

Policy-Based Physical Security Management

A Quantum Secure White Paper



Quantum Secure, Inc.

100 Century Center Court, Suite 501

San Jose, CA 95112, USA

Tel: + 1-408-4543-1008

Fax: + 1-408-453-1009

EMail: info@quantumsecure.com

Table of Contents

1.	Executive Summary	4
2.	Introduction	5
	2.1. SAFE Application Suite	7
3.	What Is SAFE Policy Manager?	10
	3.1. Policy-based physical security management	11
	3.2. Auditing And Reporting	15
4.	SAFE Enables Cardholder Identity And Role Management	17
	4.1. USE CASE: Multi National Pharmaceutical Company	18
	4.2. Value Proposition	20
5.	Introducing SAFE Integration Platform	21
	5.1. Out-of-box support for major physical security technology vendors	22
	5.2. True open interoperability between security systems	23
	5.3. System Orchestration & Messaging Engine	24
6.	Summary	27

Contacting Quantum Secure	Telephone: 1-408-687-4587 Email: info@quantumsecure.com World Wide Web: www.quantumsecure.com Postal Address: 100 Century Center Court, Suite 501 San Jose, CA 95112, USA
Copyright Notice	Copyright © 2004-08 Quantum Secure, Inc. All rights reserved. Printed in USA. Reproduction in whole or in part is expressly prohibited without the prior written consent of Quantum Secure. Quantum Secure reserves the right to modify the specifications mentioned in this document at any time and without prior notice.
Trademark Notices	The Quantum Secure logo and SAFE are trademarks of Quantum Secure, Inc. Microsoft, Windows, ActiveX, and Visual Basic are registered trademarks, and Windows NT; Windows 2000, Windows XP, Microsoft Access, Microsoft SQL Server are trademarks of the Microsoft Corporation. Actuate iServer, Actuate Active Portal, Actuate eQuery, Actuate ERDPro are registered trademarks of the Actuate Corporation. All other trademarks and registered trademarks are the property of their respective holders and are hereby acknowledged.

1. Executive Summary

Recent world events and heightened security consciousness within corporate and government organizations have made enterprise-wide security one of the highest priorities on executive's agenda. Despite all growing awareness as well as amplified investments, the number of security breaches continues to soar. Quantum Secure believes one of the weakest links in the enterprises is physical security.

Practically all facility-based physical security systems, devices and services operate in silos, very loosely connected with each other. Obtaining a comprehensive view of physical security operations for all corporate locations worldwide is very challenging. The problem further gets exasperated with localized security processes, ad-hoc event handling, countless alarms and a lack of holistic reporting from multi-vendor proprietary systems.

Quantum Secure is the exclusive provider of enterprise software to manage and streamline security identities, compliance, events and operations across disparate physical security systems. Quantum Secure's SAFE suite of enterprise applications enables corporate security managers to implement best practices globally & reduce operational cost by providing end-to-end management of complex disjointed physical security infrastructures.

Our SAFE suite provides a real-time dashboard view of your corporate risk profile and vital security metrics, such as operational performance, costs, policy compliance, etc. Through a unique policy-based and vendor-neutral approach, SAFE Policy Manager enables enterprises to proactively manage their security policies, while leveraging their existing security investments.

This white paper explores the business and technical issues underpinning the operations of an enterprise-wide security infrastructure, and how Quantum Secure's feature-rich solutions and sound security principles offer the means to effectively and durably resolve them.

2. *Introduction*

The demand for increased workplace security and employee safety is at an all-time high. Corporations and governments today are facing a new generation of security risks, such as employee pilferage, fraudulent lawsuits and theft of intellectual property. When combined with activities such as terrorism, identity theft, counterfeits, burglary, robbery and shoplifting, these risks create far greater dangers.

With this demand, corporations and governments alike continue to reassess current policies and procedures and adopt technologies that can make the workplace a safer environment, safeguarding from dangers such as natural disasters, employee accidents, incidents of workplace violence, and even privacy issues.

At the same time, regulations governing the design, operation, testing and auditing of commercial security systems have become more stringent. In most jurisdictions, compliance with these regulations is mandatory at the same time security regulations could vary between locations.

Consequently, the physical security industry is characterized by an annual spending of over \$120B worldwide in various kinds of hardware, devices, systems such as access control, video surveillance, fire and intrusion detection, and services such as guards, risks and threat assessment, cardholder identity management and monitoring control room centers. Not only the systems are disparate but also the data sets originating from these locations are flat and also disjointed. For example, alarm IDs, door names, access levels, card formats, spatial hierarchy or surveillance camera configurations are represented differently in each facility. These industry dynamics make it practically impossible to obtain a comprehensive view of physical security operations for all corporate locations.

To answer these challenges, Quantum Secure provides enterprise class software applications to centrally manage & orchestrate corporate security. Quantum Secure's unique policy-based approach allows security managers to deploy proven best practices and business rules across all domains of physical security resulting in dramatically lower cost of operations, reduced risk, and increase in efficiency & security.

Quantum Secure's SAFE Suite is the only product in the physical security industry that unifies incident management, cardholder identity management and corporate risk assessment in one seamlessly integrated Web-based console. SAFE allows corporate security departments to centrally deploy business rules using graphical whiteboards such that diverse physical security systems worldwide conform to consistent corporate policies. This approach results in unified security operations with minimal human intervention to resolve common security anomalies. Additionally, our software provides global reporting of trends, operational data and security metrics enables auditable corporate and regulatory compliance.

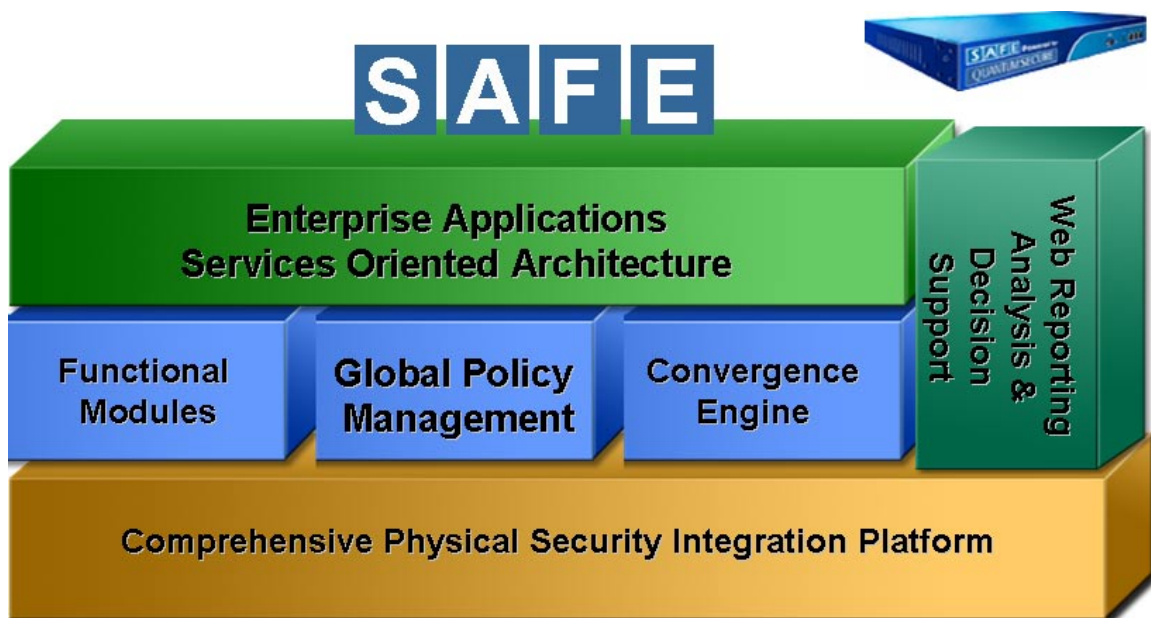
SAFE provides a comprehensive integration and application platform that works with your existing IT and physical security infrastructure to enable and manage change. With SAFE, you can flexibly and rapidly design, build, implement, and execute business strategies and security

processes. The platform enables you to drive innovation throughout your organization by recomposing existing systems while maintaining a sustainable cost structure. You can also add innovative, industry-specific business processes with reduced risk to existing systems and a strong return on investment.

