WHITE PAPER

Considerations and best practices for migrating to an IP-based access control system

Genetec™

genetec.com

Executive Summary

Migrating from an existing legacy Access Control System (ACS) to an Internet Protocol (IP) based ACS makes it easier for organizations to operate, expand, and customize their physical access control infrastructure, allows them to leverage new ACS capabilities, including efficient multi-site management and Power over Ethernet (PoE) technologies, and helps them to achieve significant reductions in their Total Cost of Ownership (TCO).

Undertaking a successful migration, however, requires planning and careful consideration. First, it is important to have a clear set of goals for a migration to ensure that an organization chooses an IP ACS system designed to evolve over time and re-uses as much of the existing security infrastructure as possible. Then, before beginning to plan a migration, an organization must evaluate their existing system in order to determine costs and time required for the migration.

Finally, together with a systems integrator, it is important that an organization follow a number of steps to realize a seamless and successful integration.

Reasons to Migrate

Migrating an existing centralized or distributed legacy Access Control System (ACS) to an Internet Protocol-based (IP) ACS has the distinct advantage of making it easier for an organization to operate, expand, and customize their physical access control infrastructure.

In particular, with an IP ACS, an organization can

- leverage IP technology to standardize their access control infrastructure, moving away from proprietary wiring and equipment,
- move intelligence to the door, reducing the number of failure points and streamlining system monitoring and management,
- simplify future infrastructure expansion and modification, resulting in significant reductions in the Total Cost of Ownership (TCO), and
- integrate all security, access control, and video surveillance into a unified platform with a single interface, thereby providing better facility monitoring and management.

With an IP-based solution, an organization can also take advantage of newer functionalities not available with legacy or more traditional systems. For this reason, the decision to migrate cannot simply be based on a simple like-for-like functional replacement of one system by another but must also take into account how to leverage the new ACS capabilities offered by IP-based solutions, including

- efficient multi-site management and monitoring,
- scaling to greater doors counts over a network,
- access to Power over Ethernet (PoE) door controllers and more advanced hardware options,
- using global cardholder management to move to a single card across all sites within an organization,
- automating cardholder and access rights management using Microsoft Active Directory,
- leveraging cards that support logical and physical security, and
- unifying 3rd party solutions over IP as opposed to integrating them using electrical wiring and relays.

Traditional physical access control systems are also becoming increasingly expensive to maintain and operate, leading to dramatic increases in system TCO. As legacy ACS components reach the end of their service life or begin failing at an ever increasing rate, the costs associated with maintaining such systems and finding suitable replacement parts greatly increase. In addition, the costs involved in leveraging a legacy system composed of proprietary hardware and software can be greater because an organization has fewer options available for system components and is unable to leverage new, less expensive equipment that offers new and valued benefits.

Lastly, because legacy systems typically operate by delivering separate power to each card reader and lock, they are more expensive than an IP ACS that supports PoE to connect and power all IP door controllers, readers, and door locks over a standard Cat5e/Cat 6 cable. PoE controllers also reduce TCO by leveraging IP infrastructure for both communications and power, thereby reducing wiring and labor expenditures, and, as PoE technology evolves, these controllers will be able to support even greater power requirements at the door, such as more powerful locks.

Goals for a Migration

Having decided to migrate from an older legacy system to a new IP-based ACS, an organization should keep the following goals in mind when trying to decide on the solutions provider who can best meet their access control needs.

A. Buying a system with a long life span

When trying to determine the life span of an IP ACS, there are numerous factors to consider:

- Is the solution non-proprietary and open architecture?
  - › An open architecture, non-proprietary IP ACS makes it easier to expand and modify the system infrastructure in the future.
- Does the solution provider have a developed ecosystem of partners?
  - › Choosing a solution provider with technology partners in such areas as asset management, human resources, enterprise resource planning (ERP) systems, and visitor management ensures greater flexibility and more options during migration and when undertaking any future system expansion or modification.
- Does the solution provider offer an off-the-shelf software development kit (SDK)?
  - › An off-the-shelf SDK allows for custom integration and scripting and makes it possible to develop plug-ins to the IP ACS in the future.

