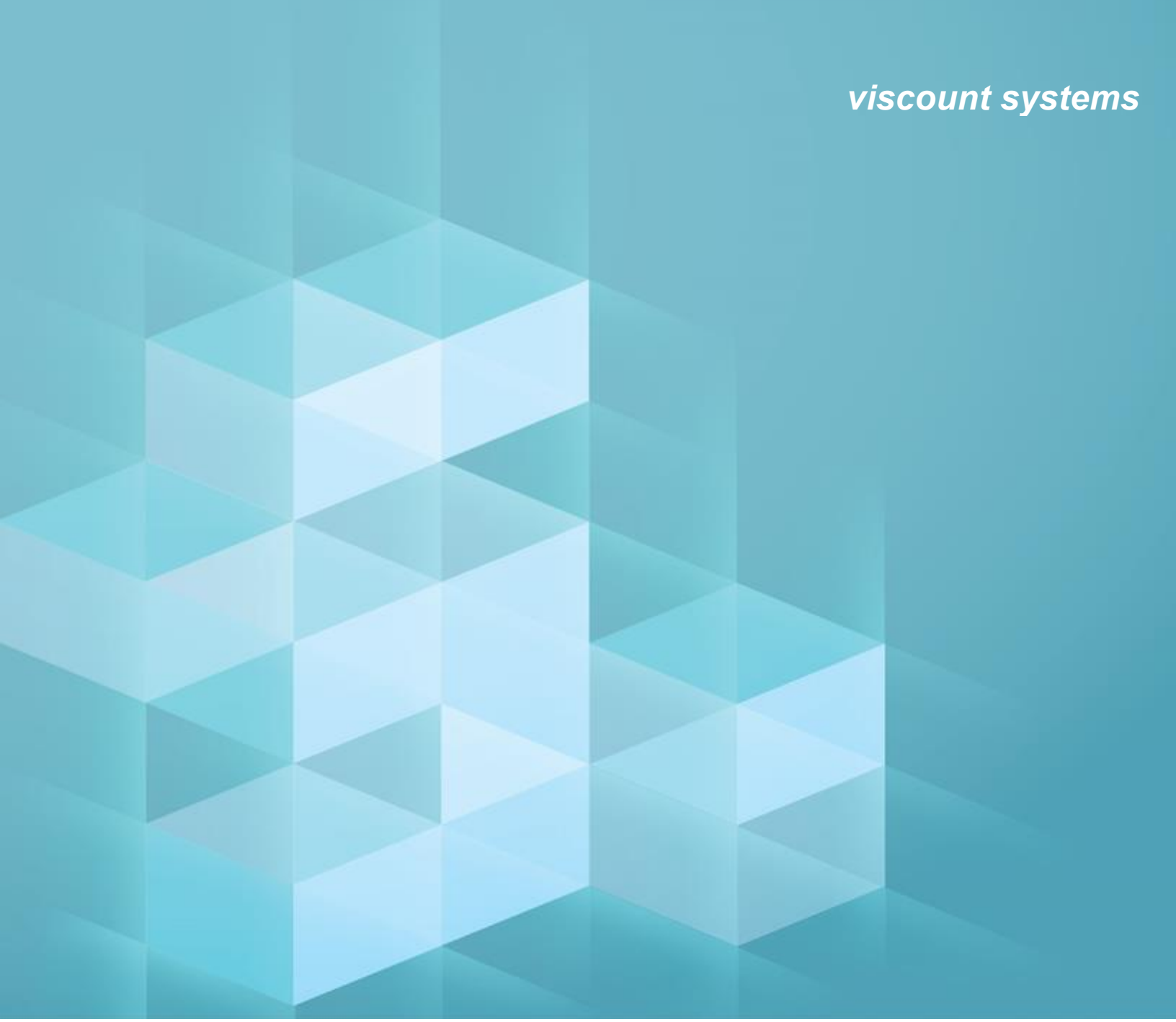


Why it's Time to Completely Rethink Physical Access Control System Architecture

It's Time to Completely Rethink Physical Access Control System Architecture

Adequate security of organizational assets (people, materials and critical processes) is a fundamental management responsibility. Physical access control systems (PACS) have been a critically important element of asset protection for more than three decades.

