Real Time
Networks

WHITEPAPER

Maximizing Security: How to Implement an Integrated Physical Access and Asset Control System

Lee Purvis, CTO, Real Time Networks |
Joshua Tanton, Software Developer, Real TIme Networks

Contact us for a LIVE DEMO TODAY

1-800-331-2882 | info@realtimenetworks.com | www.realtimenetworks.com

Real Time Networks

Table of Contents

Topic Page

Executive Summary

The importance and benefits of Physical Access Control Systems (PACS) and Asset Management Systems (AMS) operating independently of each other are well-understood in a wide range of business settings. This white paper will examine the process and benefits of integrating these systems into a unified system for controlling and managing access to physical assets across your organization.

Many professionals need to know the efficiencies they can gain by centralizing user access level management and streamlining asset assignments. Because today, their organizations are likely missing frequent opportunities to optimize user and asset management workflows, discover undetected gaps in security, and gain overall cost savings.

To properly understand the benefits of integrating both systems, let us first consider what each system brings to the table. Once we understand the purpose of each system, we can then discuss the combined capabilities and benefits when these systems are integrated.

What is the Difference Between Physical Access Control Systems and Asset Management Systems?

Physical Access Control Systems (PACS) provide a secure physical access point to an organization’s premises, allowing authorized personnel to enter secure doors and buildings. They deploy one or more access control methods at physical barriers that require users to authenticate themselves before gaining entry. Some examples of popular access control methods include locks and keys, card readers, and biometric devices.

PACSs are essential for any business as they help control access to critical spaces and resources. A user's access level is usually determined by their position, department, or duties within the organization, but other factors can also be considered. The PACS maintains the security and integrity of protected resources by managing which users can access those resources and when that access is permitted. For these reasons, you will often find a PACS to be a fundamental requirement in any secure organization.

On the other hand, Asset Management Systems (AMS) provide another secure layer of resource management and access control within organizations. Unlike a PACS, which is designed to manage access to doors and buildings, an AMS is designed to secure stored assets that are essential to employees performing their duties. An AMS manages the privileges and access to assets for authorized personnel only after they have been granted access to these secure locations by the PACS. These systems allow organizations to ensure that users only have access to the resources they need to complete their tasks, preventing unauthorized use or manipulation of critical tools and gear.

While each system provides invaluable benefits to the company independently, organizations will see far more advantages and functionality by integrating their PACS and AMS. Furthermore, this integration provides an additional barrier of security that is not achievable using either system alone. Moreover, organizations can improve resource allocation and lifecycle management by establishing an integration system to sync data between both systems.

Introducing an Integration System

System Integrations refer to the process of linking different systems together to achieve a unified and cohesive system that is more efficient than any of its individual components. These integrations are becoming increasingly important as organizations strive for greater efficiency, cost savings, and improved security. By connecting compatible systems together, previously disconnected processes can be automated, data can be shared between multiple applications, and users can access multiple functionalities from a single interface. Through this integration process, disparate systems are made to work together to streamline processes, improve collaboration between departments, or create an overall better user experience.

In terms of physical access control systems (PACS) and asset management systems (AMS), integrating both technologies allows companies to ensure that only authorized personnel have access to the resources they need, while also providing a greater level of security and resource management. Achieving this integration involves computing the delta between both models to ensure that data is synchronized between them.

The end goal of system integrations is to make it easier for organizations to manage their systems and optimize their processes. By connecting previously disconnected components, people can get more work done in less time with fewer errors and better control over how resources are used. Integrating different systems gives businesses the opportunity to move forward as one efficient unit rather than relying on multiple disparate tools that don't always work together seamlessly. With careful consideration and preparation, any organization should be able to reap the benefits of system integrations.

Various manufacturers have their own implementations of their integration systems which most commonly integrates to a specific target and/or source system. These integration systems are usually designed to handle a specific archetypal model or structure and will be commonly unsuited to handle a variety of PACS or AMS systems. At Real Time Networks, we have successfully developed a proprietary middleware integration system, called RTNConnect, that is able to integrate virtually any PACS with our KeyTracer key management systems and AssetTracer smart locker systems.

The Benefits of Integrating PACS and AMS

Organizations can expect to see a range of benefits when they bring these systems together on a unified management platform.