SAFE unifies integration technologies into a single platform and is pre-integrated with leading physical security, human resource and identity management applications, reducing the need for custom integration. The platform is based on industry standards and can be extended with commonly used development tools such as Java 2 Platform, Enterprise Edition (J2EE); Microsoft .NET. SAFE also enables enterprise service-oriented architecture, a blueprint for service-oriented business solutions.

Quantum Secure is driving an innovative change in managing physical security by embracing things that have brought success to the IT world: industry standards, open protocols, interoperability among manufacturers, short product cycles, commoditization of hardware, and license/service based products. Based on these proven security principles, Quantum Secure's SAFE Suite is designed to reduce the time required to deploy security policies and update them after deployment, make corporate security more reliable, and lower the total cost required to manage multi-vendor physical security.

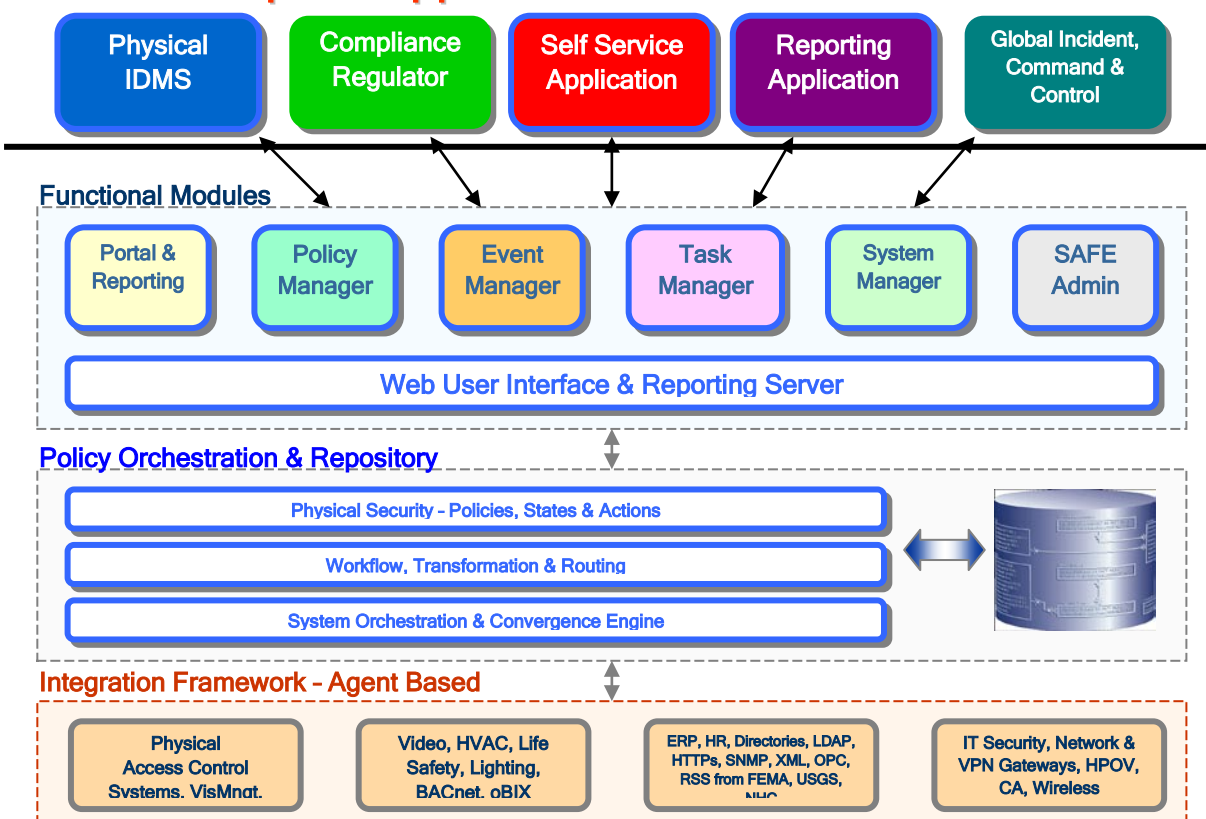
Using policy-based management, SAFE enables a collaborative approach between business entities and the security organization. Built with interoperability in mind, the SAFE Suite can be operational in a matter of weeks and can be deployed within a production environment – thanks to powerful SAFE Integration platform.



2.1. The SAFE Application Suite

The SAFE Suite offers a breakthrough approach to enterprise-wide physical security. SAFE Application Suite is a Web-based enterprise security solution for organizations that require security policy enforcement and protection across multiple sites. SAFE's three-tiered architecture, rapid integration with existing physical and IT security infrastructure, and XML-Web Services based reporting and analysis ensures quick deployment and unlimited scalability for regional and corporate security administrators.

SAFE Enterprise Applications



High-level Logical Architecture of SAFE suite is illustrated above, and key components are described herein:

- SAFE Enterprise Applications
 - SAFE Cardholder ID and Role Manager application is the central point to manage identities, roles, credentials and processes such as new card issue, background checks, role automation, change in employment, and termination across all physical security systems, such as access control, smart card, guard

stations, etc.

- SAFE Global Incident Manager is a tactical and strategic application to manage incidents resulting from access control breaches, video surveillance suspicions, power interruptions, fire alarms or hazmat spills to employee self service requests such as changes in access card privileges. It provides comprehensive centralized view of all physical security incidents with flexible user definable business rules, enabling security departments to respond expeditiously to security breaches and determine the business impact and risk.
- SAFE Risk Manager provides a framework to define essential components, common language, and clear direction and guidance for enterprise risk management. SAFE enables security organizations to measure *operational* risk, *strategic* risk and *corporate asset* risk. Operational risk is defined as day-to-day risk related to the security and safety of corporate employees, and visitor or risk due to performance gaps in security equipment, security personnel (especially outsourced security) and policies. Strategic risk is measured based on organization's business objectives and goals, potential impacts to organization's reputation as a result of fraud, natural/manufactured disasters, and potential impact of specific legislation or compliance requirements. Lastly, corporate asset risks are measured with regards to the asset itself such using Annualized Loss Expectancy ("ALE") method, fault trees, or risks from operational environment in which the asset exists and those based on "what-if" threat scenarios.
- **SAFE Functional Modules**

SAFE provides unique set of functional modules for each application mentioned above to provide simple and easy-to-use web based graphical interface designed specifically for physical security departments. These modules enhance the user experience, automate most of the manual tasks and provide rich functionality targeted specifically for physical security departments. These functional modules are:

 - **mySAFE Dashboard** provides personalized view of physical security. It allows users to customize graphical views of global security operations, policies, incident reporting, tasks, calendars, deviation & metrics reports, ad-hoc queries and analytics for security administrators and executive management.
 - **SAFE Event Manager** provides physical security operational activity monitoring functionality. The Event Manager captures all events and alarms across various access control, vis-à-vis policy violation, policy rules and view details such as source (system and sub-system), severity level, status, time and number of occurrences, contact details, related alarms, etc. in real time.