But over the past thirty years, PACS architecture has essentially remained unchanged. Some PACS manufacturers have physically moved the database server part of that architecture into the cloud. However, the application architecture (the where and how of the real-time computing, communications and control elements) has remained the same. The most important part of the system—granting or denying access—still resides in traditional hardware distributed throughout the protected facilities. Computing and networking technology has advanced significantly over these three decades. Thus today's hardware-centric PACS architecture now has a number of significant disadvantages:

- High initial and ongoing costs of the distributed computing hardware
- Native inability to make access decisions that include combined real-time information from trusted external systems, such as:
    - current threat picture
    - personnel presence information (physical and logical)
    - changing access privilege qualifications, such personnel just-authorized for on-site incident emergency response
    - environmental safety factors such as bio-hazard exposure
- Native inability to support the strongest available card and cardholder authentication (and meet U.S. federal systems requirements) without the addition of relatively expensive 3rd party solutions
- Inability to take full advantage of organizational investments in IT infrastructure

The current PACS architecture significantly limits access control system capabilities. This paper explains why next generation PACS architecture is long overdue: it presents the critical IT-aligned attributes and capabilities that next generation PACS architecture must possess.

Traditional PACS Architecture

Three decades ago, before organizations had enterprise-wide computing and network infrastructures to build on, physical access control systems had to be self-contained systems. They had to distribute their processing functions and databases out into field control panel hardware throughout facilities, due to limitations in hardware processing power and communications speeds. PACS architecture was necessarily *hardware-centric*, with custom software code stored as firmware on every hardware board. This architecture is referred to as "distributed intelligence", and the controllers are called "intelligent panels" or "intelligent controllers". Likewise, a networked card reader with built-in controller functionality is called an "intelligent reader".

Yet today, the technology limitations that required hardware-centric distributed-intelligence systems don't exist. Yet PACS architecture essentially remains the same, saddling customers with the needless limitations and high costs of hardware-centric systems.

Technology Advances

Computing power is more than 30,000 times what it used to be, and continues to increase (see Figure 1 below). Wired communication speed is more than 10,000 times what it was and also continues to increase (see Figure 2 below). Very importantly, wired corporate Ethernet networks are now highly resilient and ubiquitous.

Figure 1: Computing Power Growth

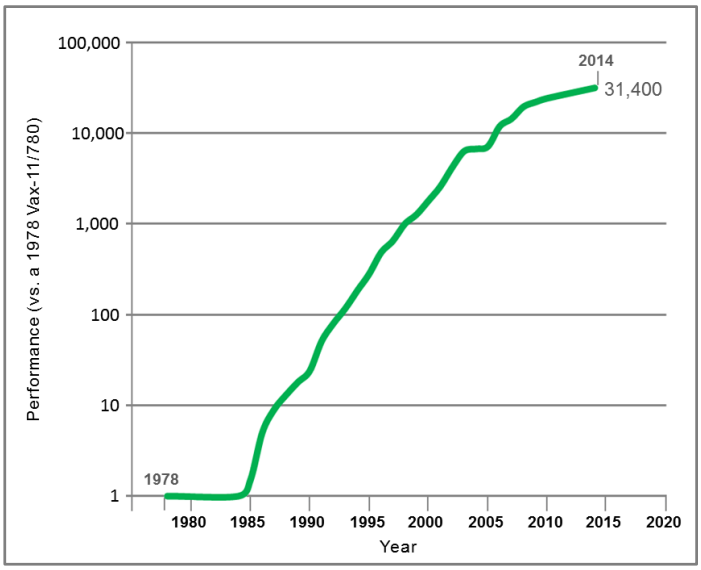
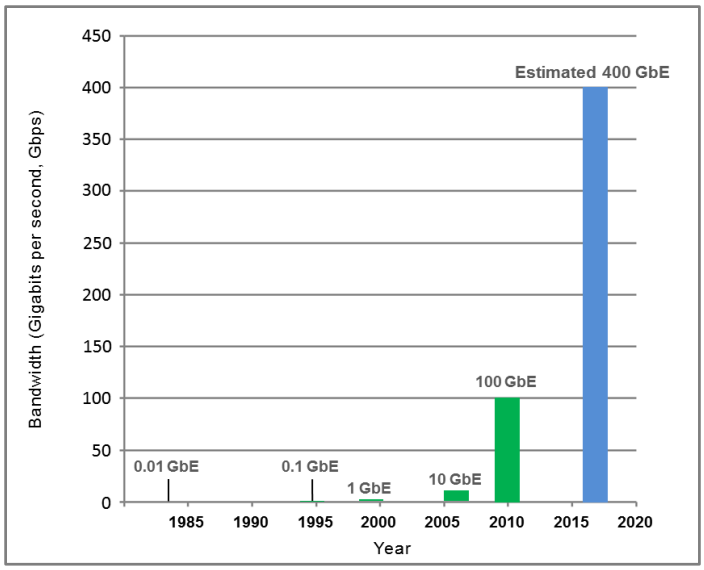


Figure 2: Network Capacity Growth



This is why today's critical business systems are *software-centric* networked systems that require specialized hardware only at the final points of physical interaction (such as telephones, cash registers, ATMs, etc.). They leverage common IT infrastructure (high-speed servers and networks) to achieve high levels of reliable performance at acceptable levels of cost. And as processing power and data speeds of existing IT infrastructure are upgraded, all business applications benefit—except PACS.