Reduced operating costs and administrative overhead

Instead of having one system to manage user privileges and a separate one to manage their corresponding access to assets, companies can reduce their operational costs by integrating PACS and AMS systems. This way, user and corresponding asset assignments can be managed entirely on the PACS. Asset assignments are then automatically made on the PACS based on the user's access levels or group assignments.

Improved security and access control for users

An organization opens itself to unnecessary inconsistencies between record systems when a PACS is managed separately from an AMS. This may allow for unverified user access to assets the user may no longer or should no longer have access to. Having the integration in place maintains a single source of truth. It ensures that the user will automatically lose access to secured assets immediately in the AMS once their privileges have been revoked on the PACS.

Increased efficiency in user management processes

Conversely, this also ensures that a user will have the proper asset assignments immediately after being granted privileges on the PACS. Due to the automatic asset assignment afforded in an integrated system, users no longer have to wait for an administrator to activate their asset assignments in a separate system manually. This reduces worker downtime spent waiting for additional administrative tasks to occur.

Greater insight into user behavior

A properly integrated system will also allow the AMS to send events or alarms, such as overdue asset alerts, improper returns, or tamper alerts to the PACS. Having this combined set of information can be invaluable to an administrator in analyzing a user's behavior instead of the limited information that can be reported by the systems separately. In addition, companies can track which user has accessed what asset at any given time, allowing them greater visibility into how their resources are used by employees, increasing user accountability across the organization.

Streamlined user authentication process and experience

An integrated access system gives users a seamless experience accessing their assets and resources. They will no longer need to remember multiple sets of credentials or go through multiple steps to gain access. Since data is shared between both systems, a user can use the same credentials to gain access to both doors and assets. This also eliminates multiple steps in the onboarding process of new users.

Improved scalability for businesses

Integrating a PACS and an AMS allows the business to scale quickly as new users can be added or removed en masse to their respective departments or job positions. Access assignments can be made rapidly without manually configuring each user and system separately. This allows companies to update large-scale user changes with greater ease.

PACS and AMS Integration Process

Integrating a PACS and AMS is a four-step process:

1 Identify the archetypal differences between systems

2 Establish the relationship between the models of both systems

3 Compute the delta between the models

4 Send the computed delta to the target system

1 Greater insight into user behavior

Each PACS system usually has its own functionality and implementation options. Functionalities vary widely, from basic user management to unified CCTV monitoring. However, only a few basic PACS data models are relevant when considering integration with an AMS.

- Users - Key actors and primary shareholders of the system.
- Credentials - Means or method of authentication for the user. Typically, these systems employ PIN and card authorizations.
- Groups - Functionality to organize users or assets in a collection.
- Access Levels - Privileges that can be assigned to a user or group, including:
  - o Access Levels
  - o Access Rules

o Clearance

o Assignments

o Clearance Codes

2 Establish the relationship between the models of both systems

Once we have identified the key data components of a PACS, the next objective will be to match and translate these to the equivalent components in the AMS. Although some relationships between system components can be easily identified, others can be more challenging.

Determining relationships between users and credentials between both systems is usually evident. The greater challenge lies in matching a PACS access level to an AMS asset assignment. Some products may implement access-level assignments directly to users, whereas organizations may implement this using groups instead. Both are effective strategies, but mapping one to the other can be difficult without proper planning.

3 Compute the delta between the models

Once the data relationships between the two systems have been established, a delta must be computed to determine any discrepancies between the PACS and AMS models. In mathematics and engineering, a delta is a quantitative difference between two systems.

In this scenario, the delta is computed by establishing any changes in data in the relationships that were established between the two systems.

4 Send the computed delta to the target system

Once the delta between the two models has been computed, it can be sent to the target system to synchronize both. In most cases, this data transmission is unidirectional and flows from the PACS to the AMS, since the PACS is usually the source of truth, and the AMS is the target. However, in special cases, alarms from the AMS can also be sent to the PACS to facilitate the monitoring and reporting of both systems on the PACS.

Essential Factors to Consider When Choosing an Integration System

Choosing the right integration system is crucial in any business or organization. It is important to select an integration system that meets your requirements while being cost-effective and reliable. Factors such as compatibility with your existing systems, security measures, ease of use, automation capabilities, and support options should all be considered when selecting an integration system.

