

# ***SIA Standards Roadmap***

*(Dated 2007/03/14)*

## Table of Contents

1	Introduction .....	3
1.1	Overview .....	3
1.2	Goals.....	3
1.3	Role of an Industry Reference Model.....	4
2	Vision and Taxonomy: SIA's System Reference Model.....	5
2.1	Field Devices .....	5
2.2	Edge Components: Devices and Applications .....	5
2.3	Applications.....	6
2.4	System Provisioning Services.....	7
2.5	Monitoring and Control Services.....	7
2.6	System Operation Applications .....	8
2.7	Middleware Services .....	8
2.8	Common Infrastructure .....	8
2.9	The New Enterprise System – A Taxonomy for the Future.....	8
3	SIA Standards Activities vs. SIA Reference Model.....	9
3.1	SIA Standards Organization .....	12
3.2	Future Activities within SIA Standards .....	13
3.3	Program Metrics.....	14
4	Other Stakeholders.....	14
4.1	American Society of Heating, Refrigerating and Air-Conditioning Engineers [ <a href="http://www.ashrae.org">http://www.ashrae.org</a> ] .....	14
4.2	ASIS International [ <a href="http://www.asisonline.org/">http://www.asisonline.org/</a> ] .....	14
4.3	Builders Hardware Manufacturers Association (BHMA) [ <a href="http://www.buildershardware.com">http://www.buildershardware.com</a> ] .	15
4.4	Building Industry Consulting Service International [ <a href="http://www.bicsi.org">http://www.bicsi.org</a> ].....	15
4.5	Central Station Alarm Association [ <a href="http://www.csaaul.org/">http://www.csaaul.org/</a> ] .....	15
4.6	Continental Automated Building Association [ <a href="http://www.CABA.org">http://www.CABA.org</a> ].....	15
4.7	InterNational Committee for Information Technology Standards [ <a href="http://www.incits.org">http://www.incits.org</a> ] .....	15
4.8	International Electrotechnical Commission Technical Committee 79 [ <a href="http://www.iec.ch">http://www.iec.ch</a> ] .....	16
4.9	National Burglar & Fire Alarm Association [ <a href="http://www.alarm.org">http://www.alarm.org</a> ] .....	17
4.10	National Electrical Manufacturers Association (NEMA) [ <a href="http://www.nema.org">http://www.nema.org</a> ] .....	17
4.11	National Fire Protection Association [ <a href="http://www.nfpa.org">http://www.nfpa.org</a> ] .....	17
4.12	NIST [ <a href="http://www.nist.gov">http://www.nist.gov</a> ].....	17
4.13	PSEAG – SEIWIG [ <a href="http://herbb.hanscom.af.mil">http://herbb.hanscom.af.mil</a> ] .....	17
4.14	RTCA [ <a href="http://www.rtca.org">http://www.rtca.org</a> ] .....	18
4.15	Underwriters Laboratories, Inc. [ <a href="http://www.ul.com">http://www.ul.com</a> ].....	18
5	Other Issues.....	18
5.1	Global Markets .....	18
5.2	Consortia.....	18
6	Standards Tactics .....	18
6.1	Marketing .....	19
6.2	Government Affairs .....	19
6.3	SIA Industry Groups.....	19
	Appendix A - Standard Life Cycle.....	20
	Appendix B - ASIS Guideline Summaries.....	21
	Appendix C - CSAA Standards Activities.....	22
	Appendix D - NFPA Standards Activities .....	23
	Appendix E - UL Standards Activities .....	24

# 1 Introduction

## 1.1 Overview

Standards are a fast growing core component of SIA's member services. Four years ago, SIA's Board of Directors recognized the need for an aggressive standards program and chartered the Open, System Integration, and Performance Standards (OSIPS) Project. This project has contributed greatly to the growth of SIA as a "Standards Capable" organization. Like all programs, it has evolved as it continues to adapt to changing needs and evolving requirements including its own initial success.

Standards are perceived many ways. Some view them as a 'static defense' to protect market position or to organize access to markets. This approach envisions standards as imposing entry barriers on new competition, organizing the activities of current competitors, and adding control to the product development process. The transition to multiple-use edge devices capable of supporting software based edge applications, a consequence of the movement to software based products, reduces the achievability of these objectives because of the capacity of software based solutions to change rapidly.

Our industry is currently engaging the spreading influence of IT industry practices for defining the requirements for solutions and the associated market and product development efforts to stay competitive. Powerful forces are driving this process and our industry will certainly succumb to the pressure to adapt to a new style of business. We will also engage a different practice in the use of standards. Standards will no longer just regulate that which is; standards will no longer be primarily a defensive weapon in a company's arsenal. Standards will become an offensive weapon and they will be a mobile offense. Standards will be used to define markets and products based on a vision of a future rather than the existence of a product or practice. Successful standards will get to market in six months or less.

As this engagement evolves and as more sophisticated integration requirements are imposed by end users, the industry must adopt standards practices that allow it to lead the process. Failure to lead means irrelevance to the process and near certain dissatisfaction with the outcome. This is because others already understand the use of standards as a mobile offense and they are practiced at attacking the unprepared or uninvolved.

SIA does not have unlimited resources and must spend what it has wisely. In today's competitive environment, efficiency and effectiveness demand a plan, a "road map", that will be a guide in this new environment. It will help us set priorities and provide direction in order for us to take the timely actions that will preserve our ability to affect our destiny.

## 1.2 Goals

This roadmap is designed to assist in the achievement of a number of goals. These goals are thought to be the most important goals and SIA's standards activities should be prioritized to achieve them. These goals are ever changing as markets and the competition evolve.

The current SIA Standards goals are:

1. Establish SIA and its OSIPS program as the preeminent venue for Security Standards
  - a. Effectively communicate the evolving vision of the SIA Standards program.
  - b. Be the leading organization for the development of Security Application Standards for the end user community.
  - c. Maintain and develop framework and other foundational standards that enable the development of security application standards.
2. Implement a calculated program of participation in both domestic and international standards activities that extends the importance of SIA Standards Program.

