Design Considerations for Real-Time Operating Centers: Best Practices for Asset Integrity and Secure Information Management for the Oil and Gas Industry
Table of Contents

About the Thinklogical Design Center ........................................................................................................... 2
Executive Summary ............................................................................................................................................. 3
Challenges in the Oil & Gas Industry .................................................................................................................. 4
Asset Integrity Management and the Real-Time Operating Center ............................................................... 5
  Asset Productivity, Process Safety and Protecting the Environment ............................................................ 5
  Asset Protection ............................................................................................................................................. 6
  Performance .................................................................................................................................................. 7
  Physical Separation ..................................................................................................................................... 7
  Robust Access Control ................................................................................................................................. 9
  Resiliency and Redundancy ......................................................................................................................... 9
  Flexibility and Scalability .............................................................................................................................. 9
  Design Considerations Chart ...................................................................................................................... 10

Real-Time Operating Center Diagram ........................................................................................................... 11

Summary ....................................................................................................................................................... 12

About Thinklogical .......................................................................................................................................... 12
The Thinklogical Advantage ............................................................................................................................. 13

About the Thinklogical Design Center

The Thinklogical Design Center (TLDC) is an invaluable resource available to our customers and partners. Led by two industry pioneers and co-founders of Thinklogical, David Cheever and Peter Henderson, the Center has worked with customers and partners to provide thousands of conceptual system designs for requirements that range from straightforward to extremely innovative and complex.

Backed by a staff of tenured, industry-specific application and development engineers, the Center helps customers and partners discern their needs and requirements, then develops the appropriate system design. Often, features and functions are utilized in the design that the customer or partner had not previously considered. Features and functions may often be created or customized based on the design discussion, utilizing Thinklogical’s rapid development capability.

An initial TLDC consultation is typically a phone call for about an hour or less. Initial system designs are usually completed within 24 hours. All TLDC services and consultations are complimentary.

To contact the TLDC, please call 800-291-3211, or email info@thinklogical.com.
The oil and gas industry faces a multitude of complex business challenges. Asset Integrity Management (AIM) is an overarching approach designed to address these challenges by getting people, processes and technology working together to improve productivity, safety and security, while also protecting the environment. Critical to these AIM objectives is the Real-Time Operations Center (ROC) and its underlying systems. The ROC is a centralized, cross-functional collaboration center with access to the video-rich data necessary to make timely and high quality decisions.

This white paper examines best practices for the design of the underlying system to securely control, manage and distribute the flow of information to, from and within the ROC. Ultimately, the authors recommend that this system should provide:

1. **High Performance.**
   The system should deliver very high levels of reliable performance between the user and the content source, enabling the transmission of high-resolution video, audio and data with no compression, signal latency, video artifacts or lost frames, thereby enabling the highest quality decision making possible.

2. **Physical Separation.**
   The system should physically separate the users from the sources of information, such as servers and PCs, to protect the information from being compromised while providing the legitimate end-user employees with the authorized data access they need to do their job well.

3. **Robust Access Control.**
   The system should provide robust restriction schemes that allow an administrator to regulate user access to sources on a port-by-port basis, while preventing any changes to the scheme by anyone other than the administrator. In addition, the system should allow for the management of user access through devices such as USB ports, restricting those ports to peripheral connectivity only and prohibiting the possible theft of data.

4. **Resiliency and Redundancy.**
   The system should be able to be configured in a highly reliable and fully redundant approach to ensure the highest levels of continuous operation.

5. **Flexibility and Scalability.**
   The system should be flexible in its ability to scale as users and sources grow, easily incorporating new video, audio and data signaling formats, new users, new locations and new applications.
In today’s environment, oil and gas companies face a complex labyrinth of business challenges. Risk is growing in the face of a changing and unpredictable geopolitical landscape. Reservoirs are more difficult to access and increasingly less productive. Shifts in worldwide supply and demand are driving a re-architecture of the global refining footprint and business model. Distribution operations must improve forecasting accuracy and manage capacity constraints in an environment of increasing regulatory and political involvement. Experienced and skilled human resources continue to be in short supply. Process safety, for both the worker and the environment, has abruptly ascended to the top of the priority list. All while shareholders continue to expect a healthy return on their investment.

