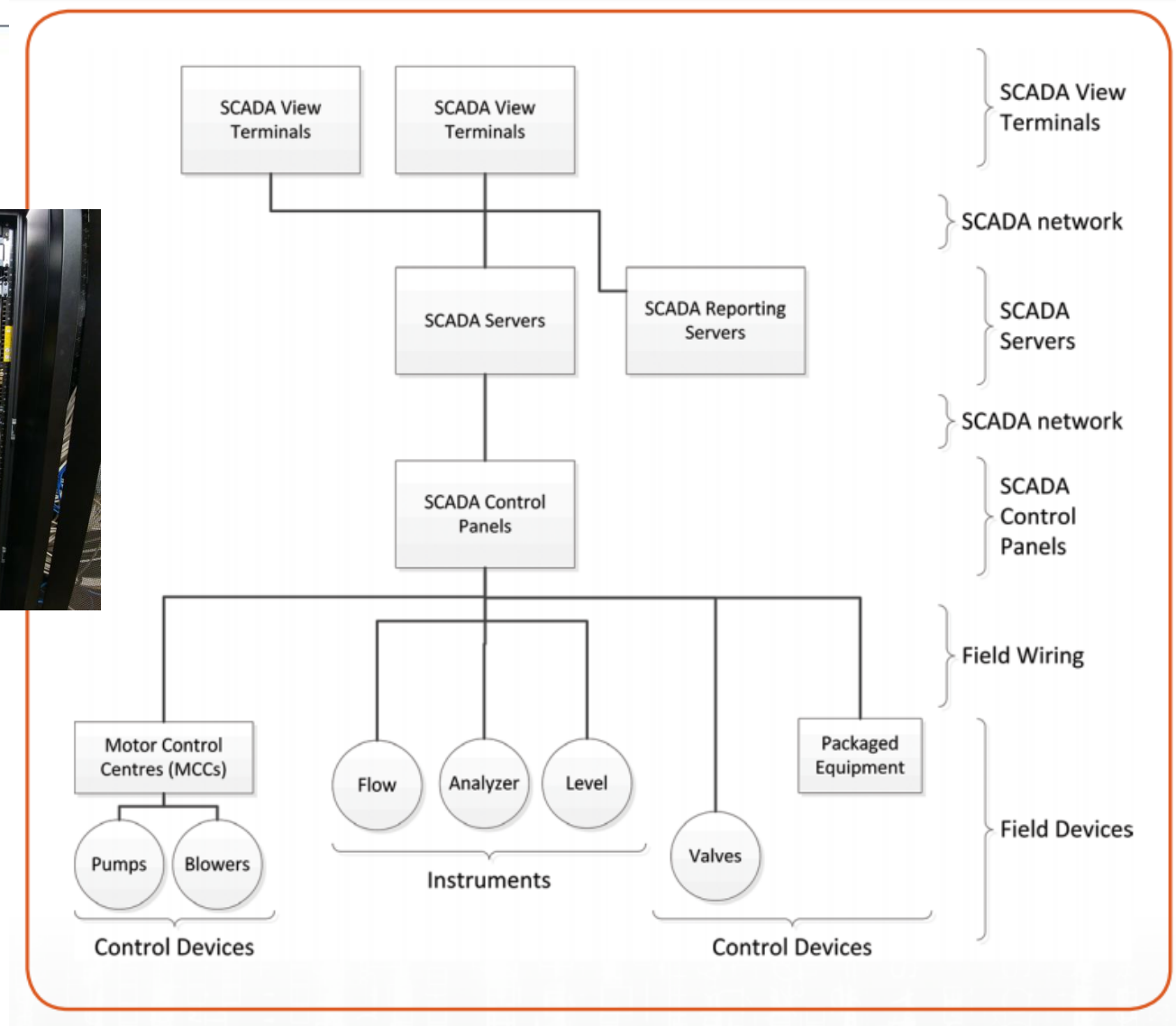
Not SCADA

Typical SCADA Architecture

What is ISA112?

- **ISA112** is a consensus-based technical standards committee **to promote best practices for SCADA systems** formed by the International Society of Automation in mid-2016

- Currently 300+ members with broad cross-section of roles, industries, and geographies

- **Committee Members:** software vendors, hardware vendors, end users, system integrators, consultants, distributors, and government from a wide variety of industries

- **Industry Sectors:** municipal water/wastewater, upstream oil/gas, pipelines, mining, power transmission/distribution, environmental monitoring, manufacturing, traffic control

- **Geographic Areas:** worldwide, with representation from Canada, USA, South America, Europe, Asia, Australia and beyond

- **Goal:** Develop a series of ISA standards and technical reports that provide guidance for system design, implementation, operation, and maintenance of SCADA systems for pipelines, water and wastewater, power, oil and gas, and other industries to support the overall integrity and reliability of these systems.

Motivations & Drivers for ISA112

Utilities, System Integrators, Consultants, Vendors, etc. are all asking for:

- Need for common terminology for SCADA systems

- Specification for minimum SCADA hardware and software requirements

- Suggested I/O interfaces for interfacing with equipment

- Standardized Control Modes: Remote vs. Local, Auto vs. Manual, etc.

- Reference architectures for levels of control

- Guidance for applying other ISA standards to SCADA systems:
  - Cyber Security
  - Alarm Management
  - HMI Design
  - Data Storage
  - Designing robust, resilient and redundant systems

A major goal of ISA112 is to provide a common framework that can be used for specifying, designing, pricing, building and maintaining SCADA systems

What is ISA112 Audience?

Pipeline · Water & Wastewater · Power · Upstream O&G · Other Industries
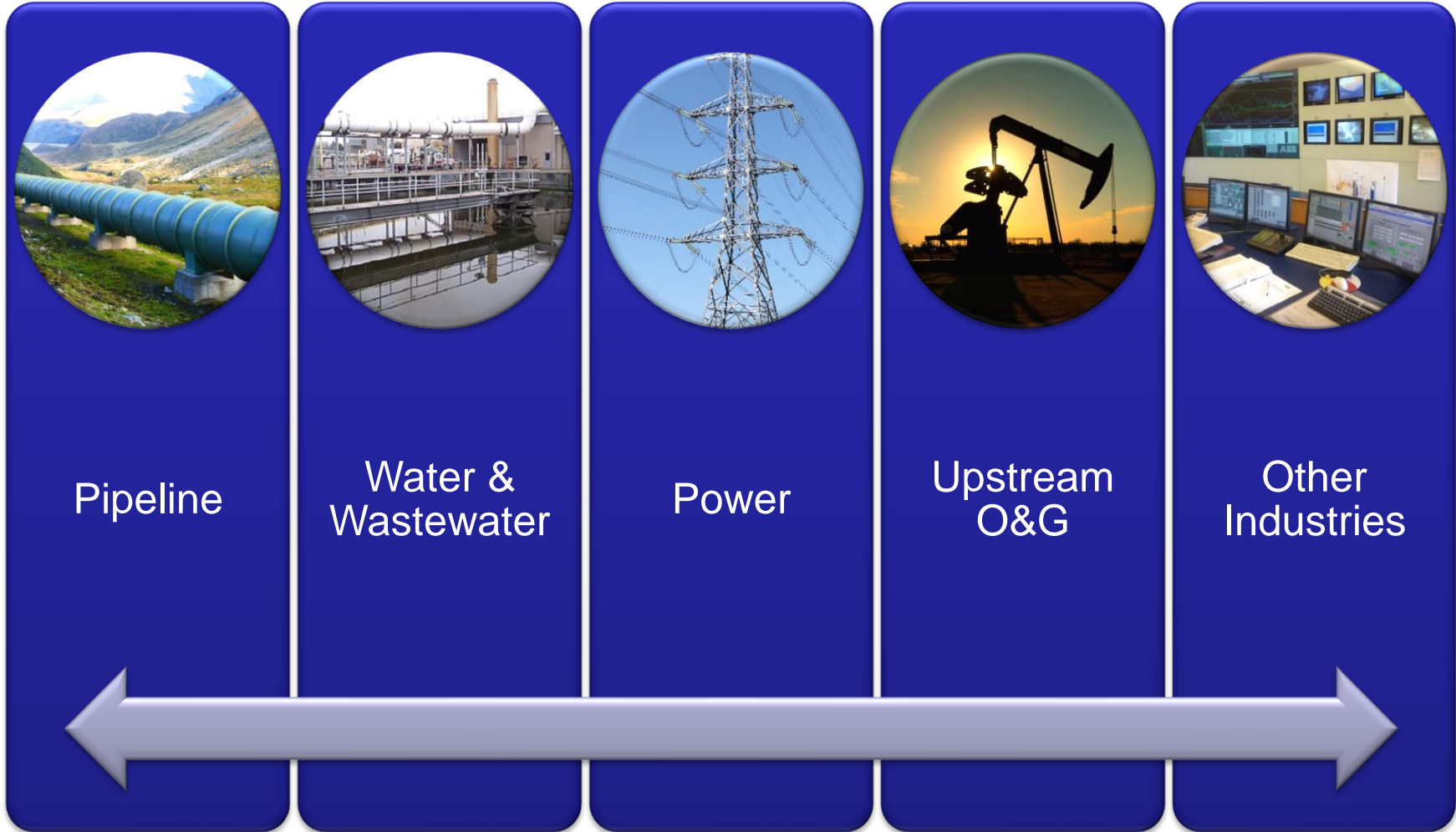
Who is ISA 112?