- **SAFE Task Manager** tracks auto-generated tasks (thru alarm and policy modules) as well as manual tasks for each individual within physical security department. Security personnel can view details such as priority, requestor, assigned to, status, task type, date and time of generation, summary, alarm details if generated thru alarms, task history, etc.
- **SAFE Admin** is accessible only to SAFE system administrator. It provides role-based access control to the SAFE system and define linkage to external authentication provider such as LDAP, etc. It allows SAFE global or regional administrators to define portal customization and personalization settings, modify graphical look and feel, modify report layouts. It also provides global system defaults (e.g. SNMP manager, Polling intervals etc.).
- **SAFE Policy Engine** (including workflow, transformation, message routing) – a patent-pending module – is the heart of the application suite. SAFE Policy Manager simplifies the creation and enforcement of policies on physical security infrastructure, enabling security, human resource, and business line managers to work together and create unified security polices for the entire organization. These physical security polices can then be managed at globally and locally based on specific role/clearances within an organization. SAFE Policy Manager examines all real-time event data collected from the physical security access control system, cameras, and sensors for fire, motion, intrusion, chemical as well other inputs from HR/director and IT security systems. It then listens for any data changes in real-time across various systems/devices connected via the SAFE Integration Platform. Depending on the policies deployed the incoming dataset may be accepted/rejected, replicated to another system, modified/assigned special attributes, notify other security systems (e.g. alarms, ID provisioning systems, RSS, incident mgmt, risk mgmt applications, etc).
- **SAFE Integration Platform** captures all security data and events using vendor specific SAFE Agents developed by Quantum Secure or using Microsoft BizTalk's standard adapters. SAFE Integration transforms the data into industry-standard XML formats (such as SPML, IncidentXML, SAML, etc) ensuring unlimited interoperability. Thus it provides out-of-the box integration with major access control systems, video surveillance, and sensors for fire, motion, intrusion, as well other inputs from HR/Directory/LDAP and IT Security systems such as VPNs and wireless gateways.

3. *What Is SAFE Policy Manager?*

The demand for better security policy compliance and enforcement increases each day. Physical security administrators know that just managing access control systems, video surveillance and fire alarms isn't enough to ensure security. If improperly configured, they can leave an enterprise unknowingly vulnerable. Similarly, if guard patrols are not properly measured and adjusted for appropriate incident responses, risks can quickly increase.

New privacy considerations and government regulations in critical infrastructure, health care, financial services, travel and many other specialized organizations are also of current concern. Security departments wanting to stay ahead of newly-introduced initiatives are faced with implementing new security procedures on a regular basis. It is no wonder that more than half of 5,000 respondents to a recent survey did not feel their security policies were in line with business goals. Two-thirds indicated that they do not keep their policies up to date on a regular basis. Most respondents also indicated that while they have the responsibility for security policies and procedures - they do not have the necessary tools to properly create and implement physical security policies.

SAFE Policy Manager Suite provides the only cost effective way for Security Departments to enforce policy compliance, administer cardholders, minimize vulnerabilities, and prevent alarms to optimize and protect assets throughout the enterprise.

SAFE Policy Manager is industry's first and patent-pending module, designed for Security Managers to visually create and implement physical security policies via easy-to-use graphical whiteboard. It provides the most complete solution for developing, deploying, tracking, training, and reporting on physical security policies. All types of policies can be managed through this system, including physical access card issuance, changes, and termination; alarm handling and notification; false alarm rerouting; employee travel warning and alerts; environment, health and safety procedures, etc. SAFE Policy Manager create accurate policies, verifies that the policies have been reviewed & approved, deploys policies such that policy rules will automatically convert into relevant configurations of underlying PACS systems, continue to monitor the compliance in real time, as well as ensure all policies are read and understood by employees, vendors, contractors, etc.

3.1. *Policy-Based Physical Security Management*

Unlike point-to-point management where physical security devices are configured one by one across the enterprises to attain the right security level, policy-based management closely follows business practices and requirements by establishing rules and relations between physical security entities such as employees, roles, doors, alarm sensors, etc. SAFE policies become global rules and are propagated across systems independently of brand or function. The global security manager does not need to know the specific language of each particular brand of equipment in order to set security rules according to business practices. A very small subset of SAFE policies is listed herein:

- The global security manager of a large corporation can define a policy to enable only certain employees to travel to multiple locations – with single card (even when each location has a different access control system). At the same time, employee access privileges should be limited to duration of visit (as approved by a manager or host). While traveling to off-site locations, employees card cannot be used at home location.
- The global security manager working at corporate headquarters can define a policy to raise an alarm when an employee repeatedly comes into the office during non-primetime hours (e.g. between 11pm-5am) – especially during quarter end financial books closing time. The policy will triggered on certain threshold and include actions such as send an alert email, direct the CCTV towards some vulnerable spots of that location, etc.
- The local security manager of a bank can define a policy to raise an alarm when a recently laid-off employee comes into the office. The policy will trigger to direct the CCTV towards some vulnerable spots of that location, as well as auto-page security.
- The security manager working at regional head office can define a policy to raise a soft alarm when any employee – regardless of the location – enters into the office without badging-in and logs into corporate (SAP, Oracle, etc.) financials application.
- The security manager of a hospital can define a policy to automatically log-out a nurse from Patient Information System as soon as she badges out of hospital building/nurse station area.
- The global security manager working at corporate headquarters can conduct a centralized audit of all access control systems (even when there are multi-vendor systems running in various locations) to report on specific employee or group of employees suspected to have committed fraud within the company.
- The global security manager can define a global policy and generate audit reports to define who has access to what information, under what conditions, what are the alerts/alarms in place, how often they generate and how to control them, and who is

managing them.