Asset Integrity Management (AIM) is an over-arching approach designed to address these business challenges. An industry-wide concept adopted by nearly all major oil and gas companies, AIM focuses on at least four areas: 1) optimizing asset productivity, 2) ensuring process safety, 3) protecting assets from security breaches, and 4) protecting the environment. The objective of AIM is to get people, processes and technology working together to decrease cycle time between key decision points, while increasing the quality of the decisions that are made. This requires multi-discipline cooperation, the efficient use of human capital, and real-time optimization across all functions: exploration, drilling and capture, refining and distribution.

In support of AIM, the nature of what was previously known as a “control room” has changed dramatically. In today’s digital oilfield, the traditional control room has evolved to a multi-faceted facility more commonly known as a “Real-Time Operating Center” or ROC. A ROC is an exponentially more data rich environment, evolving to include high resolution video and audio surveillance. It is more collaborative in two significant ways: 1) different disciplines and functions are working within the same room, and; 2) field and headquarters personnel are working together through virtual video telepresence technology. The ROC is also more flexible, through its ability to be reconfigured through rapid and dynamic access to the critical systems, information and personnel required to address any number of situations or decisions that need to be made. Finally, the ROC is, in most cases, able to function in near real-time.

A critical underlying component of the ROC is the secure control, management and distribution of real-time, video-rich information to facilitate this cross-functional, collaborative and therefore higher quality decision-making. The system chosen for this task is of utmost importance to achieving the ROC’s objectives. Instability in the system can lead to ROC downtime during critical periods. Less than adequate performance can lead to image latency, pixelation, artifacts or lost frames, impairing the ability to make high quality decisions. Insufficient security measures can result in the leaking or breach of mission critical data, hacking, cyber-attacks or even the crippling of operations. For these reasons, it is important to understand the key design considerations and best practices for the ROC’s underlying data system and how that system needs to support the objectives of AIM.

The AIM objectives of improved asset productivity, process safety and protecting the environment are closely intertwined and often at odds. For instance, in drilling operations, new technologies are continuously improving the speed of drilling. But that speed can add to wellbore instability and increase the chance of a serious process safety and environmentally dangerous event. Ironically, such an event might eliminate all efficiencies gained from the new technology and more.\(^1\)

The implication for the ROC is that it must provide access to the critical information required to make high quality decisions for productivity, safety and the environment. In today's ROC, there is extensive monitoring and control of sensor data focused on achieving the AIM objectives. These devices monitor torques and drags, mud log data, gas or hydrocarbon levels, pressures, volumes, and many more critical functions within the operation. In addition, there is video collaboration capability. Is this enough? Many oil and gas companies do not think so.

Following explosive adoption rates in other industries such as the military and intelligence community and municipal emergency response and safety, oil and gas companies are at the cutting edge of commercial enterprises that are leveraging the exponential increase in high-resolution video and audio surveillance information available to control geographically dispersed, yet mission-critical operations. The industry is recognizing that for an experienced geophysicist (or any expert) to accurately direct an outcome in the field from a ROC near his or her office, he or she often needs more than sensor information. It requires situational awareness; the sense of “being there.”

In a way, we might think of this circumstance as using only three of the five human senses. While adequate, the absence of the other two senses leaves unfulfilled key inputs required for enhanced perception and situational understanding. The evolution of the AIM/ROC model addresses this deficiency by incorporating at a higher level sight and hearing in the form of high-resolution video and audio, collected in the field and relayed in actual or near real-time back to the ROC. This robust combination of cross-functional expertise, timely sensor data and high-resolution video and audio is needed to make the accurate decisions that optimize productivity and process safety. Anything less may sacrifice the quality and insight that might otherwise be achieved when formulating these mission-critical decisions.

Asset Protection.

Enabling AIM has serious confidentiality and security implications. Exponentially larger amounts of higher quality information is being collected. Technology is being deployed to dramatically improve the ease of accessing that information. Collaboration, based on the information, is expanding — crossing functional lines within the oil and gas company, but also across multiple contractors working for the company, sometimes located in the same room. In short, the massive stores of mission critical information that are appropriately being collected to facilitate productivity and safety are, at the same time, dramatically more exposed, increasing the risk of a security breach and the impact that breach might achieve.

While the risk of a data breach from outside of the company is real, history and present experience teach us that the possibility of attack from internal perpetrators, whether employees or contractors, is at least as common and usually more deleterious. In the military and intelligence community, Edward Snowden and Pfc. Bradley Manning were both trusted workers with security clearances and authorized access to the networks they compromised. In the 2012 cyber-attack on Saudi Aramco that crippled 30,000 computers and nearly shut down Aramco operations, it is believed that the attacker was a contractor with authority to access the systems he crippled, and he did so using an ordinary USB thumb drive to inject the virus.²

The systems underlying today’s ROC must address these security concerns. They must provide an authorized user with real-time access to data when and where they need it, with no latency or performance degradation, while ensuring access to only the information they require to do their job. That is, they should not be able to easily steal or corrupt the information, even when they are authorized to access it.