Over 300 committee members

75 active authors

End Users

Software Vendors

Government

ISA 112 Committee

Hardware Vendors

Consultants

System Integrators

Current Status of ISA112

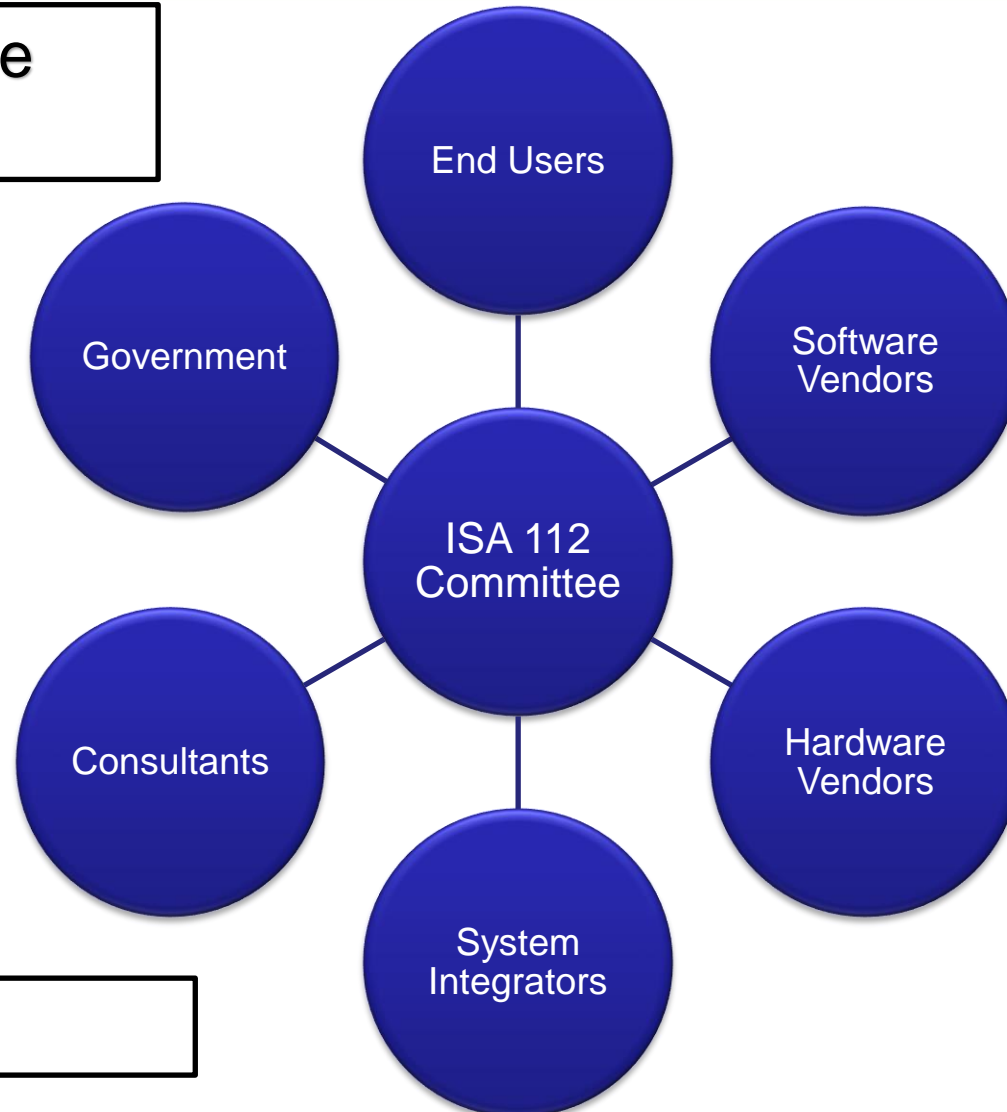|	
Jun 2016	Committee approved by ISA
Aug 2016	Initial call for volunteers (40 members)
Sept 2016	First meeting held in Newport Beach, California, USA
Jan 2017	Committee co-chairs named -Graham Nasby, originally with Guelph Water Services, now with CN Rail (Guelph, Ontario, Canada) -Ian Verhappen, originally with CIMA+, now with Willow Glen Systems (Calgary, Alberta, Canada)
Apr 2017	Monthly conference calls begin
May 2017	Second meeting in Raleigh, North Carolina, USA Semi-annual face-to-face meetings start
May 2018	Development of ISA112 Lifecycle & Architecture diagrams begins, drafts distributed to early-adopters
Nov 2018	Draft Table of Contents Developed
2019-2020	Writing Phase begins. 75 active authors contributing.
July 2020	First release of Draft ISA112 Management Lifecycle Diagram at www.isa.org/isa112 (free download)
2021-2022	Document Development / Section Working Groups As of 2021 we had 500 pages draft content, to be split between 3-part standard and technical reports.
July 2022	Release of Updated ISA112 Management Lifecycle Diagram at www.isa.org/isa112 (free download)
Nov 2022	Semi-annual face-to-face meetings resume after 3 year break due to pandemic. Monthly conference calls continue
2022-2023	**Committee review/commenting rounds, going to final ballot in late 2023**
Early 2024	**Target publication date for Part 1: SCADA Management Lifecycle, Terminology & Diagrams**
2025-2026	Target dates for Part 2: Lifecycle Implementation & Part 3: SCADA System Architecture

Work so far on ISA112

- Defining what a "SCADA System" is, including industry-specific and regional variations

- ISA112 SCADA Model Architecture Diagram (1st draft)

- ISA112 SCADA Management Lifecycle Diagram (1st draft)

- Table of Contents (1st draft)

- **….and after much, much writing, review, and discussion…**

- ISA112 SCADA Model Architecture Diagram (20 revisions later) – now posted at www.isa.org/isa112/

- ISA112 SCADA Management Lifecycle Diagram (38 revisions later) – now at www.isa.org/isa112/

- Table of Contents for a 3-part SCADA standard

  - Part 1 – SCADA Management Lifecycle, Terminology and Diagrams

  - Part 2 – SCADA Management Lifecycle Best Practices

  - Part 3 – SCADA Model Architecture Diagram Best Practices

- Approx 700 pages of technical content…now being distilled into the 3-part standard and technical reports

- The committee is now getting ready to begin formal comment cycles on Part 1, with the goal of publishing it in early 2024

What is a SCADA System?

