Advanced Command Center Design

An Executive Primer

SDI
Delivering Intelligent Technology™

An SDI White Paper

888-YOUR-SDI sdisolutions.com SDI Solutions @SDISolutions

Advanced Command Center Design
An Executive Primer

An SDI White Paper

Introduction

Command Center design and construction is more complex and challenging than ever before. New technologies, new organizational challenges, and evolving threats have made Command Center design more challenging than ever.

This White Paper will focus on the history and evolution of Command Centers, the challenges of designing technologies for Command Centers, and provide an overview of some approaches that have proven effective in SDI's Command Center projects.

History and Evolution of Command Centers

Command Centers have been around for a very long time; large organizations and governments have used them since the beginning of civilization. From the castle's keep to the pentagon, they all share some common fundamental attributes and missions that do not materially change: to achieve Situational Awareness, Manage Threats, and Secure the organization.

However, the technologies that enable Command Centers to complete their missions have changed dramatically, requiring new skills and approaches to ensure success. To be successful in today's complex Command Center environment, and to prepare for the inevitable evolution of technology to come, it is important to understand how Command Centers have evolved.

The following are among the most important recent changes in Command Centers, how they are designed and built, and the technologies they utilize:

Security/Information Technology convergence has had more impact on the evolution of Command Center design than any other single factor.

Security/Information Technology Convergence

In the 20th century, the technologies that provided electronic security were 'componentized' systems. When you purchased a security technology system, it was usually a piece of hardware that was mounted, plugged in, and it worked. These were simpler, embedded electronics that performed a single dedicated task. They were simpler to install and operate, but were also very limited in their capabilities. To upgrade their capabilities, you typically had to replace them with a newer model.

All that changed at the end of the 20th century, when security technologies began migrating to computer platforms. Computer

technology gave the systems far more capabilities, and the ability to upgrade merely by changing software. These added capabilities and flexibility came at a price: complexity. Computer-based systems require significant Information Technology skills to design, implement, and support. Many organizations found that their traditional security integrators were unfamiliar with IT, and were having difficulty evolving into the new world of converged security/Information Technology.

Technology is now interwoven into the Fabric of the Command Center and the Facility

In the past, technology was frequently considered as something separate from the base facility design. Technology systems were designed without significant interaction between the facility's designers and the technology designer. Very often, the only interaction was the technology designer supplying required power and structural requirements to the architect. Technology was often was added to the facility later, after the base building was constructed.

Today, however, technology is no longer an 'add-on'; it is interwoven with the facility and mission-specific systems. Because base building systems like access control and Building Automation Systems (BAS), have all moved to computer platforms, they now share IT infrastructure with mission-specific systems like dispatch, video surveillance and Situation Management systems. They will likely all operate on the same network infrastructure, reside in the same Data Center, and rely on the same support and backup systems.

Not only do these systems share IT infrastructure, they now communicate with each other in ways that were never envisioned in the past. For example, in many modern Command Centers, data from both base building as well as mission-specific systems all feed into a Situation Management system that acts as a 'dashboard', displaying events from many systems in the context of maps, alarms, staff, and video cameras.

The Increased Importance of the Technology Designer

This paradigm shift of technology becoming interwoven into the facility means that a new designer must be added to the traditional design team: the Technology designer. The technology designer should have authority over the systems that are based on IT systems, and should be allowed to produce a holistic design. There will likely be resistance from traditional designers, but the benefits of this approach are substantial in reduced costs and increased functionality. Consider that the traditional design approach of separate, non-integrated base building systems actually costs more and offers less functionality than an IP-based system holistically designed by a Technology designer.

The Evolution of the Console

The 20th century Command Center was full of component-based systems, many of them housed in consoles. The concept of a console emerged from the days when systems were component-based, and were operated by the users directly, using knobs and switches. This closely-linked, direct human-machine manual interface required consoles to enclose, protect, and aesthetically hide this equipment.

In today's Command Centers, systems are overwhelmingly computer-based, and systems are housed in a Data Center, with human-machine interaction occurring through computer GUIs. The majority of the equipment that was once housed inside consoles is no longer in use, and their descendants are now computer-based, and are housed in the Data Center. These computer-based systems offer the ability to interact with the systems from any location that provides network connectivity, freeing operators from the need to be in close proximity to the systems. Many organizations remove even workstation computers from operators' environments, choosing instead to house them in a data center and provide access remotely from the operators' desktops through a network using KVM (Keyboard/Video/Mouse) extension technology. There are some exceptions, with some organizations still placing PCs under desks in the Command Center, but these are disappearing as they realize that this is both a security risk as well as operationally inefficient. Housed in a Data Center, computers are more reliable, last longer, are easier to service, and are secured from physical access by malicious individuals.

In this environment, true, traditional consoles are no longer a necessity, and many organizations are instead choosing to use lighter, less costly, re-configurable furniture that allows more flexibility. For example, a recent SDI Command Center client desired to be able to re-configure the space at will. Because all systems were housed in a Data Center, users could quickly move their positions by relocating their keyboard, mouse, and screen to a different network connection.

Figure 1: Existing console-based systems before SDI re-design. All equipment is housed in consoles. Frequent issues arise from damage to equipment, and operators must physically move from one system to another.

Figure 2: SDI Command Center design. No computers are housed in the Command Center; all equipment is now housed in Data Centers, where it is protected and secure. Desks are less cluttered, and all systems are now available at every workstation.

Designing large-format displays requires an understanding of the Command Center environment and how the organization will utilize the displays. They should be part of the design from the very beginning.