> *It is long past the time to leave outdated PACS architecture behind and move to next generation PACS architecture. Not only is it technologically feasible, it is an indisputable requirement for fulfilling asset protection responsibilities in a world of advancing technology, persistent threats and evolving threat vectors.*
>
> --Ray Bernard, Leading Security Consultant, Speaker and Author

Why Next Generation PACS Architecture is Needed

Next generation PACS architecture refers to architecture that is fundamentally different, not incrementally different, from the traditional PACS architecture still common today. It is architecture built to maximally utilize the evolving IT infrastructures of today's organizations, a key future-proofing and cost-minimizing factor. It is architecture that keeps pace with technology advancements in computing, communications and integration at the system level and the device level—providing strong security capabilities in a cost-feasible manner. It is architecture built for the future, not anchored in the past.

Today's Hardware-Centric PACS Architecture Can't Keep Up

Hardware-centric PACS architecture was a necessity in a time when organizational IT infrastructures didn't exist. Now, however, the advantages of hardware-centric PACS architecture are liabilities in the context of today's and tomorrow's technology advances.

Hardware-based PACS architecture can't keep up with technology advances in computing and real-time communications for two basic reasons.

From the PACS customer perspective, it is not feasible to rip and replace installed access control hardware systems on a regular basis. Short-lived hardware-based systems can't provide a sufficient return on investment. The recurring labor effort would be cost-prohibitive, and the recurring facility disruption would be unacceptable.

From the PACS manufacturer perspective, it is not feasible to have short hardware product lifecycles. There would not be an acceptable return on the required research and development work. Short product lifecycles are workable for small consumer products like smart phones, which have no installation overhead, have quarterly sales in the 10s of millions of units[1], and whose sales revenue can pay back their R&D costs within an acceptable time frame.

Capabilities Gap

Because hardware-centric distributed-intelligence PACS can't keep up with information technology advances, an ever-widening gap exists between the capabilities, effectiveness and ease of management that a physical access control system could have, and what today's PACS products provide. Unless the concept of "putting intelligence at the door" includes all of the intelligence that should be utilized to make an access decision, such an approach actually provides less security than today's networked technologies are capable of providing.

A key issue is a system's native support for technology advances, versus requiring 3rd party devices and middleware in a piecemeal approach to system design. *Below is a partial list of current-day technologies and practices that are not natively supported by systems based upon today's PACS architecture:*

- the strongest card authentication available
- the strongest cardholder authentication available
- strong mobile device authentication and interaction
- standards-based role, attribute and policy-based privilege management[2]
- strong network security
- IT management of endpoint device security

These technologies and practices are in current use in IT security today. New devices and systems have to emulate outdated hardware in order to interoperate with current-day PACS systems.

For example, U.S. federal agencies that have traditional PACS require special additional hardware to be installed between each card reader and its access control panel. The special hardware communicates via the network to the federal systems that perform card and cardholder authentication in real-time based upon digital certificates. The special hardware decides whether or not the card number should be passed on to the access control panel. *Such additional costs and complexities relating to current PACS architecture have been a significant barrier to the widespread adoption of advanced card reader technology.*

Because traditional hardware-centric PACS architecture limits the capabilities of access control systems, advanced access control features and real-time authentication and authorization capabilities could only be achieved by implementing costly 3rd party solutions or custom-designed applications. To date, cost and reliability factors have kept such capabilities out of reach for most PACS customers—even though IT security systems have had such features for over a decade.

[1] Vendors' sales of mobile phones to end users worldwide from 2010 to 2013 (in million units), by quarter, http://www.statista.com/statistics/263355/global-mobile-device-sales-by-vendor-since-1st-quarter-2008/, retrieved on August 12th, 2014.

[2] Important access management standards and guidelines include ANSI/INCITS 359-2004 Role Based Access Control (RBAC), NIST SP 800-162 Attribute Based Access Control (ABAC), and ANSI/INCITS 494-2012 Role Based Access Control Policy Enhanced (RPE).

Although it is a significant shortcoming that current PACS architecture can't keep pace with, or cost-effectively utilize, today's important technology advances—it is even more important to realize that current PACS architecture isn't keeping pace with the security needs of today's organizations.