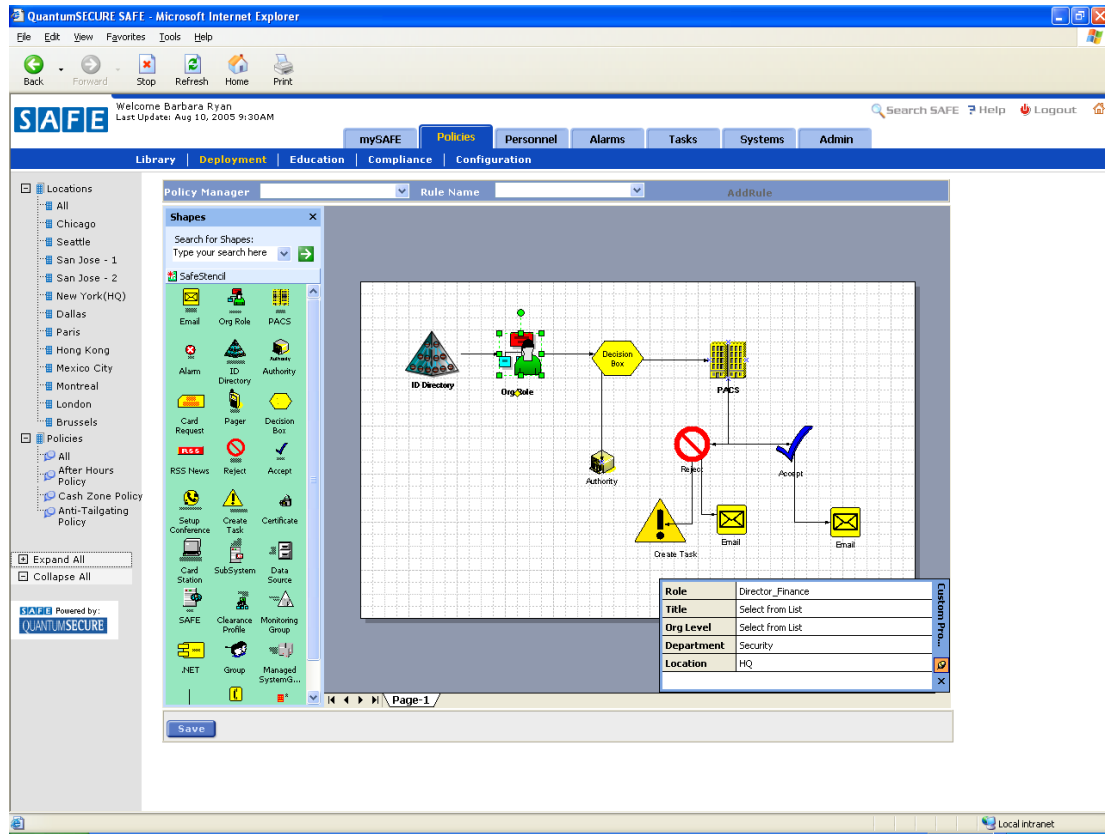
- The global security manager can define a global policy to always correlate physical access control events (badge-ins, etc.) with corporate IT and network management systems like HP OpenView or CA Unicenter to eliminate any identity theft, compliance violations, and implement tailgating policies etc.

The SAFE Policy Manager ensures that the policies are kept up-to date, and are easily changeable via a Web browser. The Policy Manager provides the tools necessary to track and measure user/system compliance. SAFE's Web-based policy manager contains wizards and visual editor where one can drag & drop design and definition of various access control systems/locations to be interconnected and networked. This user-friendly wizard guides security administrators of connecting all physical security systems in a network using a simple point-and-click methodology.

The SAFE Policy Manager also provides easy administration for custom built security policies designed by security administrators at global, regional and/or local levels. From thresholds and exception-reporting to service-level agreements and policy monitoring, SAFE Policy Manager provides automated data analysis, monitoring and real-time notification to ensure total compliance with security policies.

SAFE also enables several procedural and physical access privileges/clearances definitions and resolution (e.g. location A calls front door, and B calls perimeter door, C calls main door) as well as corporate-wide physical access provisioning management functions. This will enable the business changes (e.g. employee hiring/firing, changes in jobs/clearances, movement of employees from one location to another, temporary visitation of an employee to a different location, etc) to be transformed into specific automated activities within the SAFE system, which in turn will generate automated instruction set in various access control systems (and other systems such as biometric systems/databases) without manual intervention thereby increasing responsiveness and enforcing security policies more effectively.

The SAFE Policy Manager illustration below provides a sample of physical security policies:



SAFE Policy Manager employs a Visio-driven interface to write security policies and establish the logic and rules for the management of security incidents. This Visio interface comes with a broad set of security functions and systems that conform to standard protocols (e.g. Open Security Exchange, Service Provisioning Markup Language, oBIX, BACnet, WMI, RSS, SNMP, PKI) and also supports the creation of custom icons and rule sets. Executives and managers get a rich whiteboard interface to directly manage the operating code of the underlying security system.

In the illustration above, in the extreme left panel, you can see all the locations/facilities of the government organization that has deployed this application. The locations, represented in the panel, are live connected to the local PACS via Quantum Secure’s extensive integration server and systems orchestration layer.

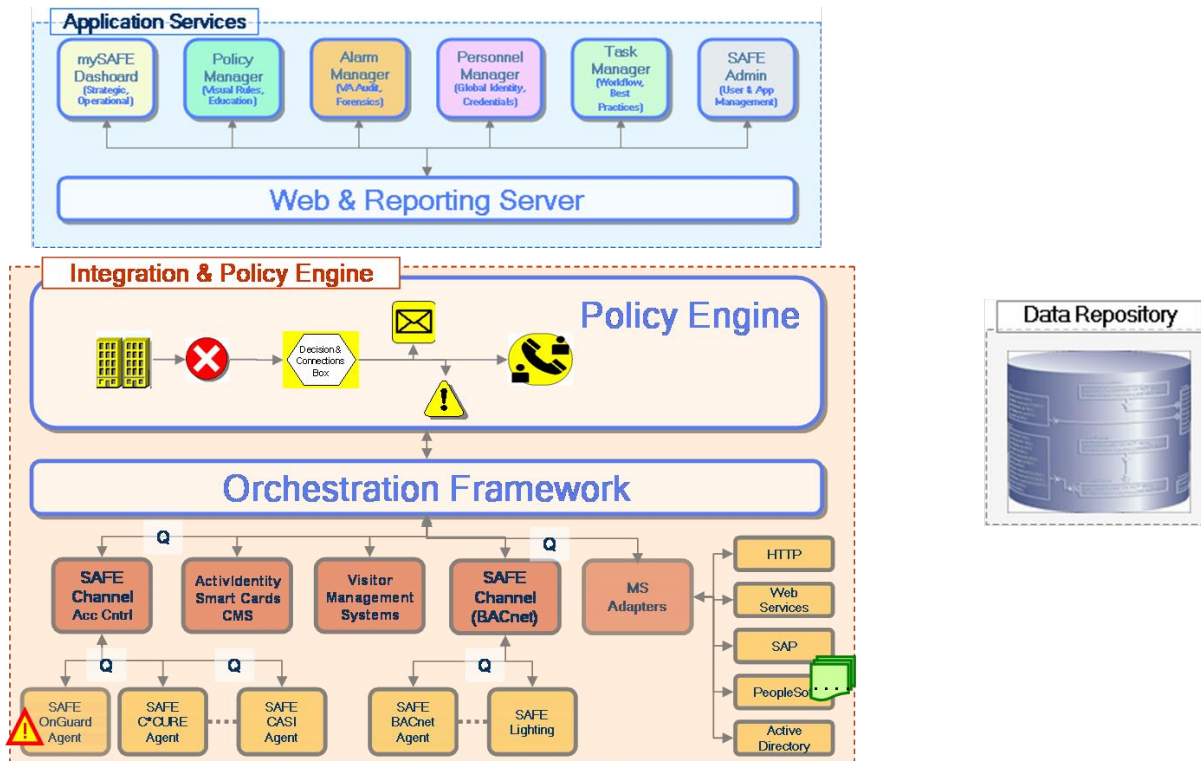
Regardless of the brand, Quantum Secure connects with most PACS and normalizes data and configurations centrally within the Policy engine. This allows security departments and PIV implementers to write graphical rules/policies using a Visio-based whiteboard and – with a click of a button – deploy that policy across all PAC systems or a location or a zone consisting of several locations. Quantum Secure’s technology ensures that no programming or technical

knowledge of any PACS is needed to draft and deploy business rules and policies. If one can whiteboard the logic, then one can deploy it seamlessly across all facilities.