The attacker is most often an authorized user with an agenda of gaining information or disrupting operations. Therefore, a robust system design must accomplish two objectives. The first is physical separation of the information sources from the user, which means locating servers and storage devices in a space that is separate from the user’s work area, and limiting the user’s ability to physically retrieve information over the system through media devices such as thumb drives and USB ports. Second, the system design must provide a higher-level restriction scheme that allows authorized users to access approved sources, and disallows all other access. In addition, the restriction scheme itself must be incapable of being violated by a perpetrator.

To meet the objectives of AIM and today’s ROC, there are several important areas to consider when choosing the appropriate control, management and information distribution system underlying the ROC. These include: distance between information and access points, performance, resiliency, security, and flexibility.

**Performance.**
The system should deliver very high levels of reliable performance between the user and the source, enabling the transmission of high resolution video, audio and data with no latency, compression, pixelation, artifacts or lost frames, thereby enabling the highest quality decision making possible.

In order to make high quality decisions in real time, the information itself must be comprehensive and of the highest quality. To truly drive improvements in productivity and safety, both data and expertise are required. In the planning stage, collaboration with 3D modeling and simulation tools across several experts is important. After the operation begins, sensor data is essential to the monitoring effort. But to truly equip an expert to advise the operation, real-time video surveillance of the situation and easy access to the advanced modeling and simulation tools are both needed. It is recommended that the control, management and distribution system underlying the ROC be capable of delivering full resolution, uncompressed video with no latency, pixelation, artifacts or lost frames through dedicated, high-bandwidth connections to mission critical sources.

**Physical Separation.**
The system should physically separate the users from the sources of information to protect the information from security breach, while still providing the users with the high performance access experience they need to do their job well.

Within a ROC, there are several categories of information to be accessed, from “sources” that may include:

- Real-time sensor measurement data
- Historical trend data
- Real-time high resolution video and audio surveillance
- Information gathered from remotely operated underwater vehicles (ROV’s)
- “Always-on” videoconference rooms and desks
- Advanced analytical tools such as high resolution exploration graphics, 3D modeling and simulation tools, etc.

It is important to consider the natural location of these sources relative to the ROC. For instance, sensor management data may be collected by servers in the field and then communicated via satellite and a landline network to a location either near the ROC or in the same building. But advanced analytical tools may be located in a separate building across campus or on the other side of the city, and these require dedicated, high-bandwidth access to be effective. The information control, management and distribution system must be able to reliably transport the data over the required distances without creating latency or degrading resolution.
If the location of data sources are not some distance apart, it is important to consider if they should be! Remembering that attackers are often trusted internal resources — employees and contractors — it is appropriate and prudent to ensure that they do not have access to the physical sources. As noted previously, Saudi Aramco had at least 30,000 computer hard drives crippled because the perpetrator had access to a single USB port.

Ensuring the sources are in appropriate IT controlled environments, with extension of the data and signals to the user access points, accomplishes this separation. By extension, we mean that the user only has access to the peripheral devices — keyboard, monitor, video wall, mouse, trackball, joystick, etc. The computing power (source CPU) is located some distance away in a secure, controlled environment. This is a very important step to thwarting security breaches; one that would have mitigated, if not negated the recent Snowden, Manning and Saudi Aramco attacks.

Another important design consideration is the use of highly efficient fiber optic-based systems to control, manage and distribute the information required by the ROC. Where possible, using fiber will provide many performance and security benefits:

- **Distance**, for connecting many rooms and allowing access from offices outside of the rooms
- **Separation**, for locating sources in a secure, controlled environment away from the users
- **Performance**, through high bandwidth, low latency, full resolution signal fidelity even over large distances (especially important for simulation, modeling and high resolution video surveillance)
- **Safety**, by eliminating the electrical emanations found with copper-based systems that might interfere with sensor measurement or pose safety hazards in the field
- **Security**, in addition to physical separation. Copper-based networks are prone to “sniffing;” fiber eliminates the potential to eavesdrop on the information flow

To achieve the appropriate physical separation and reliable connectivity to the required sources and users, implementing a fiber-based system for Real-Time Operating Centers should be considered a best practice.
Robust Access Control.
The system should provide robust restriction schemes that allow an administrator to regulate user access to sources on a port-by-port basis, while preventing any changes to the scheme by anyone other than the administrator. In addition, the system should allow for the management of user access through devices such as USB ports, restricting those ports to peripheral connectivity only and prohibiting the transfer of information.