The Outside World

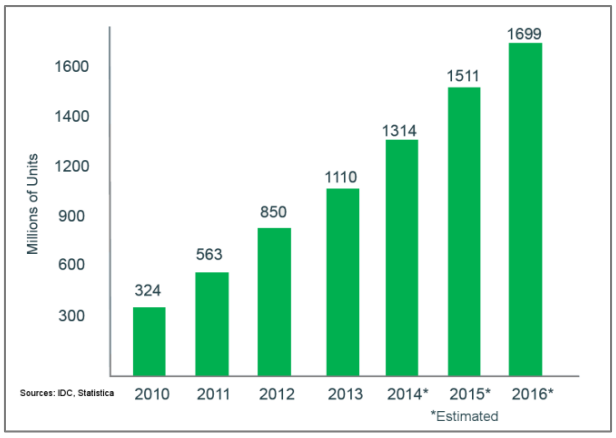
Traditional PACS architecture is based on the idea that security systems will remain closed standalone systems, interfacing only to security sensors and security devices located within one or more specific buildings, operating on a limited set of cardholder and door data entered manually or imported into the system from an external database. This was not an objective or a design choice—it was the only design option given the technology-based constraints imposed on access control system manufacturers. The world outside of a PACS system had little or nothing to offer in terms of security relevant information and communication.

Today that outside world contains an abundance of information and communication options that are highly security-relevant, and are now available through an organization's IT infrastructure and the Internet. Unfortunately today's technology trends are producing much important technology that is not available to a system based on traditional PACS architecture. Two such trends are very relevant to security: Bring Your Own Device (BYOD) and The Internet of Things.

BYOD

Personal smart devices, such as smart phones and computer tablets, allow people to communicate in a timely fashion, instantly access arriving data and look up reference data without being deskbound. Personal smart devices are productivity equipment that an organization benefits from yet does not have to buy and maintain. However, smart devices pose both physical (for example, cameras) and cyber security risks. On the other hand, they can be securely incorporated into business network infrastructure[3], and then used in ways that strengthen security, usually involving information exchange between PACS and IT systems such as a corporate directory system or identity management system.

Figure 3. Rapid Growth of Smart Mobile Devices



Given the explosive growth in the use of personal smart devices (see Figure 3) and the continuing advance of their capabilities, BYOD is a resource to consider, especially when there are no constraints on PACS real-time interactions.

For example, existing Bluetooth access reader products exist today that allow the use of smart phones as electronic access cards, After all, if airlines can use smart phones as boarding passes, and banks can use them for photographic check deposits, certainly the security industry can use them effectively for physical access control.

Consider what could be done with a next generation PACS architecture that allows reversing the roles of access card and door reader. Why not use a QR code sticker to identify the door and a smartphone's camera as the code reader? In this case the individual would carry the reader (i.e. the smartphone) to the door. Network-based real-time presence technology can verify that the phone-holder is actually at the door. Phone-based biometrics or PIN code can authenticate the individual. In this scheme the door would require only a small next generation PACS door interface board for the door control hardware, providing a reduction in access-controlled door hardware costs. While not suitable for high-traffic doors,

[3] The ability to work from anywhere at any time with any device will significantly change the way in which organizations collaborate—and that is the clear direction of this trend. For some organizations it will mean a significant change in culture, policies and procedures but the long term benefit should be increased productivity, collaboration, innovation as well as a reduction in costs. For a better understanding of these factors, see the Cisco training material on BYOD at: http://bit.ly/Bring-Your-Own-Device-BYOD-Cisco-Training

this approach makes cost-feasible to extend access control coverage to doors where the cost-benefit ratio has not been sufficient.

Figure 4. Door ID QR Code

Figure 4 shows an example QR code that contains the following hypothetical door ID data in plain text:

Door number: 0034
Site ID: HQ
Building ID: BLDG A
Door Name: DOOR 12 ENTRY

At least one secure implementation of such technology exists today that supports integration to a few existing PACS via specially developed code for each PACS. Smart devices are supported by both the door-QR-code scheme and Near Field Communication (NFC)[4] readers that communicate directly with smartphones.

However, next generation PACS architecture would enable such integrations to be done using simple standards-based configuration options, and would allow user authorization based upon real-time values of privilege attributes rather than cached values, something existing PACS architecture doesn't directly support.

The Internet of Things

The Internet of Things (IoT) refers to a world where "things" (which can be smart devices or sensors on objects, people or animals) are all potentially connected via the Internet, with the ability to collect and share data. As IoT technology continues to be developed and deployed many more sources of security-relevant real-time information will appear.

For example, where critical materials (including substances subject to regulatory control) require outdoor transit and temporary storage, policy-based asset protection rules can require that only authorized people be in proximity to the materials and that the materials are not moved outside of prescribed boundaries (virtual fencing). Violations of the policy conditions would trigger an alarm and could activate additional response measures.

Another IoT example is the use of distributed sonic sensors that are able to pinpoint the location of gunfire.

IoT technology holds the promise of closing security gaps and strengthening security response actions, but only if PACS architecture is advanced to take advantage of such technologies.

As R&D efforts become realized in the form of business and consumer technologies, PACS as well as other security systems will be required to process information in real time from an abundance of networked sources for the purpose of people and asset protection. Next generation PACS architecture must natively support such policy and rules-based real-time information assimilation and analytical evaluation.

