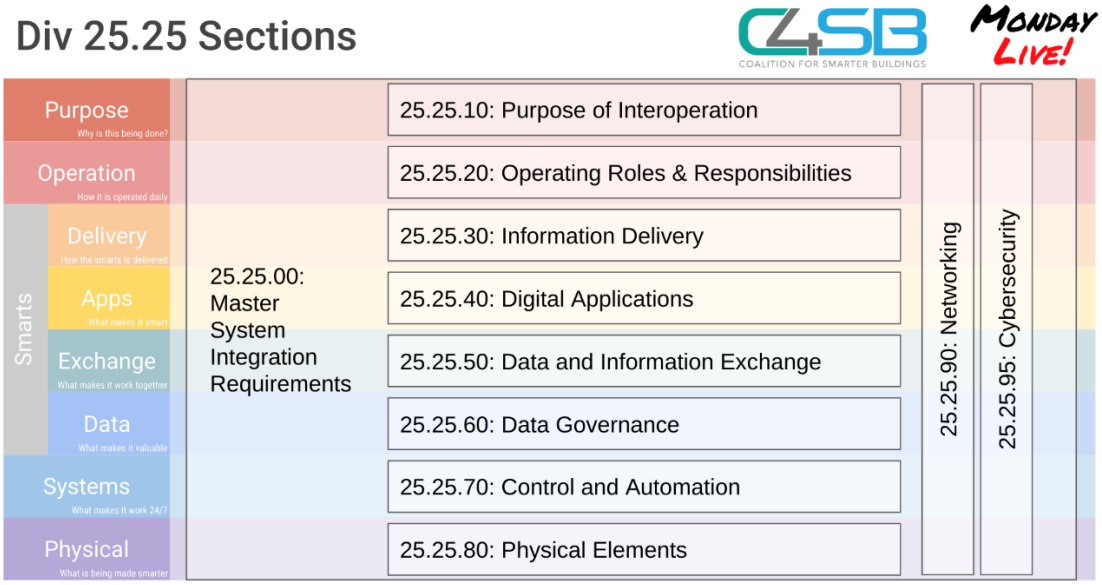


DIV 25.25 – Interoperability Framework for Smarter Buildings

A Smarter Building resource from

The Coalition for Smarter Buildings and **MondayLive!**

c4sb.org mondaylive.org

version 1.02

July 25, 2023

This page intentionally left blank

Table of Contents

Preface: How to Use this Document

This Framework is Open Source: Free to Use. Free to Contribute.

P.1 Free to Use.

This framework document and other DIV2525 material are free to use. These are made available via an open-source license [Creative Commons 4.0: https://creativecommons.org/licenses/by/4.0/.] That means anyone can use it, adopt it, apply it, or build upon it for their own buildings, projects, products, or services, as long as there is attribution to the C4SB DIV2525 project. We hope this happens. We want the building industry to be smarter, to widely adopt these principles, and for everyone to benefit from interoperable data for buildings.

The document was created by a group within the Coalition for Smarter Buildings and MondayLive! – industry experts with experience delivering connected building solutions to local and global clients, large and small. The team has run into many, many challenges along the way, and envisions better ways of doing things that are not only possible, but necessary, if widespread adoption of smarter building solutions, and the value that they can deliver, is going to happen.

P.2 Free to Contribute.

The Coalition for Smarter Buildings is a community of people passionate about promoting the adoption of smarter building technology worldwide. As part of that effort, documents and resources are collected, developed, and distributed on a voluntary basis. The quality and usefulness of these resources depends on the contributions of people who are willing to share their knowledge and experience.

MondayLive! is an open ecosystem of industry contributors who exchange information, ideas, approaches, and best practices that help the built environment advance to be smarter and enhance value.

If you have suggestions for this document, samples or templates of useful resources, or other ideas you would like to contribute, please let us know at div2525@c4sb.org.

P.3 How to Get Started

- Read It. Consider the questions and topics posed in each section: are they valuable for your project? If you don't understand why a particular point might be important, ask one of the contributors listed below, or email us at div2525@c4sb.org.
- Adopt and adapt It. Give this to your project manager(s) and design professionals (or do this yourself) and have them apply your answers to the questions to your project. Make the outline specific to your goals, your portfolio, your building systems, and your project. Have them (or you) Save a Copy As… "[Your Building(s)] Smarter Building Project Requirements."

- Bless It. As an owner, you should officially endorse the results of applying this framework to your project in the form of Owner's Project Requirements or Basis of Design. Then let stakeholders review it, and get their consensus and buy in.
- Distribute It. Give your project-specific Smarter Building Project Requirements to the staff, contractors or vendors who will be doing the work.
- Check On It. Follow up with your vendors. Make sure they understand why you are making your building smarter. Make sure they know how what they are doing fits into the overall plan. Make sure they talk to your other staff and vendors supplying or running systems that they will interact with. Make sure it works together!

Expert Tip/Best practice: Once you have adapted this framework to reflect the requirements of your project, share it with your design team and vendors as a DIV2525 Smarter Building Owner's Project Requirements or DIV2525 Smarter Building Basis of Design document.

Expert Tip/Best practice: Once you have adapted this framework to reflect the requirements of your project, create a DIV2525 Smarter Building Contractor's Project Responsibilities Matrix to organize the areas of responsibility for each vendor, making clear which deliverables should come from which supplier, where there are shared responsibilities, and who has oversight and approval. For each task or section, would describe who is/needs to be: Responsible, Accountable, Supported, +-Consulted, and Informed (RASCI).

Contributors

This DIV 25.25 Framework was created by volunteers with deep experience designing and delivering smarter building solutions. If you have contributed to this effort or would like to, and want to be included on this list, please let us know at div2525@c4sb.org.

Writing and Editing Team

Ron Bernstein

Anto Budiardjo

Tristan de Frondeville

Steve Fey

Michael MacMahon

Peter Scanlon

David Wilts

Contributors and Reviewers

Ernie Beck

Bill Behn

Rolf Bienert

Rich Blomseth

Charlie Buscarino

Robbie Danko

Don Elder

Gina Elliott

Neil Gifford

Fred Gordy

Terry Herr

John Huston

Scott Hoffman

Rick Justis

David Kniepkamp

Brad Kult

Jim Lee

Tracy Markie

Marc Petock

John Petze

Andrew Rogers

Ken Sinclair

Anno Scholten

Craig Stevenson

Matthew Turk

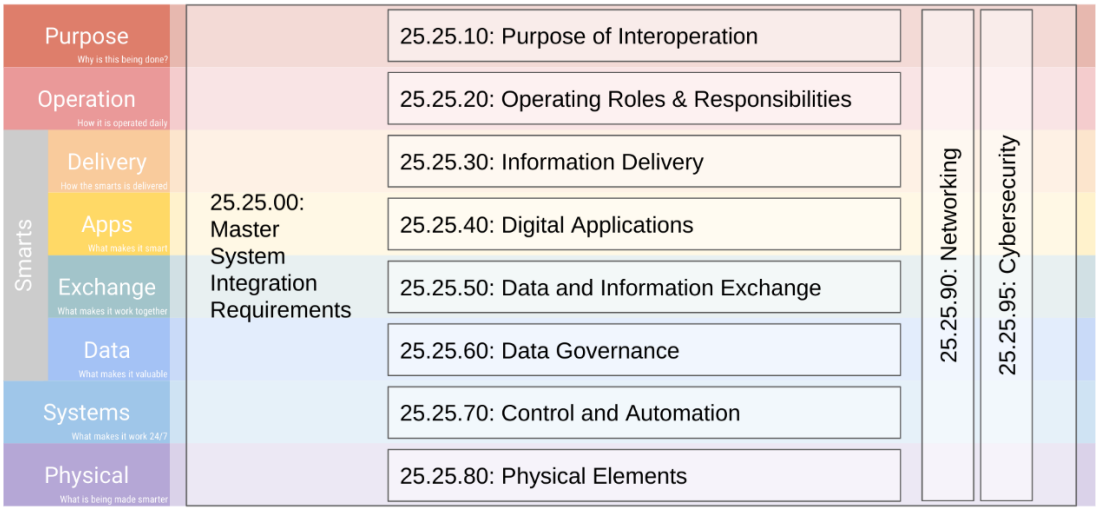
Mark Verheyen

Ben Wallace

Roger Woodward

This page intentionally left blank

Div 25.25 Sections



DIV 25.25 – Interoperability Framework for Smarter Buildings

Introduction

This Framework outlines the purpose and operational requirements for enabling data and operational interoperability in Smarter Buildings.

What is a Smarter Building?

For our purposes, a building can be called "smarter" if its building systems' data are interoperable and interconnected, to enable monitoring, verification, operation, and control, using a unified data architecture where data from one system can be exchanged with other systems as well as higher level business applications, services, and tools.

Simply put, Smarter Buildings enable buildings to provide greater comfort and productivity for occupants, greater visibility and control for the operations and management teams, and lower costs, better business outcomes, and higher value for owners.

Division 25.25 is a part of the project specification process that can be used to describe how to facilitate the collecting, exchange, and use, over time, of data across multiple building systems, enabling owners to make their buildings smarter and achieve goals such as sustainability, lower total cost of ownership, higher operational efficiency, and a better user experience.

Owners and operators of buildings, whether building, retrofitting, or operating them, should consider these requirements and incorporate them into their building's design, construction, and operations. Getting the most out of your "smarter" buildings can be complicated, but being proactive as early as possible (ideally when you start to imagine your next project) maximizes the potential value while keeping the costs of doing so as low as possible. Following this guide can help organize and inform your team so that you get what you, your operators, and your occupants want/need, you reduce confusion and change orders, and you end up future-ready for unknown things to come.

Note that some terms have multiple meanings in the industry and other terms are used interchangeably. This document strives to be consistent with accepted terminology as used by ASHRAE, AIA, CSI, NIST and others. A Glossary will be included with future versions.

Intro.1 Intended Use & Audience

This Framework document is intended to be used by owners, developers, design engineers, and project managers, for describing the design intent of a smarter building project. This group can use and adapt the DIV 25.25 Framework for their specific project, and give the resulting document (often called the Owner's Project Requirements (OPR) or Owner's Design Requirements (ODR) or the Basis of Design) to specifying engineers, contractors, and vendors who will be designing and bidding on or providing the necessary products and services.

The Framework can also be useful for system integrators, contractors and suppliers of products and services to the building industry to help them describe their offerings in the context of how they help make a smarter building work.

Intro.2 Why DIV 25.25?

The construction industry in the United States generally follows a guideline for project documents from the Construction Specification Institute (CSI) which organizes the various trades of a project into specific divisions of responsibility (and numbering system) called CSI MasterFormat (www.csiresources.org). CSI MasterFormat provides a foundation for defining project design, specification, and contracting responsibilities.

Consulting engineers writing project specifications develop the required documents following the CSI MasterFormat, helping vendors bid on work aligned with their firm's expertise. For example, Plumbing is DIV 22, HVAC is DIV 23, Electrical is DIV 26, etc.

Division 25 is part of the CSI Master Format and is labeled "Integrated Automation." It includes details for how all of the building's systems are to be integrated into a common building management system (BMS), data set requirements or "Points Lists," database development, site nomenclature, supervisory and programmable controls hardware and software, the operator user interface or "front end," and the building control system interface to "other services." These other services include both on premises and cloud-based (Internet) tools and applications such as analytics applications, reporting, energy management, remote monitoring, asset management, work order processing, alarming and alerting, and much more.

DIV 25.25 Master System Interoperation Requirements

The work of this group proposes designating a section of DIV 25 to focus on specifying details about system and data interoperability. This includes interfaces between the various supporting tools and applications, the actual control network, and the building IT network (if applicable). We propose using DIV 25.25, a sub-section which is not defined within the current CSI MasterFormat, for this purpose.

The proposed DIV 25.25 section utilizes a "Smarter Stack" (described below) to identify specific subsections and their associated interoperability and design requirements.

This effort is in the hope of improving the design of smart buildings by taking advantage of good design practices, including the latest technology trends, and helping coordinate the roles and responsibilities of the key stakeholders of a project.

As a building owner, whether or not you are procuring your project through a general contractor and a CSI-MasterFormat-based bidding process, you can use this framework to describe what you want in an organized structure where contractors can understand what role you are asking them to perform and how that role is connected to what else is going on in the building.

Likewise, contractors can use this framework to describe the parts that they provide, so it is clear what comes from them and what will need to come from others.

Intro.3 Who should be in charge? DIV 25 Contractors and the MSI Role

Smart building DIV 25 contracts are typically bid on by Controls Contractors, System Integrators, and, more commonly today, Master Systems Integrators (MSIs), whose knowledge and expertise span the many disciplines required for complex building integration. There is an increasing convergence of control networks in the building systems operational technology (OT) domain with the informational technology (IT) domain, so DIV 25 contractors must be well versed in IT technology, systems, and practices. Furthermore, DIV 25 contractors must have extensive knowledge of data, data systems, communications, cybersecurity, and related fields.

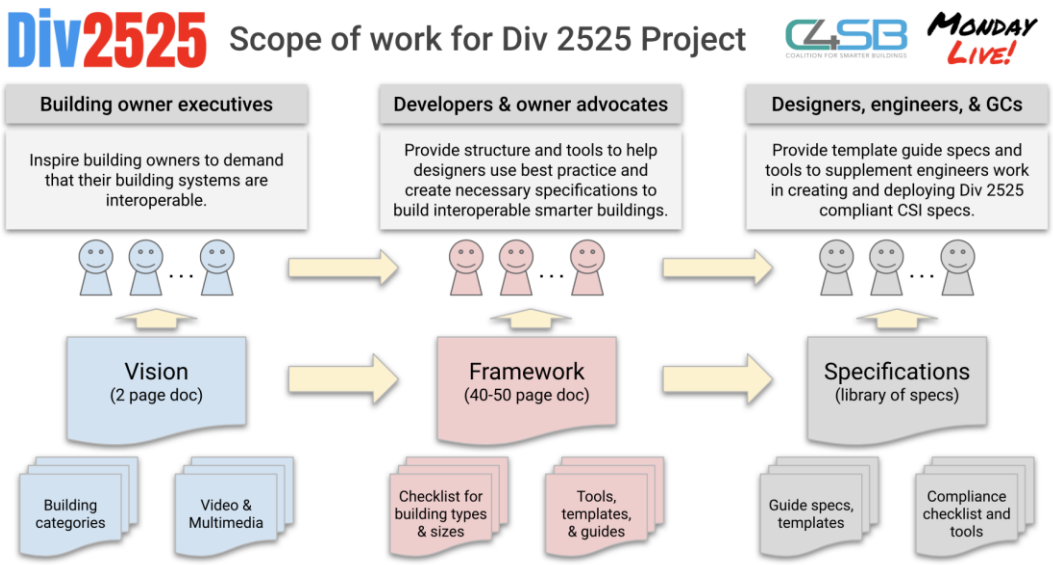
For the purposes of this document, we use "MSI" to mean the party responsible for the whole smarter building solution. The MSI may be an outside contractor, or a role filled by someone in the owner's organization.

Expert Tip: Create a Contractor's Project Responsibilities Matrix to organize the areas of responsibility for each vendor, making clear which deliverables should come from which supplier, where there are shared responsibilities, and who has oversight and approval.

Intro.4 How does this Framework fit with other resources?

The Coalition for Smarter Buildings is developing a series of resources for owners, operators, and occupants of buildings to better understand, implement, and enjoy the benefits of smarter building solutions.

Figure 1. Smarter Building Resources from the Coalition for Smarter Buildings



Intro.4.1 DIV2525 Vision

The **DIV2525 Vision** document (link below) lays out for building owners and developers the reasons why making building data interoperable can make buildings, and the occupants' experience in them, more valuable by improving occupant well-being, safety, and convenience, while reducing labor, energy costs, and greenhouse gas emissions, harnessing renewable energy sources, and managing cybersecurity risks. [https://vision.div2525.org]

Intro.4.2 DIV2525 Framework

This **DIV2525 Framework** document outlines for owners, their project managers and design consultants, the design principles necessary for connecting buildings and their systems in a unified way and at an affordable price. For each topic area,

the Framework poses questions to consider in order to make the design intent of the project clear. [https://framework.div2525.org]

Intro.4.3 Division 25.25 Specifications

The Coalition is developing resources for **Division 25.25 Specifications**, which include templates and examples for smarter buildings with different goals, uses, systems and complexity as well as additional resources from standards bodies and industry. The specifications are what contractors and vendors would comply with when bidding on and executing a specific project. Resources provided here could be used as a generalized spec, or more likely would need to be adapted by the owner's project manager or design professionals to the specific situation of a building or project.

Intro.5 Applicable to All Building Types and Sizes and Portfolios

The principles outlined in this Framework are intended to be beneficial for connecting data for all buildings, regardless of their scale, quantity, intended use, or complexity.

Intro.5.1 Single or Multiple Buildings

Making data interoperable can help increase the efficiency of a single building, and can greatly increase efficiency when implemented across a portfolio of buildings. For example, integrating multiple subsystems such as HVAC, lighting, security, energy- and power-metering, within a single building provides the owner with greater efficiencies for operational staff such as a unified user interface for monitoring and alarming of the building. It may also provide secure remote access for small, unstaffed buildings and access for service providers that provide 24/7 monitoring services.

Intro.5.2 Small and Large Buildings & Projects

Owners/operators of smaller buildings, simpler systems, or with limited project budgets will likely use a limited number of integrated systems, but installing interoperable systems will allow greater future flexibility even if Day One integrations are minimal. By adopting this method and implementing interoperable systems consistent with this framework the value of the data and the building(s) can greatly multiply, especially in the future as more systems are interconnected. Owners/ operators of larger or more complex buildings who want to maximize the value of interoperable data will benefit from following the framework to connect most or all of their building systems and data, making information from one system useful to all others.

Intro.5.3 Various Building Types

Different building types have different systems that are important to their operation and occupant experience, so the exact list of systems that will be valuable to connect will vary. But no matter which or how many systems are connected, it is important to have a common way of connecting, communicating, storing, sharing, and using data across all systems.

The DIV 25.25 specification is anticipated to be adopted mostly by commercial and institutional building owners and specifiers (not single-family residential or industrial), including owner-occupied buildings, campuses, multi-tenant (usually 4+ units) residential properties, and mixed-use facilities.

The foundation of integrated automation for building controls has its roots in the industrial sector, however industrial facilities such as manufacturing plants typically require significant process and facility integration, and much tighter regulatory and code requirements, which is beyond the scope covered in this framework.

Intro.6 Fundamentals of Integration: Be Inter-Connected

When starting down the path of making your buildings smarter, a foundational step is digitally connecting all the required equipment, devices and spaces so that your users can see and interact with the information they need to do their jobs or have the occupant experience they expect.

Intro.6.1 Access Onsite and Remotely

Buildings are inherently physical, and much of their data is associated with location-based sensors, actuators, and specific pieces of equipment (occupancy, temperature, pressure, flow, alarm, etc.). But access to the data doesn't have to be location-specific. Making data from systems interoperable within a building (or campus/ portfolio) enables unified management, whether accessed just onsite or remotely, and whether accessed for a single building or aggregated across a campus or portfolio of buildings.