ISA112 Definition

SCADA – Supervisory Control and Data Acquisition

"SCADA = a system which is a combination of hardware and software used to send commands and acquire data for the purpose of monitoring and controlling."

(DEFINITION ADOPTED BY ISA112 COMMITTEE AT MAY 5, 2017 MEETING IN RALEIGH, NORTH CAROLINA, USA)

Different Industries use the term "SCADA" to mean many different things that are specific to that individual industry. Each of these industries is correct in how it uses the term SCADA within its own context. We must be aware of this, and our definition and standard must be written so that it can be used by all industries.

Term "SCADA vs. Several Industries

- Examples of differing definitions of SCADA by industry
- Definitions can also vary by geographic area/country
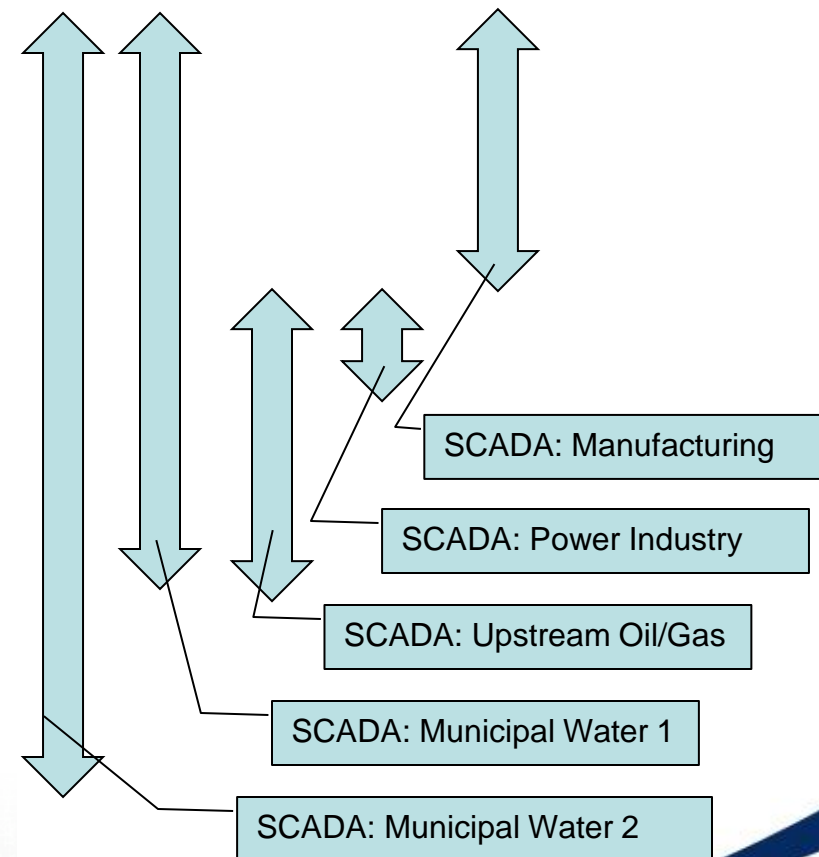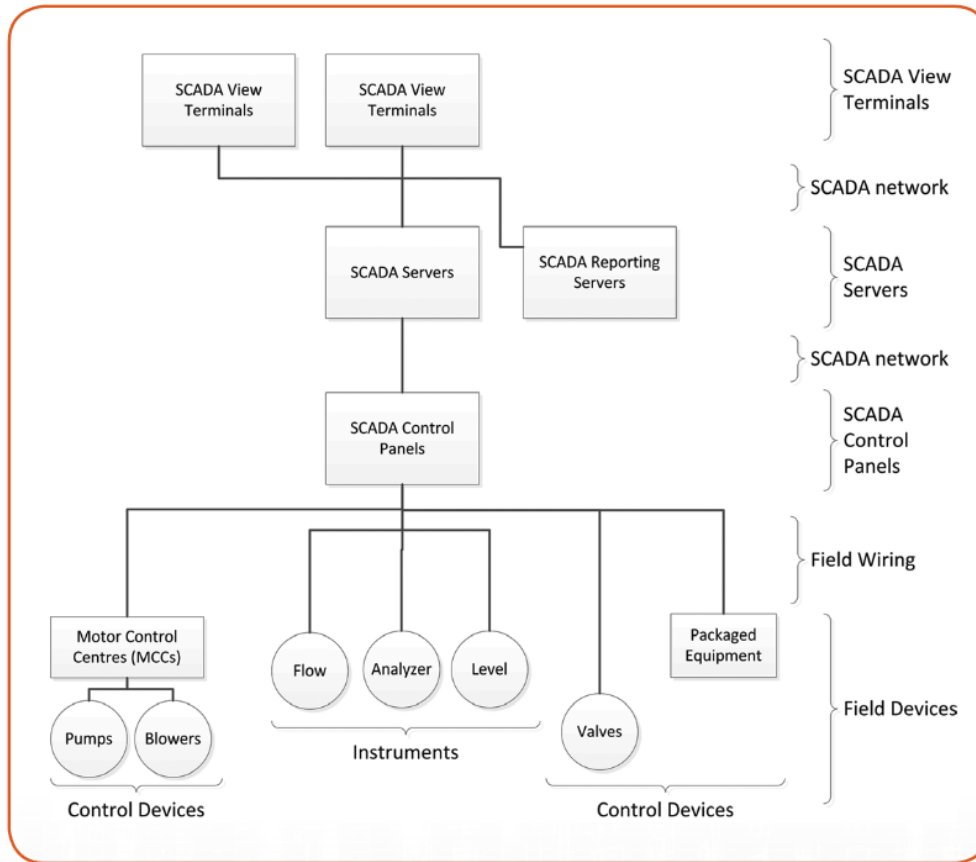
SCADA System Architecture
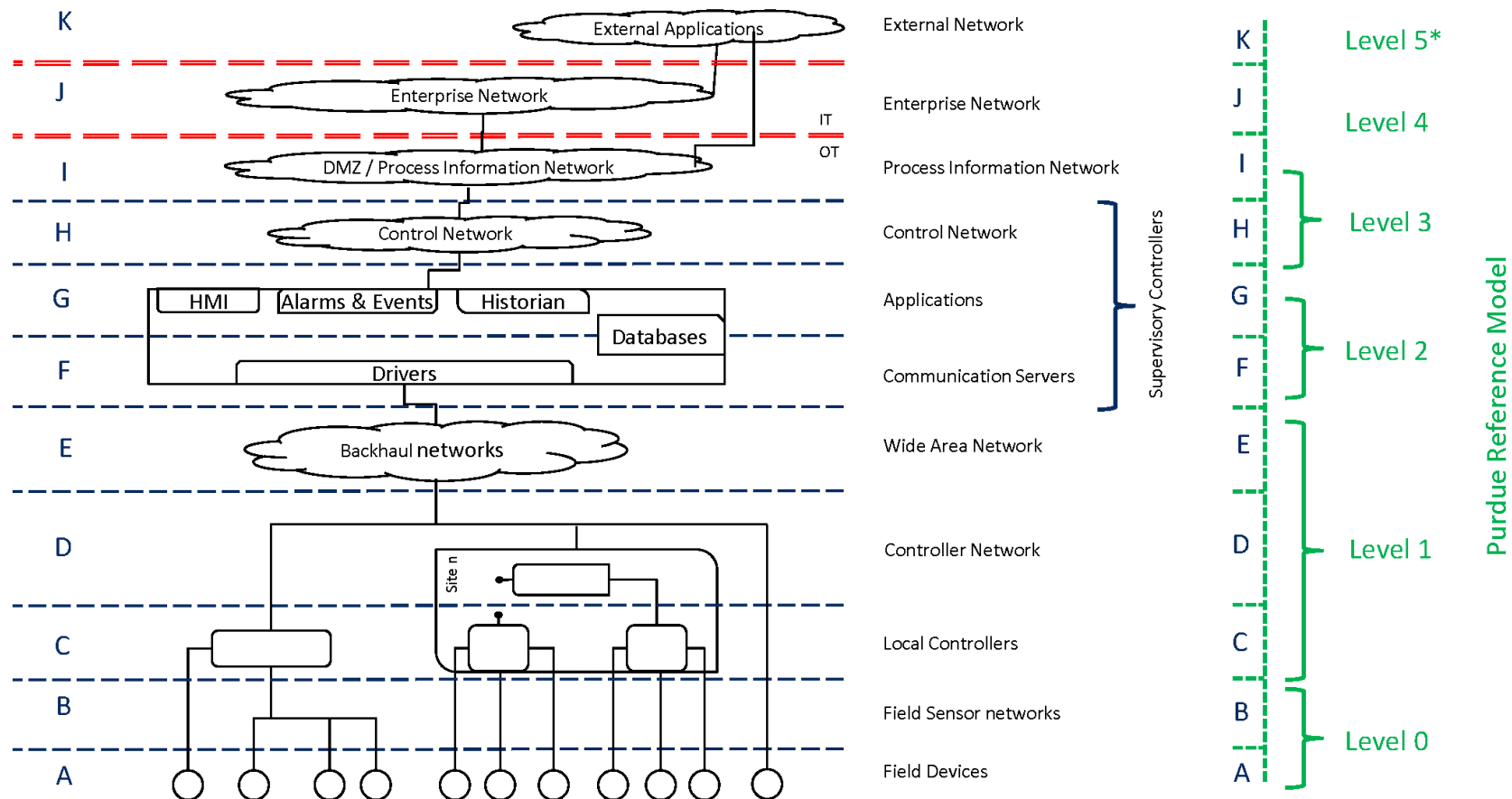
Notes:
1. Letters are used to avoid potential conflict with ISA-95 and other "Layer" models.
2. Routers and Firewalls between layers as well as other system-specific servers, applications ,and workstations are not shown.
3. Individual architectures may vary from the above general model. For example, if only local systems are used Level E may not be required
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.