> *"The Cloud in general terms is a proven architecture, and has experienced tremendous success in optimizing business operations. Our bedrock security applications of traditional access control and video surveillance must evolve in tandem to provide combined value across a secure and expandable IT-to-Cloud-based infrastructure.*
>
> *"There is a larger societal trend away from on-premise hardware and administration, and toward secure mobile devices utilizing the Cloud to drive new application growth and productivity. Emerging mobile*

[4] Near-field communication (NFC) is a set of standards for smartphones and other mobile devices to establish radio communication with each other by bringing them into close proximity. Two differences between the NFC and RFID technologies are (a) that NFC can utilize two-way communications, whereas RFID is limited to one-way data transmission, and (b) the range for NCF is no more than 4 inches, whereas recent RFID developments extend its read range to just over 50 feet.

technologies enable security industry expansion beyond 'siloed' applications, and toward combining core functionality to produce 'business optimization'.

"The future of PACS may indeed be as a subset of a broader architecture involving core security processes interacting across flexible IT infrastructure and secure expandable Cloud platforms. This net-centric integration of emerging technologies allows the use of value-added applications to deliver greater security capabilities through a continuous managed-services model. From a physical access perspective, the entire infrastructure involves secure, continuously evolving end points which integrate personal biometrics, behavior patterns, location and other information into a highly-effective real-time authorization and access control process."

—Dan Dunkel, security convergence thought leader and co-author of the book "Physical & Logical Security Convergence"

What Does Next Generation PACS Architecture Look Like?

At first consideration, the idea of moving to a fundamentally different PACS architecture may appear somewhat daunting to individuals who currently manage existing PACS deployments. A closer look will show that next generation PACS architecture simplifies PACS deployments, by moving them in the same technology direction that IT has been going for years—a proven direction that organizations have been investing in successfully for some time. That's the basic story that is elaborated below.

At the infrastructure level, next generation PACS architecture must be IT-centric, meaning that it takes maximum advantage of the capabilities of an organization's IT infrastructure. That includes not only computing and networking functionality, but also infrastructure management functionality, and network and computer (cyber) security. It must be deployable throughout the enterprise like any other business application that utilizes networked end point devices.

At the application level, next generation PACS architecture must be IT-aligned in support of the customer's preferred approaches to identity, credential and access management (ICAM), and must be easily integrated to relevant business systems.

Attributes of next generation PACS architecture include:

- **Software-centricity** – applications that run on virtual machines or in a cloud environment, as well as on physical servers, and whose only specialized hardware are end devices that interface to real world elements for authentication, authorization and portal control
- **Net-centricity**[5] – engineered for networking beyond internal communication among core PACS components, utilizing network sources of real-time data (including the Internet of Things) to (a) obtain situational awareness relating to asset protection, (b) apply policy-based control measures in response to threat and operations conditions, and (c) share information with subscribed stakeholders (people, systems or devices) to support planned organizational responses for maintaining personnel safety and asset security
- **Server-based real-time access decisions** – high-speed server-based decision engine incorporating sensor-driven and people/object-behavior-driven analytics, that makes access decisions on role, policy, and attribute information obtained in real-time as well as real-time status information such as threat levels, personnel presence/location data, access zone compromises, and environmental safety conditions

[5] Net-centricity (and net-centric) as used in this paper refers to participating as a part of a continuously-evolving, complex community of systems, devices, services and people with internetworked communications to optimize resource management and provide superior information on events and conditions needed to support rules-based automated actions and empower decision makers. Some consider "network-centric" to refer to activities within a particular network and "net-centric" to refer to activities that cross networks, which is the intended meaning for this paper.