- a. Develop and implement a program of participation in domestic standards activities to represent SIA member interests, to maintain a clear understanding of those activities, and to competitively position the SIA Standards program.
- b. Develop a plan for international standards activities to represent SIA member interests, to maintain a clear understanding of those activities, and to competitively position the SIA Standards program.
3. Develop a mechanism to deliver SIA Standards program benefits to members and participants.
  - a. Educate and inform SIA members and standards participants about standards activities that represent opportunities to improve their business.
  - b. Provide venue and support infrastructure for SIA member and standards participant sponsored Standards activities.

More end users are coming to the table and requirements are being shared. This Roadmap is meant to provide SIA Standards a guide to navigate the milestones of activities that keep the SIA Board of Directors and SIA Standards participants informed and on track with the course that is being plotted. The objective of all standards activities is for 'market relevance'. Traditional standards activities have been used as a 'static defense' tool whereby a given implementation/product is the focus of the work. The change occurring now is the change to use standards for market development whereby standards are considered in any strategic product development and provide for extensibility thereby allowing for the industry to grow and be innovative to meet market demands.

The vital importance of having an effective standards strategy is underscored by three fundamental facts; standards today are market driven, they often precede the products they describe, and they are a global phenomenon. In addition, the industry must accept that a standard is a specification used to enable multiple implementations of marketable products for world wide industry and commerce.

Finally, through the identification of standards activities and stakeholder activities, the program will be able to identify the resources required to sustain the standardization activities as well as the resources required for the roles and liaisons established with the various stakeholders.

### **1.3 Role of an Industry Reference Model**

The traditional security system model is undergoing an evolutionary change similar to that which occurred in the IT industry. This Roadmap provides a reference model for the security system of the future. There is a rapidly increasing demand for interoperable security system components based on open, public, consensus based standards. Current events show us that the demand for interoperable security integration and performance standards is so great that entities outside the security industry are taking steps to create the missing standards and compliant products. The reference model provides a foundation for the development of interoperable components based on Open, System Integration, and Performance Standards.

The relationships between standards and product life cycles are also changing (Appendix A). Standards are becoming anticipatory in that they will precede the final development of products. This approach qualifies markets and defines product requirements fostering more competition on product performance. It reduces the inherent risk in speculating about product requirements. The industry reference model will help to organize this process and ease the process of melding requirements from new participants in the rush to satisfy emerging markets. The reference model provides a mechanism to evaluate current and future SIA Standards activities by assessing their role in the model.

Finally, the reference model assists in evaluating relationships with the work of other formal standards developing organizations (SDOs), consortia, and other organizations, that may compete with or influence the SIA Standards activities. The growing diversity, in both formal standards organizations and consortia of various forms, will have a profound effect on the dynamics of standards development. Of particular interest are the changes due to the European Community use of standards as regulatory and procurement tools with consequent worldwide implications. In the technical work of standards development, complexity, interaction and constant evolution will be the normal course of events.

All parts of the roadmap are subject to change; in a world as dynamic as the world of standards, no plan can long survive in one form. The plan will be formally reviewed and revised on an annual basis.

## **2 Vision and Taxonomy: SIA's System Reference Model**

It is difficult to build a complex system when there are no words to convey your ideas and no models to effectively illustrate the scope of your vision and innovation. Complex things require clearly defined words that communicate useful, *real-world* meanings, especially when building complex enterprise security systems.

Taxonomy, defined as “an orderly classification of things according to their presumed natural relationships,” is used to refer to the words we use to describe the parts, relationships, and processes of systems. As the technology of security evolves, innovators are seeking new ways to think about systems and to readily identify and communicate the roles of hardware and software components within these complex systems. The increasing influence of IT on security is restructuring our approach and bringing new words and new definitions to our process. In line with this evolution, our taxonomy will be revised to reflect the evolving enterprise security system.

Future systems will be described by a new standards-based taxonomy. Most of its founding concepts will be imported from the IT world that has enabled (or driven) so many other industry transformations. Specialized hardware will generally be replaced by software running on generic or specialized computing platforms. And, the computing platforms will communicate through and be powered and conditioned by the underlying infrastructure used by all of an Enterprise's systems.

The following are the roles and functionality of key hardware and software components within the future enterprise infrastructure.

### **2.1 Field Devices**

From a role perspective, field devices are generally single function elements that collect and process information from the system's environment or that exercise control over elements in the environment. For example, field devices include motion sensors; cameras; card reader buttons; contacts; locks; door operators; barriers and analog measurement devices such as temperature, fluid height, flow, light, etc. Field devices are generally not interactive within the computing side of the system, but may have limited participation where provisioning or special reporting is required. Field devices may depend on the infrastructure of the system for power and environment. These devices implement special technologies and, although they will become smarter and more capable, they will exist because of their unique role and technology.

Some may argue that a particular field device is really an edge device and vice versa. That's understandable. However, it's important to think about system elements independent of the hardware that implements them, by understanding the roles performed. Roles may vary from one instance to another and the successful product developers will envision the best combinations of capabilities that meet the most customer needs.

### **2.2 Edge Components: Devices and Applications**

Edge applications are software programs (applications) running in typically small computing environments called edge devices. This is important because as software becomes the basis for edge component functionality more adaptability and scalability are possible with a single edge device. Edge devices provide connection points for field devices. The edge applications they support provide the provisioning, control, monitoring and other services that are a part of the system. Edge devices are broadly distributed and define the computing edge of the system, while providing local processing that operates independently to support designed activities. In part, it is this independent operational capability that distinguishes an edge device from a field device. Edge devices depend on the infrastructure of the system for power, communications, and environment. It is the edge application

and its provisioning that determines edge device behavior or role. Edge components will always be a part of the enterprise system, but it's a good bet they will change dramatically.

Edge devices and applications are the access point to the core applications of the system. While smarter field devices may become edge devices, and this will happen to some extent, edge devices provide a point of integration for the diverse field devices required to implement a system's functionality at a specific location. An example is a portal. A portal control edge device and application provides the point of independent operation of a portal that a system must deliver to be robust.