Large-Format Video Displays Now Impact Command Center Design

Today's large format video displays are dramatically larger, better quality, and lower-cost than ever before. Because of this, they have become a staple in today's Command Center facilities. Designing for large-format displays requires a cross-disciplinary approach that includes an understanding of technology and ergonomics, as well as

traditional architectural/engineering concepts. Some critical design aspects include:

- **CONOPS (Concept of Operations)**: It is critical to understand how the displays support CONOPS, including what will be displayed, who will view it, and who controls it. The display is a tool, and needs to be used appropriately to maximize effectiveness.
- **Display Placement**: Determining where a large-format video display is located is not as simple as finding empty wall space. It is crucial to understand sight lines, so that refraction, light levels, acoustic attributes like sound transmission and ambient noise management. For example, placing a display in the wrong location could result in glare and reflection from windows, or inability for some staff to see details on the screen. Traditional design techniques like floor plans, elevations, and sketched renderings have proven ineffective in understanding all of these aspects, requiring the use of more advanced techniques like 3d digital modeling and full-scale mockups/simulations to adequately asses the impact of display placement.
- **Support infrastructure**: Each large-format display requires power, cooling, and cabling, and these design elements must be addressed in the design phase. Large-format displays are not just big television sets; they are almost as complex as computers, and require the same design approach.
- **Integration with other systems**: Video displays are no longer confined to displaying surveillance camera feeds or television broadcasts. Today's video displays are a window into the full spectrum of systems and information sources from anywhere inside or outside the organization. For example, current display control systems for video displays can connect to and display a huge range of visual information, including video surveillance cameras, computer screen ‘scrapes’, documents, software applications, television, and video conferencing.

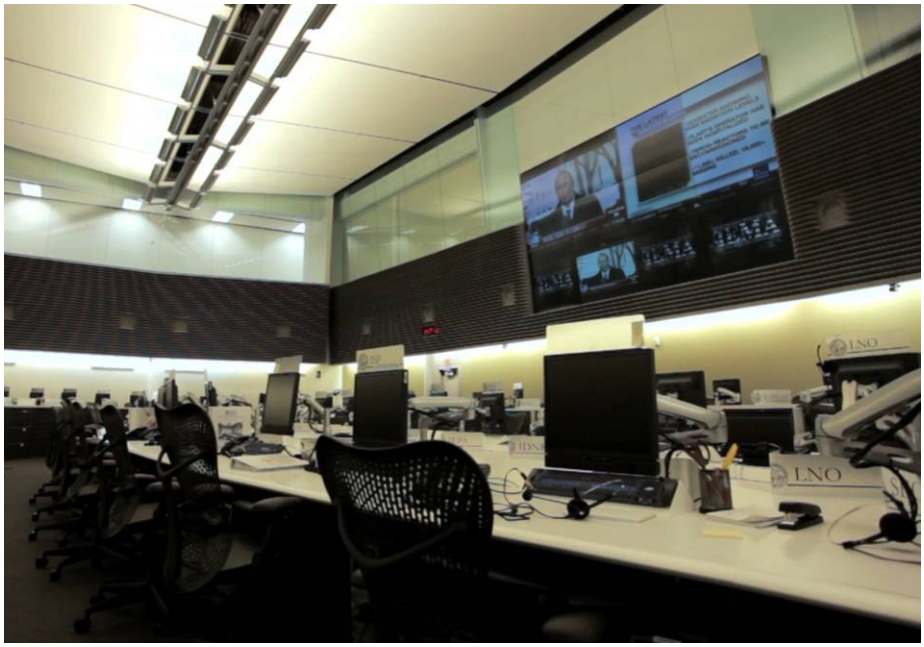


Figure 3: The large format video displays in this SDI Command Center project convey information simultaneously to a large group of stakeholders.

Under-sizing Data Center space and capacity is one of the most common mistakes in Command Center design…and one of the costliest.

Increased Need for Dedicated Technology Spaces

In the past, technology was often housed inside the Command Center, but it is now more commonly housed in a separate Data Center that is adjacent or near the Command Center. This movement of technology from consoles to the Data Center means that Data Center size has dramatically increased.

Many traditional designers do not fully appreciate the amount of computing capacity and mechanical infrastructure that modern Command Center technologies require. For example, in one SDI Command Center project, the architect's original design included only a 'large closet' for computer equipment.

SDI estimated the computing capacity required, both for immediate use, as well as in the future, and determined that a much larger Data Center was needed. To help offset the additional cost, we examined the strategic needs of the organization, and were able to show how multiple Data Centers could be consolidated into the Command Center's Data Center, saving money over the

long term and providing a more secure location.

When designing Data Centers for Command Centers, it is important to realize that the traditional metrics for estimating heat and power loads no longer apply, and must be re-examined in light of today's computing environment. The increased computing density of today's computers means more computing horsepower is packed into increasingly smaller packages, resulting in changes in how these systems are housed, powered, and cooled. Today's CPUs are capable of many more cycles per second, which increases heat output. The surface of a modern CPU can produce as much heat per square inch as a household clothing iron. And new technologies like blade servers now pack so much computing power in such a small space that per-rack heat output frequently reaches 3 times more than just a decade ago.