In addition to physically separating the users from the sources of information, it is important that the system allows the users to access the data they need for the application they are trying to execute, without giving them the ability to take, move or corrupt the data in anyway. Therefore, the system should allow for USB and other media ports to be disabled (while still allowing appropriate USB ports to be used for keyboard, mouse and other peripheral devices).

The system should allow an administrator to restrict the use of the system and access to information on a user-by-user and source-by-source basis. While the system should provide strict restriction at a very granular level, it should be easy for the approved system administrator to modify this restriction scheme as needed. It should be very difficult (in fact, nearly impossible) for a non-approved user to modify the restriction scheme without assistance from the system administrator.

Resiliency and Redundancy.
The system should be configured in a highly reliable and fully redundant approach to ensure the highest levels of continuous operation.

The system needs to be continuously available, and proven robust and fit for purpose in stringent environments like the mission critical environment of an oil and gas ROC or in the oilfield. This includes high Mean Time Between Failure (MTBF) rates, hot swappable components, redundant components and system configurations with the ability to failover to backup systems instantaneously.

Flexibility and Scalability.
The system should be flexible in its ability to scale as users and sources grow, easily incorporating new video, audio and data signaling formats, new users, new locations and new applications.

It is important for the system to be flexible in a number of ways. First, the system should enable administrators to reconfigure meeting rooms for different situations in real-time. For example, a room that supported a daily operations review for an offshore drilling rig at 7 am should easily support an emergency management team handling an onshore safety incident at 10 am.

The system should also be easily expandable to incorporate new sources of information and new users in a single, scalable system design, whether those new end points are located on the same floor as the ROC, elsewhere in the building, in a different building on campus, or across town.

The system should also be modular and easily upgradeable to meet future needs — even if those needs were not known during the original design – with minimal replacement of installed system components. This includes the ability to handle new signaling formats for video, audio and peripheral data, support a larger number of users, address new bandwidth requirements and accommodate new configurations of rooms and buildings.
Thinklogical can provide many benefits in today’s ROC, directly responding to the key design considerations and best practices described in this white paper:

<table>
<thead>
<tr>
<th>Design Consideration</th>
<th>Thinklogical Approach &amp; Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Performance</strong></td>
<td>• No latency</td>
</tr>
<tr>
<td></td>
<td>• No compression; full video and image resolution with no artifacts or lost frames</td>
</tr>
<tr>
<td></td>
<td>• Dedicated, 6.25 Gbps bandwidth per optical stream (port to port)</td>
</tr>
<tr>
<td></td>
<td>• Completely non-blocking crosspoint switching matrices</td>
</tr>
<tr>
<td></td>
<td>• Support for all major video, audio and peripheral signaling formats, including full performance USB 2.0</td>
</tr>
<tr>
<td><strong>Physical Separation</strong></td>
<td>• All Thinklogical systems are fiber optic based (single mode or multimode), allowing for extension up to 80 km (50 miles)</td>
</tr>
<tr>
<td></td>
<td>• Connect geographically disparate users and locations</td>
</tr>
<tr>
<td></td>
<td>• Physically separate sources from users for added security</td>
</tr>
<tr>
<td><strong>Robust Access Control</strong></td>
<td>• Ability to limit the functionality of USB to peripheral connection only; disallowing the theft of data or injection of viruses through USB ports</td>
</tr>
<tr>
<td></td>
<td>• Restrict users and sources on a port by port basis</td>
</tr>
<tr>
<td></td>
<td>• Prevent changes to restriction scheme by unauthorized users by implementing scheme in firmware (requires physical access to the switch to change)</td>
</tr>
<tr>
<td></td>
<td>• Fiber optics are inherently and dramatically less vulnerable to eavesdropping attacks</td>
</tr>
<tr>
<td><strong>Resiliency and Redundancy</strong></td>
<td>• MTBF of 100,000+ hours</td>
</tr>
<tr>
<td></td>
<td>• Configurable to achieve a parallel redundant system with two synchronized Thinklogical switches running parallel (mirroring with identical signals). Thinklogical’s unique “switchover capability” allows the system to automatically choose a stream to “lock onto” and then automatically failover to the parallel stream if necessary.</td>
</tr>
<tr>
<td></td>
<td>• Complete redundant, hot-swappable components such as power supplies and input/output cards</td>
</tr>
<tr>
<td><strong>Flexibility and Scalability</strong></td>
<td>• Flexible restriction scheme and on screen, drag and drop displays to enable quick and easy customization per location/room/application</td>
</tr>
<tr>
<td></td>
<td>• Scalable from 5 ports to 640 x 640</td>
</tr>
<tr>
<td></td>
<td>• Modular switches and extenders allow for reconfiguration and expansion as necessary, customized in the field to the specific customer needs</td>
</tr>
<tr>
<td></td>
<td>• Protocol agnostic, allowing all future video, audio and peripheral signaling formats to be easily incorporated into the overall system</td>
</tr>
</tbody>
</table>