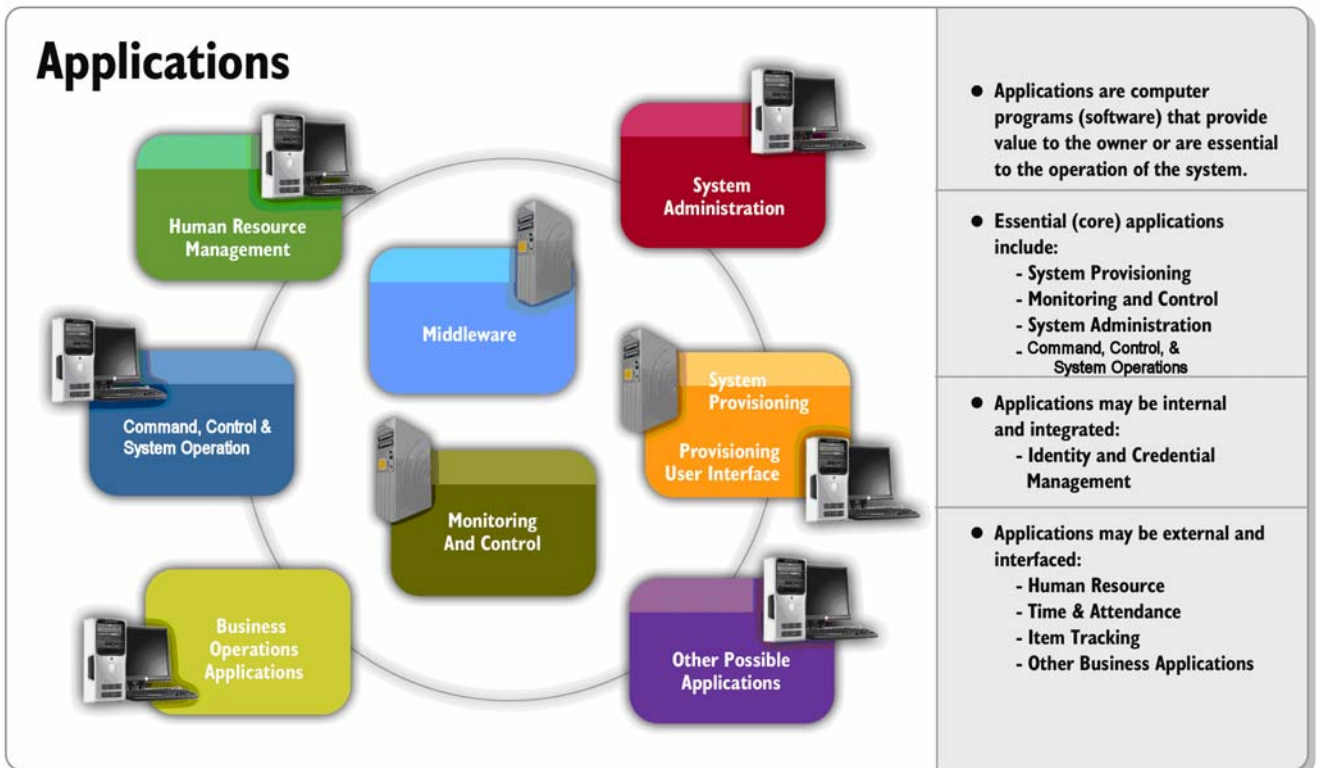
## **2.3 Applications**

The general term "application" meaning computer programs has been used for quite some time now in the IT industry. It has also been used in security systems. In the new taxonomy, this term has a more precise meaning. Historically, security system practitioners have used the term applications to mean a program that was outside the security system and that performed a very narrow set of tasks. Typically, the term application referred to an interface.

In the new taxonomy, "application" is an element of software that realizes a role that must be or is performed by the system. No longer is there an access control system, a video surveillance system, an intrusion detection system, etc. The term role is used to characterize the mission of an application program in the system. Somewhat arbitrarily, some applications are considered very essential as they are utilized by many other applications. These applications are sometimes referred to as "core applications" or "services". A service is an application used by many roles in the system. These internal applications and services are integrated into the system and the system cannot exist without them and vice versa.

For example, edge applications perform roles based on software programs and configuration data provided by "Provisioning Services (Core Applications)." System events are monitored and responded to by "Monitoring and Control Services (Core Applications)." System performance and maintenance is accomplished through "System Administration Services ". Finally, user interfaces are examples "System Operation Applications". In a security system, User Command Stations, Identity and Credential Management Stations are good examples of internal applications. Such applications are often considered integrated into the system. These applications are internal applications as the system will not exist without them.

Time and Attendance, Fuel Monitoring, and Maintenance Scheduling are made up examples of roles that may be essential to the business purpose of a system but may not be essential to the existence of the system and are not generally used by other applications or services. These applications are frequently said to be interfaced to the system. The designer's perception of the roles fulfilled by these programs will determine their classification as service or application and integrated or interfaced. Whether integrated or interfaced, the different applications (roles) exchange information and this is a central focus of SIA's Standards efforts.



## 2.4 System Provisioning Services

“System Provisioning” refers to the process of collecting and distributing configuration information needed by edge devices and other applications to achieve the system’s mission. A provisioning service is a computer application involving computer programs, databases, and user interfaces. A system may have more than one provisioning service. A well-defined system will have a properly designed solution for control over the data that defines the system’s operation. Provisioning services typically have user interfaces that assist in the management of the configuration data. These user interfaces may be system operation applications or tightly bound to and a part of the provisioning service.

Typically, all applications require some provisioning. The reason for this is that they have to interact with each other about their activities and this requires that their context information be shared. Simply put, there has to be agreement on the street names and addresses if one’s directions are to mean something to another. Provisioning services provide the means to collect, maintain, analyze, distribute, and protect the information that configures the system and is generated by the system. They usually depend on large relational database management systems.