Note: This is an interim working draft from the ISA112 SCADA Systems standards committee, as of 2022-01-26. (A previous version was posted on 2020-06-15). This diagram is still subject to change.

IT = Information Technology

OT = Operational Technology

SCADA Systems Lifecycle Diagram

CONTINUOUS WORK PROCESSES

a Governance	b Long Term Planning	c Security[1]	d Documentation	e Management Of Change (MOC)	f Verification	g Audit

New SCADA System, Major Changes Planned, or Regulatory Changes Needed — ENTRY

Planned Upgrade, New Site to be Added, or Change to System — ENTRY

1 SCADA SYSTEM STANDARDS

- a SCADA Philosophy
- b SCADA Availability / Reliability Guidelines
- c SCADA Platform Selection
- d Safety Standards
- e Security[1] Standards, Guidelines and Procedures
- f Network / Architecture Guide
- g Equipment I/O Interface Standard
- h Packaged Equipment I/O Interface Standard
- i Panel Design Standard
- j Field Wiring / Wire Labelling Standard
- k Data Point Tagging Standard
- l Equipment Tagging / Naming Standards
- m HMI Philosophy and HMI Style Guides (ISA101)
- Alarm Philosophy (ISA18.2)
- Event Processing, Logging and Messaging Guideline
- p Programming / Configuration Guides
- q Programming / Alarm / Configuration Templates
- Data Collection / Data Storage / Historian Guide
- SCADA to Business Integration / Data Sharing Philosophy
- Data Reporting Standards
- CAD / Drawing Standards
- Documentation Standards
- w MOC Procedures Document
- x System Environment Requirements[3]
- SCADA Work Procedures
- z Approved Equipment List
- aa Equipment Specification Templates
- bb Design Standards
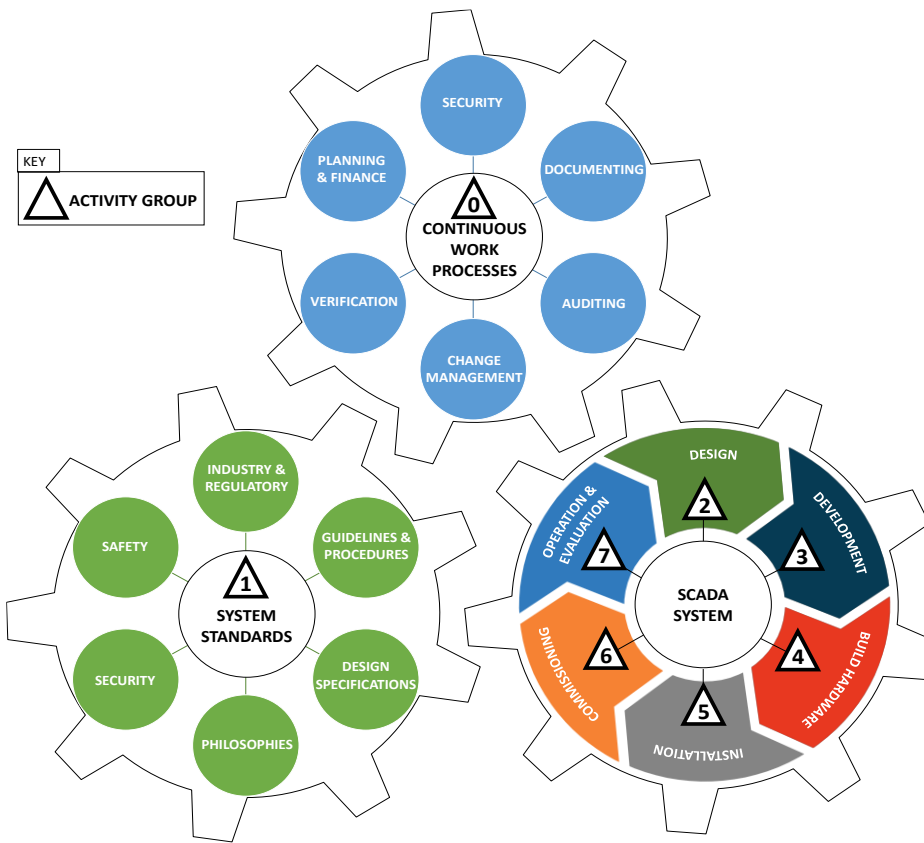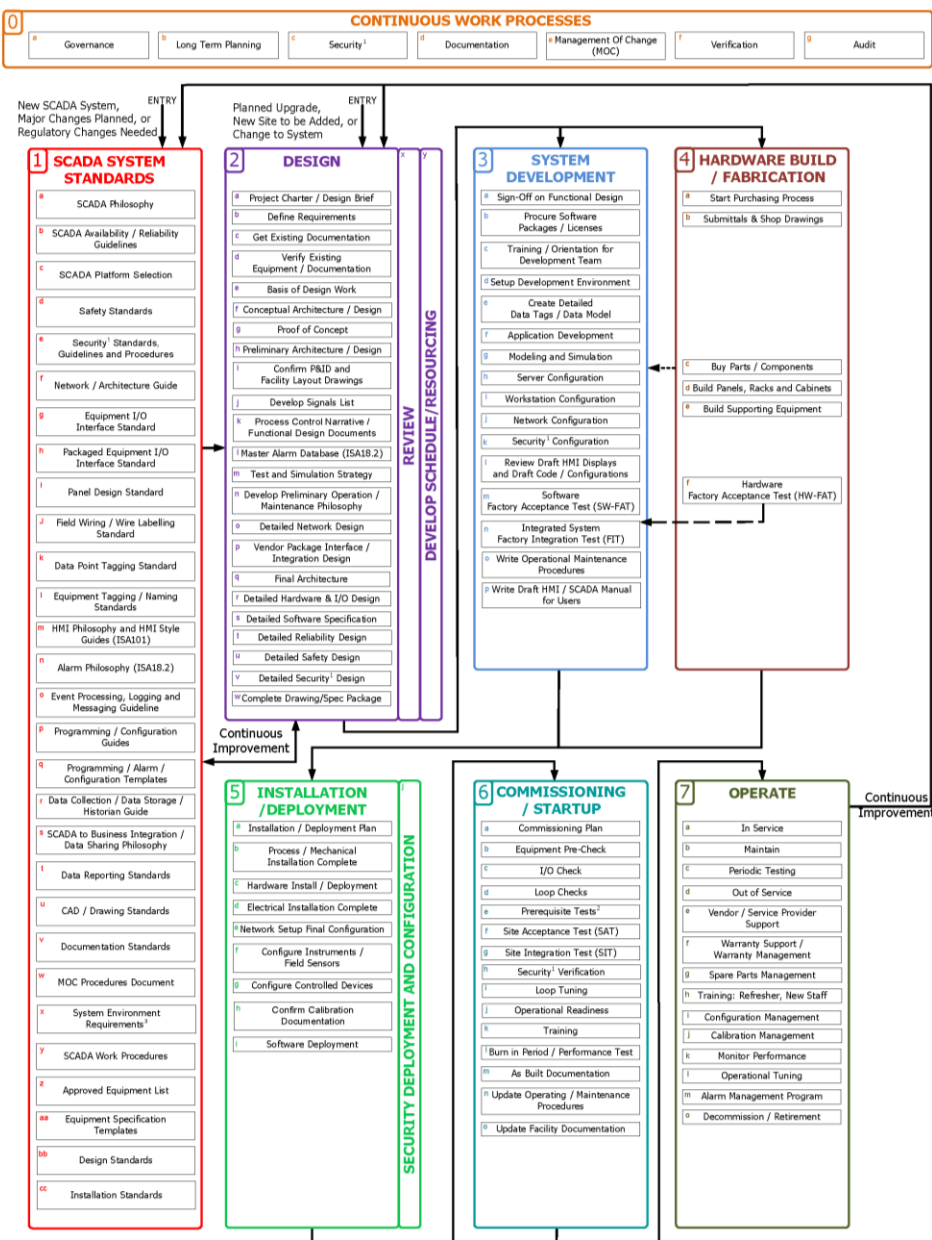- cc Installation Standards