For more information about Thinklogical products and services, or for a complimentary consultation on your specific system needs, please contact the Thinklogical Design Center at 1-800-291-3211 or info@thinklogical.com
Thinklogical is the worldwide leader in the design, manufacture and sales of high performance, secure extension and switching systems to control, distribute and manage video-rich, big data. Our systems switch real-time video, audio and peripheral signals between many sources and many destinations for applications where high and reliable bandwidth is required, co-location of computers with users is not desired, permitted or possible, and where maintaining data integrity and security is necessary or highly important.

Thinklogical extension and switching systems are installed in thousands of customer sites worldwide and across multiple industries, including:

- Global oil, gas, and energy production and distribution companies seeking secure, high performance real-time operating centers and control rooms.
- The U.S. Department of Defense Unified Commands, which operate the largest command and control centers in the world. The ability to securely, yet flexibly, restrict access to Top Secret, Classified and Unclassified information, while ensuring rapid access to mission critical, real time, video rich information in full resolution, with no latency, artifacts or lost frames, is essential to coordinating and directing U.S. and allied forces in various geopolitical regions of the world.
- Unmanned Aerial System (UAS) piloting centers, where security, full video resolution and low control systems latency are crucial to successful drone flight operations, especially over extended pilot shift times of multiple hours.
- Nuclear power plant control centers, where minimization of electromagnetic signal interference with various sensor information (by using fiber rather than copper cabling) is important, and fully redundant, instantaneous failover to an emergency control center located a safe distance from the reactor core are all crucial requirements.
- U.S. State Department Embassies in combat zones and world hotspots, where mission-critical command and control centers are used to direct security efforts local to the embassy, and provide intelligence and surveillance information to central commands in the region.

Summary
Change is constant in all aspects of today’s oil and gas industry. Implementing a secure, high-performance video and data distribution system for Real-Time Operating Centers, based on the design considerations and best practices found in this white paper, will ensure that organizations are able to manage this change effectively and capitalize on the benefits and efficiencies of implementing AIM.
The Thinklogical Advantage

- Thinklogical offers the highest extension and cross point switching performance in the industry, with dedicated 6.25 Gbps of bandwidth per optical thread, in a scalable, protocol-agnostic, completely non-blocking switching matrix.

- Thinklogical systems transport every resolution of computer or broadcast video available today, with no compression, pixelation, lost frames, artifacts or latency, and with the lowest fiber footprint in the industry.

- Thinklogical systems offer the highest Mean Time Between Failure (MTBF) in the industry (100,000 hours), hot-swappable and redundant components, and can be configured as fully redundant with immediate failover capability.

- Thinklogical systems can be designed to achieve, over significant distances (up to 80 km) if necessary, separation of the threat (users) from the target of the attack (the information). In addition, Thinklogical offers the ability to limit the functionality of USB ports, allowing for peripheral connection but prohibiting the theft of data or injection of viruses through USB ports.

- Thinklogical provides a robust and flexible suite of advanced partitioning and restriction features and functions that allow for close management of user interaction in environments with multiple users and multiple sources of confidential information.

In fact, the Thinklogical system architecture has undergone stringent independent testing with NATO and the US Department of Defense, resulting in the awarding of Common Criteria EAL-4 status, NATO NIAPC Green, and TEMPEST approval. These accreditations endorse the system for use in the most secure and most demanding military and intelligence environments, based on fiber, electrical and firmware isolation characteristics, system architecture security features and functions, and the robustness, reliability and redundancy of the switching products. Thinklogical is the only company in the world to achieve Common Criteria EAL-4 status for fiber optic based extension and switching systems.