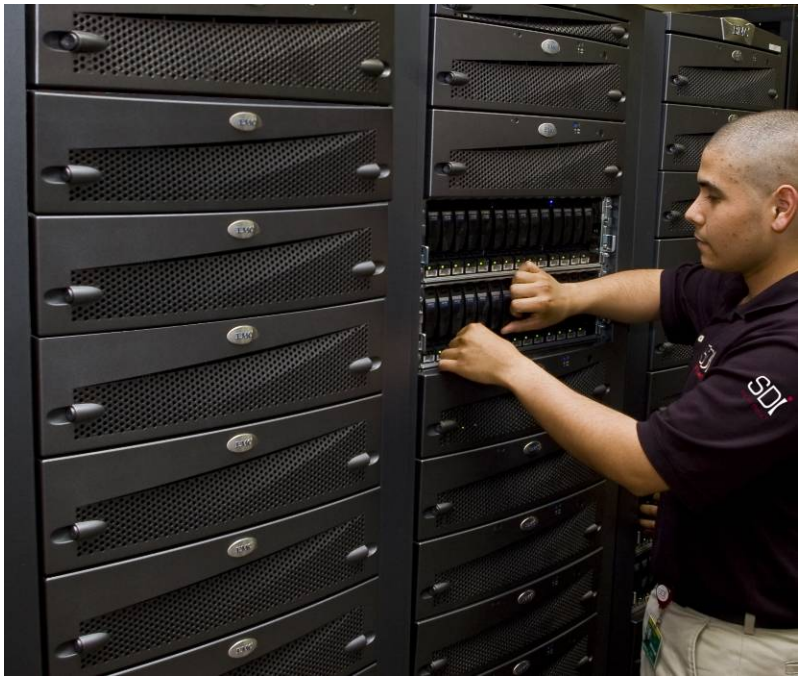


Figure 4: Storage Area Network at an SDI Airport Command Center client. Storage alone accounts for much of the square footage of today's Public Safety Data Centers. For example, this client retains video from 3,000 cameras for 15 days, requiring robust, multi-terabyte data storage.

Increased Dependence on the Network

In today's Command Center, everything is connected via the IP network, so it is critical that the network is designed, implemented, and supported properly. Network design and programming is critical to capacity, reliability, and security, and requires a dedicated network designer to ensure the design conforms to accepted network design

standards. There are three main aspects of paramount importance in Command Center network design:

- **Capacity**: Ensuring capacity requires use of advanced networking techniques for load balancing and traffic management. Systems must be tested for peak network traffic loads to ensure that they perform as designed. An improperly designed network will usually fail just when it is needed most: during an incident, when systems are stressed to their limits.
- **Security**: Today's networks are subject to many security risks, requiring techniques such as use of VLANs (Virtual Local Area Networks), intrusion detection, and a layered security approach.
- **Reliability**: To ensure the network's reliability, redundant components must be used, and the system must be actively monitored.

Increased Need for Support and Maintenance

Without proper support, computer-based systems can become unstable within a few months of regular use, and vulnerable to security threats in a matter of weeks or days.

Because modern Command Center systems rely on computer platforms, they require more support than component-based systems. Updates and patches need to be applied regularly to security software, operating systems, and software applications. The databases that computer-based systems utilize also require maintenance by a Database Administrator (DBA) to maintain peak speed and stability. Without proper support, computer-based systems can become unstable within a few months, and insecure in a matter of weeks or days.

Increased Need for Back-up Systems

Because we rely so heavily on the technologies of the modern Command Center, it is crucial that they are

Remember that systems tend to fail when they are stressed, often during an emergency; when you need them most.

- **Clustered servers**: To achieve high-availability for mission critical systems, it is highly desirable that servers are clustered together, with each primary server linked to a backup server.
- **Off-site and cloud-based data backups**: As data storage increases, many clients are opting for cloud-based storage to reduce cost and guard against data loss in large-scale incidents.
- **Redundant power and cooling**: Backup power and cooling need to be functional even when the local power grid is down.

Increased Need for Digital Storage

The amount of data that is stored in modern Command Centers has also increased, requiring new approaches to storage. Technologies like Network Attached Storage (NAS) and Storage Area Networks (SAN) have become the norm for storing legacy enterprise data.

- **More systems means more data to store**: The advent of so many new technologies in recent years means that there is more data to store as well.

- **Larger video files**: New camera technologies like high-definition have ramped up requirements for storage. Techniques like frame rate reduction and new compression algorithms like H.264 can help to reduce storage requirements.
- **Legal, regulatory, and compliance factors are driving storage**: Many organizations are finding that the value of stored data has increased in recent years due to new laws and requirements.

Challenges in 21st Century Command Center Technology Design

Security Threats Continue to Evolve

Security managers face a threat profile today that is markedly different than what was faced throughout most of U.S. history. Threats now originate from new origins, have different motivations and profiles of execution, and have the potential to do much more damage than in the past.

These threats are constantly evolving, as malicious individuals and groups strive to find new ways to defeat security measures. Security managers and their Command Centers must stay one step ahead of these threats, requiring the use of new technologies to defeat them.

The Number of New Systems and Functionalities is Extremely Challenging

One of the most stunning changes in Command Centers is the advent of so many new technologies. In the 20th century, there were relatively few systems for Command Center designers to master. Most 20th-century organizations employed only a few security systems, such as CCTV, Access Control, and Intrusion Detection.

More new Command Center and security technologies have been created in the past 15 years than in the 50 years prior.

Since the convergence of Security and Information Technologies, however, there are now many more systems to contend with. Today's organizations are implementing digital video surveillance, video analytics, biometrics, PSIM, high-definition video, mass notification, and other systems.

In the past, relatively little planning was required to implement security technologies. Security Managers knew what systems they needed, and there was relatively little difference in functionality from one system to another. Very often, cost and capacity were the major differentiators between systems.