## 2.5 Monitoring and Control Services

“Monitoring and Control Services” refers to the computer programs that monitor the events detected and reported by the system edge applications or other applications (monitoring) and automatically take action based on the character and detail of the reported activity (control services). Monitoring Services depend on Provisioning Services for context information. Generally, monitoring services may have a user interface, but primarily support general user operation interfaces. Control Services address the automatic responses of a system to the occurrence of a specific event. Control Services depend on Provisioning Services for context information and for the prescription of the actions to take when an event occurs. Generally, control applications do not have a user interface.

## 2.6 System Operation Applications

“System Operation Applications” refers to the computer programs that assist human operator’s oversight and operational control of the system. These activities are usually based on an occurrence of system events that require human assessment and/or intervention. Command Centers are the most common location for System Operation Applications. Effective system operation depends on software that can deliver to an operator all of the information needed to manage an event on a timely basis in an uncomplicated and easy manner, preferably automatically. In future systems, there will be more diverse operational applications distributed throughout the system performing specialized operational support where needed.

“System Administration Applications” refers to computer programs that provide specialists access to the detailed operations of the internal system processes. This is a technical function and requires scarce technical resources. Single Seat Support (S<sup>3</sup>), a powerful trend in IT, is the concept that special technical staff has complete visibility of all aspects of the system’s operation - all the way to the field devices from their office desk or any other location. S<sup>3</sup> allows complex tasks to be centralized and simple tasks to be distributed. Because less people do these complex tasks more frequently, they are usually performed more efficiently and with higher customer satisfaction. S<sup>3</sup> architectures mean that manufacturers have a shorter path to the system for support and that systems can be more reliable. S<sup>3</sup> will be an essential concept in the developing taxonomy of future systems.

## 2.7 Middleware Services

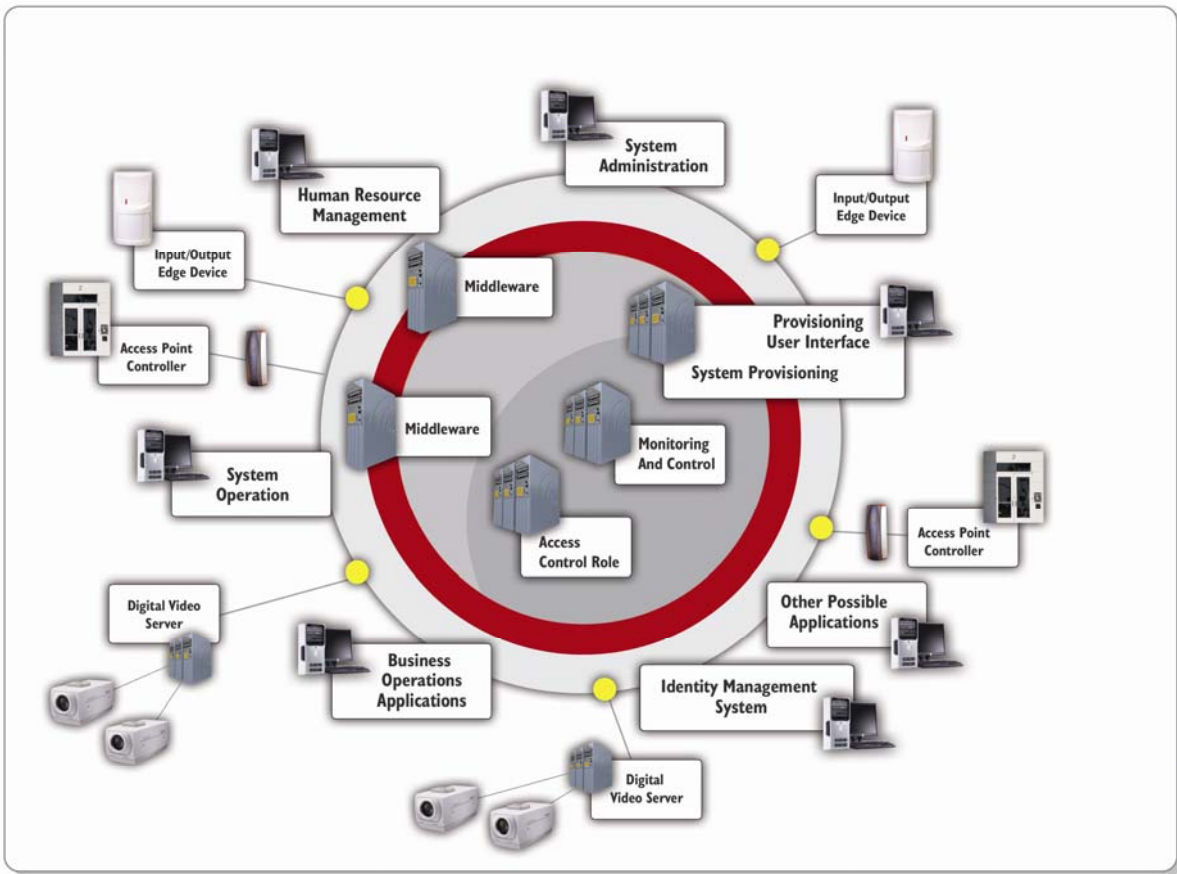
If every application had to communicate with every edge device the complexity of the systems would grow exponentially with the system and soon fail. “Middleware” refers to computer programs that specialize in communicating with many edge devices to provide localized or distributed provisioning, monitoring & control, and management support. It provides a conduit for operational and management commands, while reducing network requirements by consolidating and organizing traffic. Middleware reduces edge device load by reducing the number of duplicate transactions that must be serviced. It provides a distributed data repository service for edge devices. When a need has been identified, middleware can provide interim processing of transactions. It is a backroom process that connects edge devices to other applications while optimizing the deployment of the system.