- **Highly secure** – not relying solely on network security (i.e. security measures external to the system), but applying basic security principles and state-of-the-art security practices in software and system engineering, including standards-based high-level encryption of all network communications; and enabling all PACS end device connections to be monitored by IT for infrastructure management and cyber-security purposes as is commonly done with other network business devices
- **Simply scalable** – echoing the simplicity of network phone system expansion, *scalability for equipment* means adding another door by simply adding another end device to the network, without field hardware limitations to deal with, such as needing to install an additional access control panel for a 33rd reader because the installed access control panel supports only 32 readers; *scalability for application* means that the server application runs on a single server on site but also natively supports running in a virtual machine in a data center or the cloud, with high availability and high redundancy in the same way that Amazon, eBay, Facebook, Twitter and YouTube deploy their massively-scaled high-performance systems, which handle transactions many orders of magnitude beyond what a PACS system will be called on to perform[6]
- **IT-friendly** – easily conforming to an IT department's technology roadmap as well as its policies and practices, including end device PoE power, IT server redundancy policies, and end device auto-failover to alternate servers in the event of a server failure or network path outage
- **ICAM-friendly** – enabling unified physical and logical identity and access management, and common credentialing, through native support for corporate directory and identity management system integration, and for online authentication systems
- **Standards-based** – enabling user configurable integration via established standards rather than vendor-specific APIs (application programming interfaces) and SDKs (software development kits)
- **Smart-card-friendly** – providing direct support (no 3rd party devices or middleware needed) for digital certificate-based authentication, including all levels of U.S. federal PIV Card (FIPS-201) and corporate PIV-I identity authentication assurance; including support for all of the capabilities in NIST 800-116, having passed rigorous federal testing to appear on the FIPS-201 Approved Product List.
- **Mobile-device-friendly** – incorporating the attributes of presence and location and capable of performing real-time device authentication and acceptance
- **N-factor authentication capable** – supporting configurable authentication requirements, based upon a combination of any number of cross-system factors including (for example) location, biometrics, personal knowledge, physical tokens, real-time digital tokens, and behavior; allowing escalation or relaxation of the n-factor count requirement based upon threat level and other conditions
- **Broad authentication technology support** – accommodating a full spectrum of card-readers, cards and electronic credentials, and especially native support for credential technologies with high-security features like challenge/response protocols and biometrics, whose range of technologies includes:
    - legacy and current-day card readers and card formats from 26-bit Wiegand to 200-bit PIV and PIV-I cards
    - current-day IP-connected smart card readers and biometric readers, as well as multi-technology readers
    - emergent NFC technologies for mobile devices

[6] For detailed architecture information on highly scalable, high-availability high-performance systems, download the PDF version of Andrew Morgan's keynote address to Virtual Developer Day – MySQL at: http://www.mysql.com/news-and-events/events/VDD-MySQL-July13/MySQLKeynote.pdf

- now-emerging extensions to PIV and PIV-I cards such as *derived credentials*, which are digital certificate credentials issued to PIV or PIV-I cardholders[7] (derived from existing certificates on the card). They can be utilized for access control purposes in lieu of the card itself, for example in mobile devices. The above attributes make next generation PACS fully capable of enabling an organization to place physical access privileges under the same role-and-policy-based management scheme that is used by HR and IT, eliminating the risks that result from split physical/logical identity and access management, while also providing operational cost-savings by eliminating the duplicated access management functions.

According to studies performed by the National Institute of Standards and Technology (NIST), most organizations should now experience both cost-benefits and security benefits from bringing their physical access privileges under the same standards-based management approach used for their logical access privileges. Research performed by NIST in 2010 indicates that adoption of standards-based role based access control for information systems has grown from 2.5% in 1995 to just over 50% in 2010 for firms with more than 500 employees.[8]

Next Generation PACS Requirements Have Already Started Appearing

In the U.S. federal space, *Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors* (HSPD-12) was issued in order to mandate improvements in personal identity verification and credentials authentication to strengthen both physical and logical access control. In response to HSPD-12, the Computer Security Division of the National Institute of Standards and Technology (NIST) developed a new standard—FIPS 201—for improving the identification and authentication of Federal employees and contractors for access to Federal facilities and information systems.

Many next generation PACS architecture attributes have already become requirements that must be provably met for products to be accepted onto the U.S. General Services Administration's *FIPS-201 Approved Products List*.

> "The implementation of HSPD-12 will be facilitated via the Physical Access Control System. This subjects PACS systems to two important requirements. First, the PACS system must meet the same cyber security requirements that are applied to all federal information systems. Second, physical and logical access management will be tightly coupled. The PACS must have the capability to operate in harmony with centralized physical and security information management systems."
>
> --Ron Martin, former *Physical Security Specialist & Co-Program Manager for Identity and Access Manage* at the U.S. Department of Health and Human Services, and former *Physical Security and Program Lead for HSPD-12* at U.S. Department of Commerce.

As improved PACS technologies continue to appear for use in federal programs, they will be available as well for adoption in the private sector.

Migration to Next Generation Architecture

Next generation PACS architecture utilizes existing IT infrastructure and supports the full spectrum of legacy and current-day reader technologies. This means that a migration to next generation PACS architecture will be significantly simpler to plan, execute and maintain than previous PACS migration and integration efforts.

[7] Derived credentials are defined in NIST SP 800-63-2 – Electronic Authentication Guideline, and in Draft NIST 800-157 – Guidelines for Derived Personal Identity Verification (PIV) Credentials, which also apply to PIV-I credentials

[8] Alan C. O'Connor and Ross J. Loomis, "2010 Economic Analysis of Role-Based Access Control", National Institute of Standards and Technology, December 2010, p. 6-1.