Today, however, there are many more systems to choose from, and they have a much greater range of functionality. Also, the evolution of security technologies

has resulted in some overlap in functionality from one product category to another. The choices are not so simple, and require a thorough understanding of the technologies and products to make an informed choice.

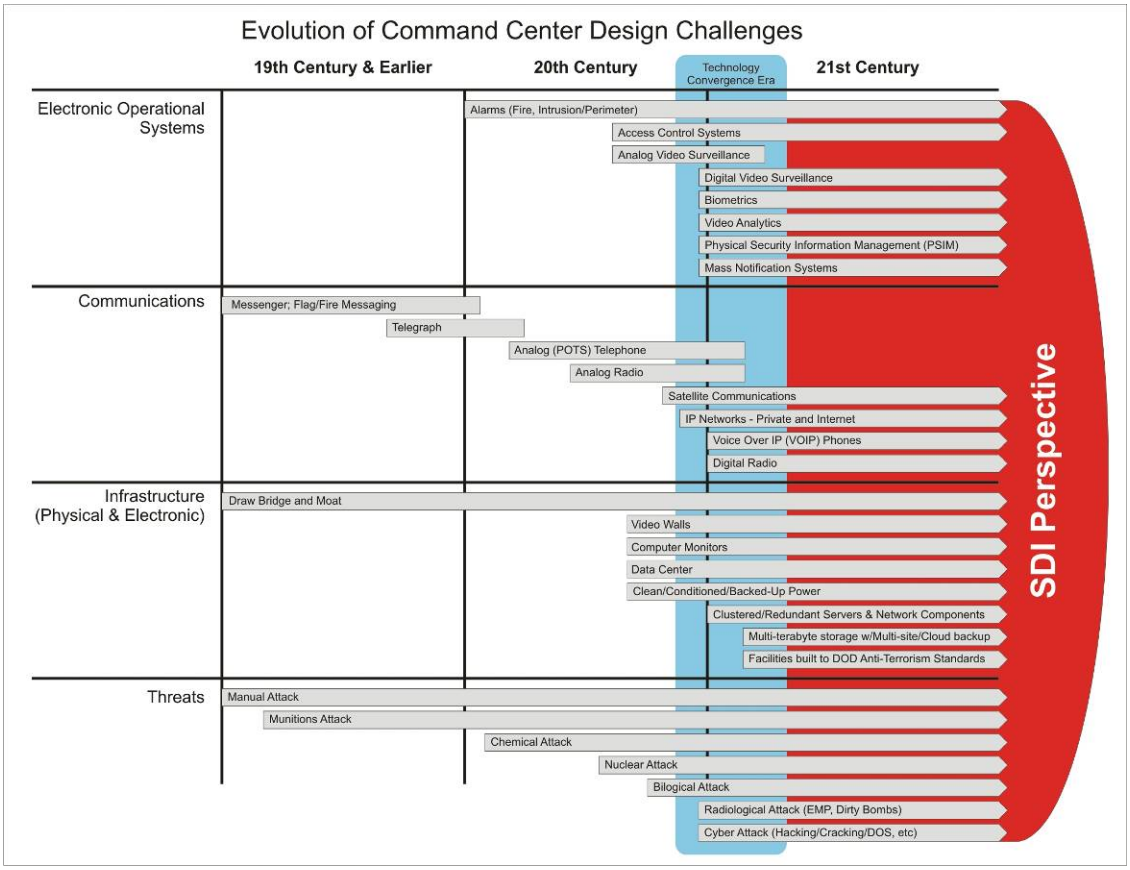


Figure 5: The growth of security technologies from the origins of the Command Center through the 21st century.

New Technologies Require Greater Technical Skills to Design and Implement

The convergence of security and information technologies is daunting to many traditional 'Toolbelt and Wirecutter' security integrators. The key to success today is having both security and IT skills.

In the past, security systems were based on component devices that were relatively simple in comparison to modern computer-based security systems. 'Toolbelt and Wirecutter' technicians with relatively low skill levels were able to implement and support these systems.

Today, however, implementing and supporting security technologies require a thorough understanding of Information Technologies. Knowledge of servers, networks, databases, and how to design and deploy them in mission-critical environments is critical to success.

Many security systems integrators are struggling to make this transition, and some are finding they cannot make the transition at all. Worse yet, some are in over their heads, and are implementing computer-based systems that have fatal design flaws that do not become evident until systems are stressed to their limits.

New Organizational Challenges

Technology evolution has also changed the way that organizations manage the design and construction of Command Centers. Specifically, technologies have changed the way that organizations procure and implement Command Center technologies.

For example, because Security Technologies now operate on a computer platform, Security departments now must frequently enlist the IT department to implement and support the systems. This blurring of the lines between Security and IT brings extra complications and questions on funding, control, and responsibilities.

Another example is the advent of mixed-use Command Centers that combine Operations and Security in a single environment. While the missions of these 2 groups differ, housing them both in a single environment can yield significant benefits when large-scale incidents require coordination between them. However, great sensitivity to each of their unique needs is required to bring them together successfully.

SDI believes that, in order to be truly successful, the Command Center must not only provide technology resources, but must also fit the organization's culture and solve organizational challenges. By learning what you face every day, we can help you create a Command Center that provides benefits beyond technology, and enhances daily and emergency operations.

Keys to Success in 21st Century Command Centers

SDI has been a leader in security and Command Center technology design for almost two decades. We have designed Command Centers for Airports and other public safety clients that utilize the latest 21st century technologies. This experience has provided us with some unique insights that allow us to design better-performing Command Centers that operate more efficiently, and adapt more easily to the evolution of technologies. These are some of the lessons we have learned:

The Technology Designer must be an integral part of the design team to successfully weave technology into the fabric of today's Command Centers.