Additionally, it is important to consider the long-term implications of integrating new technology into your environment. For example, what challenges may arise? How will you manage them? Answering these questions before committing to a specific solution can save time and money.

Compatibility with existing systems

For obvious reasons, choosing an integration system compatible with your current systems is a primary concern. Unfortunately, not all integration systems will support your PACS and your AMS. Even if they do, manufacturers usually specialize in integrating specific products or systems. In most cases, integration systems concentrate on integrating a specific PACS with a specific AMS.

A robust integration system should be able to handle the wide archetypal differences between any given PACS and AMS. It should be able to easily determine the relationships between both systems and compute its delta efficiently. Compatibility with various systems will afford more flexibility for future expansions within the system.

Level of integration

The integration level can be thought of as the amount of interaction required with the PACS. It is typically classified as either partial or full integration.

Partial integration requires a certain amount of interaction with the PACS, usually during the system's initial setup. This usually involves creating the AMS components (e.g., the users, credentials, and access levels) within the PACS to establish the relationship between the systems.

Full integration, however, requires minimal-to-no interaction with the PACS to set up the system. This level of integration automatically pulls the assets to be integrated from the AMS and creates them and their corresponding relationships on the PACS during the initial setup process.

Customization and scalability

The ability to easily configure the integration system to meet your current operational requirements is also an extremely crucial point of consideration. This can include tailoring user access levels or permissions and specifying which users or groups should be included in the integration process.

Some organizations may employ thousands or even millions of users. For operations at this scale, a proper system should be able to efficiently filter out subsets of users and update target data not to affect the organization's daily operation. Even simple options to disable users from the system to preserve the user's historical transactions instead of permanently deleting them may prove invaluable to certain organizations.

Automation capabilities

Integrated systems must be regularly updated to stay in sync. In addition, the integration you choose should be able to trigger on a schedule that fits your needs. For example, some companies may want to initiate the process on a scheduled basis, such as daily at a specific time. Others integrate manually, on demand.

Security considerations

Security is one of the most crucial factors to consider when assessing an integration system. Any data that is transferred between systems must be encrypted and secure. This means that a system must also use secure methods to authenticate and authorize any users accessing the system and protect the data using strong encryption methods.

Initial and ongoing support

Without good support, organizations may find themselves dealing with integration problems they cannot resolve promptly, leading to costly delays and unforeseen expenses that can add up quickly. Having the right support team readily available through your integration provider allows organizations to resolve access control issues quickly and efficiently. Additionally, having access to initial assistance during setup and ongoing maintenance assistance can make all the difference in keeping PACS and AMS systems running optimally.

Overall cost

It is important to ensure that an integration system is within the organization's budget and that it fits all the needs and requirements of the business. Both upfront and ongoing costs should be taken into consideration against the potential savings that can be incurred when implementing such a system.

Best Practices for Implementing and Maintaining a Successful Integration

Maintaining an effective integrated system over time is essential for any organization that wants standardized, centralized data management. It is important to follow certain best practices to ensure that your integration process will perform effectively and optimally.

- Develop a detailed implementation plan, including testing the system before deployment. This should be done in a sandbox environment before deploying in a production environment.
- Regularly monitor both systems for potential issues or discrepancies before they become problematic.
- Invest in staff training so everyone understands how the integrated system works and can use it effectively.
- Utilize tools such as analytics and monitoring software to track performance metrics related to the integrated system.