B. Re-using existing equipment

Migration to an IP ACS can enhance and protect an organization's long-term investment in their current security infrastructure by extending the life of existing components and infrastructure and by leveraging new system features and applications. With an IP-based system, an organization can consolidate their ACS assets and bring them onto a single security platform, resulting in reduced costs through the elimination of the need to maintain multiple platforms. Consolidating assets can also improve system integration, performance, scalability, reliability, security, and extensibility.

C. Work in parallel

To avoid unnecessary and costly downtime and to achieve a seamless ACS migration, as much work as possible should be accomplished in parallel before the physical migration. During pre-staging, work should be done in parallel and off-line to build the configuration of the new IP ACS into the software, including

- mapping the system,
- importing the inputs/outputs (IOs) from the system components, like doors,
- integrating the logic to control the components, and
- testing IOs and reads from readers prior to migration.

D. Keep downtime to a minimum

When migrating an existing system, an organization must take into account the impact that downtime will have on system users. Beyond scheduling migration downtime during off-peak hours, it is also important during the selection stage to determine

- the peak hours during which the ACS must be fully functional,
- whether the new IP ACS allows for pre-staging, and
- whether the new IP ACS can be connected to existing doors in parallel to further speed up the cutover period.

E. Ensure that all functionality needed by the end user remains available with the new system

It is important for an organization to review the hardware and software features currently being used in their legacy ACS and to ensure that these features will also be available in the new system. Features that should be analyzed include

- scalability, the number of doors currently supported, and the possible number of doors to be supported in any future expansion,
- cardholder management,
- access rights management, including scheduling,
- badge design, including image capture requirements,
- web client needs,
- mobile app needs,
- visitor management, and
- enrolment devices, including USB card readers.

In addition to analyzing features, an organization should also look at their current access control workflow and ensure that the solutions provider will be able to at least maintain if not improve the workflow in the new system.

Overview of Considerations

The following considerations are intended to help an organization to evaluate their current legacy ACS and determine how much of that system can be re-used.

The results of these evaluations have a direct impact on

(1) the decision as to whether a full replacement or a migration with partial or limited replacement is required,

(2) the cost of the migration, and

(3) the time required for the migration.

Hardware considerations

Any migration from a centralized or distributed legacy ACS to an IP ACS must begin by looking at the current system and evaluating the existing hardware components, starting with the credentials and whether or not the encoded information and card formats can be re-used. Migrating to an IP ACS is made easier if the existing system uses non-proprietary cards and readers, but a good IP ACS can support 3rd party proprietary credentials even when the card format is unknown as long as the reader can output the entire credential data. However, if the existing readers support proprietary communication, then a full replacement of legacy readers will likely be required.

It is also important to evaluate whether the existing intelligent controllers and downstream interface panels that connect the card readers and door hardware to the intelligent controller can be re-used. If the existing controllers are open architecture and are supported by a number of security software vendors, then it may be possible to incorporate them into the new IP ACS.

Software considerations

When evaluating the current software configuration, it is important to determine exactly what needs to be ported to the new system. Consideration must be given to the native data in the legacy credentials, the tools used to export that information from the current database, and any 3rd party components integrated into the configuration through the SDK. This evaluation is essential for determining a strategy for porting current data to the new database and for integrating 3rd party custom components into the new ACS configuration.

Network considerations

The network needs of the new IP-based system must also be evaluated when considering migrating to a PoE access control solution. Because an IP system places the controller at the door and uses PoE edge devices, migrating involves designing and implementing the proper wiring architecture—Cat5e/Cat 6 wiring to the door—and ensuring that the proper network equipment is in place.

In addition, when migrating a distributed system with both local and remote sites, an organization must also consider issues of latency and bandwidth in

relation to the speed and security of communication between sites and must ensure that the migration plan fully leverages the network potential of the new IP system.