The Technology Designer: Critical to Success

Technology is in the fabric of the modern Command Center, and requires a technology designer to be a key part of the team. Just as architects and engineers have an indispensable place in the design process, the Technology Designer now plays a crucial role in the success of a Command Center design.

This is a departure from the traditional approaches of the 20th century, and may require some adjustment in the thinking of clients, architects and engineers. But this is absolutely necessary to the success of Command Center projects, which rely so heavily on technology for success.

Get the Technology Designer Involved from the Beginning

The time to engage the technology designer is at the very beginning of the project, not at some later point. The reason is that the technology designer can help the owner make strategic decisions early on that have a significant impact on the success of the project. As an example, consider a project where the technology designer was brought in at the start, and discovered problems that required redesign. The space allocated to the Data Center was insufficient, and the placement of the large-format video displays was inappropriate for the space. By catching these and changing the design early on, hundreds of thousands of dollars, and months of wasted time were saved.

SDI's experience in Command Centers has shown us that involving the Technology Designer from the beginning of the process dramatically reduces risk. The technology Designer focuses on only on computers, but also on how people interact with them, and can provide unique insights into many elements of the design. By spotting issues early, costly mistakes can be avoided.

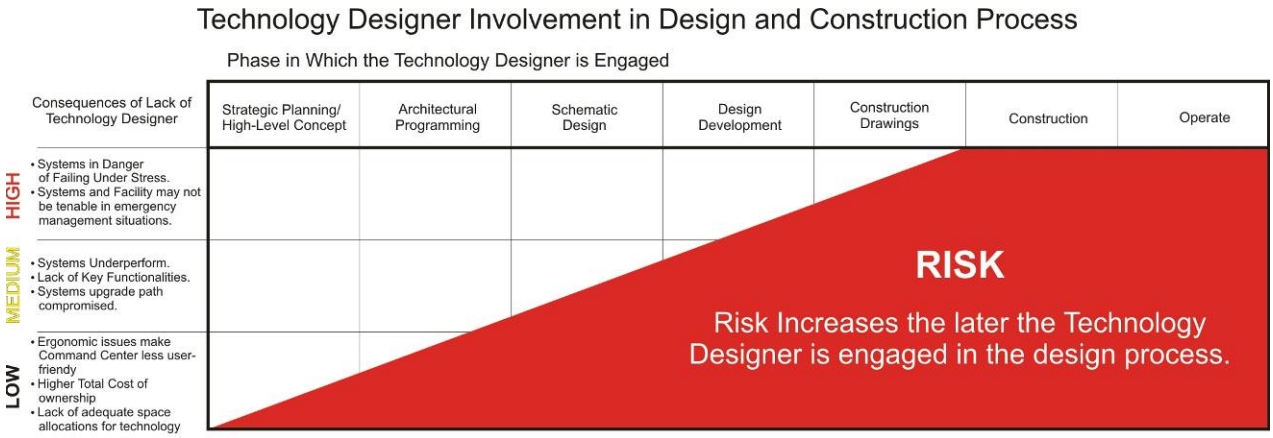
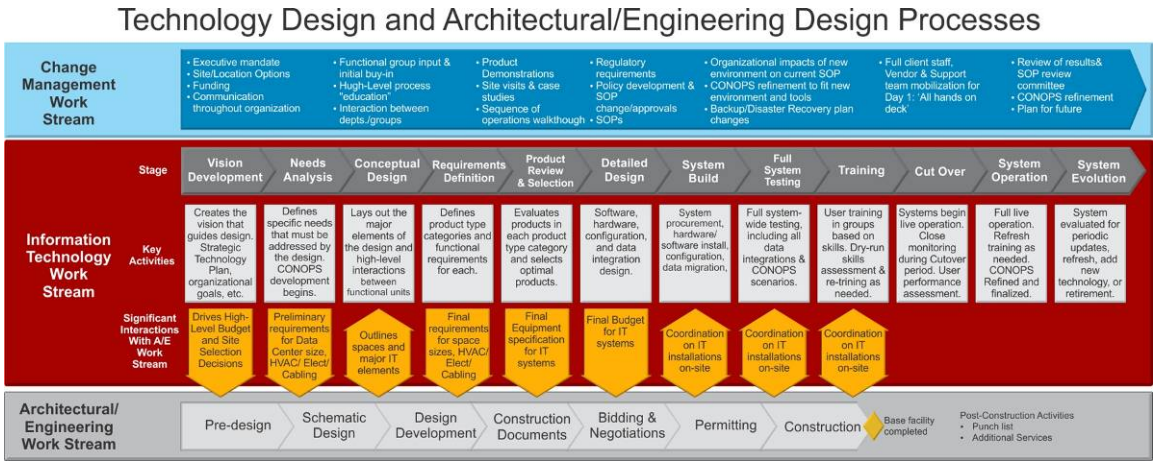


Figure 6: Risk escalates as the project progresses if the Technology Designer has not been engaged.

Aligning the Technology Design Work Stream with the Architectural/Engineering Work Stream

One of the main reasons that the technology designer must be engaged early is that the technology design work stream is just as complex as the architectural/engineering work stream, and the two must start in parallel. These two work streams impact each other in important ways, and it is crucial to understand the two work streams, how they differ, and how they impact each other. Misalignment of these two work streams is one of the most common causes of cost and schedule overruns and failure to meet project goals.