Today, most users of smarter building data expect access via a connected mobile or desktop device. In most cases, connecting data to user devices and applications is done via the Internet (often referred to as "the cloud"), which allows users to see and interact with the building both onsite and remotely, so the location of the user doesn't matter. But in some buildings, due to the owner's policy or for security reasons, data access is limited to users with devices connected directly to the onsite data network or, for campuses, connected via a private, dedicated network, such using a VPN (Virtual Private Network.) *

*Note: This document assumes that the building(s) has/have an existing IT infrastructure (data network) that is supported by the owner. In most cases, this is an Ethernet IP-based, Internet-connected data network. See Section 25.25.90.

Intro.6.2 Converging Operational Technology (OT) and Information Technology (IT)

Smarter Buildings require that all controls equipment and their data are on a common network where data can be exchanged.

Having open and managed data exchange between systems is often the biggest challenge in the creation of a smarter digital building. Well managed and secure data exchange between systems via Internet protocol (IP)-based OT and IT networks is fundamental for a smarter digital building. In most projects, enabling systems to have interoperability is very challenging because of the historical lack of convergence between OT and IT systems. Simply put, building systems have, until recently, been stand-alone, operated on proprietary or air-gapped networks and thus unable to share data. As a result, interoperability was not achievable as information

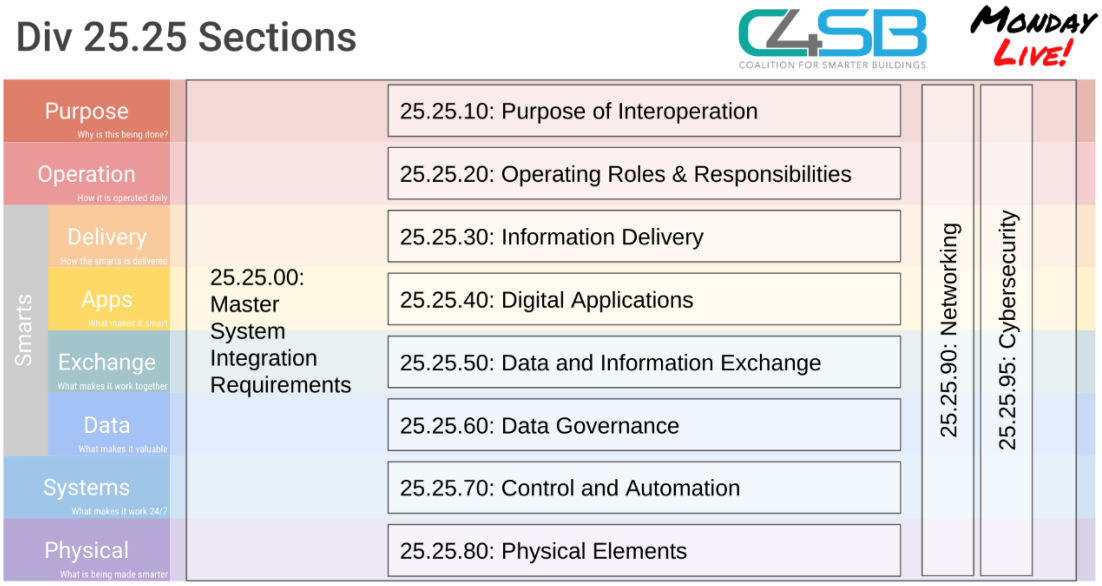
could be exchanged on a common IT local area network (LAN). In many cases the building owner does not even have an IT department and, for leased space facilities, tenants each have their own networks in their respective spaces which are not connected to the landlord's network or each other.

Overcoming this challenge and determining the most appropriate network topology and provisioning is typically the hardest task in realizing these goals. Section 25.25.90 – Networking provides an overview of different network topology architectures for consideration. Determining, and having stakeholders agree to, the chosen topology architecture allows all of the other requirements to fall into place.

Intro.7 How the Framework Is Organized: The Smarter Stack

The sections of this framework follow those presented by the Coalition for Smarter Buildings and MondayLive! in The Smarter Stack, which outlines the layers of products, services, architecture, policies, and responsibilities necessary to make a building "smarter."

Figure 2. The Smarter Stack



This document provides information for each section with guidance on how to apply the requirements. It is important to understand how each section builds upon the others. To effectively use this framework and apply the stack, the project designer must understand and address all of the sections.

There are (11) total sections in the stack – (8) "horizontal" sections and (3) cross cutting sections:

- **25.25.00 Master Systems Interoperation Requirements:** This cross-cutting section discusses the contractual, technical and project management requirements to deliver a fully integrated smarter building. It usually includes a Contractor's Project Responsibilities Matrix that defines, for the project construction and installation process, who has what responsibilities when it comes to integration of the physical systems with an interoperable data structure, and what the expected Deliverables are.

- **25.25.10 Purpose of Interoperation:** Section 25.25.10 lays out the owner's project-specific goals for having interoperable data and a smarter building. It would include foundational information that establishes the project objectives for data integration, interoperability, access, enterprise access, and general technical objectives.
- **25.25.20 Operating Roles & Responsibilities:** Section 25.25.20 describes who will use the information presented in the Section 25.25.30 Information Delivery layer, in order to achieve the Section 25.25.10 Purposes identified for the building or project. Section 20 defines who are the user groups (when the building is operating), and what are their needs relative to the building(s). It can include defining personas, process flow charts, user needs, user skill sets, and (for staff) training/career paths.
- **25.25.30 Information Delivery:** Section 25.25.30 provides requirements associated with how actionable information is delivered across systems, buildings, and the enterprise from the Section 25.25.40 Applications to the people/roles defined in Section 25.25.20. Section 30 defines the digital devices (such as mobile, wearable, laptop, desktop), user interfaces (UIs), front-facing apps, machine-to-machine (M2M) connections, or other methods that present ways for users to interact with the digital information. This section is also the place to discuss how separate data applications need to work and be presented together to deliver functionality not possible in one application alone.
- **25.25.40 Applications:** Section 25.25.40 is about the software applications that use data from the building and external sources to provide actionable information to the user. It lays out how applications are to co-exist within the building environment, and how data is used and retained for use by the applications. Applications may also provide control logic, machine learning, administration of systems, and additional management capabilities. The application layer should provide software developers with the key requirements for developing interoperable applications.
- **25.25.50 Data and Information Exchange:** Section 25.25.50 relates to the movement of Data and Information between applications, systems, storage, and users. It outlines the technical attributes of common, interoperable system data and how data is exchanged, normalized, and converted within and between applications. Topics include naming conventions, data typing (International System of Units (SI) vs Imperial Units (IU)) and structure, semantic tagging, API requirements including documentation and behavior, and additional details relating to how data moves between applications and data sources.
- **25.25.60 Data Governance:** Section 25.25.60 outlines the project's governance (policy) requirements for data ownership, format, context, temporal and spatial structure, naming conventions, storage (hardware and software), database structure, access, continuity, and data security and privacy.
- **25.25.70 Control Systems:** Section 25.25.70 defines the control and automation systems that connect to the physical elements listed in section 25.25.80, and that provide "built in" controls and the digital communication bridge to other components of the same system, as well as to other systems, applications, buildings, or entities outside of the portfolio. Topics include data required for meeting sequences of operation, the control automation platform requirements, and how each control system supplies data to higher level applications.
- **25.25.80 Physical Elements:** Section 25.25.80 should be used to describe the physical elements of your project/building/portfolio – the actual devices and spaces – that the digital smarter building system will connect to, monitor, control or interact with. This section can also be used to articulate what needs "smarter" functionality and what does not.

- **25.25.90 Networking:** Section 25.25.90 is a cross-cutting section, supporting all of the above sections, and addresses the physical means of transporting digital communications for building systems and their associated components. Such a digital network would include the server(s), cabling, routers and other related hardware and software.
- **25.25.95 Cybersecurity:** Section 25.25.95 is a cross-cutting section discussing risks, assessment strategies, and design of cybersecurity best practices for OT systems. This section presents basic, moderate, and advanced suggestions for managing cybersecurity risks both at the physical security and the logical security levels for OT building systems along with guidance for working within and alongside IT based infrastructures.

The rest of this document provides an overview and details for each of the DIV 25.25 sections.

25.25.00 – Master System Integration Requirements

This crosscutting section discusses the contractual, technical and project management requirements to deliver a fully integrated, smarter building. It usually includes a Project Responsibilities Matrix that defines, for the project construction and installation process, who has what responsibilities when it comes to integration of the physical systems with an interoperable data structure, and what the expected Deliverables are.

A key role to designate is who is the overall manager of making the smarter building systems work, which we refer to as the Master Systems Integrator (MSI), who can be a vendor or an owner's project manager.

This section includes:

- Operational Responsibilities
- General Requirements for Interoperability
- Project Management Guidance and Tips

00.1 Operational Responsibilities

Division 25 Integrated Automation, by its nature, requires coordination and responsibility for integrating the various systems, components, applications, and interfaces into a common infrastructure and management system. Contractually, the role of the Master Systems Integrator has emerged as the mechanism for achieving the integration goals. This, of course, is project dependent, where smaller projects with minimal integration may choose to have a mechanical contractor's controls group or "Controls Contractor" perform this work. This is valid when primarily the only systems to integrate fall under the Division 23 Mechanical Systems or use traditional integration methods defined by ASHRAE. Mechanical systems tend to be more complex, have more unique suppliers, and require advanced sequences of operation running in programmable controllers. To deploy these systems, controls contractors have developed the subject matter expertise to implement building OT control networks, install the BMS front end, and provide the owner with operational and maintenance interfaces. Thus, many advanced Division 23 controls contractors are well-versed in deploying smaller integrated projects using traditional building systems when properly designed and scoped.

But once the project requirements extend beyond this scope, expertise is needed across many divisions and systems. Hence the MSI (Master Systems Integrator) role has emerged. A well-qualified MSI will have experience and expertise to install, configure, and coordinate with various stakeholders and contractors to implement interoperable control systems and IoT offerings. Furthermore, an MSI has the expertise to partner with the Owner's IT teams to provide holistic integrated solutions implementing Owner-prescribed cybersecurity policies. (See Section 25.25.95.) An MSI requires extensive knowledge of IT infrastructure requirements, including Ethernet cabling, IP ports, hubs, switches, and routers. On the logical/data side, the MSI is typically responsible for setting up the Owner's Unified Graphical User Interface (GUI) and the Building Management System front end, services, backup procedures, graphics, and data point integration. For more complex, advanced projects, creating a site nomenclature, points lists, semantic interoperability, site database, API interface integration, and cloud services integration may be required.

The MSI role is most often a direct-to-owner relationship, as is the IT contractor, and extends beyond any one specific contractual project. However, if an owner does not have an MSI in place or there is a new project, the MSI contract can be bid under the General Contractor. Then, once the project is complete, the MSI may shift to a support role direct to the owner. There are multiple options here and for whom the MSI works is project dependent.

00.2 General Requirements for Interoperability

As an introduction to what is covered in sections that follow, typical data integration requirements associated with the 25.25 scope include how to:

A. Manage data and information access across all project integrated system domains (sec 00)

B. Support consulting engineering during a design assist phase to ensure owners requirements are achievable and within budget (sec 00)

C. Provide design drawings, as-builts, data maps, database structures (sec 00)

D. Review subsystem submittals for integration requirements and compliance to owners' requirements (sec 00)

E. Integrate APIs into the common user interface(s), which could include a "Single Pane of Glass (SPoG)" or BMS front end (sec 30)

F. Define remote access to building system data (sec 30)

G. Develop owner visualization requirements, including color coding, style, layout, workflow, reporting, etc. (sec 30)

H. Orchestration of interoperable systems (sec 40)

I. Define and implement equipment alarming, alerting, and visualizations (sec 30 and sec 40)

J. Define API integration requirements for cloud/web services (sec 50)

K. Develop and manage database structure, software, and tools (sec 60)

L. Define the site data nomenclature including tagging, naming, context, location, and interval requirements (sec 60)

M. Develop IT integration requirements (sec 00, 30, 90) in coordination with owner IT for data availability, access, restrictions, active directory, single-sign-on (SSO), password policies, onboarding, offboarding, intrusion alerting, product security compliance, and more.

N. Provide cybersecurity plan for OT systems in coordination with owner IT (sec 95)

00.3 Project Management Guidance and Tips

The following general guidance and tips are offered to help owners and engineers successfully navigate the MSI responsibilities:

A. When engaging a Master Systems Planner or a Master Systems Integrator (MSI), consider developing (or coordinating with design professionals to develop) the Smarter Building Owner Project Requirements (OPR) as part of a general owner plan for how the building is to operate, including an owner-developed BMS Framework for building management systems (BMS).

B. Do an initial Scope & Gap Assessment of the scope and scale of the project requirements, what might already exist in the building(s) and where the gaps are (if retrofitting existing buildings), and use that as the basis of design for the consulting engineer to develop the DIV 25 integrated automation spec.

C. Create a Contractors Project Responsibilities Matrix (as mentioned above) to organize the areas of responsibility for each vendor, making clear which deliverables come from which supplier, and where there are shared responsibilities

D. Bring the IT and OT groups together prior to developing project specifications to get on the same page and reduce confusion, finger pointing, and lack of coordination during design, installation, and operation.

E. Interview and assess bidders for the MSI contract based upon the owners BMS framework and scope.

F. Work with a consulting engineering team that understands and agrees to meet or exceed the owner's project requirements and also help establish the BMS framework requirements for the specific project.

G. Engage a general contractor that has the experience and management capabilities that parallel the project's integration requirements as they will have to ensure all parties address and deliver the owner's requirements.

H. Provide well defined "desired outcomes" of all integration scope (section 10). This identifies not just the technical integration requirements, but what that integration does to meet the OPR.

I. Ensure proper data ownership and management to meet the owner's needs (section 60). This often relates to cloud data access by 3rd parties and how to manage access, privacy, and security.

25.25.10 – Purpose of Interoperation

In an Owner's Requirements Document, or more detailed Specifications, section 25.25.10 would lay out the owner's project-specific goals for having interoperable data and a smarter building. It would include foundational information that establishes the project objectives for integration, interoperability, data access, enterprise access, and general technical objectives.

This section includes:

- General Reasons for Interoperability
- Importance of Project-Specific Smarter Buildings Goals

10.1 General Reasons for Interoperability

Frequently, the goals for "why is this a smarter building?" fall into three groups: owner's mission/ESG (Environmental, Social, Corporate Governance)/business outcome goals; operational goals; and occupant experience goals. With those in mind, some general reasons that may be cited and/or adapted to your specific project include:

10.1.1 Owner's Mission/ESG/Business Outcome Goals

A. We want building systems that interoperate with others to help maximize their value to owners, operators, and occupants.

B. We need reliable and real-time building energy and emissions data to report to shareholders, employees, and customers, on our organizational commitments regarding our impact on the environment.

C. We need energy and emissions data to comply with local disclosure ordinances in all our locations.

D. Our (owners') intention is to invest in an interoperable-data-connected set of systems that will increase convenience for occupants, employees, and facilities staff, while reducing ongoing facilities operational effort and costs. To work well, data and system interoperation needs to be done correctly upfront.

E. Smarter buildings can help us deliver better business outcomes.

E.1. As real estate owners, we are aiming for lower costs, improved marketability (and rent revenue) and higher asset and property values.

E.2. As a business that owns our own buildings, the reliability and productivity of our facilities directly supports the business' output and revenues. (e.g., You can often quantify how much avoiding downtime is worth.)

10.1.2 Operational Goals

A. Portfolio Management: Interoperable data for all our buildings is needed to improve access to information important to enterprise decision-making. Smarter buildings provide convenient, credible and efficient portfolio-wide views of key performance indicators enabling consistent management of and reporting on systems, buildings, processes, and expenditures across our multiple buildings and disparate locations.

B. Compliance: Interoperable systems allow us to quickly access operational data across all building systems to comply with government energy and emissions disclosure regulations.

C. Mitigate Risk: Decrease the risk of productivity downtime by improving building resiliency. Could include integrating a renewable energy microgrid to deliver a more secure electrical supply to smarter ways to respond to emergencies to getting data-informed discounts on insurance.

D. More efficient sequencing: Interoperable data enables fault detection diagnostics and machine-learning algorithms that can improve performance of systems such as heating and cooling.

E. More efficient maintenance: Integrated systems allow for staff optimization, enabling fewer staff to support more buildings and engage service providers with more transparency.

F. Fewer truck rolls: Remote visibility and control of interoperable systems reduce the cost of facilities personnel deployment, ongoing service, and support.

G. Shift maintenance from reactive to preventative: Real-time data on the performance and condition of important equipment can enable "data-informed" preventative maintenance routines.

H. Extend equipment life cycles: Real-time data on the performance and condition of important equipment can help optimize and prioritize the timing of renewal investments.

I. Common communication: The owners wish to avoid any system that is not interoperable because any such system will require new and custom 'connections' from that building system to other systems inside and outside of the building, which adds cost and complexity.

J. Grid Interactivity: Interoperable systems allow a building to be Grid-Interactive, compliant with the "National Roadmap for Grid-Interactive Efficient Buildings" (GEBs – document available at https://gebroadmap.lbl.gov).

K. When: System data interoperation is necessary both during construction and building operation. (You could establish a date certain here. "During construction" requirement may or may not be necessary, depending on your project.)

10.1.3 Occupant Experience Goals

A. Interoperable data enhances the occupant experience by providing context-aware functionality that combines data from multiple sources to deliver outcomes not possible from a single system. For example: HVAC control, room scheduling, and occupant location data.

B. A smarter building with data from multiple systems available in a centralized way enables the creation of user-centric applications to deliver convenience, comfort, and higher value to building occupants. (Such as: List the occupant convenience outcomes you envision for your building…)

10.2 Importance of Project-Specific Smarter Building Goals

While general reasons may be useful to provide broad understanding or context, this section will be most valuable to the contractors bidding on or providing the services if it focuses on the specific goals of making data for this particular project interoperable, so that goals for this specific building (or portfolio) can be achieved. The best goals are stated as action items (start with an active verb), cite a specific use case or scenario, are measurable, and include a timetable.

Below are some examples:

10.2.1 Example 1: Simple Building: Energy Disclosure Compliance

I am the owner of a 5,000 SF commercial office building, and must comply with a new local energy disclosure ordinance. I have no facilities staff to track the required data or submission process. I want to maximize my investment so that any "smart" technology installed now is useful for future "smarter building" enhancements.

A. Owner Mission/ESG/Business Outcome Goals:

   A.1. Benchmark the building annually using D.O.E. Energy Star Portfolio Manager.

   A.2. Conveniently comply with annual reporting required by the Local Energy Disclosure Ordinance.

   A.3. Be ready to use the data collected for reporting for future "smarter building" enhancements, yet to be determined.

B. Operational Goals:

   B.1. Compliance data recording should be automatic (monthly and annually), not requiring any staff time or effort.

   B.2. Annual reports should be automatically generated and ready for easy submission by one person (1 hour max/year).

C. Occupant Experience Goals:

   C.1. Building occupants (and the general public) should be able to see the building's latest compliance score via the building website.