2 DESIGN

- a Project Charter / Design Brief
- b Define Requirements
- c Get Existing Documentation
- d Verify Existing Equipment / Documentation
- e Basis of Design Work
- f Conceptual Architecture / Design
- g Proof of Concept
- h Preliminary Architecture / Design
- i Confirm P&ID and Facility Layout Drawings
- j Develop Signals List
- k Process Control Narrative / Functional Design Documents
- l Master Alarm Database (ISA18.2)
- m Test and Simulation Strategy
- n Develop Preliminary Operation / Maintenance Philosophy
- o Detailed Network Design
- p Vendor Package Interface / Integration Design
- q Final Architecture
- r Detailed Hardware & I/O Design
- s Detailed Software Specification
- t Detailed Reliability Design
- u Detailed Safety Design
- v Detailed Security[1] Design
- w Complete Drawing/Spec Package

REVIEW DEVELOP SCHEDULE/RESOURCING

Continuous Improvement

3 SYSTEM DEVELOPMENT

- a Sign-Off on Functional Design
- b Procure Software Packages / Licenses
- c Training / Orientation for Development Team
- d Setup Development Environment
- e Create Detailed Data Tags / Data Model
- f Application Development
- g Modeling and Simulation
- h Server Configuration
- i Workstation Configuration
- j Network Configuration
- k Security[1] Configuration
- l Review Draft HMI Displays and Draft Code / Configurations
- m Software Factory Acceptance Test (SW-FAT)
- n Integrated System Factory Integration Test (FIT)
- o Write Operational Maintenance Procedures
- p Write Draft HMI / SCADA Manual for Users

4 HARDWARE BUILD / FABRICATION

- a Start Purchasing Process
- b Submittals & Shop Drawings
- c Buy Parts / Components
- d Build Panels, Racks and Cabinets
- e Build Supporting Equipment
- f Hardware Factory Acceptance Test (HW-FAT)

5 INSTALLATION /DEPLOYMENT

- a Installation / Deployment Plan
- b Process / Mechanical Installation Complete
- c Hardware Install / Deployment
- d Electrical Installation Complete
- e Network Setup Final Configuration
- f Configure Instruments / Field Sensors
- g Configure Controlled Devices
- h Confirm Calibration Documentation
- i Software Deployment

SECURITY DEPLOYMENT AND CONFIGURATION

6 COMMISSIONING / STARTUP

- a Commissioning Plan
- b Equipment Pre-Check
- c I/O Check
- d Loop Checks
- e Prerequisite Tests[2]
- f Site Acceptance Test (SAT)
- g Site Integration Test (SIT)
- h Security[1] Verification
- i Loop Tuning
- j Operational Readiness
- k Training
- l Burn in Period / Performance Test
- m As Built Documentation
- n Update Operating / Maintenance Procedures
- o Update Facility Documentation

7 OPERATE

- a In Service
- b Maintain
- c Periodic Testing
- d Out of Service
- e Vendor / Service Provider Support
- f Warranty Support / Warranty Management
- g Spare Parts Management
- h Training: Refresher, New Staff
- i Configuration Management
- j Calibration Management
- k Monitor Performance
- l Operational Tuning
- m Alarm Management Program
- n Decommission / Retirement