## 2.8 Common Infrastructure

“Common Infrastructure” includes electrical power, environmental support, cabling, communications, and sometimes computing resources. Sharing a common infrastructure may reduce costs by eliminating duplication in sharable power, environments, and networks. Sharing a properly designed infrastructure and system means increased availability and easier management. Additionally, total operating costs can be lowered by shared power, greater scalability and better response to peaks, lower network investment, and reduced system migration costs.

## 2.9 The New Enterprise System – A Taxonomy for the Future

The schematic below illustrates the complexity and simplicity of future systems. The concentric circles represent the Common Infrastructure as three layers. The outer circle is the backplane where all of the edge components plug into the system. The next layer represents the network layer that supports information distribution to and from the edge device layer around the domain of the Enterprise. This is the domain of middleware. The center layer represents the core components of the infrastructure. All of the elements previously discussed have been plotted on this diagram. It may be a little unsettling to see the entire enterprise infrastructure as a flat disk upon which applications and edge devices rest. But, this serves to emphasize the concept of sharing a common infrastructure. In this new model, this taxonomy provides for all of the services of the enterprise with a much greater capacity to expand, change and support new and valuable applications in a shared resources environment.



### 3 SIA Standards Activities vs. SIA Reference Model

SIA Standard's goals are restated below along with a summary of the tactics contemplated to achieve them.

1. Establish SIA and its OSIPS program as the preeminent venue for security standards development.
  - a. Effectively communicate the evolving vision of the SIA Standards program.
    - i. Develop an aggressive and successful program of recruitment of participants, including end-users, specifiers, manufacturers, installers, and others who can contribute to the development of high quality standards.
    - ii. Developing Information/Marketing Brochures, white papers, and similar documents that communicate the profitability of participation in standards activities.
    - iii. Promote SIA's Security Applications Standards activities as a mechanism for end users to define and standardize solutions to their security requirements. These standardized solutions will provide:
      1. well defined market segments for security solutions
      2. well defined solutions with end user stakeholder buy-in
      3. expansion of market opportunities for the solution providers
      4. reduction of the risk and cost of new product development
    - iv. Articulate through case studies how participation gives genuine competitive advantage to participants.
    - v. Provide useable reports relating SIA standards activities to specific SIA industry groups.
    - vi. Aggressively publish and disseminate the SIA Standards Roadmap as a summary of SIA's approach to standards development.
    - vii. Develop a family of presentations that can be incorporated in participant, member and staff presentations about SIA standards activities. These can be leveraged to a variety of audiences.

- viii. Develop an outreach program for selected venues (ASIS, ISC West and ISC East) at which these presentations may be given.
  - b. Be the leading organization for the development of Security Application Standards for the end user community.
    - i. Develop and publish timely, market relevant Security Application Standards driven by and with participation from stakeholder groups within the end user community.
    - ii. Use SIA's Government Affairs program to build awareness and develop mandates for participation by Government Agencies in SIA's Standards program.
    - iii. Work with end users on the development of project proposals for new work.
  - c. Maintain and develop framework and other foundational standards that enable the development of security application standards.
    - i. Regularly identify gaps in framework and foundational standards that need to be addressed to meet the evolving vision.
    - ii. Revise framework and foundational standards to fill identified gaps.
- 2. Implement a calculated program of participation in both domestic and international standards activities that extends the importance of SIA Standards Program.
  - a. Develop and implement a program of participation in domestic standards activities to represent SIA member interests, to maintain a clear understanding of those activities, and to competitively position the SIA Standards program.
    - i. Identify the standards activities that are relevant to the industry and qualify the role that SIA Standards participation will take as it relates to the role.
    - ii. Identify standards activities where SIA's participation may lead to expanded market opportunities for SIA members.
    - iii. Establish metrics for roles, and identify resources required for the role.
    - iv. Prioritize the industries/market segments activities.
  - b. Develop a plan for international standards activities to represent SIA member interests, to maintain a clear understanding of those activities, and to competitively position the SIA Standards program. Fundamentally, our vision is that SIA can become a significant international standards activity if it can demonstrate an ability to consolidate both US domestic security standards and emerging market's standards by sharing information, access, and efforts to meet consolidated goals. Our basic approach is:
    - i. Identify and develop working relationships with the Standards infrastructure in emerging markets that are generally under represented in international and large market Standards environments.
    - ii. Develop market specific sharing and participation programs that will share SIA developed work and incorporate where possible partner market work in SIA's activities. Build mutual stakeholder relationships.
    - iii. Identify areas of common interest and work to harmonize activities in these areas
    - iv. Identify means by which disparate interests may be harmonized. Work to influence mutual approached to evolving activities.
- 3. Develop a mechanism to deliver SIA Standards program benefits to members and participants.
  - a. Educate and inform SIA members and standards participants about standards activities that represent opportunities to improve their business.
  - b. Provide venue and support infrastructure for SIA member and standards participant sponsored Standards activities.

The SIA Standards activities have been undergoing a change from the traditional efforts to Open, Systems Integration and Performance Standards (OSIPS) activities. Standards are becoming increasingly complex and dynamic in nature (see Appendix A); this increases the difficulty in their development. The current reference model for system will be revised to ensure it timeliness and relevance to the evolving perception of our market spaces. Future models should identify the interrelationships among standardization activities and groups participating in those activities for effective standardization.

Shorter product life cycles as well as increasing economic dependence on standards by all parties have led to demands for more standards and a shorter time frame for development. This demand for greater productivity

and responsiveness from a relatively fixed resource will continue to intensify. SIA Standards must address this problem at all levels because its present success will lead to demand it cannot fulfill without aggressive recruitment to ensure a qualified work force.

The use of object-oriented techniques promises significant benefit to the design and development of systems. The same can be said in the development of standard interface definitions. The use of UML in standards activities has proven to be of great value in defining those interfaces. It greatly assists in the communication of model concepts both domestically and internationally, especially within the IT community.