10.2.2 Example B: Moderate Buildings: Local School District

Our local school district, [Our County School District], wishes to run all our schools as smarter buildings, with interoperable data and systems that enable and verify the district's ESG goals, efficient operations for our small number of facility staff, and a comfortable experience for our students, staff and visiting public. The district's goals for this smarter building project include:

A. Owner Mission/ESG/Business Outcome Goals:

   A.1. Benchmark all schools quarterly using D.O.E. Energy Star Portfolio Manager.

   A.2. Report quarterly to the public on meeting the district's energy and emissions goals.

A.3. Provide central managers with data to conveniently comply with annual reporting required by Local Energy Disclosure Ordinances, in [three] different municipal jurisdictions.

A.4. Report on annual energy and emissions operations to U.S. Dept of Education, to comply with federal grant requirements funding these improvements.

B. Operational Goals:

B.1. Let building maintenance staff (typically 1-2 per building) focus on daily cleaning and minor troubleshooting while off-loading higher-level mechanical system management to the central facilities team.

B.2. Provide the central Facilities Team (4 people) with 2-way, remote monitoring and control of key building systems in (12) schools.

B.3. Reduce truck rolls by 75% and maximize equipment uptime (98%+).

B.4. Key systems include: exterior and interior lighting, HVAC, door access control, kitchen refrigeration coolers.

C. Occupant Experience Goals:

C.1. Calendar integration: Enable after-hours events in the building's schedule to override non-school-hours HVAC and lighting controls, so that the public can use school facilities in the evenings or on weekends, while still conserving energy when the schools are not in use.

10.2.3 Example C: Complex Buildings: An Office Building Within a Corporate Campus/Portfolio

The role of a workplace in the culture of an organization is changing due to the impact of COVID, the increased adoption of technology to enable work to be done from anywhere, and the proven fact that people can be productive at home. As a result, organizations are changing the work environment to provide a good reason for people to go into the office. The workplace is also a key tool to attract and retain the best talent.

With this in mind, a smarter building on a smarter campus would have integrated, interoperable systems to transform the employee experience as well as the operations model for building management.

A. Owner Mission/ESG/Business Outcome Goals:

A.1. Demonstrate and validate the organization's commitment to reducing its environmental impact on the community and planet, especially for ongoing operations.

A.2. Streamline compliance with the local energy disclosure ordinance(s).

A.3. Attract and retain top talent for our business.

B. Operational:

B.1. Streamlined facilities staff: With better tools, information, and interoperability, a leaner staff can support more buildings and assets. Remote monitoring, troubleshooting, and support with integrated systems

increase productivity while also improving the standard of care for the building and for the people in them.

B.2. Security & Access: Creating a secure campus for all is the first and foremost requirement. After that, the security credential (now typically a phone) can be leveraged for multiple different purposes to save time and streamline the user / tenant experience. As an example, utilizing the phone for two factor authentication for IT services as well as confirming actions to be taken around campus, such as calling elevators, charging point of sale vending to an account, buying lunch, and more.

B.3. Grid Interactivity: Enable Interoperable systems to be Grid-Interactive, compliant with the "National Roadmap for Grid-Interactive Efficient Buildings" (GEBs – document available at www.gebroadmap.lbl.gov). Make select building systems so that they interact with the grid, and also increase the building energy efficiency independent of the grid signal. Grid signals will include price, carbon, load restriction, load curtailment, and load increase, and come from [Utility or Aggregator] or [Hybrid Local controller]. The grid-interactive systems for this project include: central HVAC equipment, select lighting systems, hot water heating, solar PV generation, EV-charging stations. (See list in DIV 25.25.70, below)

C. Occupant Experience:

C.1. Provide a unified occupant experience where an occupant's mobile phone can serve as a universal key for occupant activities such as building access, elevator control, indoor comfort, IT-network access, room booking, mail and delivery notification, in-house and external food service.

C.2. Increase communication with building occupants by delivering individually-tailored messages from corporate and facilities to their mobile phones.

25.25.20 – Operating Roles & Responsibilities

This section is about Who will be expected to interact with the applications, data, and systems in the smarter building, to achieve the Purposes (goals) laid out in section 25.25.10. This section can also be used to outline the operational processes, in a list or task flow chart(s), that each group is expected to follow to achieve those goals. And finally, this section can connect the people to the processes by specifying roles, responsibilities, job descriptions and career paths (usually for staff) and training requirements (for any user group).

To provide a clear picture of who will be expected to interact with the smarter building, this section outlines the following steps:

- Define the Users of Your Smarter Buildings
- Define Responsibilities, Job Titles, and Training Needs (if applicable)
- Define the Process Each User Group is Expected to Perform

20.1 Define the Users of Your Smarter Building(s)

"Who" can be generally broken down into three groups:

- **Owners.** The people who own the property or are designated to act on the owners' behalf. Can include C-suite executives, governing boards or committees, portfolio managers, and project managers.
- **Operators.** The people who run the building(s) and portfolio, including property managers, facilities personnel, production staff, and (don't forget) the system administrators. Often there are both internal (staff) roles (by department or function) and external (vendor provided) roles.
- **Occupants.** The people who use the building, either in a role internal to the organization (non-facilities staff, employees, or students) or external (visitors, customers, general public.)

One additional group includes the contractors, consultants, and specialty service providers that support the facility. While not specifically "users", they should be considered part of the team and play a vital role in the continuous operational maintenance, and management of the building. They may have special access credentials, job-specific tools and requirements in order to access the systems they maintain. There will likely be external, internet-based tools and access required for off-site tools and applications requiring well-defined roles and responsibilities for access the data and systems.

20.2 Define Responsibilities, Job Titles, and Training Needs (if applicable)

A well-prepared Owner's Requirement Document or Specification will outline the specific roles, job titles (as applicable to staff or vendors), areas of responsibility (and possibly specific tasks) each user group would be expected to perform, training needs and methods to be delivered for each group, and an org chart to depict the relationships among the different users. The owner will typically have many user groups that will provide input on the owner's requirements including the IT group, facility maintenance and operations, and many types of process, office, clinical, educational, and human resource staff. It is crucial to get input for all of these groups into the owner's general project requirements. This may include requirements for certain data sets being made available to non-OT teams or the BAS needing to interface to certain process or clinical equipment.

Expert Tip: Managers of some projects find it useful to create an Operational Responsibilities Matrix, similar to the Contractors' Project Responsibilities Matrix, but focusing on who is expected to do what in terms of interacting with the smarter building, *when the building is operating.*

Figure 3. Sample Operational Responsibilities Matrix

10 MAIN STREET OFFICE BUILDING
SMARTER BUILDING OPERATIONAL RESPONSIBILITIES

	OPERATIONAL ROLE		
Group	Owner	Operator	Occupant
Title (add as many columns as necessary)	Portfolio Manager	Facilities Manager	Tenant

TASK			
ESG Reporting	Approve and submit annual local disclosure report.	Monitor monthly utility bills and EnergyStar scores	Read/consume latest ESG scores via building website or app
HVAC Control		See, control, and troubleshoot HVAC, in-person (at equip) and via mobile device	No direct settings avail.
HVAC Comfort		Manage comfort issues submitted by tenants.	Building will automatically know when I am in, what spaces I use, to set HVAC. Report comfort issues via building app
Etc. (add as many rows as necessary)			

In addition to an operational responsibility's matrix, developing a project delivery responsibility matrix will similarly help all stakeholders define and understand their scope, roles, and responsibilities. This significantly reduces the eventual finger-pointing during construction on a project. This matrix should include:

- Basis of Design – Owner Project Requirements, Frameworks, Playbooks, Standards
- Design Phase - Including Engineering, Equipment Selection, Data Set Requirements, Points Lists, Network Infrastructure, Connectivity, and Interoperability
- Implementation Phase – Including Installation and Integration and the BMS Integration and Programming
- Commissioning and Handover – Including documentation, drawings, points list, tagging sheets, and database files
- Warranty and Maintenance
- The typical stakeholders include:
- • Consulting Engineer
- • Owners BAS representative
- • General Contractor
- • Architect
- • Master Systems Integrator
- • Mechanical
- • Electrical
- • Communication
- • Structured Cabling
- • Other specialty subcontractors

- IT/Cybersecurity
- Facilities Management and Engineering
- Security
- The project responsibility matrix typically includes all of the physical and logical components and interconnections required for the project. It includes:
- DIV 22 – Plumbing
- DIV 23 – Mechanical/HVAC
- DIV 25 – Integrated Automation
- DIV 26 – Electrical
- DIV 27 – IT Structured Cabling
- DIV 27 – Communication/Teledata
- DIV 27 – Audio/Visual
- DIV 28 – Electronic Security and Physical Security
- DIV 34 – Transportation
- Other specialty systems (Solar PV, EV Charging, Backup Generators, etc.)
- Furniture, Fixture, and Equipment (FF&E)

Construction Administration Note: Some elements of a project have multiple stakeholders involved and must clearly define who is in charge of what. An example is designing and installing the OT IP backbone infrastructure of a building. This typically includes a DIV 27 low voltage wiring contractor to design and install the wiring (Ethernet, Fiber), the owner's IT group or consultant/contractor that configures the OT IP network and provides and installs the equipment such as switches, routers, patch panels, etc. It may also require the DIV 25 contractor install software on the BMS server, assign IP addresses, set up all of the required integrations, and test all of the data pathways. The DIV 25 contractor may also be engaged in defining the "spots and dots", the location and quantity of all of the OT equipment requiring Ethernet connectivity.

Regarding staff training requirements, specifications should define all the training required and the mechanisms that this training should use. This includes hands on and classroom training. Consider requiring that all training be recorded and delivered as MP4 videos for archiving. More complex facilities may want to ensure these training videos are accessible from the BMS server for use by any authorized person. Very long training videos should consider requiring the use of indexes and tables of contents to help personnel find the information they need rapidly. Of special interest in the context of networked data systems is the training on how and where information is stored, the backup and restore routines, any required scheduled maintenance, server software monitoring and maintenance (patch files, security updates, user credentialing, and more).

20.3 Define the Process Each User Group Is Expected to Perform

A well-prepared Owner's Requirement Document or Specification may also include flowcharts to illustrate the processes that the smarter building system will support for each user group, putting the responsibilities listed above into context in relation to how the data flows and what other users do.

Process flow charts are especially useful to illustrate how and when users need to interact with digital information from the building, which is the basis for defining the requirements for Delivery (sec 30) and Applications (sec 40). This also may include details about the data source, structure, context, semantics, rate of update, and who and how the data is to be used. Applications that may use the data may come from an operational/maintenance application interface, from 3rd party analytics application, or from energy management and optimization application. The users of each of these applications vary substantially but all are sourcing the same network and the same data, just using it in substantially different ways.

25.25.30 – Information Delivery

This section relates to how information is to be delivered to the users so they can perform their "smarter" tasks related to the building.

Since we are dealing with digital information, the most important part of defining "delivery" is specifying what the digital user interfaces (UI's) are that user groups in section 25.25.20 will use. Digital UI's can take the form of mobile applications, desktop or laptop applications, websites and browser applications, digital twin models, machine-to-machine interfaces, and (soon, more) augmented reality interfaces. Related to the delivery of information is defining the sources of and structures of the data. This include databases, query tools, API (application program interfaces), data semantics, naming conventions, and more. Most of these topics are covered in other sections, but it is worth noting here that these elements of a system must be well coordinated. Lack of coordination can lead to "islands of automation", interface "silos", where the user has way too many custom, vendor specific interfaces to deal with which reduces overall operational efficiency. The "Single Pane of Glass" for user interfaces may look like one application managing everything or it can simply be a browser that has many tabs for system specific interfaces. Requiring user interfaces to be interfaced using a common IP network browser can be a significant benefit to the user.

A well-prepared Owner's Requirement Document followed by a good design Specification will outline which delivery mechanisms (which UI's) are expected to be used by each user group identified in DIV 25.25.20 Operations, and what the functional requirements are for each UI.

This section discusses:

- What digital devices do you expect your users to use?
- Do you expect a Single Pane of Glass (SPoG) interface?
- General Requirements for Interfaces
- Defining Multi-System Views and Interface Functionality

30.1 What digital devices do you expect your users to use?

List the devices you expect the users listed in section 20 to use when interacting with the smarter building. There are two sections here.

Interface platform:

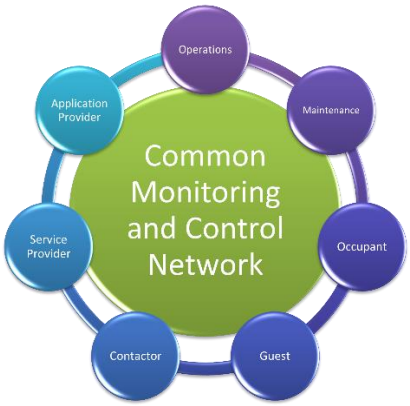
- Web browsers on any browser enabled device (laptop, desktop, tablet, phone)
- Custom applications (PC, Linux, MAC/IoS, Android enabled)

Physical interface devices:

- Mobile phones
- Mobile tablets
- Kiosks
- Digital signage displays
- Voice activated/intercom/digital assistant (Alexa, Google Play, etc.)
- Wearable digital devices, such as smart watches
- Augmented reality devices

30.2 Requirements for a Single Pane of Glass (SPoG) interface?

SPoG is a term floating around for the building automation world for the last few years. First, let's define SPoG – it is referred to as a "Single Pane of Glass" and is most often used when referring to the user interface of a building automation system. It is the single computer monitor (the glass) that the operator, technician, engineer, and manager use to interface with their entire building automation and control system. The concept is one in which there is a single place to access all of the tools necessary to view system operations, diagnose problems, and manage all of the building's integrated systems. These include the traditional mechanical, electrical, and plumbing systems along with many others.



The value of a SPoG is necessary information can be accessed from one computer workstation, which enhances operational efficiency and the reduces training, support, and maintenance of multiple computer systems, software, tools, and infrastructure. Typically, the building or campus Master Systems Integrator is the one responsible for the development and delivery of this system. There is hardware, the computer, monitor. and software, the application(s), interfaces, drivers, APIs, and more, that must be integrated.

There is some debate as to what a SPoG allows and restricts from a solution provider, product vendor, or integrator's perspective. Some suggest the best solutions is a single computer software application that does everything – often referred to as the Building Management System (BMS) Front End Graphical User Interface. Others suggest a more efficient mechanism is having a single workstation but allowing multiple software applications on the single computer. A third options is deploying a single application that can launch secondary applications from within it – often called a "container application" as it contains the access to any other application via program calls, hot links, embedded redirects, and more.

One of the first questions to ask is: Do you expect all interactions by all users with all of the smarter building functions, to be through a single user interface (SPoG)? That does not necessarily mean one monolithic application that tries to do everything for every system. It simply refers to the user interface being one computer/device access point to gain access to the various application interfaces needed to operate the facility. Here we are typically referring to the interface used by normal day-to-day system operation and is not considering specific diagnostic or maintenance tools. Those tools typically require custom software and interfaces supplied by the system vendor.

So, for this framework we will assume that the SPoG is ONE WORKSTATION, Multiple Applications. Having a single non-integrated application is not overly practical in today's smart buildings and smart campuses. However, a single BMS front end with required interfaces for general data, monitoring, alarming, and control is very beneficial and part of any DIV 25 contractor's responsibility. But there will be multiple applications – that's the nature of the industry today. What we don't want to see is a dozen or more custom laptop computers for each system with dedicated interfaces (serial ports) for each system. In typical medium to large buildings, the software applications typically reside on a networked server, with access from any workstation on the network. This is for general user interfaces and does not include advanced diagnostic tools, configuration tools, or maintenance tools.

There are several architectures for the user interface worth discussing here. As software and hardware systems have evolved over time, the reliance on customized solutions has changed. Stand alone, hardware-based solutions have given way to more distributed, open, and flexible solutions. Here are a few system architectures to be aware of.

Client Server – In this architecture there is a central server with a host application typically running on an IT managed computer server located in a dedicated IT room. Client applications are deployed to any workstation that requires access to the server and the server's data and user interface. There are two types of "clients":

Thick Client – A thick client is an application that is loaded onto the computer workstation and communicates to the server in order to render information to the user. Thick clients require continual management and administration at the workstation. These clients are typically vender specific and require licensing and potentially annual service contracts. Thick clients may also store site data locally on the computer workstation as well as on the system server. Modern systems are moving away from thick clients as they are more costly to maintain, require additional administration, pose greater cyber security risks, and don't allow any workstation in the building to provide an operator user interface.

Thin Client – Think clients are more acceptable where any operator workstation with a standard, open suite of applications can access the server and render information to the user. Think clients such as standard web browsers, sometimes with required browser "add-ons" are a more acceptable platform for client server user interfaces. Thin clients do not store much or any data locally on the workstation. However, certain graphics, images, and other information may be "cached" or stored locally to speed up the graphical rendering. For example, the large image of an air handler, which does not change, may be cached locally so that when an operator selects that graphical page, the image loads quickly from local memory. However, the data on the page such as temperatures, pressures, etc. are sourced from the real-time data from the server. A balance between local cached information and that downloaded from the server is required in order to provide a smooth and responsive graphical user interface system.

Stand Alone Application – This is a solution where the supplier requires an application and its interface to the control network be installed on every workstation requiring access to the user interface. Common standalone applications are provided for system diagnostics, controller programming, system configuration, and more. These applications are well suited to run on field enabled laptop/notebook computers so that technicians have access to the interface while working directly on equipment. However, these applications are typically not the primary interface to the building operations team. They are removed from the system once their tasks are complete. Sometimes these applications require custom drivers and interfaces to comm ports, USB ports, WIFI, or Bluetooth interfaces to equipment.

Data Storage/Management – All user interfaces must reliably access and display information sourced from the control network. The control sensors and actuators report their data across the control system to the BMS front end application (assuming a client/server architecture). The BMS application requires a system database be included and available for access by any client. Clients may be the BMS front end Graphical User Interface or any other API that requires data to perform its function. The storage and administration of that data is part of the BMS front end's role and a project may require drivers such as MQTT, SOAP, RESTful, web services, or other types of interfaces to that data. When selecting a BMS front end and the software and data architecture that support is, it is important to define all of the application interfaces required, not just the GUI for the BMS operator. Applications such as system analytics, fault detection and diagnostics, computer maintenance and management systems (CMMS), and others all require direct access to the system data and are often directly integrated into the BMS platform by the DIV 25 contractor.

Server Location, Maintenance, and Support – There are several options for where the physical server is located. It can be on site in an environmentally controlled IT equipment room. In a remote owner-maintained data center, or in a 3rd party cloud-based data center. There are pros

and cons for each option and this should be discussed with the design team. General best practices say to keep the intelligence at the point of control, meaning, keep the BMS server and its user interfaces as close to the actual equipment and building network as possible.

Often the BMS front end is involved in real-time monitoring of alerts, alarms, and equipment status. Building equipment failures can have a direct impact on the health and safety of the building's occupants. Depending upon the type of facility, there can be strong justification for having a full-time building operations center with 24/7 staffing to ensure a high degree of reliability and maintenance.