Continuous Improvement

Notes
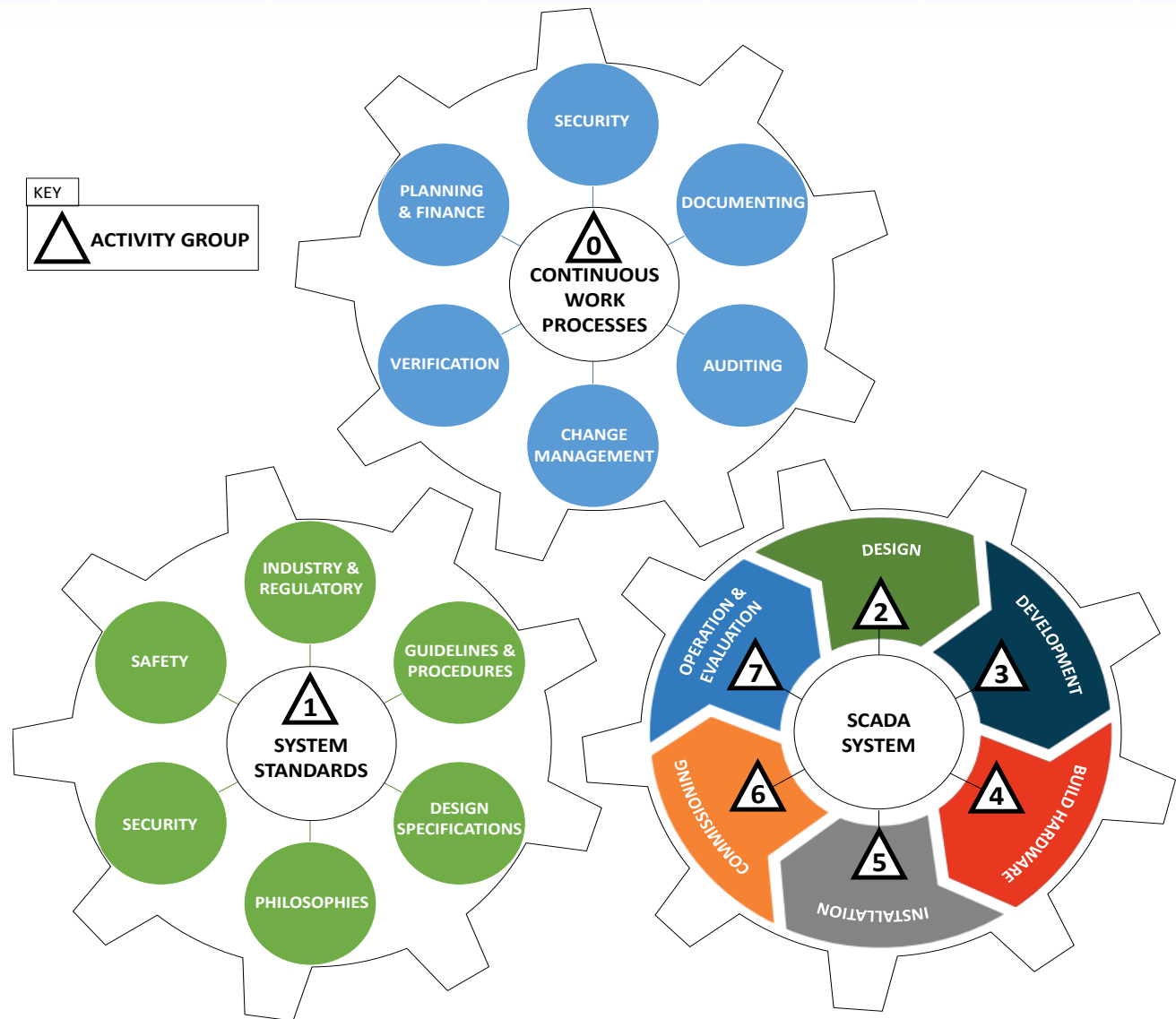1) Security includes physical security, operational security, and cybersecurity.
2) Prerequisite tests typically include both cold and hot commissioning or dry / wet commissioning as applicable.
3) System Environment Requirements can include separate systems for development, testing, training, production, backup, disaster recovery, digital twins, and other uses, as part of development and Management Of Change (MOC) procedures

Note: This is an interim working draft from the ISA112 SCADA Systems standards committee, as of 2022-07-08. (A previous version was released on 2020-06-15.) This diagram is still subject to change.

KEY — △ ACTIVITY GROUP

0 CONTINUOUS WORK PROCESSES: SECURITY, PLANNING & FINANCE, DOCUMENTING, VERIFICATION, AUDITING, CHANGE MANAGEMENT

1 SYSTEM STANDARDS: INDUSTRY & REGULATORY, SAFETY, GUIDELINES & PROCEDURES, SECURITY, DESIGN SPECIFICATIONS, PHILOSOPHIES

SCADA SYSTEM: 2 DESIGN, 3 DEVELOPMENT, 4 BUILD HARDWARE, 5 INSTALLATION, 6 COMMISSIONING, 7 OPERATION & EVALUATION

SCADA Systems Lifecycle Diagram

SCADA Lifecycle Activity Groups
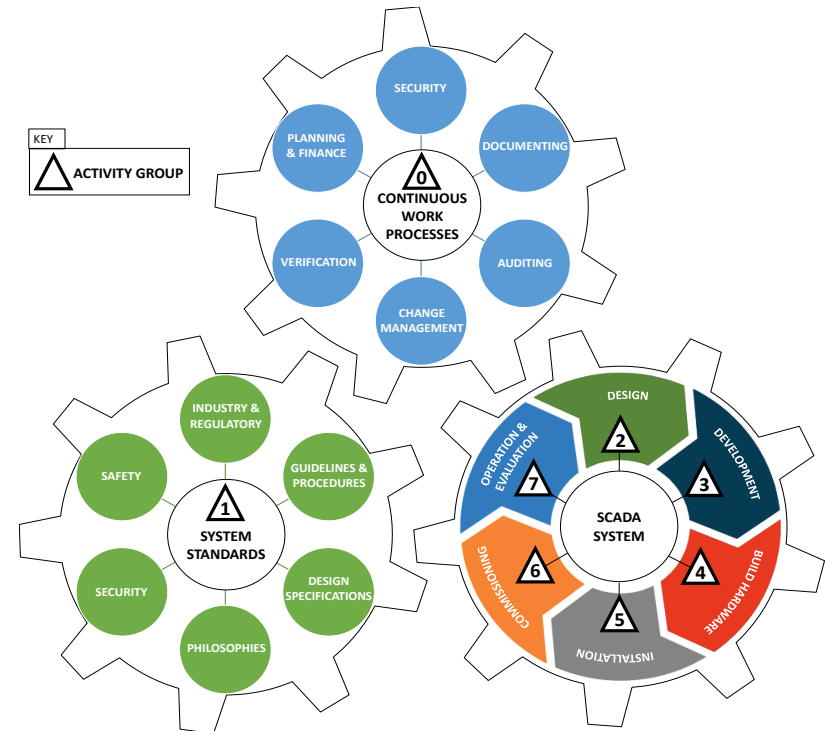
- **Continuous Work Processes**
  - Governance
  - Long Term Planning
  - Security
  - Documentation
  - Management of Change (MOC)
  - Verification
  - Audit

- **SCADA System Standards**

- **Design**
- **System Development (programming)**
- **Hardware Build / Fabrication**
- **Installation / Deployment**
- **Commissioning / Start-up**

- **Operate**
  - Operations
  - Maintenance
  - Monitor Performance
  - Operational Tuning
  - Minor Improvements
  - Alarm Management

SCADA Continuous Work Processes

0	CONTINUOUS WORK PROCESSES						
	a Governance	b Long Term Planning	c Security[1]	d Documentation	e Management Of Change (MOC)	f Verification	g Audit

Governance – defines who owns, uses, pays for, and maintains SCADA system
Requires a written SCADA Governance Policy doc endorsed by top management / board

Long Term Planning – Planning for 5, 10, 15, 20, 25+ year outlook
Some organizations may also use a SCADA Master Plan as part of their planning

Security – ongoing Physical Security, Operational Security and Cyber Security measures

Documentation – keeping system documentation up to date for operations and maintenance

Management of Change (MOC) – managing / controlling / documenting system changes

Verification – periodically checking that SCADA system is working the way it is documented

Audit – periodically checking that work processes are being followed and documented

SCADA System Standards – End-User Specific Standards

New SCADA System, Major Changes Planned, or Regulatory Changes Needed

ENTRY

1 SCADA SYSTEM STANDARDS

a	SCADA Philosophy
b	SCADA Availability / Reliability Guidelines
c	SCADA Platform Selection
d	Safety Standards
e	Security[1] Standards, Guidelines and Procedures
f	Network / Architecture Guide
g	Equipment I/O Interface Standard
h	Packaged Equipment I/O Interface Standard
i	Panel Design Standard
J	Field Wiring / Wire Labelling Standard
k	Data Point Tagging Standard
l	Equipment Tagging / Naming Standards
m	HMI Philosophy and HMI Style Guides (ISA101)
n	Alarm Philosophy (ISA18.2)
o	Event Processing, Logging and Messaging Guideline
p	Programming / Configuration Guides
q	Programming / Alarm / Configuration Templates
r	Data Collection / Data Storage / Historian Guide
s	SCADA to Business Integration / Data Sharing Philosophy
t	Data Reporting Standards
u	CAD / Drawing Standards
v	Documentation Standards
w	MOC Procedures Document
x	System Environment Requirements[3]
y	SCADA Work Procedures
z	Approved Equipment List
aa	Equipment Specification Templates
bb	Design Standards
cc	Installation Standards