There has always been a need by users for validation of the conformance of products with standards. There are many ways that this is accomplished. This can take the form of self-declaration and/or third party certification. Conformity assessment activities such as testing, certification, and accreditation are closely associated with standards and provide the consumer or end user with a measure of confidence in the products and services being purchased. For this reason, conformity assessment has become a critically important aspect of conducting business in the global marketplace and is often made visible through product marking or other marketing and promotional efforts. Rapidly evolving technologies such as information technology and telecommunications, for example, have requirements that are far different from those of steel or textiles or highly regulated technologies such as medical devices. The stakeholders in the standardization process – companies, government agencies, public interest organizations, and individuals – choose the method of standards development and the conformity assessment scheme appropriate for their particular needs. SIA is not in the business of providing conformity assessment services.

Federal, public and private sector organizations are increasingly using standards as procurement documents, deriving specifications from voluntary standards. This use may be seen as a positive force for increasing the acceptance of standards in the marketplace. Standards developing participants must be sure to interact constructively with the procurement user community and possibly encourage their participation in any given activity.

It is clear that an increasing level of dependence on standards and effective conformity assessment characterizes the future market for member products. Thus, as standards develop, it is essential that the standard include the test metrics for conformity assessment. In some sense, it is the conformance tests, rather than the standard, that establishes the true reality of true standard. Failure by SIA Standards to participate, either by not developing test suites in its standards development effort or by failing to review test suites developed by others and working to ensure their harmonization with SIA's activities, will be a major omission with potentially serious consequences.

Recent OSIPS activities have begun to address the need for interface definitions at a variety of levels. The initial OSIPS activity focused on developing an integrated family of American National Standards that were 'binding independent' served two functions:

- The Framework and Other Global Interfaces – A compendium of foundational work that provides a common foundation for future work
- Component Interfaces – Role specific interface data models that are the building blocks of real products and real systems.

The OSIPS Framework effort defines a set of common design elements required for the family of standards as well as cross-industry interfaces that are required for any component interfaces that are defined and will be shared. These types of standardization activities are accomplished within the Pan-Industry Data Modeling Subcommittee.

Bindings also are examples of cross model standards that prescribe specific methods of implementation of interfaces. The "Bindings" efforts will provide a standard by which the message encoding protocol, message transport protocol and electrical interfaces may be used to implement a specific OSIPS Framework or Component interface data model. Ideally, these "Bindings" will be content agnostic and support all of the various component and OSIPS Framework and Component interface standards. The first OSIPS Binding activity is in formation.

A new OSIPS activity is the Security Applications Standards Subcommittee. The Security Application Standards Subcommittee would address specific applications of security technology to solve specific problems and produce standards that define those solutions. These efforts would combine the component interfaces along with specific binding standards to serve specific application needs; such as Access Control Operations at Vehicular Gates. Other additional future potential areas of work are discussed later in this section of the document.

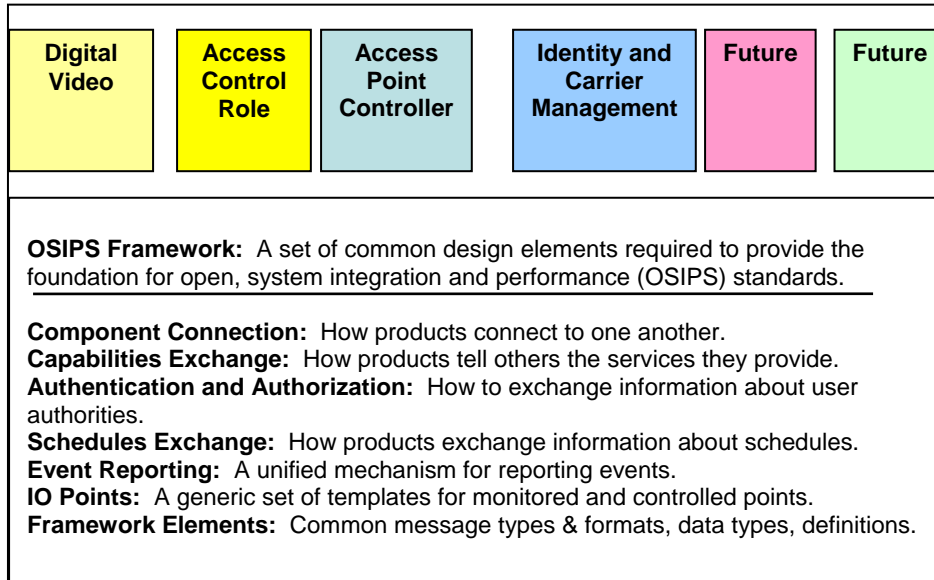


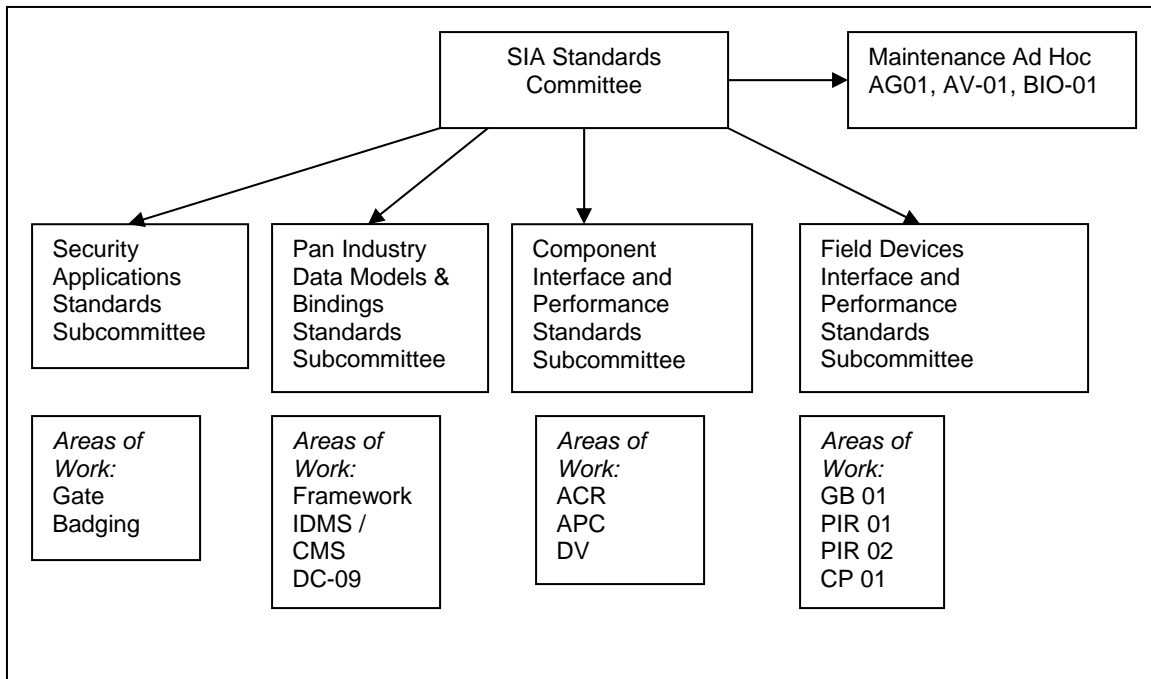
Diagram of Recent OSIPS Activities within SIA Standards