Some of the specific reasons for this improved migration picture are as follows:

- Next generation PACS architecture has high alignment with the organization's IT skills, knowledge and deployment resources.
- Server redundancy and fault-tolerance can be easily established by IT in accordance with IT policies for the critical business systems.
- The new PACS deployment can be put in place in parallel with the existing PACS system, which can be left in place (powered down) to provide a complete and fairly instant fallback position.
- There is no technical requirement to change out access cards at any facility, and card migration to an enterprise-wide standard—if required—can be staged on a facility-specific or region-specific basis, with the retiring readers left in place for a short time to maintain a fallback position.
- Because next generation PACS architecture eliminates the now-needless distributed-decision-processing hardware, migration schedules are significantly shorter than previous such efforts.
- Going forward, the adoption of new technologies can be accomplished by IT or with IT oversight, with a much higher degree of understanding than has been possible in the past.
- The incorporation of new technologies, as well as integrations with current and future IT and business systems, can be targeted to address security improvements on a risk-prioritized basis, without feasibility or affordability constraints due to former hardware-centric system limitations.

Superior Total Cost of Ownership

Next generation PACS architecture can achieve a much lower Total Cost of Ownership both now and in the future than hardware-centric PAC architecture can provide, based upon:

- eliminating unnecessary physical access control hardware and vastly simplifying system deployment
- eliminating the typically hidden costs of firmware and hardware upgrades, version compatibility issues, etc.
- maximizing the utilization of existing IT infrastructure, conforming to IT policies for system security and resilience, and being deployable in the same manner that IT deploys other business systems
- providing high interoperability through native support of standards such as those relating to PIV and PIV-I
- enabling unified logical/physical identity, credentialing and access management through software components that are easily integrated with other business systems
- being a platform architecturally ready to incorporate emerging identity, credential and access control technologies

PACS Architecture Comparison

A comparison of the diagrams in Figures 5 and 6 on the following page will reveal significant differences between current-day PACS architecture and next generation PACS architecture.

Figure 5 shows the hardware-constrained architecture that is limited in its interface capabilities and in the scope of its real-time operations. There is little to no native support for integration with Identity Management Systems, cloud-based authentication systems, and the emerging access technologies that will continue to arrive.

Figure 6 illustrates a software-based and net-centric approach that uses simple interface boards to support legacy devices, and also supports networked current and emerging device technologies. Additionally, it provides a high level of native support for Identity Management Systems integration as well as cloud-based security services. A next generation

PACS product would fully support the strongest authentication and authorization processes currently established under the U.S. federal FIPS-201 standard for combined highly-secure physical and logical access control, including Federal Bridge services, without requiring 3rd-party interface products.