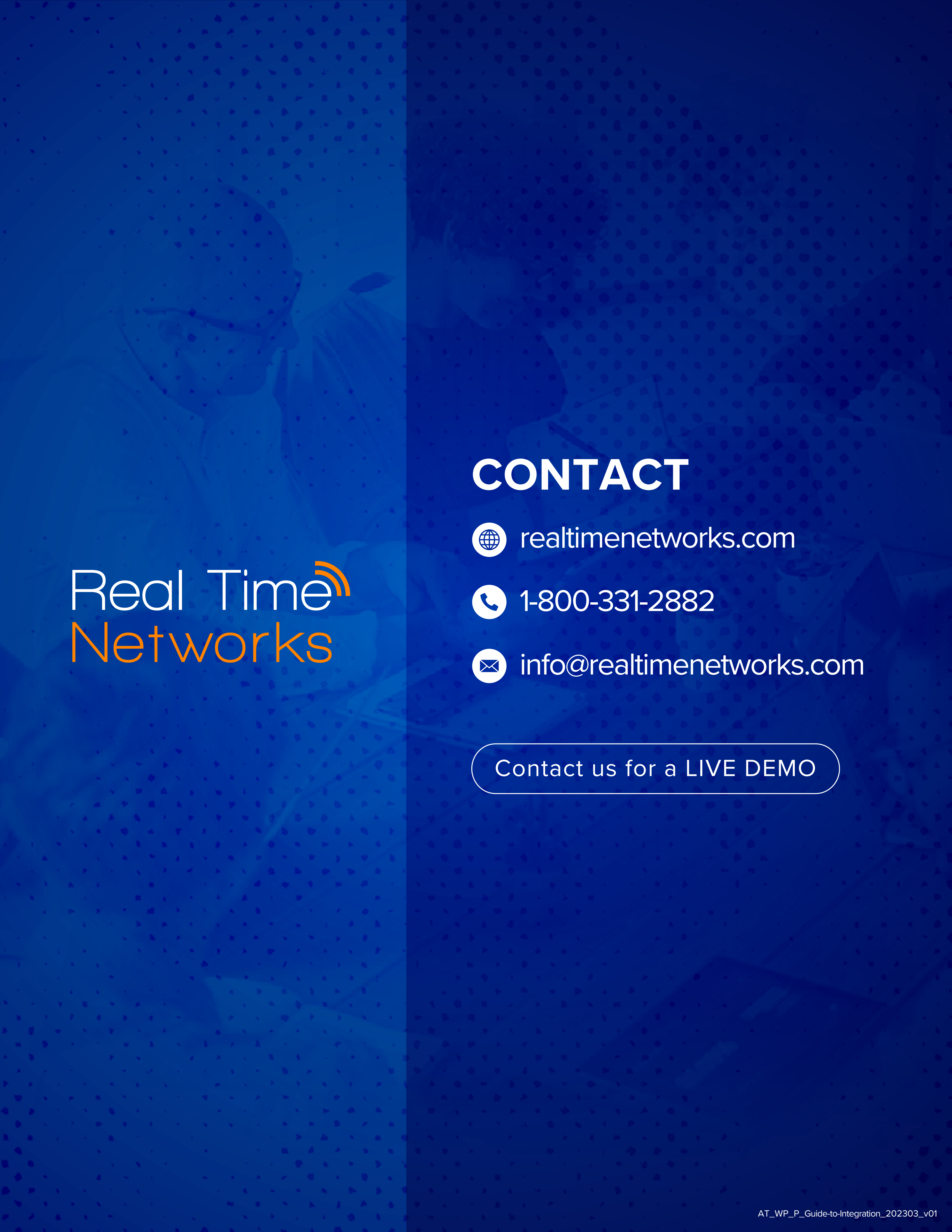
- Make sure all security measures are up-to-date and compliant with industry standards, such as encryption protocols, authentication requirements, and operating system levels.
- Use feedback from integrated system users to identify areas where improvements could be made.
- Establish regular reviews of your integration process to assess its effectiveness to the organization.

Available PACS Integrations

At Real Time Networks, we are proud to have collaborated with multiple companies in successfully integrating with numerous types of PACS and AMS systems. We currently support the integration of our AssetTracer and KeyTracer products with various PACS systems, including: **LenelS2 OnGuard**, **LenelS2 Netbox**, **Genetec Security Center**, **Software House CCure 9000**, and **Honeywell ProWatch**. In addition, we have deployed solutions based on **Microsoft Azure Active Directory** and **Microsoft Active Directory** integrations.

Integrating these systems helps businesses to optimize their management process, improve security within the organization, and maximize cost-effectiveness. By following the steps outlined in this article and leveraging the tips for maintaining an effective integrated system over time, businesses will be well on their way towards achieving success with integrating their access control systems.

If you are looking into integrating your PACS and AMS or would like more information, please contact us at 1-800-331-2882 or info@realtimenetworks.com.



Real Time
Networks

CONTACT

🌐 realtimenetworks.com

☎ 1-800-331-2882

✉ info@realtimenetworks.com

Contact us for a LIVE DEMO