Less critical facilities can justify having the BMS server located in an owner managed data center or in a cloud/3rd party managed data center. A risk assessment should be developed by the owner and the design team to develop the right strategy for the project.

The general maintenance and support of the server all factor into the decision process. If the owner is to maintain the server and its supporting hardware and software, then the owner must employ or engage the services of qualified personnel who can manage backups, software updates, security patches, and the like. If the server is managed by a 3rd party and these functions are part of the service contract, then the owner does not have be engaged in the process. However, the manager of the data center may take the BMS server offline at any time to provide maintenance, which would interfere with the real-time monitoring of the facility. This can also cause loss of trend data, synchronization issues, and delays in graphical interfaces. Owners should evaluate the pros and cons for their particular situation.

Database Development and Interoperability – One of the primary functions of the BMS server is the development of the site BMS database. This database contains a virtual repository for all of the physical sensor and actuator values including both current value and historical logs as well as all of the logical data values used by the control systems. Building the site database requires knowing all of the network-available data points, their object types, units, and all related semantic information. This database is sometimes referred to as the "data lake" or "digital twin". Open, interoperable systems require that this BMS database be designed and implemented such that any application or application interface (API) be able to access the database. There are many ways this can be achieved using standard protocols, drivers, or custom interfaces. The key here is knowing what the scope and desired outcomes are for the BMS server. The more flexible and adaptive the server database is the more useful it will be to the owner and the owner's representatives.

Advantages of a SPoG:

- One place to look for everything.
- One login gains access to all (permitted) systems and information
- Administration of user access and permissions can be all in one place and defines who sees what and who can modify what based upon the owner's criteria.
- Data from multiple systems can be viewed and mixed together easily. (Check how well your SPoG can do this.)
- A good SPoG should be flexible enough to be tailored for different operation functions.
- A good SPoG should be flexible enough to allow for the addition of future requirements that an interoperable solution would enable.

- Best Practice: "Light and Loose:" One strategy for connecting digital systems together is to be "light and loose," rather than deep and complex. So, while interconnections between systems enables new functionality that is the point of a smarter building, too many interconnections can be paralyzing to set up and to maintain. Minimizing how many data connections there are, and how many dependencies there are from one system to the next, allows things to work easier, at set up and over time, especially when one of the component systems is updated (which will be often, and usually without regard for how other systems might use that data).
- A "light and loose" SPoG can report on a limited set of data (often called key performance indicators, or KPIs), while also providing links and views into component systems for deeper looks at data and to use component system functionality.

Disadvantages of SPoG:

- May requires custom software development (and upkeep).
- Check how "standard" your vendor's SPoG offering is, how much you can customize views and functionality to fit your needs, and how the UI is kept current with changing devices, operating systems, APIs, etc.
- Practicality, budgets, and vendor willingness to support the SPoG may limit the capabilities.
- Single point of failure: Updates to or problems with component systems can interrupt how the rest of the UI works (depending on how light vs. deep certain connections are.) The system architect may consider keeping certain sensitive systems separate (or access limited).
- SPoG interfaces may be designed as "monitor only", but this is a design choice and not a technology limitation.
- ~~Data security is easier when there are separate applications for different functions performed by separate user groups.~~
- Single-sign-on may not be available for all relevant systems.
- Can take a long time to specify all user roles and requirements

30.3 General Requirements for Interfaces

Whether you decide you need a SPoG, or are better served by (or just need to have) multiple interfaces for your smarter building, there are some common interface requirements that are best practices/recommended/good to ask for:

30.3.1 Key objectives are to deliver information to users using easily accessible platform(s):

A. The user interface of all systems will be delivered on current versions of web browsers (without a specific plug-in, add-on, etc.).

B. The user interface of all systems will be available on mobile devices, either via a mobile web browser or via a specified mobile app. If a mobile app is specified, it should be available for both iOS and Android devices, through the respective mobile platform's app store.

C. The interface for select systems will be a digital twin model, available to appropriate users via a web browser, a specific desktop app, a mobile app, or embedded within the SPoG graphical user interface.

D. The web-browser-based UI will be kept up to date with browser updates, and mobile app UIs will be kept current with mobile OS updates, within [xx] days of updates being published.

E. The user interface shall meet the owner's requirements for the layout, style, color-coding, presentation, naming, tagging, access control, and related user interface requirements. Typically, this information is provided in an OPR – Owner Project Requirements document. Ensuring these requirements are met provides greater operational efficiency by staff interfacing with multiple UIs across a single building, a campus, or an enterprise. Also helps with training and staff transportability.

30.3.2 UI Network Access

UIs delivered via web browsers, mobile apps, or machine-to-machine interfaces require secure interface and access to the site IT network and should follow guidance according to requirements in sections 25.25.90 Networking and 25.25.95 Cybersecurity

There are multiple options for how UIs connect to the owner's network. A few considerations include:

A.1. Will the UI and its associated computer server and user interface be by a web browser that requires securely access pages on the public Internet?

A.2. Will the UI be stand alone and isolated from the public internet?

A.3. Will the UI have a VPN connection to a remote server?

Based upon the answers to these questions, the system designer will need to account for access restrictions and requirements, IP network pathways, security, and other related factors.

30.3.3 Consistency in the Presentation of UI Elements (naming, color coding, structure, etc.)

A. Define a naming and tagging convention for use within the facility and for use by all suppliers

B. Include definitions for abbreviations and acronyms

C. Define a standard color coding for user interface graphics (piping, wiring, air, water, steam, gas, etc.)

D. The owner should have a consistent naming framework as part of the Owner's Project Requirements or the Building Controls Framework and should be used by all contractors, suppliers, and consultants.

E. User interfaces should use the same naming convention that the physical devices use. There should be consistency between the internal database(s) and control network data object naming, and all API naming and tagging.

30.3.4 Administrator Users

A. Admin users will have permissions to all administrative functions for any central interface and all of the component applications. (See also sec 95)

B. Do you also need to have separate admin roles (and permissions) for different apps?

C. Admin users will be able to control what is viewable/controllable by any given user.

D. Admin user credentials are required to on-board and off-board general users.

30.3.5 Users will be able to access information securely via a single sign-in.

A. Pro Tip: This sounds great, and is something to shoot for, but implementation may be complicated by: (a) whether component systems can handle single-sign-on; and (b) whether user profiles and related permissions are sync'd from one app to the next.

B. Common methods for implementing single-sign-on include OAuth and LDAP. (See also sec 95)

C. Will the user interface automatically log off after a timed period inactivity?

30.3.6 User interfaces will be accessible by users regardless of their current location.

A. This enables mobile and remote access to the smarter building.

B. Alternate: for security reason, some projects may require that user access be limited to when a user is on premises via a dedicated workstation.

C. Dedicated workstations may be required in certain situations as they may be directly connected to the OT building controls network rather than the owner's IT network. Cross-over network access may be restricted or not present.

D. Requiring a VPN for site-to-site access can be a good mechanism to manage cybersecurity. This is beneficial for campuses that don't have direct physical network cabling to all buildings. The owner's IT group is then responsible for setting up and maintaining the VPN, however, specifications for which user interface applications and workstations require VPN access are the responsibility of the system designer and the DIV 25 contractor. Once a VPN is set up, the owner can grant access to contractors, suppliers, and other 3rd parties allowing them access only to specific network locations and applications.

E. In some cases, remote or mobile user access might make sense only for select systems or functionality. However,, once your interface(s) is Internet-connected, anything less than "all mobile access" can be complicated to design and implement.

30.3.7 New users will be provided with access to the information they need via a documented process.

A. Documentation is key to being able to onboard new users, troubleshoot issues, and fix larger problems.

B. Pro Tip: You can ask for it, but full documentation of all processes is hard to get and may be expensive to provide. Providing a contractor "check-list" of OPRs relating to documentation deliverables is a good way to help ensure project close-out goes smoothly. Additionally, the development of project documentation should continue throughout the project, be reviewed periodically, and signed off during different project phases. Leaving all the documentation to the end will cause turn-over and commissioning delays.

30.3.8 Information required by users will be provided via a digital mechanism such as secure API so that future user interface technologies such as AR/VR can be provided.

30.3.9 All Applications listed under 25.25.40 shall be able to be delivered to users subject to their role and security credentials as established by the site admin.

30.3.10 All Data managed by systems listed under 25.25.60 shall be accessible by users subject to their role and security credentials.

30.3.11 Data pertaining to multiple different systems shall be viewable on a single page or in a unified view, in accordance with the needs of users. Examples include a single user interface page with all equipment alarms across all subsystems. Energy management data is also a good example of cross-domain user interface page (See SPoG section above to check if this is what you expect).

~~30.3.12~~ Some user interface applications may have the ability to allow internal communication between users to, for example, escalate an alarm from a junior tech to a senior tech to, perhaps, process or authorize a work order. Internal user-to-user messaging may be a "nice-to-have" feature, but may not be practical or required for all projects.

30.3.13 User interface hardware and data exchange with items in sections 40, 50, 60, and 70, will follow open standards when possible.

30.4 Defining Multi-System Views and Interface Functionality

Whether you use one unified SPoG, or multiple UIs, an important advantage of a "smarter" building that has multiple systems connected together is being able to see and interact with data from those multiple systems at the same time. Some multi-system functionality will therefore need to be developed as applications separate from, or "on top of," dedicated system apps. If section 40 – Digital Applications defines such "multi-system" apps for the project, this part of section 30 is where the requirements for displaying these "multi-system" apps would be defined and explained.

An example of a SPoG with multiple applications is when one BMS front end embeds another application within it. This "windowing" is a common mechanism to merge multiple applications

into one SPoG. There are multiple ways this can be done. One common mechanism is for the BMS front end to have embedded "hot links" via standard HTML5 web services. So, it looks like you've never left the "container application" – the BMS front end, but the data is being served by a separate application. It is all transparent to the user and can provide a wide variety of services all within one container. A second model is where one application makes an API call to another application to fetch data, the displays it in the native visual interface. Refer to section .40 for more information on digital applications.

The specification should define how and what is needed here. The DIV 25 contractor may be required to install add-on software, enable specific functionality, or work with 3rd party suppliers to provide this integration. In the end, it is highly beneficial for the owner's staff to have as much integrated into the daily work flow applications as possible. A simple example of this is an email user interface and a calendar/scheduling application integrated into one UI. As an example, a facility energy manager may wish to see both the energy consumption of the HVAC system combined with the solar PV generation on the same screen, but both data sets are sourced from different applications. Data integration between vendor systems is now very practical and achievable using standard API interface such as MQTT, RESTful, OPC, OBIX and other platforms.

25.25.40 – Digital Applications

This section is about the software applications that use data from the building and external sources to provide actionable information to the user. It identifies the applications that are part of the smarter building functionality, lays out how those applications are to co-exist within the building environment, and explains how data is retained and used by the applications. The application layer should provide software developers with the key requirements for developing interoperable, multi-system applications.

This section discusses:

- What is an Application in the Smarter Stack?
- Define What Applications You Have and What You Need
- General Requirements for Applications
- Examples of Single-System Digital Applications
- Examples of Multi-System Digital Applications
- Digital Applications Do Not Include…

40.1 What is an Application in the Smarter Stack?

Applications make up the 'intelligence' layer of the Smarter Stack, manipulating data, transforming it into useful and actionable information, providing control logic, business intelligence algorithms, machine learning, administration of systems, and additional management capabilities.

Digital applications typically monitor and/or manage one or more systems that help a building operate the way it is intended. Applications can run specific systems, can integrate across multiple systems, or might be required for the operation of the building (per sections 10 and 20), but not be tied to a specific system.

Sometimes what people commonly call applications or "apps" (like on their smartphones) wrap together a lot of the layers of what we refer to as the Smarter Stack (from connecting to devices, to data storage, to business intelligence, to user interface) to perform a specific function. For the purpose of this DIV 25.25 Framework, we are using "application" to refer only to the layer where data is manipulated and transformed into useful and actionable information or where it is directly involved in the sequence of operations of a single system or of multiple systems. Where the data comes from (70, 80), how it is stored (60), how it is accessed (50), and how it is displayed (30) are covered in their respective sections.

If devices are connected and data is exchanged well, per sections 50, 60, 70 and 80, the Application layer may be the most creative layer of the Smarter Stack.

40.2 Define What Applications You Have and What You Need

A well-prepared Owner's Project Requirement document and the BAS designer's Project Specification can use this section to identify all the digital applications that are expected to run the building(s) and how they work with each other to deliver the desired smarter building functionality.

It is recommended that the process of identifying all the needed applications follow four steps:

1. Inventory all the applications, existing and planned (if new construction or adding systems)

2. Identify the key things each application does to fulfill the Required Outcomes (operations model and occupant experience outcomes identified in section 10, delivered to users identified in section 20, via UIs identified in section 30).

3. Define the key data each application creates and requires (in line with section 60)

    A. Identify the key data sources for each application, which could be from controllers in the building, other building applications, the BMS front end, or third-party external sources.

    B. Define the application interface requirements, protocols, rules, and methodologies.

    C. Identify any application network access requirements, permissions, dataflows, data usage expectations.

    D. Identify any custom integration requirements for each application (i.e., scripting, rules engine development, data transfer interval configuration, etc.).

4. If the existing applications do not deliver what is needed, then look at integration needs and opportunities to create new applications. It is preferred that any new applications should use standardized data available from section 50.

Here are some examples of applications and their data sources:

1. Energy Management – Data sources: Real time utility meter data, historical utility meter data (imported from utility feed), networked submeter, internal equipment controller with internal CTs (current transducer used for power/energy calculations),

electrical panels with CTs measuring specific circuits and plug loads (often used for high energy usage equipment).

2. Automated Fault Detection and Diagnostics – Data sources include field equipment and controllers across multiple subsystems.

3. Centralized Alarm Management and CMMS Interface – Data sources include networked sensors, actuators, and embedded controllers, programmable controllers, and supervisory controllers across multiple domains.

4. Scheduling – Data sources include external IRTC (internet real time clock web services) used for time synchronization, master schedule database, local and regional offset databases, and supervisory controller data (such as override and local scheduling rules).

5. DER (Distributed Energy Resources) and Load Management – Data sources: Solar PV Inverter, standby and co-generation equipment, power monitoring equipment, load shed/automated demand response signals from utility, onsite real-time energy demand, weather data from internet sources, building weather station, equipment and controller with setback and load shed mode control, and more.

40.3 General Requirements for Applications

Common requirements that all digital applications in your Smarter Stack should include:

40.3.1 Applications will have the capability to provide all user interfaces (UIs) with setup, configuration, operation, etc., as per 25.25.20. (Reference assumes these requirements are described in 25.25.20.)

40.3.2 Applications in 25.25.40 are to be installed/removed with minimal impact to the overall building operations and tenant experience (unless, of course, the application is directly integrated with a building subsystem's sequence of operation, safety systems, or other integrated operational system).

40.3.3 Applications will have the capability to retrieve data from other applications and systems as per 25.25.50.

40.3.4 Applications will have the capability to store and share all their data as per 25.25.60.

40.3.5 Applications will store their data in open, standard database formats such that other applications can read and write to the application's database. This may not be practical in all scenarios, however, the more open the application's database, the smarter the building becomes.

40.4 Examples of Single-System Digital Applications

Some examples of single-system digital applications include:

- A mobile app reporting on indoor air quality, fed from data collected by IAQ sensors

- An application that pushes new firmware to a set of controllers within a building or across a portfolio
- A supplier cloud-based application that captures runtime, event, and error log files for controllers to help improve product reliability and functionality.
- A building HVAC automation system that controls the chiller plant and multiple zoned HVAC systems (multiple controllers but all still HVAC)
- Individual AV systems in different conference rooms
- Lighting system processors which in turn manage the lighting sub-systems in different rooms and zones

40.5 Examples of Multi-System Digital Applications

Digital applications also can exchange data with other digital applications. This *multi-system* exchange enables outcomes that one system cannot provide by itself. Some multi-system applications have a 'closed' data architecture making it difficult to exchange data with other sources and systems, and others have more open data exchange capabilities. To facilitate the best outcomes and be ready for future opportunities yet to be invented, best practice for smarter buildings is to have applications that can store and exchange standardized data and information as openly as possible.

This may require that specifications define how data is to be exchanged and restrict the usage of proprietary protocols, proprietary databases, and undocumented interfaces.

Examples of multi-system digital applications include:

- Computerized Maintenance Management Systems (CMMS) that tie together work order ticketing and inventory supply management.
- Energy Management Information Systems (EMIS) that summarize, analyze and manage utilities utilization, such as electricity, oil or gas fuel energy, and water use
- Digital Twin applications to create a virtual digital model with the real-life building data. Digital Twins can be utilized to optimize building operations and utilization as well as greatly reduce operational cost across a portfolio.
- An analytics tool that consumes data from controllers, monitoring/status applications, and other sources to provide dashboard interfaces and insights into predictive maintenance
- Backup generators that work in tandem with key critical load applications to manage power outage recovery
- An organizational calendar (such as Outlook or a room scheduling application) for people and spaces can be utilized for automation, operational, and tenant experience required outcomes, such as:
    - Energy efficiency and automation of access, HVAC and lights around occupied / unoccupied spaces
    - Occupant experience – having rooms "know" when spaces will be utilized and preparing the room for use beforehand

- Operations requirements – enabling building staff and occupants to automate systems purely by scheduling a space for use in the calendar
- Calendar integration applications in a convention center example, utilizing the event calendar entry and the estimated number of attendees to manage:
    - Pre-cooling to the desired set point – The number of attendees can be shared from the calendar application. Based upon an average BTU per person, the anticipated increased heat load on the space can be easily calculated. With the additional heat load, the room can be pre-cooled to a set point below the desired occupied set point, so, when occupants come into the space, the room temperature will equalize to the desired set point.
    - Indoor Air Quality – This can also be useful for managing air changes per hour based on actual occupancy levels, CO2 sensors, and predictive duration to ensure a healthy building.
    - Lighting – The space can have brighter "work lights" active if the space is occupied before or after the calendar event. For a set amount of time before and after the scheduled calendar entry, the room can recall an occupied "event" lighting scene. Outside of those two considerations, only emergency lighting will be on and additional lighting can be turned on based upon occupancy for occupant safety.
    - Audiovisual Systems – Similar to the lighting system, the sound reinforcement and background music systems can automatically turn on and off at a preset time before and after the scheduled event in the space.
    - Refrigeration Systems – A supervisory software application coordinating the defrost cycles of multiple refrigeration/freezer equipment to ensure load balancing and product safety where the electrical power system plays a key role in ensuring no defrost schedule will overload any one electrical circuit and that load shedding/energy management applications can interact with the defrost schedule.

Digital applications are part of the foundation of AI applications where real-time and historical data are combined with operational trends and occupant usage patterns to optimize control strategies. While we most often hear of AI applications to manage energy efficiency, they can also manage occupant comfort and performance, predictive maintenance, optimized scheduling, optimized work order flow, and much more.