In the panel that reads “SafeStencil”, Quantum Secure provides extensive live objects representing various physical security systems, devices and programming methods which can be clubbed together to form a policy/rule. For example, the *Directory* icon can represent an organization’s central directory server, which now gets connected in real-time with Quantum Secure so that one can use any of the attributes of the directory server to create business policies. Similarly, PACS icons represent physical access control systems, and you can define an attribute of this for a location or a zone (consisting of many locations) or for all locations. SAFESTencil maintains set of attributes and properties of each stencil. One can right click on it and configure the attribute while creating a business policy.

You can drag and drop any of the shapes from the stencil onto your drawing. You can also re-size shapes to make them fit nicely into your drawing. Using these stencils and connectors, one can create a seamless logical business process. Once a process is deployed, Quantum Secure will take the process and automatically translate it into local system’s configurations, rules and policies such that a business process can flow end-to-end.

The illustration below shows the integration layer, orchestration framework along with application services used to manage the creation and deployment of policies across the entire physical security infrastructure.



3.2. *Auditing And Reporting*

As long as corporate operations are running smoothly, and no security breach is found, one might wonder why corporation need security auditing. Unless there is a specific reporting tool, putting together a security policy audit is a lengthy and difficult process. It requires time from security managers and consultants going through pages of complex vulnerability assessments.

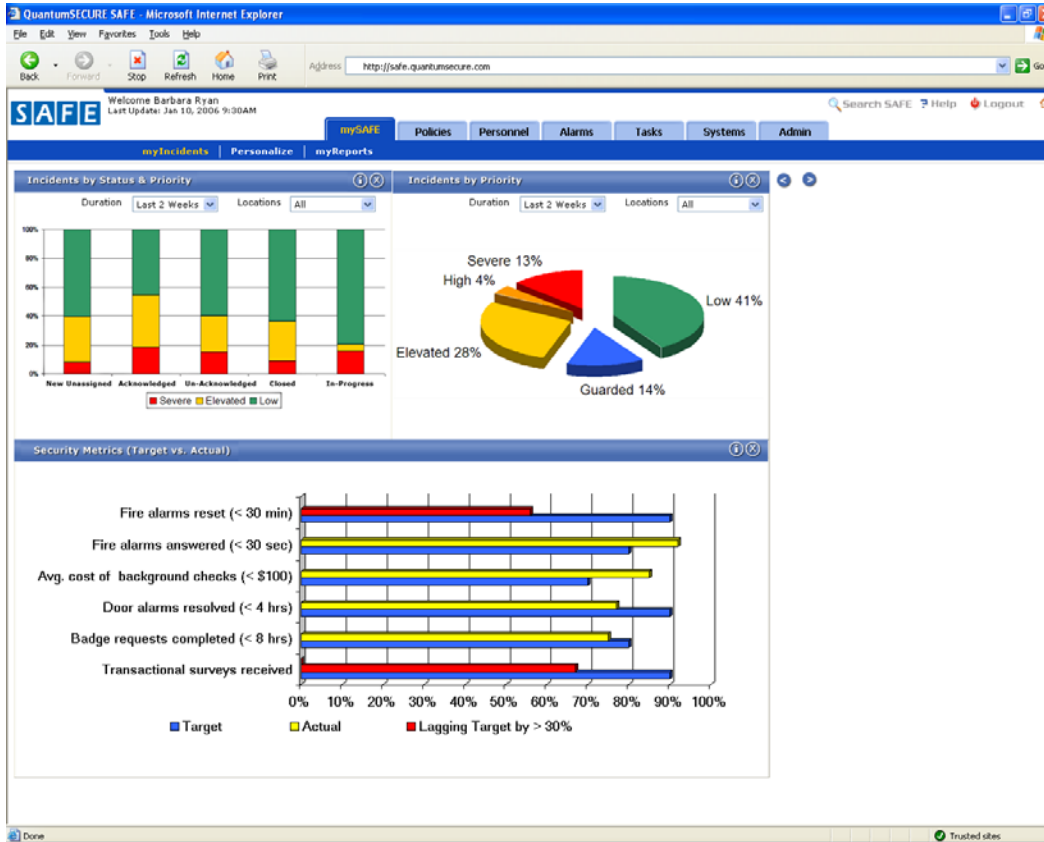
Using SAFE Policy Server, security administrators have total control, as all security rules are enforced from the same server, whose repository contains all the information needed to get fast answers. The SAFE Web Reporting server can instantaneously generate comprehensive policy audit reports on any given security infrastructure (be it an access control system or a door, a specific person, a group of IP cameras or an incident or specific SAFE policy). Reports can be established for any version of a SAFE policy, past, current, or under deployment.

SAFE audit consists of a comprehensive gathering of all the policies described for the particular security incident. Local constraints, such as contractor hours or access panel's firmware restrictions are automatically taken into account. The security manager receives a detailed report and knows exactly what happened when a particular incident was created and all the follow-ups done to close/resolve the incident. This feature also gives immediate troubleshooting hints when something goes wrong, and helps verify and discover potential vulnerabilities.

Security managers can find out in minutes whether fast action is needed, and instantly correct and update their corporate business line managers; thus, no one is taken by surprise and forced – under fire – to make large impact decisions that may have disruptive consequences (such as evacuation, plant shut down, supply chain delayed, etc.). Corporate policies from SAFE will allow organization to create an oversight and alerting system such that violations and deviant behavior is tracked and reported before major damage occurs. SAFE is also useful in understanding behavioral patterns of a large, geographically distributed enterprise that can be used to program the patterns in our policy manager such that significant deviations can generate alerts.

This wide range of reporting capabilities enables organizations to orchestrate their worldwide physical security from a single Web-based console, providing a risk-management view of operational vulnerabilities. For example, the visual dashboard combines diverse systems into a holistic, scalable view of the security landscape in real time. The ability to move across horizontally across locations and systems and drill vertically through layers of information offers security managers and executives immediate access to the entire scope of security information as it occurs.

The illustration below provides a sample of SAFE Dashboard reports:



4. SAFE Enables Cardholder Identity And Role Management

End-to-end Identity Management Lifecycle – also called User Credentials & Entitlement Management Lifecycle – now extends to all aspects and facets of an enterprise. Employees, contractors, consultants, vendors and customers are now given access to a wide range of corporate assets, from office buildings, secured computer centers and test labs to IT applications, systems and databases. All these assets must be protected from identity theft by seamlessly integrating security and access control systems with each other re-enforcing authentication rules at all times.

SAFE Host server acts as a single source of verification system which enforces chain of trust, responds to the relying party with information, manages cardholder's identity in all remote local PACS, maintains complete audit trails of all activities and conducts inter-company credential validations based upon defined policies and rules in real-time. The inter-company connection can be made using secure web services, native APIs or custom-developed APIs.

SAFE Agents are deployed in the remote offices which are connected to the master SAFE host server interpreting policy decisions and taking actions in the remote PACS and visitor management systems. SAFE Agents also gathers all real time data, manages policy conflicts and resolution and serves information to the master host server in real-time.

SAFE Host server connects with the master HR directory server and inherits employee and contractor roles, identities, and other information (such as location, department, title, etc.) based upon unique policies deployed and logic engine. These roles are mapped to groups of physical clearances (or physical access privileges) such that a new hire is automatically provisioned in the appropriate PACS without individual local security administrator going into the local PACS and provisioning the new hire. As a result, dramatic cost savings, error free and streamlined operations can be achieved.