Understand Your CONOPS

As the number of systems increases, and the complexity of the systems grows, it is more important than ever to understand the Concept of Operations (CONOPS). CONOPS provides the operational guidance that dictates how the systems will be used, and is invaluable in determining which systems are

needed, how they will be used, and what benefit they will provide. CONOPS should help drive the selection and design of technologies, but, all too often, technologies are selected and implemented without a thorough understanding of the organization's CONOPS. This results in underperforming systems, or, worse yet, 'shelfware' that is rarely or never used.

CONOPS is more complex than many realize; it is not a static guideline; it evolves as the organization evolves, as new threats emerge, and as new technologies and tools become available. CONOPS drives technology selection and design, but is also impacted by the development of new technologies. This means that CONOPS is a living, evolving body of knowledge that continually changes.

When designing a Command Center, it is imperative to revise CONOPS in light of the new systems and new environment of the Command Center. By having a well-developed CONOPS, you will be better equipped to understand which systems are required, how they should be integrated, and how they will benefit the organization.

Follow a Structured Planning Methodology

The bewildering array of challenges in designing a 21st century Command Center means that projects can easily get off-track. To effectively manage these complex projects, a structured methodology must be used to reduce risk and ensure that the goals of the project are met.

SDI has developed a methodology that has proven successful on many Command Center projects. This approach employs classic consulting methodologies and innovative approaches like simulation exercises and digital modeling. Below is a high-level overview of our methodology.

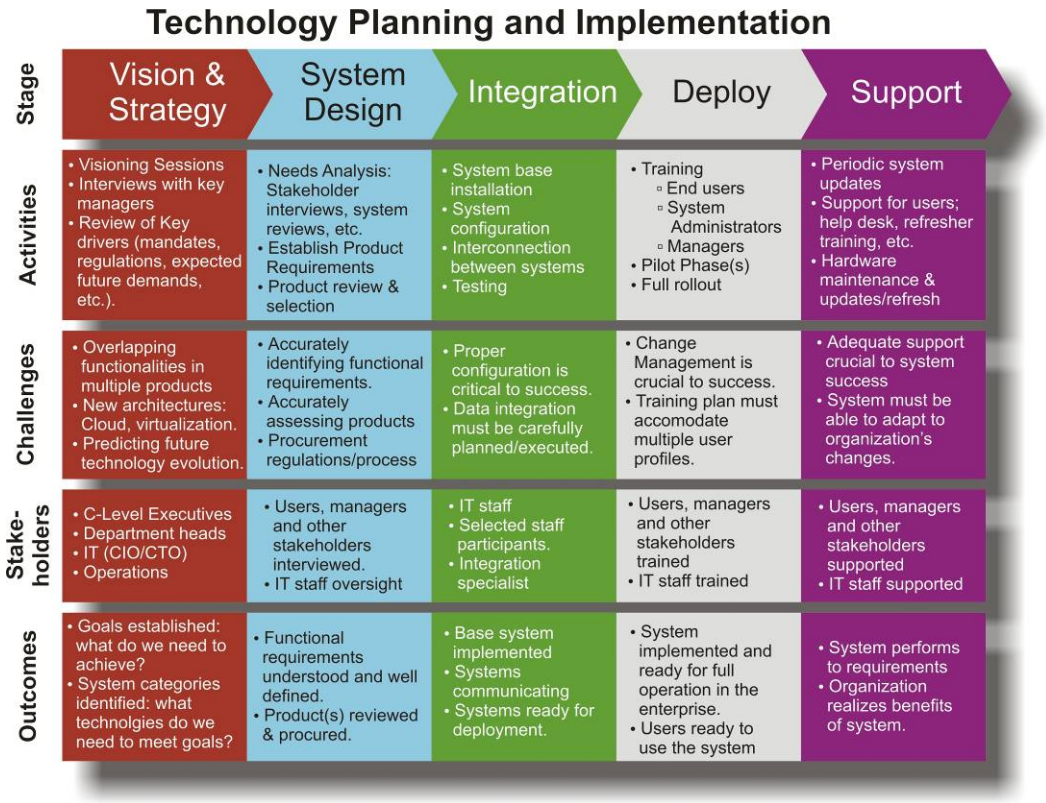


Figure 7: High-Level overview of SDI design methodology.

Understand your Level of Robustness/Survivability

A key part of Command Center design is the approach to ensuring survivability in the event of weather, accident, or deliberate attack. But there is a very wide range of possible approaches, with significant cost implications. These must be evaluated carefully using a threat assessment to find the right balance between survivability and cost. Some of the survivability approaches used by SDI clients include the following:

- Clustered servers and network switches allow systems to continue operating seamlessly even in complete server failure scenarios.
- Multi-site backups preserve a duplicate copy of important data offsite so that, in the case of complete facility destruction, data will still be preserved.
- Mirror critical systems in a secondary location: The events of 9/11 showed that it is possible that the entire Command Center facility could be destroyed. Critical systems should be mirrored in a secondary location that can replace the Command Center of it is destroyed.
- Facility hardening: External threats like Electromagnetic Pulse (EMP), lightning, storms, and explosion all can be mitigated in various ways. The most effective way is to carefully examine potential Command Center sites for vulnerabilities. For example, follow the Department of Defense Anti-Terrorism guidelines for facility design. Also do not locate the Command Center on the highest or lowest floor of a building, and locate it in the center of the structure.