40.6 Digital Applications Do Not Include…

It is important to recognize what digital applications *for this section* are NOT designed to do. These most often fall into supplier/vendor specific applications for managing their devices independent of outside input. The functionality these applications provide is discussed more in section 25.25.70 Control Systems. Some examples of these applications include:

- Controller programming and application configuration
- Applications that log usage data from controllers
- Supplier-specific automated firmware update applications
- Supplier-specific maintenance applications

- Diagnostic applications
- System-specific user interface applications - typically for advanced system insights, setup, configuration, etc.

As with other subsections of DIV 25.25, in order to describe all the requirements needed for the project, the Owner's Project Requirements doc (and potentially any project Specifications) would need to include sub-sections for each digital application/system in which requirements specific to that application/system are listed. This could involve a lot of work and many pages to be complete, and is not shown in the summary outline above. This version of the Framework document includes examples of application-specific requirements in the Appendix.

25.25.50 – Data and Information Exchange

This section relates to the movement of data and information among applications, systems, storage, and, eventually, users.

DIV 25.25 as a whole describes how the building should work as a smart*er* building – which is to say, with functionality that depends on the interoperation of multiple building systems working together. This section 25.25.50 – Data and Information Exchange, is at the crux of making the building operate smart*er*, not just as an assembly of separate, siloed systems, even if one or more of the systems is "smart" on its own.

As noted in Section 25.25.40, the interoperability of applications is required to fulfill the intended occupant/tenant experience, operational requirements, and ownership goals. In a smarter building, data and information must be exchanged among various systems to enable this interoperability.

This section 25.25.50 – Data and Information Exchange, discusses:

- Which data exchange requirements need to be specified?
- Data and Information Portability
- What are well-behaved APIs?
- General requirements for data exchange
- Sample use case requirements

50.1 Which Data Exchange Requirements Need to be Specified?

One of the greatest challenges for building and operating smarter buildings is that, depending upon the type of data, the methodology for exchanging data and information is in many cases still new to the industry. For example, the exchange of real estate asset financial reporting and cash flow data may not yet a have standard established. In these cases, the project must define the format and method for exchanging the data.

On the other hand, the exchange of energy consumption data has been done for a long time and is relatively well understood. However, the units of measurement chosen by the organization greatly determines the format of the data exchange because energy data can be expressed in many different ways. So, the project must specify what units or other format certain pieces of data must follow.

The important point is that if any data or information is to be exchanged between systems, the methodology for that exchange needs to be well understood and documented *for the project*. ASHRAE has created good methodologies for building data that can be utilized as an example.

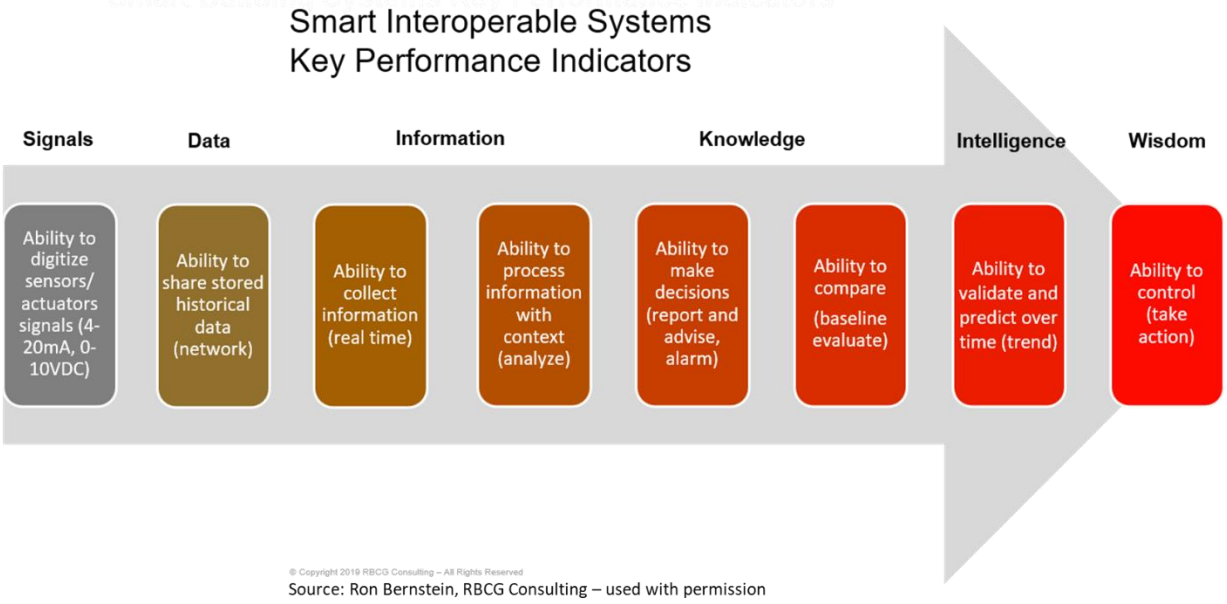
This section requires defining how data is to be exchanged between each tier of the system, which would include (list which exchanges are required for your project, examples shown):

- Subsystem to Subsystem data exchange (HVAC to Lighting)
- Subsystem to BMS data exchange (HVAC to GUI)
- System to System (API: HVAC to Energy Management)
- System to Application (HVAC to Analytics App)
- BMS to Cloud Services (Enterprise portfolio data aggregation)
- Cloud Services to BMS (utility meter data to energy management application/dashboard)

50.2 Data and Information Portability

Data sources and destinations can exist on all tiers of the building control, management, and operations systems. Sensors create data, actuators consume data, controller manipulate data. Along the way, there is a requirement that the data have an established context so that it can be understood and used by "others". Others includes controllers, applications, interfaces, and services.

The graphic below helps provide context as to the evolution of building system "smarts" starting from signals from sensors and ending with actionable intelligence and the wisdom to manage the system.



Source: Ron Bernstein, RBCG Consulting – used with permission

As we move from left to right, the data provides more and more value. More context is added such as location, frequency, range, duration, reliability, comparative parameters, historical

analysis, and more. All of this requires a strong set of rules and objectives for how data is shared, how it is sourced, and what can the destination do with it.

50.3 What are well-behaved API's?

API stands for application programming interface – a set of definitions and protocols to build and integrate application software. An API is the software intermediary that allows two applications to talk to each other: the Interface. APIs are an accessible way (for programmers) to exchange data within and across systems.

Most companies that produce equipment or software say that they can integrate with other systems, and that they have an API. A common statement is, "We can integrate with any system, as long as they use our platform". Proprietary platforms, databases, protocols, and data structures defeat the intention of smarter buildings. Defining requirements and verifying the API documentation is critical to achieve reliable project success. API documentation should include a set of data points or "points lists", a data architecture diagram, a well-defined owner-based nomenclature, detailed data semantics and metadata information, and a library of programming commands to receive information from the system and write data points to the system. Most critically, the API documentation should include all necessary information to enable other software programmers to utilize data from the system.

Think of the API as a black box; inside the box is where the magic happens – that's the programming logic, the "secret sauce" that is the innovation of the supplier. How that black box communicates what it does, how to interact with it, what it can do, and how it can help other applications with their tasks is the role of the "interface".

The data transferred via these interfaces may not be a single data point, it may be a collection of data such as a trend log, it may be an aggregated set of data such as the power requirements across multiple loads, or it may be even more complex data assemblies using constructs such as multi-state variables, variable arrays, time-based data, and compound data blocks using character string values,

An example of a complex data set might be the time-based percentage of measured occupancy of a space versus the anticipated occupancy of that space with 15-minute intervals over an eight-hour period. Add in the historical information over a 90-day period to predict the cooling load of the HVAC system to optimize occupant comfort and reduce energy. Data sets can get arbitrarily complex as analytics tools and AI applications take raw and complex data into their applications and provide actionable results. Throw in "fuzzy logic", self-tuning, and predictive outcome-based routines and the level of complexity surpasses what most owners and engineers typically consider for their requirements. But advanced applications are now taking advantage of the available data and using it in these complex ways through modeling, simulations, and historical analysis to help predict future optimizations.

Not all APIs are created equal. And because exchanging data with other systems is fairly new to building systems, smart building APIs are evolving and will become more well-established as their value increases. Many building systems were developed inside closed, proprietary platforms, the mechanics of which are not readily shared with outside vendors or customers. Many were created before we had mobile devices and apps and were not designed to work effectively or quickly there. The new standard for open data architectures where data is easily exchanged among all component systems is stretching older systems and applications in ways they were not designed to handle. Older systems and their associated applications may not be able to work within the new environment, however, there are vast number of "drivers" and interfaces openly

available in an attempt to bring the old into the new. In many cases, these tools are simple converters from a proprietary format into one or more open formats. This can significantly benefit organizations with a multitude of older, incompatible and non-interoperable systems.

A well-behaved API is easy to program (for software developers), exchanges (extracts and receives) the required data reliably and quickly for users, and is easy to maintain as things evolve in a multi-system data architecture.

50.4 General Data Exchange Requirements

A. Use the same words for the same things, including the names associated with buildings, floors, rooms, zones, and spaces, across your whole smarter building portfolio. This includes acronyms, terms, definitions, naming standards, use of special characters, and more. Data standardization, naming conventions, and common ontologies (how things are assumed to be organized, which can be different between systems) need to be considered and agreed upon prior to implementation for any meaningful data and information exchange to occur. Please refer to section 25.25.60.

B. All data will be normalized, as per 25.25.60. This is often a task of the BMS front end software applications which contains the database, user interface, and translation and normalization tools. Simple normalization might be converting units. Another might be changing a name.

C. Applications utilize the API tools as determined by the owner/tenant.

D. Applications will utilize the owner and/or tenant provided common naming conventions for assets, spaces, and zones (preferably with universal unique identification UUIDs tags) to ensure interoperability and ease of configuration.

E. Applications will have the capability to send and receive commands and data from other systems and interact via openly published API commands or similar IP-based open data exchange methods.

F. Applications follow the appropriate open-standards and protocols based upon the provided owner and tenant requirements. (This information has to be defined in a specification language prepared by qualified design professionals.)

G. The exchange of data uses open and currently accepted and published mechanisms. Examples of current open data exchange mechanisms include BACnet IP, LON IP, MODBUS IP, RESTful, MQTT, OBIX, and OPC. While some of those listed here are considered “protocols” for data communications, they do, as part of their standards, define many of the details necessary for improved interoperability. For ontologies, tools such as Haystack, Brick, ASHRAE’s S223P Semantic Interoperability are useful starting points for developing owner focused standards. It is also important to understand the mechanisms may differ with device-to-device, device-to-system, and system-to-system data exchanges. Choosing the right set of tools will be dictated by the data source and destination requirements.

~~H. Data exchanges shall be based on established information models.~~

~~I. All data exchange mechanisms will be resilient by established government standards.~~

J. All data exchanges shall follow recommended cybersecurity requirements outlined in section 25.25.95. An example for a highly secure environment is the requirement that every data exchange must provide end-to-end encryption of data.

K. Data that contains PII (Personally Identifiable Information) shall be separated and identified as such. Building automation data that may contain personal information might include the name associated with an office, the temperature setpoint default of a space associated with an individual's profile, user access logs, all access credential information, all security/access credentials and usage logs, etc. While these are uncommon in typical BAS designs, the installer and integrator must be aware of any data that may be considered PII or owner confidential.

50.5 Example Requirements for Project Purposes/Goals

Below are some examples outlining what would need to be defined for data and information exchange specific to certain project goals. Your Owner's Project Requirements doc should include similar details specific to your project goals.

50.5.1 Enabling Remote and Efficient Building Operations

If a goal is to empower building operations, management, automation, and reporting by asset (such as elevator, air handling unit, or lighting ballast), require data about the following to be exchanged and available across systems:

A. Schedule requirements – normal hours of operation, shoulder hours, off hours, etc.

B. Utility utilization / metering data (instantaneous power usage and storage capacity when possible)

C. Automation interoperability, triggering or receiving commands as appropriate

D. System alarm, alert, and event notification

E. Ticket tracking in conjunction with service, scheduled maintenance, and failure repair

F. Remote application interface to view, configure, and manage the above information

50.5.2 Contact-less Tenant Experience

If a goal for a multi-tenant space such as an office building is to deliver a contact-less tenant experience and if you require data from the systems to be exchanged and available across systems, then an approved access control credential (key card, fob, phone app, etc.) can be utilized to trigger any of the following, :

A. Parking (gate opening, charging, tracking, etc.)

B. Elevator control (taking tenant to pre-programmed floor)

C. Door control and access control (opening and closing)

D. Room scheduling and booking

E. Unified communications call launch in collaboration spaces

F. Access to room control systems (for lighting, shades, temperature, and audiovisual devices) and associated extra services such as food ordering / in-room dining, etc. based upon the building type

G. Point of sale (POS) integration for cafeterias and vending

H. Fitness center access and machine control

50.5.3 Grid-Interactive Efficient Building

Based upon grid signals for price or carbon offsets, automating and optimizing building performance, building systems should have the following:

A. States of operation:

A.1. Running or Idle Normal, Running or Idle Curtailed, Running or Idle Heightened, Override On/Off, Cycling

B. Electrical Usage:

B.1. Instantaneous power usage and/or storage capacity (when appropriate)

C. Grid Interactivity Response:

C.1. 1-3 levels of Shed (use less energy or release stored energy) and 1-2 levels of Load Up (use or store more energy)

50.5.4 Return-to-Work Efficiencies Based on Occupancy

Many commercial buildings are challenged to run efficiently as people return to work after the COVID pandemic, and want to use space occupancy to automate and optimize building performance. To facilitate that, all building systems should have the following:

A. Data on states of operation:

A.1. Active daytime state

A.2. Standby daytime state (with appropriate recovery based upon system)

A.3. Active off-hours state

A.4. Quiescent / overnight state (off or lowest consumption mode)

B. Based upon the states above, be able to operate the following energy-consuming or energy-conserving systems:

B.1. Lighting control (recalling appropriate scene)

B.2. Shade control

B.3. Temperature control

B.4. AV and multimedia systems

B.5. Elevators, escalators, and conveyance systems

B.6. On site energy storage

50.5.5 Modeling and Simulation of Building Operations

Modeling and simulation of building operations is an important consideration for data and information exchange. Modeling can be utilized to estimate the energy use impact of major, capital-intensive changes such as reglazing or switching to an all-electric approach for heating and hot water. Modeling can also be used to test out different space utilization plans to optimize the use of both space and utilities. All the data sets described in the use cases above contribute to more accurate granular modeling.

These "digital twin" uses of data will become increasingly important as tools and applications are developed that will require data on broader and deeper level. The use of cloud computing resources for modeling will make this type of real estate asset management possible.

If your design team plans to model or simulate building operations, you should define the outcomes they expect, and the data they will need in the design and specification and list modeling as an important Application in section 25.25.40 above.

Data modeling requirements are typically based upon an adopted semantic and metadata structure. Platforms such as Haystack and Brick offer starting points for some of the information needed to provide modelers with consistent data sources. The ASHRAE 223P Semantic Interoperability and 231P Common Descriptor Language teams are working on additional tools and proposed standards to help tighten the interoperability requirements of building equipment and BMS software applications.

50.6 Data Interfaces, Gateways, Translators, Protocol Routers

A key aspect of data exchange is understanding the need for physical devices that convert or manipulate data and transfer it elsewhere. The objective of any smart system is to reduce the necessity of these types of data manipulation devices as they are difficult to maintain, complex to configure, and can significantly slow the efficiency of a smart building system. It may be practical in some instances to require all communication using only one prescribed protocol and one prescribed ontology. But, in typical project where integrated automation is required, the system designer must account for multiple protocols, interfaces, and tools needed to transport data from source to destination.

A few hardware devices that are common include:

- Protocol Routers – in the IT world, these are referred to as IP routers, but for other protocols and communication channels, the router term is often used in a more general sense where the device receives data on one side of the box and pushes out the other side, typically translating or encapsulating the data into one or more network protocols.
- Protocol Bridge – this type of device is signified by its ability to change media types without necessarily changing protocols. An example would be a powerline carrier to Ethernet bridge, or an RF to Fiber bridge.
- Network Interface – this is typically a device that connects a proprietary device with a custom interface to an open protocol network. An example is a fire panel interface card that uses an RS-232 port to export information to a BMS front end using IP. Interface

devices (cards, modules, boxes, controllers) are commonly connecting one physical device to a network.

- Protocol Gateway – this is a device that converts one protocol to another, typically leaving the base data intact. Incoming messages have their protocol headers and footers stripped out and then re-encapsulated in the outbound protocol format. An example would be a LON to BACnet gateway.

Other data interfaces include:

- Drivers – software applications that can be embedded into other applications to all communication to proprietary or other open protocols
- Aggregators – applications that communicate and collect information from multiple devices using a vendor specific or custom protocol and converts the data to an open protocol or database format for use by other applications
- Web Services – IP based applications that share data using standards based on TCP/IP and UDP/IP protocols. Examples include HTML5 for standard web browsing data formatting and presentation.
- A gateway device or hub that manages communication between a set of devices and the digital network. This could include a hub that translates MQTT protocol used by a set of devices, to IP protocol that the IP backbone uses

25.25.60 – Data Governance

This section outlines the project's governance (policy) requirements for data ownership, format, context, temporal and spatial structure, naming conventions, storage hardware and software, management, database structure, access, continuity, and data security and privacy

Where section 50 is about the movement of data, section 60 is about data "at rest." This includes how it is stored, organized, recorded and available for retrieval. Having organized data is crucial to the success of an integration and interoperability initiative.

Data itself can typically be categorized into three groups:

- Master Data - Master Data is the unique information which rarely, if ever, changes. Street addresses, model numbers, or the gross floor area of a building are all examples.
- Metadata - Metadata is data about data. How the data was collected, when it was collected, where it was collected from, details about the data such type, unit, range, calibration, reliability, precision, priority, etc.
- Transactional Data - Transactional data is data generated by systems supporting daily operations. Examples include energy utilization / metering, the quantity of service calls, or the financial net operating income (NOI) of a property. Transactional data can include calculated data, combined data, and compound (complex) data, where raw values are transformed via formulas and the results are stored as separate values or sets of values.

The management and understanding of data at its most granular level is crucial for the success of an interoperable smarter building. The formatting, standardization, and alignment of data ensures data portability and the easier implementation of new requirements in the future.

This section includes:

- You Need a Data Points List
- Should I Have an Independent Data Layer?
- General Requirements for Data Governance

60.1 You Need a Data Points List

Operating "smarter buildings" requires data, and making the smarter building solution work correctly requires knowing what data you have to work with. So, you need a Data Points List.

A Data Points List is what is sounds like. It's a list of all the data collected, and made available, by each of the systems involved. Depending on the complexity of your solution, the list of systems involved might be long. And the data points for each one will likely also be long. So, compiling the data points list can be arduous, and will likely require several iterations. It's kind of a pain, but it is necessary.

The Owner's Project Requirements doc should state that all the vendors need to provide a Data Points List for their respective equipment and/or systems. Note that some required data might not be part of any "traditional" supplier's list, and the mechanism and responsibility for bringing that data into the project might need a special process.

To ensure the combined systems will be able to execute the intended smarter building functionality that requires sharing of certain pieces of data, the owner's project design team might pro-actively create a list of required fields for certain systems, and include those in the project Specifications.