Similarly, a termination of an employee or a revocation of an employee's certificate or changes in role of an employee will lead to appropriate de-provisioning of the employee's credentials in all local PACS, orchestrated by master host SAFE server.

A visitor, holding a valid PACS card but not provisioned in the local PAC system, will be automatically provisioned after thorough authentication, verification and HR-check process based upon deployed policies. These policies also determine when to revoke that visitor's access from the local PACS due to end of the term or contract or visitation.

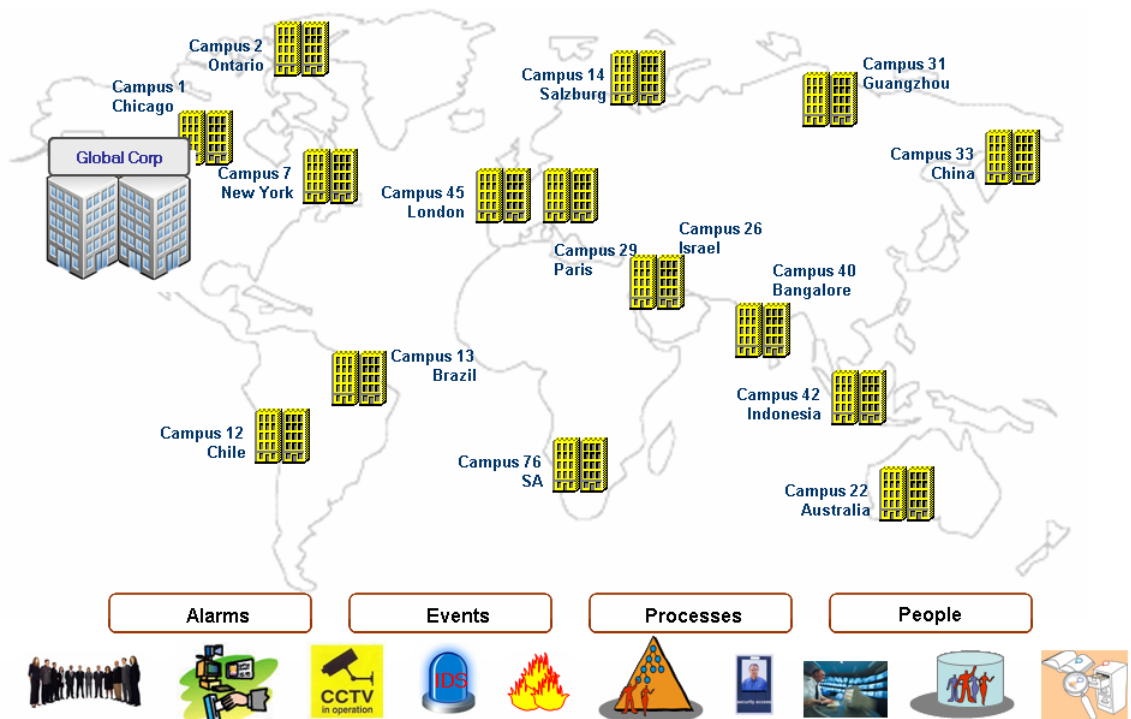
An intelligent policy-based workflow keeps all parties in loop, and before actually revoking the privileges, the workflow manager seeks appropriate permissions for extension – again, based upon policy rules. If extension is received by SAFE through an email process, then the visitor will continue to enjoy the access privileges in the local PACS; otherwise, his access rights will be terminated.

4.1. USE CASE: Multi-National Pharmaceutical Company

Noname Pharma is a publicly traded company having offices in over 50 national and international locations. Every location is protected by access control system (from multiple vendors) and many locations have classified area (test labs) where only few people are allowed. It is further controlled by either badge access control system or by Fingerprint access control system. The company employs over 5000 employees and 30% of the workforce is mobile.

Noname Pharma spends an average of 40 hours per month per location to manage (granting and modifying) access privileges for its dynamic and mobile workforce. All personnel credential management is done manually, making the environment difficult, time consuming and unsecured. All access control systems have active access rights to many people who have been terminated some time ago but their accounts have not yet been terminated in the system.

Lastly, each time employees go from one location to the other, they are issued a temporary badge because their own badge does not work, leading to an immense problem of many badges per employee. This not only affects company's productivity but also leaves the door wide open for non-compliance with strict legal requirements related to Sarbanes Oxley (SOX) and HIPAA.



With implementation of Quantum Secure's flagship product – SAFE Policy Manager – Noname Pharma streamlined all tasks globally related to employees physical access control provisioning,

authentication and management through structuring sets of corporate policies which governs all systems in real time in background.

SAFE seamlessly integrated company's HR system provided by PeopleSoft and also with company's LDAP directory server. Additionally, SAFE integrated to all 50 access control systems (provided by at least 10 different vendors) the company have in all locations, including two fingerprint scanning biometric system. The results were as follows:

- One workflow based, centralized physical access control and user credential management system – managing (granting, revoking, modifying) access rights worldwide, based upon policy rules set forth at the corporate office for all locations.
- Request for changes in access control can be initiated from the corporate office or from the individual location using Web-based tool.
- Allowed for “global roaming” with one's own badge identity card to access all facilities worldwide based upon authorization rules. Elimination of all temporary badge solution. This was a welcome relief from earlier disjointed and time-consuming user experience whereby provisioning was a manual process.
- Central card management and replication of a cardholder's records, including images, user defined fields, biometric templates. This goal was achieved by structuring three corporate policies which took less than one hour to define and structure.
- Centralized global reporting (such as, transaction, local configuration, full audit trail, capacity report, exceptions report, etc.) with an executive dashboard. Centralized partitioning of card records
- Completely eliminated “ghost/orphan account” issues – for example, all the people in the access control systems in all 50 locations matched to all the current and active employees (and contractors/consultants) in the PeopleSoft system. SAFE, based upon the policy rules set in the system, cleaned up all the access control systems worldwide eliminating huge intrusion risk.
- Eliminated over 1500 hours per month of the manual process of managing user access grants and credentials worldwide in all locations directly saving the company over \$60,000 per month in cost reductions.
- Allowed Noname Pharmaceutical to comply with all the government regulations as far as employee access control are concerned.
- The biometric driven fingerprinting system also eliminated non-active employees and now has started enforcing strict authorization rules based upon the corporate policy set

forth in SAFE system. For example, SAFE will only provision employees in particular category, as defined in their main HR system, to access certain test labs.

- SAFE also provided for a centralized backup of all user access control systems for disaster recovery at any site. One corporate policy definition achieved this result.
- Auditing with drill-down capability for increasing levels of detail on specific incidents and alerts
- Provided for a seamless integration of physical security access rights of people to that of IT systems enabling an end-to-end identity management and user provisioning. This translates into less oversights or omissions whenever there are changes in status of an employee (active, non-active, and modification in privileges). SAFE Policy Server is capable of writing and managing cross over (physical to logical & vice versa) policies and rules.

4.2. Value Proposition

Quantum Secure's SAFE Policy Manager provided unparalleled savings and measurable impact on all key facets such as cost reduction, employee productivity, security and compliance.