Remember the 3 Tenets of Command Center Design

There are 3 main tenets of design that SDI follows in Command Center design:

- **Reliable**: The Command Center must be reliable in order to achieve its mission. This means that systems must be designed to perform under stress, must be resistant to attack, both physical and cyber, and must be maintained religiously.
- **Flexible**: The Command Center must be flexible enough to accommodate the unplannable conditions that arise during emergencies. Systems and spaces must be capable of adapting to new users, unforeseen circumstances, and extremely high loads.
- **Scalable**: Command Centers are not static environments. As new technologies are introduced almost daily, the Command Center must be capable of growing and supporting these new technologies. Plans must include future expansion to avoid obsolescence.

Use 3-D Modeling to Refine the Design

Building 3-D Models allows you to 'sit' in virtual seats in the Command Center before anything is built. This is invaluable in optimizing sightlines and preventing layout errors.

The use of 3-D modeling is invaluable in visualizing the finished Command Center before construction begins. While floor plans are sufficient to understand space layouts, they cannot convey the full experience of being 'inside' a 3-D virtual model. Being able to 'walk' through the space, 'sit' in the seats, and see exactly what people will see inside the Command Center is extremely valuable.

3-D modeling can also detect design flaws that are not visible in floor plans. For example, one SDI Command Center project was the design of an $18 million Emergency Management Agency facility. Large-format video displays were to be mounted into the forty-foot high walls of a huge room. The locations of two video was determined by a designer with no experience in Command Centers. After the client asked SDI to review the design, we built a 3-D digital model of the space to examine sightlines. By 'inhabiting' the virtual model and 'sitting' in the virtual seats, we were able to determine that the placement of the walls was too high to be useable. Catching this mistake before any steel was erected saved the client several hundred thousand dollars and major time delays.

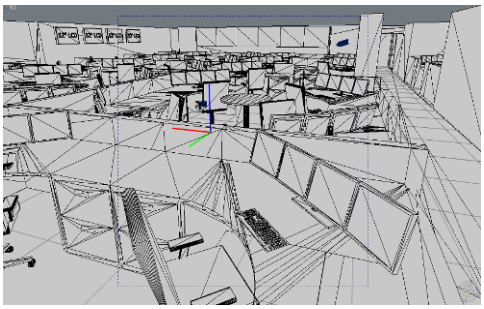


Figure 8: wireframe of 3-D model of SDI Command Center.

Figure 9: 3-D model with lifelike shading enables visualization of sightlines and other ergonomics

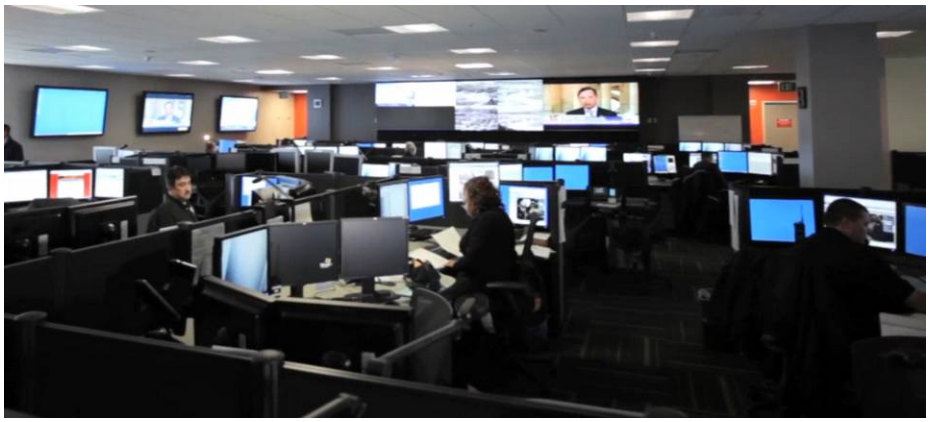


Figure 10: Completed Command Center: sightlines and traffic patterns of the actual environment are exactly as they had been modeled in the 3-D digital model

The Profile of the Command Center Drives Design

It is absolutely imperative that you understand the profile of the Command Center you are building. There are multiple profiles possible, each with unique needs, and each requiring the appropriate design approach. For example, PSAPs may not require large-format video displays, but Security Command Centers can benefit greatly from video walls and large LCD screens. Likewise, the daily life of an Airport Operations Center (AOC) can be very different from that of an Emergency Operations Center (EOC).

Different Profiles for Different Missions

Command Centers are not all the same; there are many different profiles, each with a unique focus on a specific mission. Some of the more common Command Center profiles are the following (please note that the acronyms are not absolutes; different organizations may call their Command Centers by different names):

- **Emergency Operations Centers (EOC)** are focused on the management of emergencies. They are often not occupied until they are 'activated' when an incident occurs. Unlike other kinds of Command Centers, they have unpredictable usage profiles that require them to adapt quickly to unforeseen needs. Technology infrastructure must be designed to accommodate outside users from multiple organizations, and must be scalable for the sudden influx of people when emergencies occur.

- **Operational Control Centers (OCC)** focus mainly on the operations of a complex facility such as an airport.

The OCC is where the daily management of the organization occurs, and is focused on routine work that is essentially the same every day, with occasional emergency response activities. These facilities are much more predictable than an EOC, but also have far higher ergonomic standards because workers staff the OCC every day.

- **Security Command Centers (SCC)** is the facility in which video surveillance, alarms, access control, and other key security systems are managed. SCCs support both routine work as well as frequent emergency response activities (although usually on a much smaller scale than the EOC). SCCs frequently employ large-format video displays for displaying video surveillance feeds.

- **Building Operations Centers (BOC)** focus mainly on the operations of the building, housing building automation, asset management, work order, elevator management, and other systems relating to the operation of the building. They are more focused on operations than security, but are frequently engaged in emergency situations as a kind of EOC.