Involving an experienced Master System Integrator during the project design process is a good idea, to help create the data specifications that will be requested from each vendor/supplier.

Complex points lists are evolving into equipment profiles where the points list includes additional information about system or device above and beyond just the raw data. Equipment profile use the points list as its foundation and can then add location, vendor, make, model, instance, SOO implementation details, recommended and default setpoints, COV or Polling requirements, update intervals, addressing information and more. A complete points list will have sections for:

1. Design - including point name, object type, description, units, range, resolution
2. Integration – including monitoring, alarming, trending, priority, read/write/command, point properties
3. Commissioning – which points are to be end-to-end commissioned (tested and validated from the sensor or actuator all the way to the BMS front end graphics)
4. Implementation Notes – details about specific attributes and implementation requirements for each point (optional, but helpful).

60.2 Should You Have an Independent Data Layer?

What is an Independent Data Layer, and what are the Pros and Cons of having one?

Integrating multiple sources and uses of data for a portfolio is hard. Different component systems collect and use data at different time intervals, name things differently, format things differently, update things differently, store things differently, and exchange things differently. Some need and store the same information (like room numbers or names), requiring intensive attention to ensure data matches everywhere when it changes. And, if the same data fields are

recorded in multiple places, and they don't match, it's impossible to be sure which values are the correct ones. Integrations involving multiple systems are specific to the exchange between each pair, greatly multiplying the number of exchanges to build and update and keep track of. That means, if I want or need to swap out a particular system or vendor, I have to start over from scratch. All this makes developing and maintaining a modern, mobile app-fronted experience hard. And the opportunity to develop new, even higher-level functionality even harder.

Enter: The Independent Data Layer

An Independent Data Layer (IDL) is a centralized layer of an information stack where data from source devices and systems is collected, normalized, stored, and made available to applications higher in the stack or parallel in the stack (system-to-system) in a unified and consistent way.

[Pros:

- Enables consistency between systems and from system to applications
- Enables analytics tools to more easily extract and use relevant data to provide operational insights
- Provides an extensible platform to build additional tools and applications upon
- Typically, is done once for a project – not needed to recreate on an ongoing basis
- Provides support for IT based web services, cloud services, and enterprise applications

Cons:

- Can be time consuming to develop
- Can be costly to develop
- Requires significant subject matter expertise across multiple domains
- Can be error prone – garbage in = garbage out
- May be beyond the scope of simple to moderate facilities

Inserting an IDL into your information stack architecture can be a great idea, but, it too is hard. It requires, by definition, deploying a separate layer, different than whatever your component system suppliers deliver. And that requires time, expertise to set up, operate and keep up to date, and money.

There are not many easily deployed IDL solutions offered by vendors yet, but more Master System Integrators and platform companies are developing solutions that are more "productized," so the market is moving in this direction. A collection of vendor resources is available at www.c4sb.org.

60.3 General Requirements for Data Governance

A comprehensive Smarter Building Owner's Project Requirements document should define for the project what is needed for the following elements relating to data "at rest:"

60.3.1 Data Governance

A. Ownership – Who owns the data and has rights to use it?

A.1. Recommended: All data is owned by the building asset owner and the appropriate tenant for data about their space as well as their portion of

common area maintenance costs. A suitably designated party may also have access and/or ownership of the data if approved by the appropriate owner and tenant.

A.2. Recommended: All data required for government and environmental, social, and governance (ESG) reporting is an allowable use per the need or desire of the owner and/or tenant.

B. Privacy – What privacy policies, procedures and safeguards need to be in place? Does your portfolio include sensitive information? At what level? What about privacy of sharing data from one company who is part of the smarter building solution with another? What about sharing data with outside companies or entities?

60.3.2 Data Architecture

A. Definition: "Data" here refers to all data and information related to the building wherever stored and however created. Data represent assets in buildings, which can be physical, virtual, or logical. Data can also represent relationships between assets.

B. Recommended: Standardized metadata structures should be adopted for specific data types to match the owner's requirements. The standardized metadata structure should follow industry standard file types and formats where available. If a metadata structure does not exist, the metadata structure chosen or invented will be clearly documented and shared

C. Recommended: Avoid creating multiple conflicting metadata and site nomenclature standards. This can easily happen if two or more subsystem suppliers and integrators work in silos, making enterprise level integration cumbersome and inefficient.

D. Recommended: Data shall use storage models that are open, standardized and allow access to web services that allow for accumulation and storage as further defined in this section 25.25.60 (if further definitions are provided).

E. Recommended: Data structure relationships and classifications should be generalizable to new situations.

F. Recommended: All Data is to be made available to any legitimate system using mechanisms set out in 25.25.50 – Data and Information Exchange.

60.3.3 Data Naming, Tagging and Ontology

Data "at rest," or stored, should comply with common organizing, naming, tagging and labeling conventions established for the project. Collectively, this is called "ontology."

A. Nomenclature – calling the same things by the same names is important, e.g., all exhaust fans should be called the same thing, like "Exhaust Fan," and not "Exhaust, Fan," "Fan – Exhaust," "Fan – Restroom," etc.

B. Nomenclature – Recommend requiring that data labels and field values (such as equipment names) avoid using site-/building-specific tagging, instead relying on semantic tagging (see next point) and metadata relationships.

C. Semantic tagging – data can be "tagged" to provide context, so that queries recognize what belongs together. The industry has starting adopting some tagging standards created by Haystack and Brick, among others.

60.3.4 Cybersecurity

See section 25.25.95 for more on cybersecurity.

60.3.5 Reliability and resiliency

A. Storage and retention – define requirements for how, where, and for how long data needs to be stored.

B. Backup and recovery – define requirements for backing up all data, and procedures for data recovery in the event of a loss

C. Frequency requirements for collected data must be defined. Use caution when setting update intervals not to collect meaningless or over-saturated data logs.

60.3.6 Application example: Grid Interactivity

Specific applications that are part of your smarter building solution may require access to retrieve data from or write data to other systems. This section should specify the rights to do so.

A. Example: All data required for Grid Interactivity is an allowable use for sharing per the need or desire of the owner and / or tenant. (See section 25.25.41 for more details of this example.) Data may be sourced from the local utility in a historical way (downloaded spreadsheet from the utility's website), or it may be real-time using tools such as the Green Button interface.

B. Buildings may also interface to grid services through one or more utility web-services interfaces such as Open Automated Demand Response (OpenADR), load aggregators, microgrid interfaces, and even solar, battery, and EV charging station interfaces.

25.25.70 – Control Systems

This section defines the control systems directly connected to the physical elements listed in section 25.25.80, and that provide "built in" controls and automation, and/or the digital communication bridge to other components of the same system, as well as to other systems, applications, buildings, or entities outside of the portfolio.

The control system may be referred to as the Building Automation System (BAS) and, based on the ASHRAE Guideline 13, include Tier 2 infrastructure equipment and their controllers, and Tier 3 packed equipment with embedded controllers, programmable controllers, and supervisory controllers. The control system includes those components that ensure the building's control sequences of operation are met. Often the BAS networked controls can run autonomously from the BMS front end and along report to the front end for alarming and event management. Some vendors lump the BAS and BMS into one solution. For the discussion in this framework, we separate the two to be more in line with ASHRAE and provide more clarity for specifiers.

Topics include:

- List what control systems are included. For your project, use this section to define (list) the control and automation systems that connect to the physical devices (identified in section 25.25.80) and that provide "built in" controls and a communication bridge to other components of the same system, as well as to other systems, applications, buildings, or entities outside of the portfolio.
- Define what each needs to do *to work with other systems* (following requirements of sections 25.25.50 and 25.25.60 above) to deliver the intended smarter building functionality. This includes interoperability requirements common to all control systems and interoperability requirements that might be specific to an individual control system. These can include:
  - Define data required for meeting *multi-system* sequences of operation.
  - Define any control system platform requirements for interoperability.
  - Define how each control system supplies data to higher level applications.
  - Define any system-to-system integration requirements
  - Define what each needs to do *to run the physical layer below it*. For this, it's ok to reference sequences of operations defined in another CSI division specific to certain equipment.

Expert Tip: You can think of the systems and equipment identified in sections 25.25.70 Control Systems + 25.25.80 Physical Elements as needing to run "on their own" in order to meet the building's basic operations. In other words, if the "smarter building" applications and communication didn't work (because Internet connections were down, or an app was offline), the building should still operate "in normal mode." Designing the control system with the "Intelligence at the Point of Control" using a distributed architecture will help remove single points of failure and over-reliance on higher level applications and networks. Remote visibility and control, and higher-level automation might not work, but basic building operations like doors opening and locking, lights can be turned on and off, there is heat and air conditioning, etc., would.

70.1 Which Control Systems are Included?

For your project, use this section to list the control and communication systems that provide "built in" controls and that connect the physical components to the digital network. Make a list, ideally coordinated with the components list in section 80.

Examples include:

- A Building Automation System (BAS) that controls HVAC equipment.
- A lighting controls system.
- A fire alarm control panel.
- A set of power/electrical panels with a supervisory controller aggregating submetering, quality, and other useful data and performing backup generation coordination.
- A refrigeration panel and supervisory controller for multiple coolers, freezers, cases

- A solar inverter(s) interface panel and supervisory controller providing power information from PV and batteries and managing co-generation and other DERs.
- An edge control panel (PLC) for a specific device
- ~~A gateway device or hub that manages communication between a set of devices and the digital network. This could include a hub that translates MQTT protocol used by a set of devices, to IP protocol that the IT backbone uses~~.

70.2 Requirements for Control Systems to Work with the Smarter Building

All the control systems specified for your project will need to adhere to requirements that will enable them to operate as part of the smarter building. You can organize requirements for interoperability based on which are common to all control systems, and which are specific to an individual system.

The following list *is an example*. All of these are not necessary for ALL projects. Your list may be different.

70.2.1 Common Interoperability Requirements

For this project, all systems should comply with:

A. Exchange of data between field device networks to use open protocol standards that maintain interoperability.

B. Data shall use models that are open, standardized and allow access to web services that allow for accumulation and storage as referenced in section 25.25.60 Data.

C. Control system applications shall support portability.

D. Control system applications must be interoperable and, where practical, self-installing.

E. Communication channels shall use standard media to facilitate data transfer.

Such media can utilize (your spec should specify which are acceptable):

- Twisted Pair Copper Wires (RS-485, Free-Topology)
- Multiple Twisted Pair Copper Wires (Ethernet)
- Power Line Wiring (HD-PLC)
- Fiber Optic Cable
- Radio Frequency (450 kHz to 300 GHz fixed, multi-band, and frequency hopping)
  - WIFI
  - LoRa
  - Zigbee
  - zWave

F. Hardwired connections to equipment and devices will utilize established industry standard plugs and terminals that provide mechanically secure and long-term reliable contacts. Wired connections shall not emit electro-magnetic radiation that exceeds authorized frequencies and transmission power levels specified for the project's geographic region.

G. Wireless connections will communicate over authorized frequency ranges and transmission power levels specified for that geographic region.

H. Control signal connections will not be placed in close proximity to power cables such that interference, noise, and transients are introduced onto the control signal communication that may disrupt or prevent reliable data transmission.

70.2.2 System-Specific Interoperability Requirements

The following control systems have interoperability requirements specific to each, as noted. Your document will be longer here, because you will fill in the details for each system. This section lists requirements for each system to interoperate with other systems, in addition to the common requirements in the preceding section.

Each system has other requirements to perform the control and operations of its component equipment, and those are described in the specification division for each system (such as DIV 21 Fire, DIV 23 HVAC, DIV 26 Electrical, DIV 27 Communications, etc.)

A. HVAC BAS System

B. Lighting Control System

C. Water/Steam/Boiler Control System

D. Access Control System

E. Elevator Control System

F. Electrical Control System

G. Solar/Generator/DER Control System

H. EV Charging System

I. Refrigeration Control System

70.2.3 Requirements for Control Systems to Independently Run the Physical Building

At a higher level, more sophisticated projects may require articulating what needs to happen WITHOUT the smarter building technology.

Sometimes Internet connections go down, unified dashboards have issues, and mobile apps don't work. So, it is useful to define which building operations must work independent of whether the smarter building higher level functions are working.

Use this section to identify the basic building operations that are required to work in the event that higher level smarter building functionality isn't available.

To think this all the way through, follow the following steps for your project:

A. Define desired conditions and systems that require no intervention needed from within the internal and external spaces. Samples include:

- Fire alarm system must be fully operational.
- Fire suppression system (e.g., sprinklers) must be fully operational.
- HVAC smoke evacuation system, triggered by the fire system, to work independently and be fully operational

- Emergency exits must always operate.
- Exterior and interior doors must be accessible for egress and ingress.
- Lab pressurization must be maintained.
- Gas sensor alarming system (refrigerant leak detection, H2S, SO2, VOC and other toxic sensors) must be fully functioning independent of any other system.

B. Define desired conditions and systems that will work based on manual intervention from within the internal and external spaces. Samples include:
   - Emergency power (generator or battery system) must be able to be turned on and off manually.
   - Exterior doors must be lockable and unlockable.
   - Elevators must function manually and in fire-support mode.
   - Hot water heaters must function, at least manually.
   - The building must have heat, equivalent to fully occupied and fully unoccupied (off-hours) modes.
   - Lights (perhaps only in specified areas?) must be able to be turned on and off via manual switches or circuit breakers.

C. Define desired conditions that allow for automated processes to provide intervention within the internal and external spaces. (This is when your building operates as a smarter building.)

70.2.4 Network Infrastructure

The control systems will require specific network infrastructures for their installation and operation. While most of the details regarding the network for communications is typically covered in DIV 27 Communications, it is good to address any specific requirements for the smarter building in DIV 25.

For example, BACnet IP requires that all devices that will communicate with each other exist on the same subnet. If not, them more complex “routers/bridges” are required to bridge two subnets – something to avoid if possible.

A good network diagram capturing all of the wiring, pathways, connections, ports, and equipment will help all project team members efficiently and effectively provide the network backbone.

Network infrastructure drawings typically provide very sensitive detailed data about the facility such as MAC addresses, IP address, locations, and functionality. These drawings and documents should be labeled sensitive and be tightly controlled. Bad actors may use this detailed information to access the control network. See the Cybersecurity section for details.

The control networks will typically require a lot of wire. Understanding the wiring, cabling, cable tray, panels, ports, and rack requirements is, again typically a DIV 27 and sometimes DIV 26 section, but the DIV 25 spec must include the overview architecture, responsibilities, and connectivity of all control network elements.

Coordination between the parties is very important. Specifiers may opt to include the same information in multiple divisions and identify the primary and secondary responsible parties. Duplicating information in specifications is acceptable as long as the divisions of responsibility are clearly identified. Using the phrase, “installed by others” and then identifying the contractor or division is very appropriate.

25.25.80 – Physical Elements

In the ASHRAE 4 Tier model, this is the Tier 4 Sensors and Actuator tier. It includes all of the end devices, the pumps, motors, probes, thermostats, relays, and all of the various sensors. In some cases, these “end devices” are connected to Tier 2 programmable controllers connected by a set of wires (4-20 mAmp, 0-10 vdc, dry contacts, etc.). The controllers process analog and digital signals coming from and to the sensors and actuators and convert them from or to digital information that is then shared on the network. However, as compute horsepower shrinks in size and costs, more and more end devices are becoming “smart” by adding in communication capabilities. The age of IoT devices (Internet of Things) is based on the principle that the end device has the ability to exist and provide value on a network without the need for a secondary controller, supervisory controller, or other such device.

Examples of smart end devices include smart, networked thermostats, occupancy sensors, valves/valve actuators, motors, drives, IAQ (Indoor Air Quality) sensors, daylighting sensors, sun shades, AV panels, lighting fixtures, leak detectors, door sensors, acoustic sensors, weather stations, and many more.

In this section it is important to not only select what types of devices are required but also how they will communicate or through what device they will communicate. If the end devices are not “smart” then this is typically left to the contractor responsible for the end devices and only the Tier 2 programmable controllers need to be specified as smart.

Smart end devices may also have alternate communication paths such as to a cloud application that directly communicates to the devices in the building over an open IP communication path. IoT based systems require this cloud-to-device open pathway to perform their functions. A simple example of this is a solar inverter that has an RF interface to an Ethernet module. The Ethernet module acts as a bridge to the inverter and communicates to a vendor specific portal that captures solar performance, alarms, and energy related data. The internet access is not required for the solar system to produce energy, the inverter does its job even if the internet connection is lost, but the higher-level interface, data collection, and user interface would be disabled until connection is restored.

Certain devices can retain data for extended periods of time and only send data logs on a periodic basis. These devices can have substantial internal storage and can maintain their own logs and use a “store and forward” approach to reporting. This is effective for historical logging but not for real-time alarming. Devices that use this methodology would need to provide their maximum data storage time limit and the data upload interval must be lower than the max limit in order to ensure no data is lost. Some devices may choose to implement a rolling dataset where only the latest data is stored locally. Sometimes referred to as a “FIFO – first in first out” or a “rolling-box-car” storage where older data is replaced with newer data and there is a fixed size of the data log file. Knowing this can be very helpful to analytics tools.

Enterprise APIs that collect data from a multitude of IoT end devices can offer owners great insights into a subsystem operation, efficiency, and related metrics. The down side is that you

now have an alternate network path to a device that must be managed and maintained. Understanding the impact on network design and network cybersecurity is extremely important when deciding who and how access is provided to smart Tier 4 end devices.

In addition to the sensors, actuators, and equipment, it is also useful to define the physical structure of the facility here. This includes the rooms, spaces, zones, floors, and structures that make up the facility. This provides the foundation for the site nomenclature such that all networked devices have the same physical location identifiers. This foundational information is critical to applications such as security, lighting, thermal comfort, energy management, space resource management and more.

This section should be used to describe the physical components of your portfolio/building/ project – the actual devices and spaces – that the digital smarter building system will connect to, monitor, control or interact with. This section can also be used to articulate what needs "smarter" functionality, what does not, and any enhancements needed to those elements to enable such functionality.

To do this for your project, compile and share the following lists:

- Building List
- Space/Room List
- Device & Systems List
- Required Physical Improvements List

80.1 Building List

What is/are the name(s), address(es), size(s), and major use(s) of the building(s) in the project? (List them in a table.)

When building a site nomenclature document, it is important to identify the scope of the total project. This means to account for the entire enterprise under one nomenclature. If a project has multiple campuses, start by identifying all of them using a moniker such as a two-letter acronym. Then move to each building within the campus and select a unique 2, 3 or 4 letter/number acronym. By combining the campus and the building numbers you are then guaranteed that no two buildings will have the same identifier. This is critical for campus and enterprise applications that will eventually collect information from networked devices, BMS servers, and cloud servers. Having a unique set of identifiers and having this built into the owner's OPRs will greatly reduce the installer and integrator time and cost. As building databases are created for the digital lake/digital twin, consistency and reliability are primary factors in ensuring the building is not only smart, but efficient.

80.2 Space/Room List

What specific spaces (indoor rooms or external spaces) will be covered? Expand the building list table to list the rooms and spaces or refer to a floor plan. If appropriate and helpful, rooms/spaces may be grouped or coded by "smarter building functionality."