Figure 5. Traditional PACS Architecture

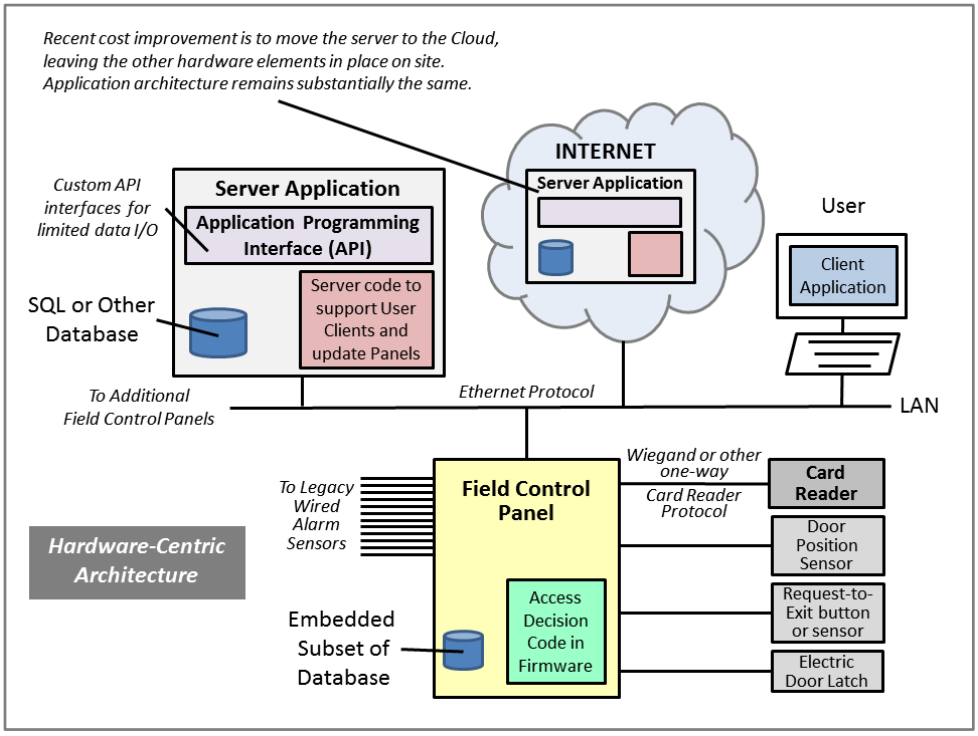
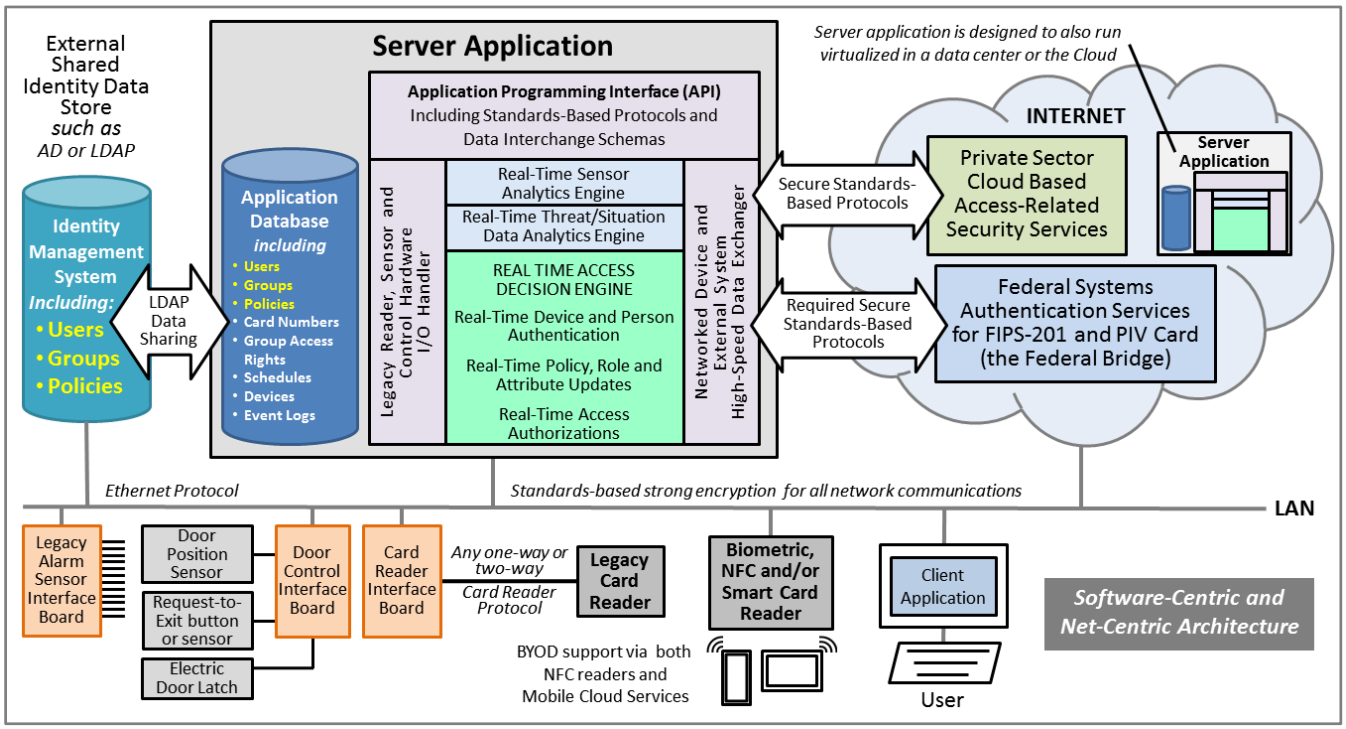


Figure 6. Next Generation PACS Architecture



Conclusion

Today's PACS architecture only leverages existing network hardware technology—it doesn't utilize the organization's full IT infrastructure, which includes systems providing advanced security services and sources of security-relevant real-time information. A close look at most organization's IT roadmaps will show that traditional-architecture access control systems are off on a side road.

There are two questions to consider about making the transition to next generation PACS architecture.

- *Will your organization's currently deployed PACS be a satisfactory technology five to ten years from now, given the pace of technology advancements relating to enterprise access management?*
- *From the security-effectiveness and cost-effectiveness perspectives, is continued investment in legacy PACS technology the smartest approach to addressing your organization's critical asset protection and incident response needs?*

The addition of one or more of the attributes of next generation PACS architecture to traditional PACS deployments may provide some desirable incremental benefits. However, until a full transition is made to next generation architecture, existing PACS deployments will continue to fall further and further behind technology advances, and thus will continue to have shortcomings and weaknesses—as well as needless costs—that constitute a liability to an organization's asset protection program.

For most organizations, transitioning to next generation PACS architecture is not a far-off future option, but a very real and almost immediate requirement.

Viscount Systems Inc.
4585 Tillicum Street
Burnaby, BC V5J 5K9
Email: info@viscount.com
Web: viscount.com