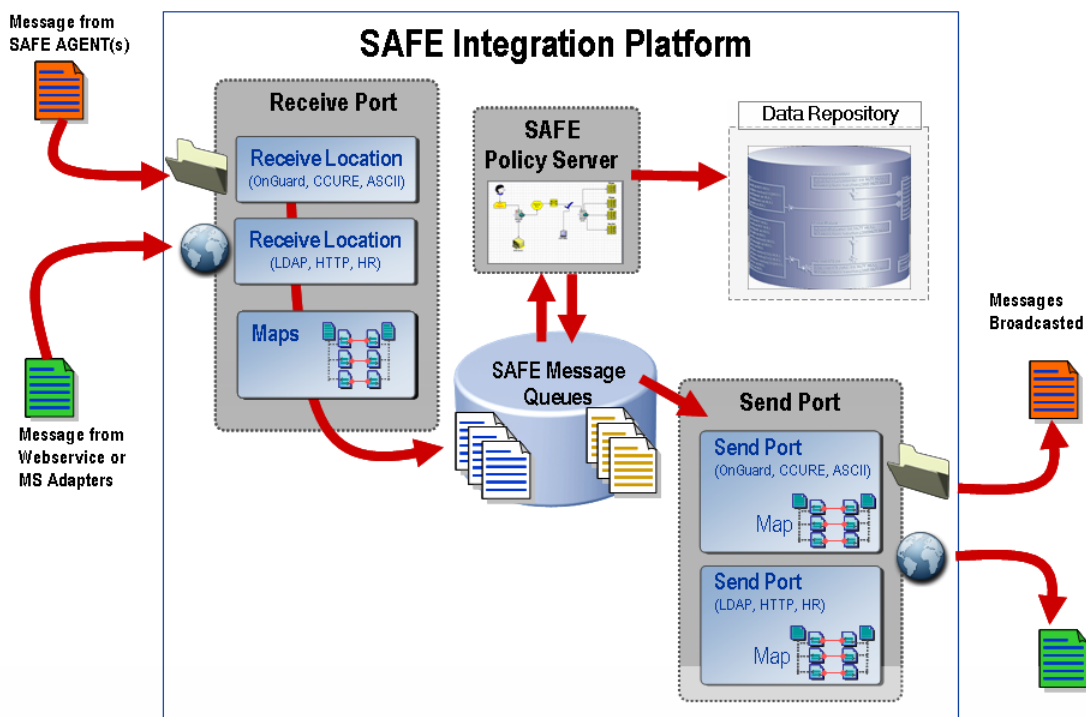
- **Security & Compliance:** Noname Pharma increased security compliance by closing all gaps in their environment. SAFE provided for all regulations needed to comply with certain government laws related to physical access control. It also reduced risk for undetected break-ins and theft due to tighter security management. A combination of IT and physical security systems gives comprehensive view of potential intrusion across IT and physical security domains.
- **Employee Productivity:** Fully automated management system provided for less time for manual process and intervention making employee's time very productive. It also simplified the security administrator's job by making all data in one central repository.
- **Cost Reduction:** Saved Noname Pharma over \$60K per month worldwide together with streamlined business process. Additionally, it saved a lot of calls to either help desk or security guard stations from people.

5. *Introducing SAFE Integration Platform*

In today's enterprise no application or device is an island even then many are still created with an internal focus. The reality is that integrating all physical and logical security devices together has become one of the main challenges for security departments. Connecting devices is about more than just exchanging bytes. As organizations move toward a net-centric business model, the real goal – creating security processes that unite separate devices into a coherent whole – comes within reach.

Quantum Secure has partnered with Microsoft to help achieve this goal. Quantum Secure has embedded Microsoft's BizTalk® Server within its SAFE Integration Platform to enable organizations to connect diverse physical security devices & applications, as well as IT & HR systems and Web services to graphically create and modify orchestration to send/receive data from those data sources. This approach brings a simple-standard way to manage and monitor the data transfer, devices, applications and support for single sign-on, etc. In addition to Web Services SAFE Integration Platform supports the ability to define Web services-based business processes by using the Business Process Execution Language for Web Services (BPEL4WS, commonly called just BPEL).

SAFE Integration Platform implements all integration scenarios as one or more orchestrations, each of which consists of executable code. These orchestrations are not created by writing code in a programming language such as C# or JAVA, however, instead, a business analyst uses the Orchestration Designer to graphically organize a defined group of shapes to express the conditions, loops, and other behavior of the business process. Each orchestration creates subscriptions to indicate the kinds of messages it wants to receive.



The message processing shown in the preceding figure is as follows:

1. A message is received through a receive adapter. Different adapters provide different communication mechanisms, so a message might be acquired by accessing a Web service, or access control system, or reading from a file, or in some other way.
2. The message is processed through a receive pipeline. This pipeline can contain components that perform actions such as converting the message from its native format into an XML document or validating the message's digital signature.
3. The message is delivered into a database called the Message Box database, which is implemented by using Microsoft SQL Server™.
4. The message is then sent to SAFE Policy Server, which takes whatever action the security policy/process requires.
5. The result of this processing is saved in the SAFE Data Repository.
6. This message, in turn, is processed by a SAFE Policy Server and sent to a pipeline, which may convert it from the internal XML format to the format required by its destination, add a digital signature, and more.
7. The message is sent out through a send adapter, which uses an appropriate mechanism to communicate with the application for which this message is destined.

The SAFE Integration Platform is built completely around the .NET Framework, with native support for communicating through Web services, along with the ability to import and export business processes described in BPEL. It is designed to work well both with the emerging world of standard Web services and with the large number of physical security applications and devices already in place.

5.1. Out-Of-The-Box Support For Major Physical Security Technology Vendors

Effectively exchanging messages between devices & applications is an absolute requirement for integration. Given the diversity of communication technologies that exist within the physical security and IT world, the SAFE Integration Server supports a variety of emerging & legacy protocols and message formats.

To achieve this goal, SAFE Integration Server works with XML documents internally. Whatever format a message arrives in, it is always converted to an XML document after it is received. Similarly, if the recipient of a document cannot accept that document as XML, SAFE Integration Server converts it into the format expected by the target application (such as Access Control, Fire, HVAC, LDAP, etc).

Even though more and more applications understand XML documents, most physical security devices and applications do not. SAFE Integration Server talk to a wide range of other proprietary devices and applications, and relies on a range of custom built SAFE Agents and off-the-shelf adapters to make this possible. SAFE Agent is stand-alone application (typically running as a Windows Service) to provide a communication mechanism, meta-data, and data

exchange auditing and monitoring services. The SAFE Integration Server provides built-in SAFE Agents for major physical security access control & video surveillance vendors, as well as adapters for popular applications such as LDAP based directories, PeopleSoft, Oracle, SAP, etc. All SAFE Agents are built on a standard base called the SAFE Integration Framework which makes it easier to create new Agents.