Wiring considerations

The wiring in a legacy ACS, including reader-to-panel wiring, interface module to controller wiring, and I/O wiring to interface modules, is another important consideration for any migration since it may be possible to re-use some of the existing wiring in the new IP ACS. Prior to migration, it is important to compare the characteristics of the existing cabling, including wire gauge, against the requirements for the new IP ACS equipment. Additionally, if an organization is looking to expand their current ACS during migration, consideration must be given to the extra wiring that will be required since this will add to the overall cost of the project.

An organization must also validate reader-to-interface module or controller wiring because standard or non-proprietary reader wiring can typically be re-used, as in the case of readers with a Wiegand or Clock-and-Data interface. However, since proprietary readers often have fewer wires, migrating to non-proprietary readers can require additional wiring, resulting in increased costs. Since it is possible to re-use existing interface module wiring that leverage well known standards, such as RS-485, another important consideration is to validate interface module to intelligent controller wiring.

Power considerations

Prior to migration, consideration must also be given to the type of power in place in the current ACS, specifically whether the system is 12V or 24V and DC or AC and whether it can provide enough current for the new hardware components in the IP ACS. And, because the amount of additional power and wiring required can have a significant effect on the overall cost of a migration, an organization must ascertain whether the current system can be used to power the panels and readers in the new IP ACS or if separate power sources will be needed for each component.

Training considerations

Any successful migration to an IP-based system requires comprehensive training on how to use the new software. Therefore, consideration should be given to the type of training required for the various ACS users based on their tasks and/or the client applications they will use with the new IP ACS. Typical users can include receptionists, IT staff, security operators or other personnel, and system administrators, and their training needs can range from operator training to system administration and in-depth technical training.

Support during the migration and later

For any successful migration, it is important to take into account the level of support provided by the integrator installing the new ACS and by the manufacturers and solutions providers whose components will make up the new system. ACS migration requires the expertise of pre-sales engineers to help build the migration plan, technical specialists and field service engineers to configure and support the software and offer advice for migration, and support engineers to address any issues arising after the migration has been completed. With larger or more complex system, installers and manufacturers should work hand-in-hand to ensure a successful migration.

Steps in the Migration Process

There are a number of steps involved in the realization of a successful and seamless migration. In the initial steps, the customer—or end user—works with a systems integrator and possibly with manufacturers and solutions providers to build a quote and a migration plan. As the plan is being implemented, technical support and field engineers will be required to design and configure the new IP-based system and to integrate all of the components.

1. Get the facts

The first step for the systems integrator is to put the configuration of the current ACS down on paper, including such details as the location of electrical and telecom closets, wiring, and the type of power currently in place. It is also important to develop a complete list of the hardware components, servers, and networking equipment currently being used in the system and to provide details about current software features that will be required in the new system.

2. Understand the requirements of the new system

In order to develop a successful migration plan, the integrator must understand the following requirements of the new IP ACS:

- Hardware components
- Software components
- Network configuration
- Wiring
- Power

Understanding these requirements is critical for designing the architecture of the new system.

3. Site survey

The next step is a walk-through of the facility with the customer and the systems integrator—and possibly with manufacturers—in order to ensure that nothing has been overlooked with regards to the existing system and that all of the new system requirements are clearly understood. The site survey can also be the first step in the overall process. The purpose of site survey is

- to develop a clear picture of the existing architecture and layout of the existing system and wiring,
- to determine where equipment is concentrated, and
- to measure the distances between access control panels, power sources, and readers.

4. Determine components that can be re-used

A complete picture concerning an organization's current ACS and the requirements for the new system is essential for determining what hardware, software, power, wiring, and networking components can be re-used. For example, it is possible to re-use cards and card readers if the hardware is non-proprietary, which would mean that the new IP ACS could potentially use the information stored on the existing cards.

5. Testing existing components

After determining what components of the existing system can be re-used, such as controllers, interface modules, cards, and readers, either the systems integrator or the manufacturer(s) should test these components to ensure compatibility.

6. Define new equipment needs

With a clear understanding of what can be re-used from the existing legacy system and what is needed in the new system, the integrator must now determine the new network and access control needs for the IP ACS.