SCADA Philosophy Document
SCADA Availability/Reliability Guideline
SCADA Platform Selection

Safety Standards (for automatic shutdown systems)
Security Standards, Guidelines and Procedures
Network / Architecture Guide

Equipment I/O Interface Standard
Packaged Equipment I/O Interface Standard
Panel Design Standard
Field Wiring / Wire Labelling Standard
Data Point Tagging Standard
Equipment Tagging / Naming Standards

HMI Philosophy and HMI Style Guides (ISA1010)
Alarm Philosophy (ISA18.2)

Event Processing, Logging and Messaging Guideline
Programming / Configuration Guides
Programming / Alarm / Configuration Templates
SCADA to Business Integration / Data Sharing Philosophy
Data Reporting Standards

CAD / Drawing Standards
Documentation Standards
MOC Procedures Document (Change Management)
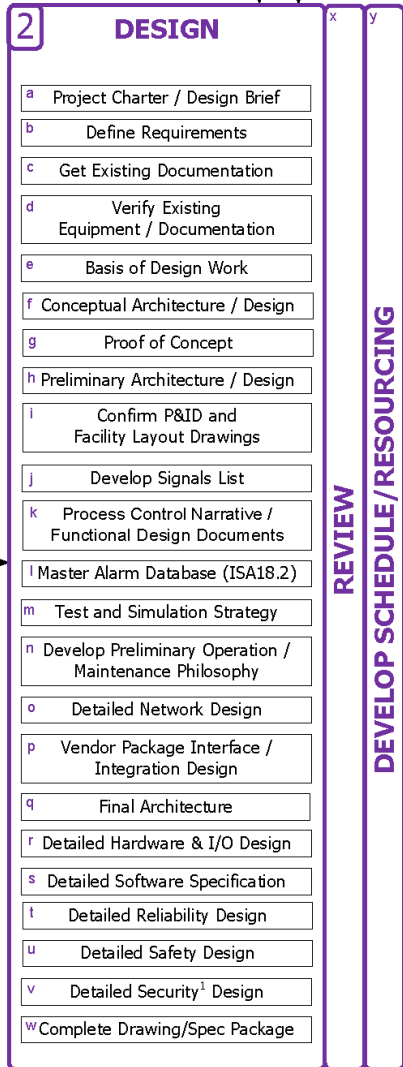System Environment Requirements

SCADA Work Procedures
Approved Equipment List
Equipment Specification Templates
Installation Standards

SCADA Design Work Processes

Planned Upgrade,
New Site to be Added, or
Change to System

ENTRY

Project Charter / Design Brief
Define Requirements

Get Existing Documentation
Verify Existing Equipment/Documentation

Basis of Design work
Conceptual Architecture/Design
Proof of Concept
Preliminary Architecture/Design

Confirm P&ID's and Facility Layout Drawings
Develop Signals List
Process Control Narrative / Functional Design Documents
Master Alarm Database (ISA18.2)
Test and Simulation Strategy
Develop Preliminary Operation / Maintenance Philosophy
Detailed Network Design
Vendor Package Interface/Integration Design
Final Architecture

Detailed Hardware & I/O Design
Detailed Software Specification
Detailed Reliability Design (UPS's, redundant equipment)
Detailed Safety Design (automatic shutdown systems)
Detailed Security Design (check of security & cyber security details)

Complete Drawing/Spec Package (for group that will do building / programming)

SCADA Programming & Hardware
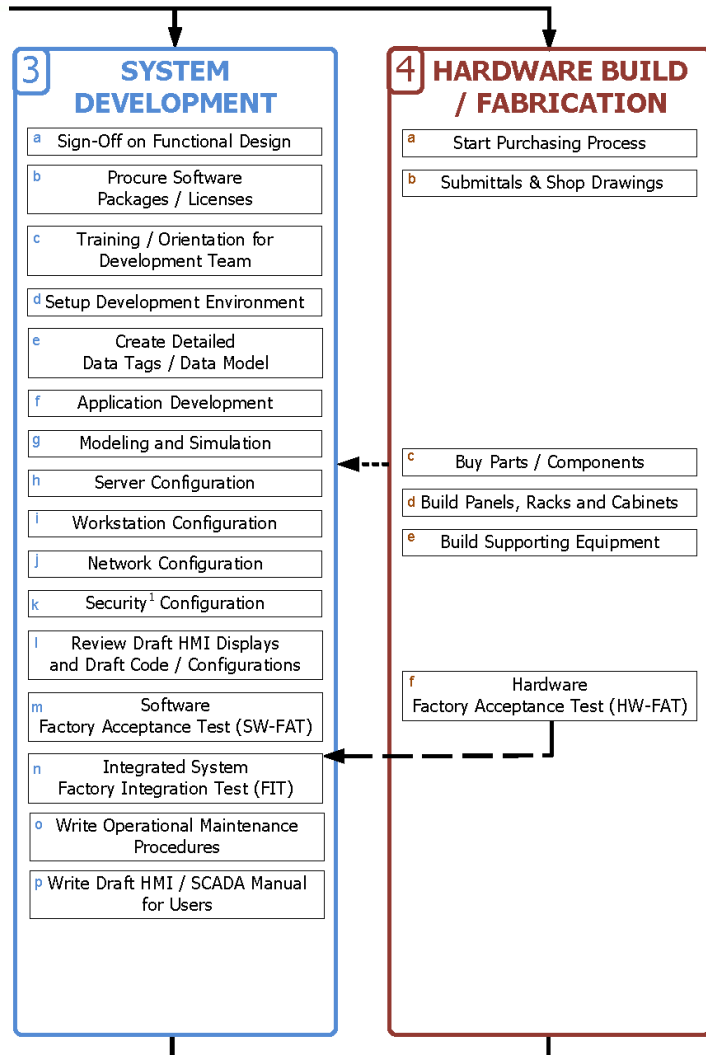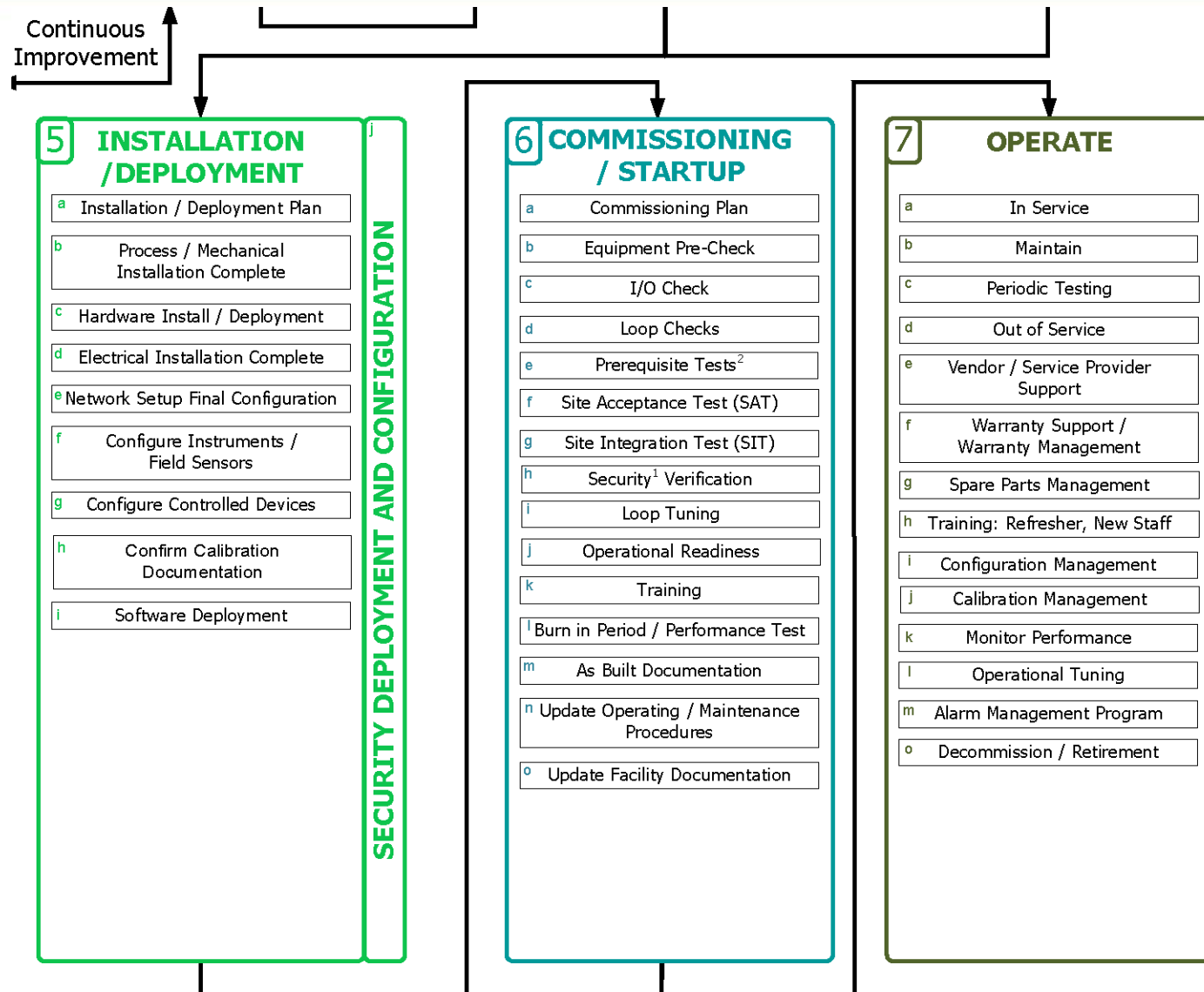