### 3.1 SIA Standards Organization

Currently, the SIA Standards activity is comprised of numerous loosely coupled activities. A purpose of the Roadmap is to identify an organizational infrastructure thought to ensure the successful achievement of the Standard's Program objectives.

SIA Standards Committee is considered to be a management level body dedicated to the oversight of the program and from which coordination of the various activities and subcommittee efforts can be effected. It is also the group which oversees strategic issues such as policy, procedures, and strategic oversight of the program such as Roadmap maintenance. This group is responsible to the SIA Board of Directors. This committee also oversees the entrance of new proposed work and the exit of mature work to be subsequently ratified by the Security Industry Standards Council (formal consensus body for final approval of all of SIA's American National Standards).

An analysis must be done of the existing committee structures and their current body of work and a transition envisioned that will map the activities to the new reference model.



The above diagram depicts an organizational structure that relates to the Reference Model and organizes the current SIA standards activities accordingly.

The Field Devices Subcommittee oversees the work being done on Field Devices within the industry and may include interface and performance standardization activities. To reiterate from the taxonomy discussion above, field devices are generally single function elements that collect and process information from the system's environment or that exercise control over elements in the environment. For example, field devices include motion sensors; cameras; card reader buttons; contacts; locks; door operators; barriers and analog measurement devices such as temperature, fluid height, flow, light, etc. Field devices are generally not interactive within the computing side of the system, but may have limited participation where provisioning or special reporting is required.

The Component Interface Subcommittee addresses interface work and performance activities for specific edge components. To relate back to the taxonomy, edge components are considered edge applications operating on edge devices. They typically provide a connection point and management over for field devices and are the point of contact for core applications of the system.

The Security Application Subcommittee may build upon the existing component interfaces for a specific application requirement. In the area of performance related standardization this group may also address standardization activities for application requirements.

The Pan Industry Data Models and Bindings activities serve to aid in integration whereby common structures and interfaces are leveraged to enable communication cross the enterprise with predefined transactions, message structures and agreed upon bindings.

### 3.2 Future Activities within SIA Standards

The Roadmap must consider future activities. Initially, specific industry bindings and common capabilities shared by multiple components will become projects within the Pan Industry Sub-Committee. The Security Applications Subcommittee will approach projects driven in part by the demands of end-users and specifiers. Its work will build upon the existing component interface standards by creating standards for solutions to end user needs. There is also interest for the development of performance requirements for specification application areas as well.

In addition, as manufacturers develop implementations, there may be the opportunity for SIA to sponsor Industry “Plug Fests” to showcase various manufacturers’ effort to implement the various interface activities.

### 3.3 Program Metrics

The SIA Standards program needs to ensure that metrics are put in place to evaluate the various activities. The following are areas to be monitored:

- Production (Life Cycle) of Standards
  - Project Proposal initiation (area of new work and quantity)
  - Public Reviews (number conducted, number of comments received, types of comments (editorial vs. technical))
  - Final Publication (quantity, sales)
  - Total Life Cycle Trends for “Time to Market”; Periods from Project Proposal to Final Publication.
- Adoption in the Marketplace
  - Standards References’ appearance in specifications
  - Standards References’ appearance in polls
  - Standards References’ appearance in benchmarking
- Participation Evaluation
  - Quantity of participants
  - Qualification (SIA members, non-members, end users)
- “Plugfest” Evaluation
- Webtrends analysis on claims of conformance.

## 4 Other Stakeholders

SIA provides the core competencies for the electronic physical security such as an understanding and diversity of experience in its participants in meeting the application requirements of a ‘security’ specialist. However, there is a need to monitor other activities and areas of interest that may influence the SIA Standards activities. There are a variety of organizations that SIA monitors that may influence standards roadmap activities.

The following is a brief listing and attempt not only to identify their interest but discuss their influence and impact on SIA Standards activities. Further revisions of this document will elaborate further on each stakeholder below to clarify the role and expected relationships that SIA Standards will undertake with each entity below.

### 4.1 American Society of Heating, Refrigerating and Air-Conditioning Engineers [<http://www.ashrae.org>]

*Scope:* ASHRAE, the American Society of Heating, Refrigerating and Air-Conditioning Engineers, is the society for engineers and others who work in this complex and evolving field. The technical expertise of ASHRAE members positions it as a highly credible source of research, standards, publications, education, and other products.

### **BACnet** [[www.bacnet.org](http://www.bacnet.org)]

*Scope:* The purpose of this standard is to define data communication services and protocols for computer equipment used for monitoring and control of HVAC&R and other building systems and to define, in addition, an abstract, object-oriented representation of information communicated between such equipment, thereby facilitating the application and use of digital control technology in buildings.

### 4.2 ASIS International [<http://www.asisonline.org/>]

*Scope:* To advance security practices through the development of security related standards

### **Mission Statement of the ASIS Commission on Guidelines**

To advance the practice of security through the development of guidelines within a voluntary, non-

proprietary, and consensus-based process utilizing to the fullest extent possible the knowledge, experience, and expertise of ASIS membership and the security industry.