- **Public Safety Answering Points (PSAP):** Also known as 9-1-1 centers, these facilities are charged with the management of public safety personnel such as police, fire, and EMS. They are focused on call handling and dispatching of emergency responders. Operators typically sit at console workstations, and have relatively little interaction with each other. Typically, large format video displays are not used in these environments.

- **Fusion Centers** are spaces designed for the interaction of multiple organizations in a facility that enables and encourages collaboration. Fusion Centers are typically utilized by government agencies that need to collaborate proactively on sensitive intelligence issues. The key value of a Fusion Center is that stakeholders are able

to work together in neutral territory, exchanging knowledge and experience that cannot easily be communicated via written or more formal, less interactive channels of communication.

Consider Co-Locating Multiple Command Center environments

It is sometimes desirable to co-locate 2 different kinds of Command Centers in the same facility, For example, having an EOC next to an OCC can have definite advantages during emergencies. Being close to each other allows easier communications when coordination is required between emergency managers and Operations, Security, and other departments or groups. However, poor design can have a negative effect if the commotion of the EOC is allowed to impact the OCC environment. Architectural approaches like glass walls/doors, or moveable walls provide the flexibility to achieve collaboration without disruption. Glass walls or doors can also allow visual communications between EOC and OCC staff, and allow sharing of visual resources like video walls.

Figure 11: 3-D Model of SDI Command Center showing layout of Co-Located Airport Operations Center (AOC) and Emergency Operations Center (EOC).

Synergies in housing multiple Groups in a single Command Center

Some organizations find that using the Command Center to house multiple groups can have considerable benefits:

- **Leveraging costs:** By combining multiple groups/departments within a single space, the costs of building the Command Center can be spread across multiple departments' funding sources. Because the groups will utilize the same mechanical infrastructures (such as Data Center power and HVAC systems), the per-square-foot costs for each department will be lower than separate facilities.
- **Enhanced communications in large incidents:** Large incidents require the interaction of multiple groups to coordinate the response to large-scale incidents. As demonstrated on 9/11, coordination between groups that do not ordinarily work together can be a crucial capability in large-scale incidents.

Don’t Forget Support, Meeting, and Collaboration Spaces

While the Command Center is the key part of the design, in order to be of maximum utility, the Command Center should ideally have some adjacent spaces for executive briefings, meetings, and possible press conferences. One very useful technique is to separate the spaces with glass partitions. This allows maximum use of large-format video displays, as well as person-to-person visual connections that can be important in emergencies.

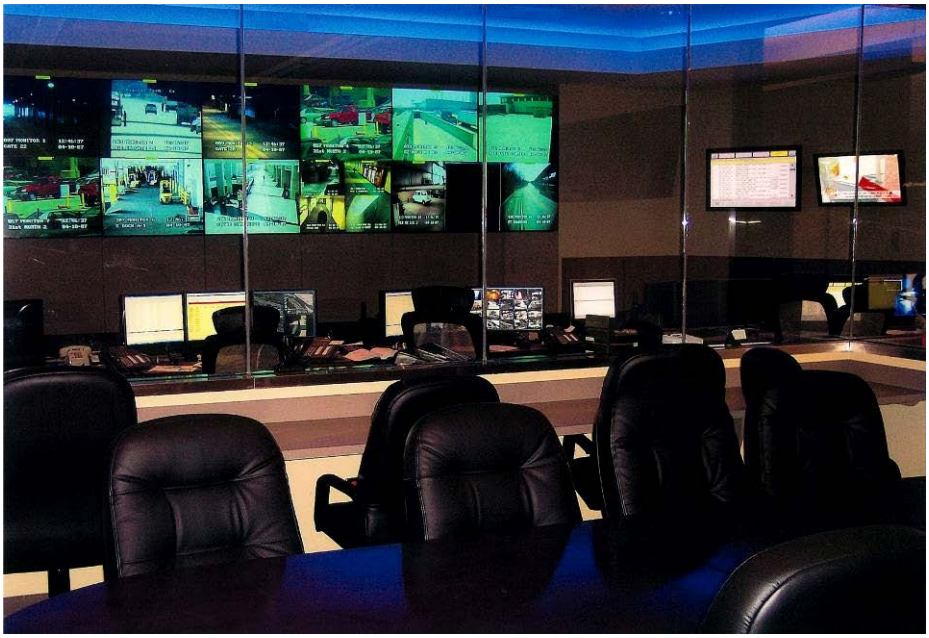


Figure 12: This SDI Command Center design includes an executive meeting room behind the Security Control Room. This space, separated by a glass wall, allows managers to meet and discuss situations in private, but still maintain a visual connection to the operators and large-format visual displays.

Conclusion

Organizations charged with ensuring public safety are faced with unprecedented challenges today. Ever-evolving threats, organizational challenges, and new technologies combine to make Command Center technology design more difficult and risky than ever before.

However, by involving the Technology Designer from the start of the project, using structured methodologies, and engaging a team that has the experience to guide you safely through the process, you can avoid the pitfalls that are so common in Command Center design.

This SDI White Paper was authored by Thomas Condon, Senior Consultant, with input by Mark Moscinski, Safety and Security Industry Executive, and Don Zoufal, Safety and Security Executive.

SDI is a next-generation integrator of complex IT systems that delivers comprehensive, mission-critical IT solutions and services that ensure client security and revenue generation. From airports to banks to commercial properties, SDI serves as a trusted advisor, helping to mitigate risk, eliminate downtime and increase efficiencies for its customers' most critical environments.

Visit sdisolutions.com.