Likewise, the space, room, zone list should be consistent in naming conventions across all buildings within the enterprise. Start with a master nomenclature list and use the same abbreviations and acronyms everyone. Include in the OPRs and ensure all parties use the same

document. If a specific project/building, has unique spaces/rooms/zones, be sure to update the master nomenclature document.

One element of the space/room criteria is to identify where the OT networking equipment will reside. Given that a typical building's control network is pervasive throughout the entire building, from basement to roof, to minimize the cabling requirements, locations throughout the facility will need to feed to network switches. Identifying these spaces early will help reduce costs and align the scope of each subcontractor's networking integration effort. Just like a power pathways and water piping plan, a good control network design is part of any smart building design effort. Detailed "riser" drawings will identify the locations for all connectivity points for the OT network.

80.3 Device & System List

What are the physical devices and system assemblies that operate in those spaces and will be part of the smarter building system? Create another table and list them. Recommend organizing this list by system type to align with CSI sections, though some items may need their own sections outside of the CSI outline. This information will be very important to the MSI (Master System's Integrator) DIV 25 contractor as they will need to know every device, the type, location, quantity, points list, and integration requirements into the Tier 1 BMS front end.

If there are any specific devices or systems that are noteworthy because they are *excluded* from the smarter building project, you could list those here, too. There may also be devices are subsystems that have special integration requirements. Commonly, fire panels have very limited integration into non-fire systems and use either a contact closure, secondary enunciation interface (which is a one-way communication out of the panel) to the BMS server. Other examples may be accessing control/security reporting events/alarms, solar PV system, EV charging stations, kitchen equipment, freezers/cold storage devices, etc.

80.4 Required Physical Improvements List

What physical changes or improvements must be made to enhance the existing physical environment, so that it can support the intended smarter building solution? Describe these in narrative paragraph(s). Refer to project floor plans, if available and appropriate. Physical improvements should be also listed (or cross-referenced to/from) the other CSI division(s) where related work is specified.

80.5 Physical Device Location Map and List

This section of the specification provides a list and supporting details for all networked devices, their locations so that the IP cabling requirements for "drops" are identified. Many HVAC and refrigeration devices have built in Ethernet daisy-chaining ability, which can greatly reduce the number of home-run wired Ethernet connections. Identifying which physical devices have this ability and which don't is beneficial as it will provide the IT installation team an indication as to the number of cable runs and number of networked switches needed for the project as defined in the next section .90.

For example, HVAC VAV boxes often come with daisy chaining such that one connection from the local switch to the first box is required. Then each box connects to the next in its lineup. Some network designs then use a "loop" methodology where the last box in the lineup is then connected to a smart switch. If there is a failure in any one box, the rest of the boxes can continue to

operate. If no loop is installed, then any one box that fails will take down all boxes after it in the lineup.

25.25.90 – Networking

The "network" addressed in this section is the physical means of transporting digital communications for building systems and their associated components. Such a digital network would include the server(s), cabling, connection ports, routers, switches, and other related hardware. Architecting this network is a DIV 25 responsibility when it comes to the OT network. There are multiple architectures available to the owner. They include, but are not limited to:

1. A completely isolated OT from IT network
2. A converged OT/IT network
3. A partially integrated OT/IT network
4. Separate IP networks for each subsystem (legacy model).

Each of these options has their pros and cons. The decision process is based upon an assessment of need, resources, functional requirements, and serviceability. The type of architecture should flow down from the OPRs to the individual project design team.

All smart building systems, equipment, and devices require data communication, both between the individual components, Commination is required for device-to-device, between devices and their supervisory controllers, subsystem-to-subsystem, and any communication to the BMS front end, cloud services, and enterprise services. The goal of a smarter building is to acquire added insight and control by integrating the various building systems and components that help manage the property so that they can share information and interact with each other. As part of that, the goal of this section is to achieve a properly provisioned, *unified* data network for all of the operational technology (OT) building systems.

This section includes:

- How converged should my network be, between OT and IT?
- How do I do it?
- Who "owns" and will manage the network? The IT side? The OT intersections? Internal or external people?
- How do I plan for both initial CAPEX and ongoing OPEX costs associated with the OT and IT network?
- How will contractors/vendors get onto the network? Efficiently (easily?) and securely.
- What is the end result?

90.1 How converged should my network be, between OT and IT?

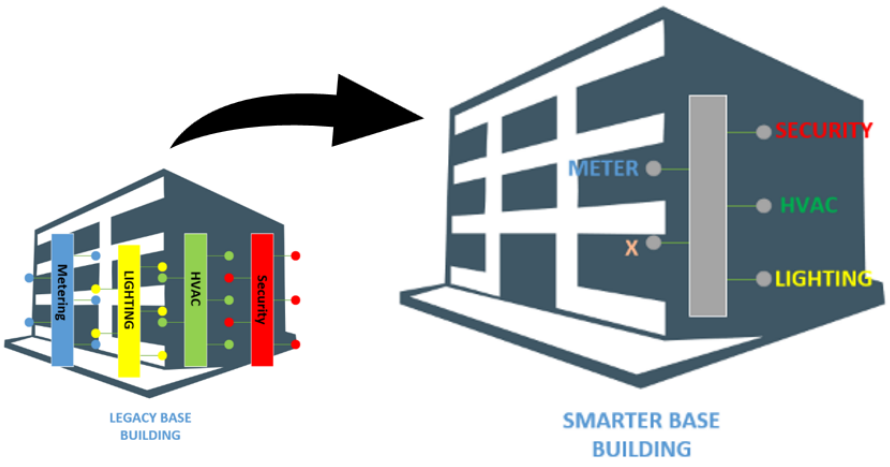
Smarter Requires a Unified Network

Historically, each legacy OT building systems has been installed with its own communication network, independent of other systems and the building's base IT network. BACnet had its RS-485 "MS/TP" network, LON had its FTT Free Topology Twisted Pair network, Modbus had its 2-

wire registry-based network, and many vendors had their own serial bus networks. Other protocols like Bitbus, Profibus, CAN, KNX, DALI, Zigbee, zWave, HDPLC, and others had their own network wiring/connectivity and communication standards. In recent years, more and more technology platforms are utilizing the benefits of TCP/IP and UDP/IP over Ethernet, WIFI, and Fiber Optic media. With one transport layer standard available across multiple media types, the network infrastructure in a facility becomes much less complex and more easily serviceable.

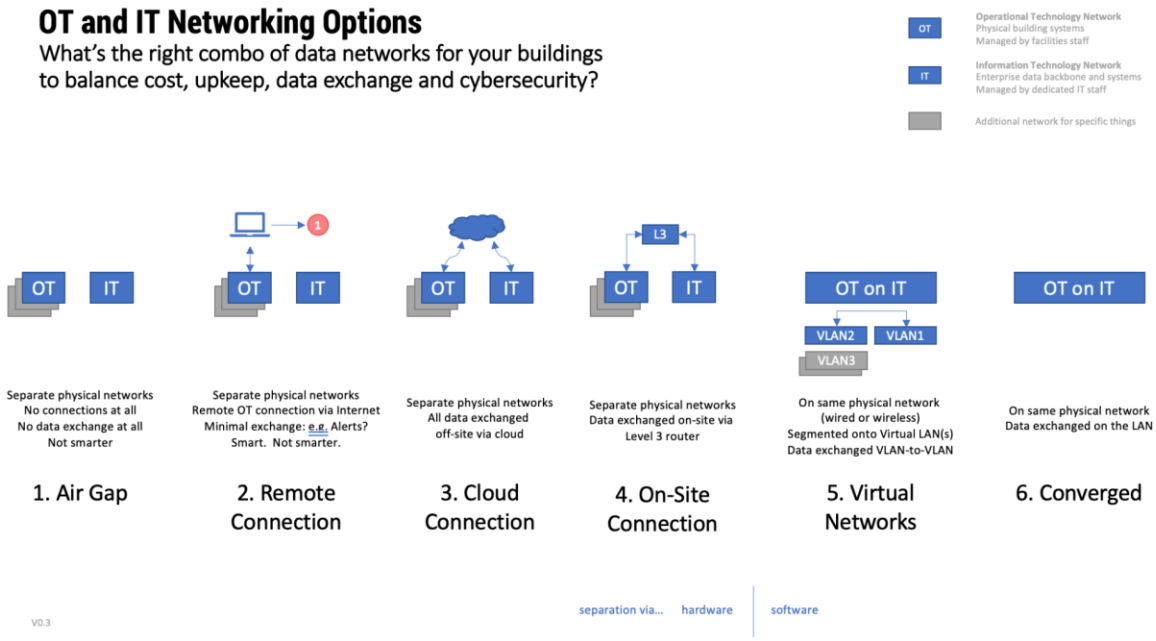
When each building system vendor would build their own network for their own system located in the various areas detailed in section 25.25.80 – Physical Elements, a building would end up with duplicate effort, multiple non-integrated networks, increased complexity, no interoperability and substantially higher cost. And, because each network was developed separately, they do not communicate in consistent ways, which creates barriers to exchanging data and control signals, and impedes smarter building functionality.

Luckily, OT system designers don't have to invent new ways of connecting. IP (Internet Protocol) networks already do these things, connecting servers, switches, routers, desktops, laptops, printers, and mobile devices to local and cloud storage, on prem and cloud apps, powerful AI engines, and new transaction marketplaces using a common network. And OT networks have evolved to be more like IT networks, sharing similar parts with similar communication needs from one system to another in the building and connected to the cloud and the outside world, preferably via the Internet. So, to enable a smarter building to share all the needed data and control inputs, OT network designers should either follow the model of IT networks, or, eliminating duplication, piggy-back on the IT network already there or planned for the building.



Smarter buildings are moving from the old, siloed, non-connected network controls to a well-integrated, common control network backbone and infrastructure.

There are a range of options for connecting OT and IT data networks. The figure below depicts these, from no connections between OT and IT on the left, to full convergence of OT operating on the IT network, on the right. Options are shown distinct from one other for clarity of definition. Often a building or portfolio may need to establish connections between systems and networks via a combination of the methods shown.



Note: in all cases, whether integrated with IT network or not, to provide maximum flexibility for future enhancements, internet protocol (IP) is the preferred basis for digital connectivity.

Case A: We have certain systems that we do NOT want to connect.
Perhaps information contained in certain systems, or the functions they perform, are too sensitive to risk exposure to outside networks. In that case, it is best to establish a separate OT network for the sensitive systems. One method to do this is "air gapping" those systems from each other and from the general IT network. (Scenario 1 in the diagram)

Case B: There is no IT network, but we want a smarter building.
There is a need to have connected OT systems independently. (Left hand side of Scenario 2, where either all OT systems connect on one OT network, or there are direct on-site connections between OT networks. Or, left hand side of Scenario 3, where each OT network is independently connected to the cloud, and connected to each other there.)

Case C: IT network will connect OT.
The building/company has an existing IP-based IT network that will act as the common network for exchanging smarter building OT data.

C.1. OT systems have their own digital network to communicate within their own system. A connection from each OT network is needed to the IP network, usually either via physical networking switches (Scenario 4), or…

C.2. Physically connect all OT devices to the common IT network, and use networking software to establish virtual networks for all of some of the OT devices, and then a virtual switch to manage data exchanges between the virtual networks. (Scenario 5), or…

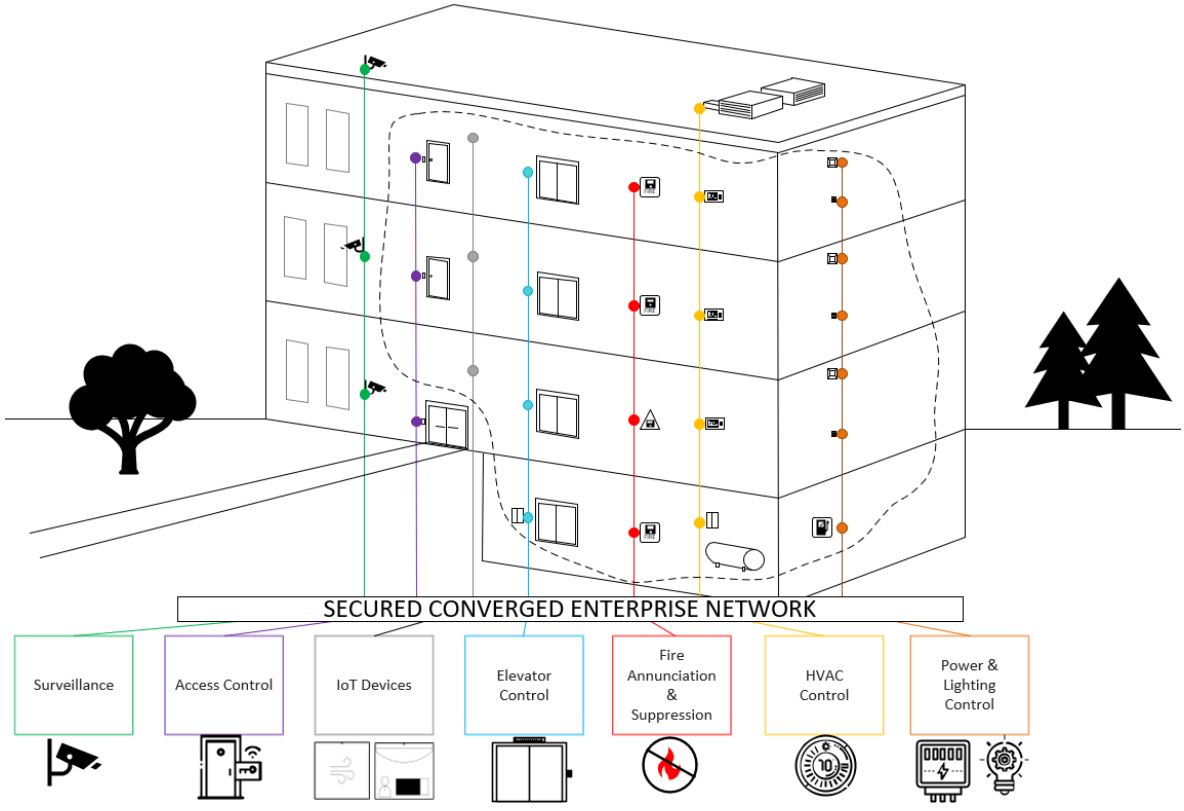
C.3. Physically connect all OT devices to the common IT network, with no separation between OT and IT devices and data traffic. (Scenario 6)

90.2 How do I do it?

The owner/developer would need to recognize the necessity for a consolidated network architecture and implementation plan (including roles and responsibilities) and state the desire for one, generally in the Owner's Project Requirements framework/play book document. The Architect or lead designer would incorporate space allocation and direct the project design team to include the network design into their scope of work. The size and scope will be determined throughout the design cycle from Schematic Design, Design Development, Construction Documentation, Integration, and Commissioning.

The size and scope of the cabling and active network equipment will vary depending upon the needs of the technology, location of the technology in the building, and the floorplates and number of floors. All of which will be flushed out during the design cycle. The network needs to be configured by qualified integrators who can manage and interact with the General Contractor (GC) and system integrators. They would take their direction on the configuration from best practices, owner IT standards, project requirements, and include Cybersecurity best practices, which are covered in the next section 25.25.95 – Cybersecurity.

What you end up with is something like the example below.



Communication with the various integrator groups is key. Assigning someone with the responsibility of delineating processes for connecting to the network and owning the dissemination of information is critical. This role generally falls to the network integrator DIV 25 contractor who then coordinates through the general contractor, or directly to subcontractors for each system.

90.3 Who "owns" and will manage the network during design, installation, and operations?

Connecting all OT systems to your IT network has some complexities that must be managed. A good first step is assessing the available resources. For the owner, this involves the IT team (if there is one), IT consultants (if the owner does not have internal resources), OT domain expertise of IT requirements, and the roles of contractors and consultants. Identifying a roles and responsibilities matrix can be quite valuable to answer simple questions such as: Who should be in charge? Should you rely on your IT team? Who manages the OT intersections? Can you do this with internal staff, or do you need external people?

90.3.1 Who is involved during design?

The network architecture design and implementation requires coordination between the owner/developer, project design engineers, construction team, and the various contractors. A resource such as a qualified network integrator will be required to be identified who can procure, install, and configure the network components based on the space allocated (where), the project design engineered Division 27 specification (how), and with input from building systems submittals (what). If the owner has an IT team, then they may be consulted or be responsible for a portion or all of the network, dependent upon their capabilities and how it is segmented.

90.3.2 Who is involved during installation?

Do you have a General Contractor managing everything at your project site? Is it an existing building that already has a data network? Does the project need a temporary network during construction? Should the team managing the existing facility's systems be involved in managing the new parts during construction?

90.3.3 Who is involved during operations?

Once construction and installation are complete, who do you need to operate your smarter building network? Do you have an internal IT staff capable of managing more devices, some that are not traditional IT hardware or software? Do you have an OT facilities staff capable of managing a data network, or at least the OT devices that are operating on the data network? Do you need a combination?

And do you have those resources within your organization, or do you have to contract with outside vendors to help?

There is no one correct answer. The combination that is right for your smarter buildings may vary from building to building, location to location, or over time. You just have to know to pay attention to revisiting these questions during each operational and budget review cycle.

90.4 How to fund the required OT AND IT effort? At the start and ongoing?

90.4.1 Where do the funds come from?

There is a general impression that being connected costs more. And while that may be the case, as technology advances and it costs less to deliver what cost more in

the past, and as forward-looking vendors re-shape and reprice what they can deliver, sometimes your building can be smarter for the same or a lower cost than traditional construction.

But sometimes it does cost more. And whatever it costs, it's likely that the smarter solution will have to be procured from a different combination of vendors than before. So, you may have to allocate budgets accordingly.

Remember, historically each of the building systems would require their own dedicated network, so reallocating the costs could be an answer to paying for both installation and management of a centralized network. As this network is part of base building infrastructure, if done correctly, it adds value to the property. There will be ongoing costs of maintenance and support either from the network integrator or your own IT department. Again, these costs were most likely sunk into the submittals of the building systems and may as well be reallocated.

90.4.2 CAPEX or OPEX?

In terms of when you might have to pay for smarter functionality, there likewise may need to be a shift from the traditional budget process. Smarter buildings need to not only be *built* smarter, they need to *operate* smarter. So, there will likely be a portion of the costs that are ongoing since they support operations.

Here there are trends in two different directions:

First, a familiar method of paying for buildings with capital expenditures (and debt financing) could be used to support a project, and the overall project cost that is financed is expanded to include a set amount of operational support. For example, construction costs could not only include installation of a system (or the several systems involved), but the first five years of active support (including software licensing costs, updates, and maintenance). This helps spread out the costs by putting *more* into CAPEX.

There is a second trend in the opposite direction: more and more technologies and supplies are being offered as a service. Software licensing, data hosting, and even energy, are increasingly available via a subscription, sometimes monthly, sometimes annually. This method of paying as you go also helps spread out costs, and is aligned with when the services are consumed. Going this route means making a long-term commitment to including those costs in your OPEX budgets.