7. Understand the existing databases and data

Determining how to import existing cardholder and credential data into the new IP ACS is the next step in the migration process. So as to fully leverage existing 3rd party software data, technical specialists or field engineers will need to export cardholder and credential data from the existing system into a standard or usable file format, such as CSV or Microsoft Excel file. The export process either leverages the current system's export tool or requires the development of custom scripts to export the data from the database.

In addition, the new system should also provide the ability to import data from a standard or usable file format. Since some data manipulation may be required after the export, this should also be taken into account. Before undertaking this process, it is good practice to evaluate the type and format of the exported data.

8. Plan the migration

To keep downtime during migration to a minimum, the systems integrator must carefully plan the hardware migration and ensure that as much software and hardware installation as possible is accomplished in parallel. In addition, network configuration and custom development, whether building a bridge to any 3rd party software or developing customized software, must be included in the migration plan. Lastly, the systems integrator must develop a detailed schedule for cutover and for activating the components in the new system.

9. Test the new IP system

In order to ensure a seamless migration, the integrator should undertake a complete walk-through of the new IP system before executing the migration and making it operational. By pre-staging the new IP ACS in parallel with the current system, the new system—the software and hardware—can be tested prior to cutover.

10. Execute the migration and acceptance testing

Following the schedule developed as part of the migration plan, the systems integrator and customer can now begin cutover from the old to the new ACS. At this point, it is important to have manufacturers on standby in case any problems arise with any of the new ACS components. Then, the systems integrator and customer must go through the acceptance test plan to ensure that all of the steps of the migration plan were executed properly and that all of the equipment in the system is working properly.

The Genetec Approach to Migration

To ensure a seamless migration, Genetec is available throughout the migration process, from initial surveying and migration planning to system testing and support. In its role as solutions provider, Genetec provides systems integrators with access to pre-sales engineers, field engineers, and technical support engineers to help with various aspects of a migration.

Working with Synergis, Genetec's IP access control solution, also gives customers the advantage of working with an open architecture platform. With Synergis, an organization is not locked into proprietary hardware and is able to upgrade to the latest supported technology at any time. This open architecture platform also offers customers much more flexibility when it comes to 3rd party system integrations as long as a technology vendor offers software interfaces (eg. API or SDK) or integration protocols to facilitate the integration process.

Genetec's Synergis Cloud Link appliance, a key component of the Synergis IP ACS, allows customers to execute a seamless migration while leveraging their existing networking infrastructure and existing equipment and wiring. Synergis Cloud Link is a true IP and PoE-ready intelligent appliance with two on-board Gigabit Ethernet ports that enable customers to efficiently leverage their corporate or security network and to re-use much of their existing access control infrastructure, including readers, credentials, compatible interface modules, and wiring. To further speed up the migration process, the Synergis Cloud Link appliance