System Development

- Sign-Off Functional Design Doc (Process Control Narrative)

- Procure Software Packages / Licences
- Training / Orientation for Software Development Team
- Setup Development Environment
- Create Detailed Data Tags / Data Model
- Application Development (PLC & HMI Programming)
- Modelling and Simulation (to enable testing as they program)

- Server Configuration
- Workstation Configuration
- Network Configuration
- Security Configuration (check all security settings are right)

- Review Draft HMI Screens and Draft Code / Configurations
- Software Factory Acceptance Test (SW-FAT)
- Integrated System Factory Integration Test (FIT)
- Write Operational Procedures (how to use the control system)
- Write Draft HMI / SADA Manual for Users
- Develop Software Training Materials

Hardware Building / Fabrication (e.g., PLC panels & control consoles)
- Start Purchasing Process
- Shop Drawings / Submittals
- Buy Parts / Components
- Build Panels, Racks and Cabinets
- Build Supporting Equipment

- Hardware Factory Acceptance Test (HW-FAT)

SCADA Install, Commission, Operate

Continuous Improvement

5 INSTALLATION /DEPLOYMENT

a. Installation / Deployment Plan
b. Process / Mechanical Installation Complete
c. Hardware Install / Deployment
d. Electrical Installation Complete
e. Network Setup Final Configuration
f. Configure Instruments / Field Sensors
g. Configure Controlled Devices
h. Confirm Calibration Documentation
i. Software Deployment

j. SECURITY DEPLOYMENT AND CONFIGURATION

6 COMMISSIONING / STARTUP

a. Commissioning Plan
b. Equipment Pre-Check
c. I/O Check
d. Loop Checks
e. Prerequisite Tests[2]
f. Site Acceptance Test (SAT)
g. Site Integration Test (SIT)
h. Security[1] Verification
i. Loop Tuning
j. Operational Readiness
k. Training
l. Burn in Period / Performance Test
m. As Built Documentation
n. Update Operating / Maintenance Procedures
o. Update Facility Documentation

7 OPERATE

a. In Service
b. Maintain
c. Periodic Testing
d. Out of Service
e. Vendor / Service Provider Support
f. Warranty Support / Warranty Management
g. Spare Parts Management
h. Training: Refresher, New Staff
i. Configuration Management
j. Calibration Management
k. Monitor Performance
l. Operational Tuning
m. Alarm Management Program
o. Decommission / Retirement

ISA112 Current Work Plan

Jun 2016	Committee approved by ISA
Aug 2016	Initial call for volunteers (40 members)
Sept 2016	First meeting held in Newport Beach, California, USA
Jan 2017	Committee co-chairs named -Graham Nasby, originally with Guelph Water Services, now with CN Rail (Guelph, Ontario, Canada) -Ian Verhappen, originally with CIMA+, now with Willow Glen Systems (Calgary, Alberta, Canada)
Apr 2017	Monthly conference calls begin
May 2017	Second meeting in Raleigh, North Carolina, USA Semi-annual face-to-face meetings start
May 2018	Development of ISA112 Lifecycle & Architecture diagrams begins, drafts distributed to early-adopters
Nov 2018	Draft Table of Contents Developed
2019-2020	Writing Phase begins. 75 active authors contributing.
July 2020	First release of Draft ISA112 Management Lifecycle Diagram at www.isa.org/isa112 (free download)
2021-2022	Document Development / Section Working Groups As of 2021 we had 500 pages draft content, to be split between 3-part standard and technical reports.
July 2022	Release of Updated ISA112 Management Lifecycle Diagram at www.isa.org/isa112 (free download)
Nov 2022	Semi-annual face-to-face meetings resume after 3 year break due to pandemic. Monthly conference calls continue.
2022-2023	**Committee review/commenting rounds, going to final ballot in late 2023**
Early 2024	**Target publication date for Part 1: SCADA Management Lifecycle, Terminology & Diagrams**
2025-2026	Target dates for Part 2: Lifecycle Implementation & Part 3: SCADA System Architecture

ISA112 Publications

- www.isa.org/isa112
    - Freely available copy of ISA112 SCADA management lifecycle
    - Freely available copy of ISA112 SCADA model architecture
    - List of committee members, copies of presentations/articles, and other materials

- ISA112 upcoming publications
    - ISA112 Part 1– Terminology, Definitions & Lifecycle
    - ISA112 Part 2 – SCADA Systems Management Lifecycle
    - ISA112 Part 3 – SCADA Systems Model Architecture

- ISA112 Technical Reports
    - Titles and Topics TBD
    - To be focused on examples and best practices for "how" to implement SCADA systems
    - May be industry and/or application specific

More Information on ISA112

- www.isa.org/isa112/

- Download the current ISA112 lifecycle & diagrams

- Contact the committee co-chairs

  - Graham Nasby
    graham.nasby@grahamnasby.com

  - Ian Verhappen
    ian.verhappen@willowglensystems.com

The ISA112 committee is still actively looking for volunteers from end-users, vendors, system integrators, consultants, utilities, and government entities to help with writing, editing, and reviewing content.
To join the committee or to get involved, feel free to contact Graham or Ian by email. If your organization would like to know more about ISA112, Graham can also give an online presentation on request.