90.5 How will contractors/vendors get onto the network? Efficiently (easily?) and securely.

If the project is new construction and systems like HVAC and access control need to be operational before the building's base IT network can be set up and running (e.g., a server room may require special ventilation and cooling). The permanent IT network may not be available while the contractors are installing and provisioning the HVAC and access control systems that serve the IT network. These cases may require certain temporary equipment be installed to allow contractors to install and commission their subsystems prior to the final system integration.

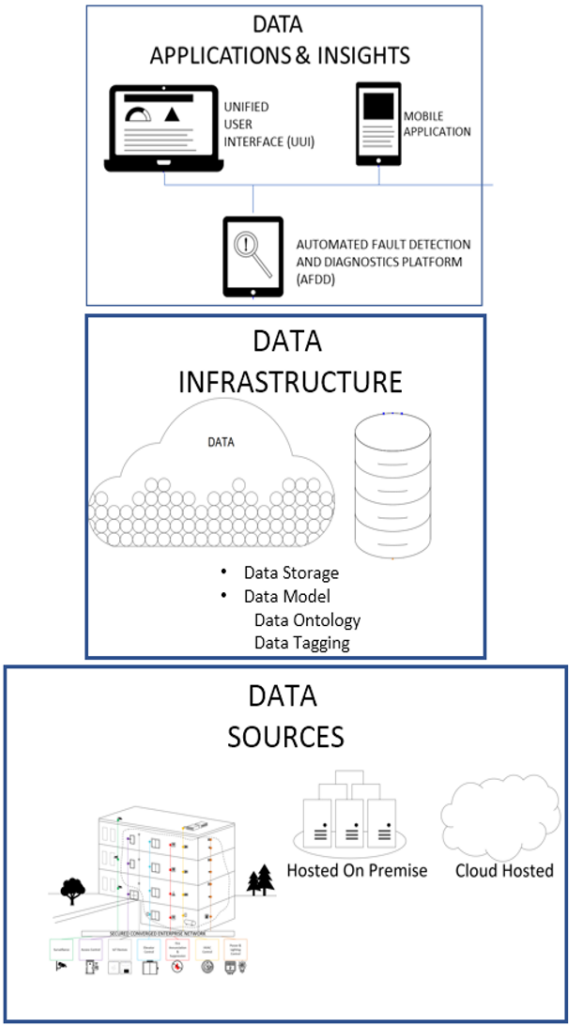
A common, simple solution is to allow a temporary cellular modem-based internet connection to a subsystem for purposes of installation, configuration, and commissioning prior to the final IT backbone being complete. This "jump switch" or similar device can be installed easily onto an

Ethernet sub-network by a contractor to provide remote access for programming, testing, and commissioning. Just remember to remove it prior to connecting to the IT LAN.

This network design requires coordination between the Owner IT team, the project design engineer, the construction team, and the various contractors.

90.6 What is the “net” result of your networked system?

Your property is now equipped with a digital communication network infrastructure to serve as the foundation for build up into the smarter stack by connecting valuable data to applications that enable advanced visibility and control of your spaces and operations.



30 - Delivery

40 - Applications

50 - Exchange

60 - Storage

70 - Control

80 - Physical

25.25.95 – Cybersecurity

This cross-cutting section discusses risks, assessment strategies, and design of cybersecurity best practices for OT systems. This section presents basic, moderate, and advanced suggestions for managing cybersecurity risks both at the physical security and the logical security levels for OT building systems along with guidance for working within and alongside IT based infrastructures.

Do I really need cybersecurity for my building systems?

In today's connected world, building Operational Technology systems are subject to the same cybersecurity threats as IT systems. Whether your building or all of its systems are 'smart' and connected to the Internet or not, data accidents can happen and bad-intending actors can try to digitally plug into major devices and software systems, and cause problems. The impact of these threats differs in the fact that OT systems are responsible for controlling the mechanical and electrical systems within a facility, in addition to the potential for data loss.

For your IT systems, cybersecurity threats must be managed continuously reflecting the changing nature of the threats and the major risk coming from the users themselves. It is no different for OT systems.

In addition to the typical IT related threat vectors, OT systems pose an increased risk for disruption to the physical building. Bad actors can disrupt or damage a facility if they can get access to the control system. Control systems in general should be designed to have fail-safe conditions as part of their underlying design. No controller should be allowed to have a networked message with a data value change that would put the system under control into any unsafe condition. For example, you would never allow a programmable controller to override a temperature or pressure setpoint that is above or below a hard coded value in the controller. Furthermore, any controller that received a request to change a value to an unsafe or out of range condition should immediately flag that message as an alarm, which can help quickly identify potential cybersecurity threats in real-time. More likely it was someone who entered a wrong value, but the end result should be the same, which is part of any cybersecurity check and balance systems.

The IT industry has developed a comprehensive set of risk management principles to identify, protect, and respond to cybersecurity threats. Although these principles can be equally applied to OT systems, it is critical to understand that the two worlds are very different operationally and technically. Threats to the OT system must be responded to in real-time or something potentially catastrophic could happen. The OT system should have full monitoring capability for outside threats both in access and disruption. Therefore, the risk management practices outlined in this framework reflect these differences and the recommended solutions to them.

To simplify the framework, we start out by asking several fundamental questions:

- What is the acceptable risk to my building(s) or business?
- What are the major risks I need to focus on?
- How do I protect OT systems from these risks?
- If my facility has a high-risk profile, what other steps will I need to consider to minimize my risk?

95.1 What is the acceptable risk to my building(s) or business?

Risk varies widely in the OT world based on the size, type, sophistication and usage of a building. A retail store in a strip mall has a very different risk profile than a pharmaceutical research and manufacturing facility. The table below provides a basic guideline for classifying low, medium, and higher risk facilities.

Figure 4. What Risk Level is My Building?

	Low	Medium	High
Typical Facility Types	Small retail, office, local government	Class A office, K-12, light industrial, warehouses	Universities, pharma/ biotech, hospitals, data centers, petrochemical, utilities, banking
Typical OT Systems	Smart thermostats, intrusion security, cameras, fire	BAS, access control, video surveillance, elevator control, lighting control, fire & life safety	BAS, access control, video surveillance, elevator control, lighting control, fire & life safety, power management, digital signage, occupant tracking
Operational Characteristics	9 – 5, limited or no remote access, no access to PII	Remote access for service providers, extended business hours, converged IT and OT networks	24/7, occupant health and safety, explosive materials, large public venues

95.2 What are the major risks I need to focus on?

The #1 risk to be managed is around who has access to the systems and in particular if this access is possible over the Internet. The table below identifies the top 5 risk areas common to OT systems.

Figure 5. What Risks Do I Need to Focus On?

Risk	Description
Remote User Access	Where remote access is possible over the Internet, the security of this connection is critical to preventing the system from being exploited by cybercriminals and malware.
System Backup	The ability to quickly recover from a cyber event or a system failure such as a server crash is directly related to having a current, secure backup file.
User Administration	It is essential to know the names of every individual that has access to the OT system both inside and outside of the organization. Administration of these individuals includes adherence to policies governing user credentials, employment status, job responsibilities, and auditing.

Risk	Description
Software Maintenance	Software is subject to having security flaws which are identified over time and suppliers provide patches and upgrades to address them.
Malware Protection	Malware in the form of viruses, worms, trojans, bots and ransomware is pervasive with new types constantly emerging. Malware infects OT systems through user activity and directed attacks from cybercriminals.

95.3 How do I protect OT systems from these major risks?

There are often numerous options for how to protect your OT systems from cybersecurity threats. It is helpful to organize options into a matrix similar to the one below, and identify which approach is going to be used for your smarter building(s).

Figure 6. Mitigation Strategies for Different Risks

Risk	Risk Mitigation
Remote User Access	To secure remote users a firewall or firewall appliance must be installed between the Internet and the OT system. Encrypt data that is transmitted between remote users and the firewall, only authorized users are granted access, and the OT system should never have a public facing IP address.
System Backup	There are many options and suppliers to backup OT systems automatically. Backups should be done daily and saved for at least one month. Backups are to be saved in a secure location and never on the same server as the OT system itself. The owner's designated System Administrator will maintain a disaster recovery plan including an annual test of the system.
User Administration	Administration of users begins with the assignment of a Systems Administrator, who is responsible for setting and enforcing user policies. Because OT systems invariably are serviced by 3rd party suppliers, these policies must be adopted throughout the supply chain.
Software Maintenance	OT applications and their operating systems should be kept current through software maintenance agreements, and security patches applied when they become available.
Malware Protection High Risk Processes or Environments	All servers, workstations, tablets, and smartphones should be protected with anti-virus / anti-malware software to mitigate these threats. Consider air-gapping the OT network from any outside network access. Or, at a minimum, implement a strong firewall and setup substantial restrictions for access. Also consider implementing a one-

Risk	Risk Mitigation
	way flow of information for monitoring and alarming with no "command and control" capability outside of the OT internal network

95.4 If my facility has a high-risk profile, what other steps will I need to consider to minimize my risk?

The OT network is often connected to the IT network in a building. For this reason, particular care must be taken to control and continuously monitor network traffic, in order to identify abnormalities that can represent malicious activity. Malicious actions are not limited to cybercriminals but can also include disgruntled employees, contractors, or others.

Network monitoring is also useful for knowing exactly what devices are on the OT network. Not only is this helpful for asset management, unknown devices that are detected through monitoring are potential security threats to your facility.

Actively monitoring can also include vulnerability scans of IT devices such as servers and workstations to determine if software is out-of-date, detect malware, misconfigurations, and more.

To go even further with monitoring, OT systems like IT systems can undergo PEN (penetration) testing. This is the equivalent of a white hacker being employed to identify any and all ways in which the OT system can be attacked and compromised. Obviously, this is something that only high-risk systems would normally undertake where the consequences of a system breach could impact business continuity, life safety, and / or loss of critical data.

95.5 Cybersecurity For Facilities

Facilities managers, owners, and end users have an increasing need to secure facilities from ever-increasing cyberattack threats. The following topics should be considered as part of an assessment and planning interview with your cybersecurity legal counsel toward implementing comprehensive cybersecurity plan for facilities.

1. Facilities overall data security objectives

- Data availability: timely and reliable access to info
- Data confidentiality: protecting privacy
- Data integrity: preventing or detecting modification (or lockup) of data by unauthorized persons
- Grant and regulate appropriate access by outsiders

2. Threat potential

- Interconnected networks leads to an increased number of entry points and paths for intrusion
- IP addresses which are public or not secured are open doors for hackers
- Interconnected systems lead to increased data exposure when data is aggregated
- Using the same password on a router as on a building controller device can enable intruder to gain access to control systems

- Expansion of collected data leads to potential compromise of security
- Systems that interact need to have compatible security
- Handoff and interface areas, where handshakes can be weak points, are paths for intrusion
- When non-secure new devices (especially those which are IoT connected) are integrated into a larger building management system, the danger is that they can compromise other parts of the system. For example, hackers of Las Vegas casino gained access to an internet-connected thermometer installed in an aquarium display.
- Failure to timely apply security patches to software and firmware can leave devices and systems exposed to attack
- See the Cybersecurity Risks for Facilities chart below

3. Potential impact of cyberattacks on facilities

- Crashes
- Shutdown
- Slowdown
- Data lockup (via ransomware)
- Interference with operations
- Loss of operational control
- Change data, conditions, sensors, alarm alerts (to hide sabotage to apparatus)

4. Planning: Policies and response

- Evaluate OT vs IT threats and risk
- Assess current security and vulnerabilities
- Develop a plan for remediation
- Evaluate impact (cost vs effort vs timeframe vs benefit) of various measures
- Determine desired security level: Platinum (best in class), gold (all areas reasonably secured), or aluminum (meets minimum legal/regulatory requirements)
- Implement plan
- Mitigating risk involves policies, people, and processes. All three must work in harmony to be successful

5. Action items

- Review vendors agreements with attorney to ensure cybersecurity obligations and liability minimize risk to the facility; amend now or at renewal time to improve. Assess new vendors as potential security risks.
- Develop or update a cybersecurity incident response plan (including a ransomware attack response plan), and practice it
- Develop or update a disaster recovery/business continuity plan
- Review and update security-related policies
- Review staff access levels to systems and deauthorize access, where inappropriate. Improve controls on who has access to software and passwords.
- Implement security incident and event management (SIEM) systems to monitor network activity and flag suspicious activity
- Review employee on/offboarding procedures

- Review building systems for compliance with cyber standards (e.g., new UL and ISA tests for IOT devices)
- Maintain adequate cybersecurity insurance; review current policy limits and exclusions (e.g., “business email compromise”)

6. **Additional tips for improving facility cybersecurity:**

- Require strong passwords which must be changed at least every three months
- Make sure employees know not to share or post passwords.
- Train employees regularly on good cyber hygiene practices
- Review data backup frequency. Make sure critical data is backed up more frequently and all data is backed up offsite. Evaluate frequency based on ransomware lockup’s effect; i.e., how many hours/days of data could you lose and still function?
- Follow your policy for retention and disposal of all sensitive information.
- Install software/firmware security patches as soon as possible.
- Encrypt highly sensitive data in storage whenever possible.
- Segregate sensitive data to reduce cross-over access by an intruder
- Implement IP address restrictions
- Disable/close unused ports on wireless routers
- Employ two-factor authentication (password and additional private information).
- Verify vendor’s email or faxed instructions to change their bank account information by calling the vendor using the phone number in you file, not by email or by using the phone number provided in the instructions.
- Have an outside firm conduct regular risk analysis/risk assessment tests.

95.6 Sample Cybersecurity Risk Assessment Matrix

The following matrix is an example of a multi-tier assessment for cybersecurity risks. Note there are an extended set of “tiers” where threats, and therefore, controls are needed to reduce cyber threats. Each tier has a High, Medium and Low assessment based on Outside, Internal, an Physical threats where the Outside and Internal threats are logical/cyber/network threats and the Physical threats are more in line with intrusion, panel access, unauthorized computers, use of USB sticks, etc. This example can be extrapolated for both simple and very complex scenarios.

Tier	Function	Security Level	Cyber Security Risk
Enterprise Tier			Outside Network Threat - High Internal Network Threat - Medium Physical Intrusion Threat - Low
	Building Management System - Front End	System	
	Backup Servers	System	
	Firewall/VPN Access	System	

Campus Tier			Outside Network Threat - Medium Internal Network Threat - Low Physical Intrusion Threat - High
	Building Automation System	System	
	Outdoor Lighting	System	
	Irrigation Control	System	
Building Tier			Outside Network Threat - Low Internal Network Threat - High Physical Intrusion Threat - Medium
	HVAC	System	
	Lighting	System	
	Security	System	
Equipment Tier			Outside Network Threat - Low Internal Network Threat - High Physical Intrusion Threat - Low
	Air Handler	Equipment	
	Lighting Panel	Equipment	
	Fire Panel	Equipment	
Devices Tier			Outside Network Threat - Low Internal Network Threat - Medium Physical Intrusion Threat - Low
	Thermostat	Embedded Device	
	Lighting Controller	Embedded Device	
	Energy Sub Meter	Embedded Device	
Source:	*© 2023 Ron Bernstein, RBCG Consulting – www.rb-cg.com – Used with permission.*		

96 Appendix

This Appendix includes more detailed examples of select sections of the Framework.

25.25.41 – Grid Interactivity – Sample Requirements

[This is an example section for a specific application, as defined by section 40. Your project will likely have numerous applications whose requirements need to be similarly defined.]

This section relates to all systems that want to provide grid-interactivity and be Grid-Interactive Building (GEB) compliant.

41.1 General Requirements

- All systems within the building will interoperate with others per the requirements of Div 25.25.20.
- All applicable systems will be able to receive and respond to a grid signal. Applicable systems are typically those that have substantial energy loads for their normal operation such as HVAC, lighting, refrigeration, elevators/escalators, etc. The grid signal is called an event, and it comes with a duration. A grid signal can be a request to use less energy or release stored energy, use or store more energy, respond to a grid price (typically a 24 hour ahead schedule of 5–60-minute prices), or respond to a grid carbon intensity metric (typically a 24 hour ahead schedule of 5–60-minute carbon intensity metrics).
- It is best if the system has a CTA-2045 ECOPORT. This is an open standard for Grid-Interactivity and includes both the physical connection and the software/logical interface as defined by the CTA standard. ECOPORTS are generally associated with individual pieces of hardware with embedded controls such as a water heater, boiler, or air handler.
- Another approach can be a gateway that speaks to the building systems, and yet can receive grid signals in an open standard way such as CTA-2045, or OpenADR. Systems or integrators using gateways must ensure that the equipment under control has the necessary logic to process a load control signal or have a supervisory controller manage the process. As an example, if a refrigeration controller is given a grid signal from a gateway to enter into “Load Shed Level 1” that signal might be interpreted to reduce load by 5% for a duration of 60 minutes. The programmer of the equipment must know and understand the requirements for all grid related signals and strategy behind them. The minimum requirements for a grid signal response are below.
    - 1-3 ways to use significantly less energy than normal for the duration of the event.
    - 1-2 ways of using significantly more energy than normal for the duration of the event (optional).
    - If the system can vary its energy use on a continuum, like a battery, Electric Vehicle (EV) charger or variable speed pump, then it should respond to a 0% to 100% command in unit intervals (0, 1, 2, 3%….).
    - If the system can be set to a cycling state where it is on x% of the time during a y minute long interval, then it should respond to a cycling command (x, y).

- If applicable, the system delivers the following data:
    - Confirms that it is responding to the event. Even better is if it can respond to status queries with “Operational States” as outlines in CTA-2045. There is a table of Operational States from CTA-2045 below.
    - Instantaneous Power used by the system (like a speedometer)
    - Total Energy used since system start (like an odometer)
    - Power Storage Capacity (how much electricity can it use or store in Watt-Hours)
    - Total Storage Capacity (if the system is at its most baseline state, how much electricity will it use until fully ‘loaded up’)
    - Setpoint, mode, fan speed, or any other valuable piece of data (these are usually in profiles based on device type).
    - After an event, which is either when an “End Event/Shed/Load up” command is sent, or at the end of the duration time, the system must return to normal operation or a normal schedule. This is to protect ‘bad behavior’ if grid-connectivity is lost.
    - It is assumed that if a manual change to the system control points is made either remotely or locally by the user/owner, that this ‘overrides’ the event and the event ends and the system thus responds to the user/owner input. This should occur rarely because the system is supposed to still deliver the comfort value even during an event, although there is always a balance between energy conservation and occupant comfort that must be taken into account. This is easier with systems that have ‘storage’ (water heating/cooling), then HVAC (which typically responds by a setpoint offset), however storage HVAC systems are being developed, because storage is so critical in an intermittent renewable world.
    - If an override state is entered during the event, the system must send a notification that it is in override state and if the system is queried at any time during the event, the system must answer that it is in an override state and operating ‘normally’. Additionally, reporting the duration remaining of the current event is valuable for the BMS monitoring application and provides valuable insights to the operator.
    - CTA-2045.1 provides the ability to update the system firmware module that provides grid-interactivity through the ECOPORT module. This should be implemented for all CTA-2045 ECOPORT systems.