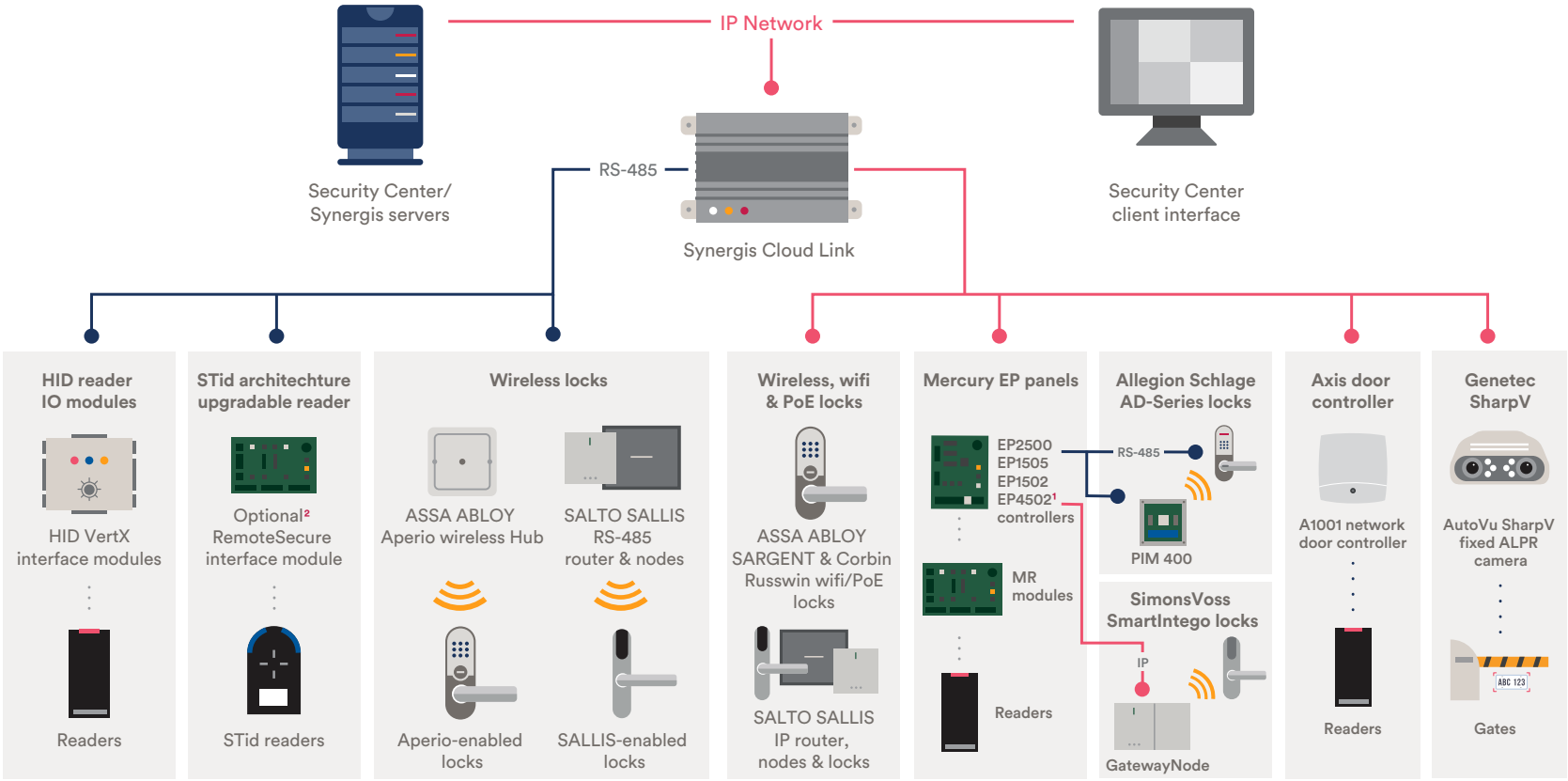
- can be installed prior to Synergis software being deployed,
- can be partially configured in advance, and
- supports web-based access for testing connectivity to door hardware, such as door sensors and relays.

Genetec also works with various technology partners whose devices and systems are deeply integrated with the Synergis solution. For example, to help speed up deployment time and reduce the costs associated with migration, the Synergis Cloud Link appliance features native support for non-proprietary access control hardware from HID Global and Mercury Security, and for wireless and PoE locks from SALTO and ASSA ABLOY, including Sargent, Corbin Russwin, and Aperio. In addition, HID, Mercury, SALTO, and ASSA ABLOY modules can all be supported on the same Synergis Cloud Link appliance.

Some of Genetec's Access Control Hardware and Software Partners

Architecture overview

Synergis Cloud Link supports a variety of third-party interface modules and panels. Simply install the intelligent appliance on your network and connect to downstream devices over RS-485 or IP. With Synergis Cloud Link designed to be an open platform, your investment is protected for years to come.



1 The Allegion Schlage AD-Series report into the Mercury EP2500 or EP1501 and SimonsVoss SmartIntego locks report into the Mercury EP2500, EP1501 or EP1502
2 The RemoteSecure interface module is an optional device that hosts keys onboard for ANSSI compliance

For more information, visit:

genetec.com/synergis