5.2. True, Open Interoperability Between Security Systems

The SAFE Integration Server provides the following out-of-box adapters (provided by Quantum Secure, Microsoft, and Microsoft-Certified partners):

Physical Security – SAFE Agents	IT & Application Adapters	Technology Adapters
<ul style="list-style-type: none"> • Access Control <ul style="list-style-type: none"> ○ Lenel-Onguard ○ Tyco-CCURE, Kantech ○ AMAG-SMS ○ Hirsch-Velocity ○ GE-PicturePerfect ○ Honeywell-Nextwatch ○ Sielox-Pinnacle ○ ODBC, OCI, Progress ○ SQL, XML, Custom • Digital Video Management <ul style="list-style-type: none"> ○ DVR – Event Servers ○ MPEG • Building Technologies <ul style="list-style-type: none"> ○ BACnet ○ LonWORKS ○ OBix • SmartCards <ul style="list-style-type: none"> ○ ActivIdentity CMS ○ Gemplus ○ ISOProx II, ISO 14443, ○ Common Biometric Format (XCBF) ○ Others • SPML, SAML • Physbits 1.0 • Guard Patrol Systems • Asset Management • RFID systems • Government Feeds <ul style="list-style-type: none"> ○ NACI ○ FEMA, USGS, USFD ○ Criminal & Terrorist DB 	<ul style="list-style-type: none"> • LDAP • Critical Path • Novell DirXML • SunONE • Viisage • Oracle Xellerate, IDMS • Tivoli IDM • AutoCad • Ascentn • BOC Information Systems • Captaris, Cincom • eCraft Manageme • Fenestrae, Intercim • J.D. Edwards • Metastorm • Oracle Financials • PeopleSoft • Scala Business Solutions • Siebel • SolutionForge Ltd. • Sysrepublic, Temenos • Visionware • Microsoft Excel, PowerPoint, Word • SAP R/3 • PDF, PostScript 	<ul style="list-style-type: none"> • 2392A, 70092, 3270, 5250 terminal emulation • ACORD, ACORD AL3 - XML • Adabas • AFP • AS/400 File System • ASCII ANSI, ASCII Unicode • ASTM • Basic, Btrieve • C, C# Assemblies • Choicepoint CLUE • CICS, CISAM • CORBA • cXML • DB2, DB2 for AS/400 and OS/390 • DB2, UDB • Delimited Text Files • EBCDIC • ebXML • Enscribe • FIX • EDI x.12, EDI-Fact • Flat files, HTML • HL7 • HTTP/HTTP • IFX, IMS, IMS/DB, IMS/TM • Informix • Ingres, Ingres II • JetForms • LegalXML • MVR • Microsoft Message Queuing (MSMQ) • NonStop SQL/MP • Oracle DB, RDB, SQL Server • Pathway • PCL, RMS

		<ul style="list-style-type: none"> • RPG • RSS • Sybase • Tuxedo • Undocumented Binaries • VSAM • VT102, VT400-7, VT400-8, VT52 terminals • Web Services, XML • WebSphere MQ
--	--	---

5.3. System Orchestration And Messaging Engine

System Orchestration

Sending messages between different physical security devices & applications is a necessary part of solving the integration. Yet in most cases, it is only a means to an end. The real goal is to define and execute a security processes based on these applications. SAFE Integration Server employs straightforward techniques to achieve this by creating drag-and-drop diagrams and create System Orchestration.

System Orchestration typically involves receiving some data feeds, running the incoming data set thru SAFE Policy engine and then sending data to others. SAFE Integration Server provides a Visual Mapper to define a transformation—a map—from one incoming data set to the other. To the developer creating it, each map is expressed as a graphical correlation between two XML schemas that defines a relationship between elements in those schemas. The W3C has defined the Extensible Stylesheet Language Transformation (XSLT) as a standard way to express these kinds of transformations between XML schemas; therefore, maps in SAFE Integration Server are implemented as XSLT transformations.

The transformation defined in a map can be simple, such as copying a name and address from data set to another. More complex transformations are also possible by using functoids. A functoid is a chunk of executable code that can define arbitrarily complex mappings between XML schemas, and Visual Mapper represents it as a box on the line connecting the elements being transformed. Because some of those transformations are fairly common, SAFE Integration Server includes a number of built-in functoids.









These built-in functoids are grouped into categories that include the following:

- Mathematical functoids. Perform operations such as adding, multiplying, and dividing the values of fields in the source document and storing the result in a field in the target document.
- Conversion functoids. Convert a numeric value to its ASCII equivalent and vice-versa.



- Logical functoids. Used to determine whether an element or attribute should be created in the target document based on a logical comparison between specified values in the source document. Those values can be compared for equality, greater than/less than, and in other ways.
- Cumulative functoids. Compute averages, sums, or other values from various fields in the source document, and then store the result in a single field in the target document.
- Database functoids. Access information stored in a database.

SAFE Integration Server also provides for creating custom functoids directly in XSLT or by using .NET languages like C# and Visual Basic .NET. Functoids can also be combined in sequences, cascading the output of one into the input of another.

Next, the Orchestration Designer is used to create an orchestration by connecting a series of shapes in a logical way, rather than expressing the steps in a programming language. Some of the most commonly used shapes are:

-  **Receive.** Enables the orchestration to receive messages. A Receive shape can have a filter that defines exactly what kinds of messages should be received, and it can also be configured to start a new instance of an orchestration when a new message arrives.
-  **Send.** Enables the orchestration to send messages.
-  **Port.** Defines how messages are transmitted. Each instance of a Port shape is connected to either a Send or Receive shape. Each port also has a type, which defines things such as what kinds of messages this port can receive; a direction, such as send or receive; and a binding, which determines how a message is sent or received by, for example, specifying a particular URL and other information.
-  **Decide.** Represents an if-then-else statement that allows an orchestration to perform different tasks based on Boolean conditions. Expression Editor can be used as part of Orchestration Designer, to specify this conditional statement.
-  **Loop.** Enables performing an action repeatedly while some condition is true.
-  **Construct Message.** Enables building a message.
-  **Transform.** Enables transferring information from one document to another, transforming it on the way by invoking maps defined with Visual Mapper.
-  **Parallel Actions.** Enables specifying that multiple operations should be performed in parallel rather than in sequence. The shape that follows this one will not be executed until all

of the parallel actions have completed.

-  **Scope.** Enables grouping operations into transactions and defining exception handlers for error handling. Both traditional atomic transactions and long-running transactions are supported. Unlike atomic transactions, long-running transactions rely on compensating logic rather than rollback to handle unexpected events.
-  **Message Assignment.** Enables assigning values to orchestration variables. These variables can be used to store state information used by the orchestration, such as a message being created or a character string.

After an Orchestration has been defined in this way, the group of shapes and relations between them is converted into the Microsoft intermediate language (MSIL) that is used by the .NET Framework common language runtime (CLR). Ultimately, the group of shapes defined becomes just a standard .NET assembly. And of course one can still add explicit code to an orchestration when necessary by calling a COM or .NET object from inside a shape.

6. *Summary*

Quantum Secure provides economical rules based flexible and scalable packaged solution to achieve full compliance with regulatory requirements such as SOX, PIV-I, PIV-II, HIPAA, etc. The solution can also automate and manage critical physical security processes as well by becoming an important “glue” amongst physical security & enterprise IT infrastructure.

The policy engine provides an easy, flexible and intuitive way to code business rules to achieve end-to-end compliance of a business process. Quantum Secure’s approach eradicates manual interventions at all points which are not only error prone but are also very costly. Another benefit of this approach is that the mandatory reports related to compliance with SOX directives are made available in real-time for all the facilities.

This approach leverages the existing deployed technological infrastructure of any company to achieve compliance, making it the most economical & holistic approach.

Additionally, SAFE is designed to addresses your specific security & business needs:

- **Built on an open platform** – reduces IT complexity while supporting scalability and growth through a comprehensive integration and application platform.
- **Tightly integrated to optimize cross-functional business processes** – enables comprehensive collaboration within and beyond your security organizations.
- **Enhanced by industry-specific features and best practices** – enables you to reduce total cost of ownership, achieve a faster return on investment, and benefit from a more flexible physical security infrastructure that helps drive innovation.
- **Designed to support international operations** – promotes efficient and successful global operations and competition.