**See Appendix B for a Summary of ASIS Guidelines**

**4.3 Builders Hardware Manufacturers Association (BHMA) [<http://www.buildershardware.com>]**

*Scope:* Builders Hardware Manufacturers Association is the trade association for North American manufacturers of commercial builders' hardware. Since its founding in 1925, BHMA has endeavored to promote the general development and welfare of the builders' hardware industry and its member companies. BHMA currently authors 31 ANSI/BHMA standards in the builder's hardware category, covering everything from hinges to locks to power door. In addition, BHMA is involved in international standards, code and life safety regulations and other activities that specifically impact builders' hardware

**4.4 Building Industry Consulting Service International [<http://www.bicsi.org>]**

*Scope:* BICSI is a professional association supporting the information transport systems (ITS) industry with information, education and knowledge assessment for individuals and companies. BICSI serves more than 25,000 ITS professionals, including designers, installers and technicians. These individuals provide the fundamental infrastructure for telecommunications, audio/video, life safety and automation systems. Through courses, conferences, publications and professional registration programs, BICSI staff and volunteers assist ITS professionals in delivering critical products and services, and offer opportunities for continual improvement and enhanced professional stature.

**4.5 Central Station Alarm Association [<http://www.csaaul.org/>]**

*Scope:* The standards activities undertaken by CSAA shall encompass the development of American National Standards specific to industry practice and conduct for the monitoring of electronic security systems. These standards shall apply to all operations of security system monitoring, and to the monitoring of all types of electronic systems which provide as their primary function the protection and safeguard of life, property, or information, but only where there are no existing standards which would suitably serve the same purpose. These standards shall include standardization terms and definitions, specifications, requirements, procedures, and methods which apply to monitoring facilities, personnel, operators, and situation handling.

**See Appendix C for a Summary of CSAA Standards Activities**

**4.6 Continental Automated Building Association [<http://www.CABA.org>]**

*Scope:* CABA is a not-for-profit industry association that promotes advanced technologies for the automation of homes and buildings in North America. Our mission is to encourage the development, promotion, pursuit and understanding of integrated systems and automation in homes and buildings

**4.7 InterNational Committee for Information Technology Standards [<http://www.incits.org>]**

*Scope:* Standardization in the field of information technology which encompasses storage, processing, transfer, display, management, organization, and retrieval of information

Technical Committee B10 - Identification Cards and Related Devices

[http://www.incits.org/tc\\_home/b10sd4.htm](http://www.incits.org/tc_home/b10sd4.htm)

Development of national and international standards in the area of identification cards and related devices for use in inter-industry applications and international interchange, e.g.:

Physical characteristics and test methods for identification cards

- Integrated circuit cards with contacts
- Contactless integrated circuit cards
- High and low coercivity mag stripe cards

- Optical memory cards
- Machine readable passports & visas
- Health care identification card (ANSI only)
- Thin flexible cards and tickets with mag stripes (new International project)

This technical committee is the U.S. TAG to [ISO/IEC JTC 1/SC17](#) and provides recommendations on U.S. positions to the [JTC 1 TAG](#). Some well known ISO/IEC JTC 1 / SC 17 activities include 14443 - Identification cards - Contactless Integrated Circuit Cards (CICCs) - Proximity integrated circuit(s) cards and 7816 - Identification cards - Integrated circuit(s) cards with contacts.

Technical Committee M1 - Biometrics [<http://m1.incits.org/m1sd4.htm>]

The Executive Board of INCITS established Technical Committee M1, Biometrics, in November 2001 to ensure a high priority, focused, and comprehensive approach in the United States for the rapid development and approval of formal national and international generic biometric standards. The M1 program of work includes biometric standards for data interchange formats, common file formats, application program interfaces, profiles, and performance testing and reporting. The goal of M1's work is to accelerate the deployment of significantly better, standards-based security solutions for purposes, such as, homeland defense and the prevention of identity theft as well as other government and commercial applications based on biometric personal authentication. Additional well known ISO/IEC standards are: 19785 Information technology - Common Biometric Exchange Framework Format and 19784 Information technology - BioAPI - Biometric Application Programming Interface

Technical Committee L1 - Geographic Information Systems (GIS)

Geographic Information Systems form a distinct class of information systems through their unique requirements for collecting, converting, storing, retrieving, processing, analyzing, creating, and displaying geographic data. The generic nature of GIS, organizing information by location, is interdisciplinary and not specific to any application.

The work of L1, Geographic Information Systems (GIS) consists of adopting or adapting information technology standards and developing digital geographic data standards. Digital geographic data standards are concerned with creating, defining, describing, and processing such data.

Technical Committee L3 - Coding of Audio, Picture, Multimedia, and Hypermedia Information

The L3 Technical Committee on Audio/Picture Coding serves as the U.S. TAG to ISO/IEC JTC 1/SC29, "Coding of Audio, Picture, Multimedia and Hypermedia Information. L3 activities and project development are conducted at the international level for the standardization of coded representation of audio, picture, multimedia and hypermedia information - and of sets of compression and control functions for use with such information - such as: audio information, bi-level and limited bits-per-pixel still pictures; computer graphics images; moving pictures and associated audio, multimedia and hypermedia information for real-time final form interchange; and audio visual interactive scriptware.

#### **4.8 International Electrotechnical Commission Technical Committee 79 [<http://www.iec.ch>]**

IEC Technical Committee 79 – Alarm Systems

*Scope:*

- To prepare international standards for detection, alarm and monitoring systems for protection of persons and property, and for elements used in these systems;
- The scope includes, but is not limited to:
  - intruder and hold-up alarm systems,
  - fire alarm systems,
  - hazard alarm system,
  - social/emergency alarm systems,
  - other monitoring and surveillance systems (for example, personal or baggage screening, video and access control systems),
  - associated transmission and communications systems
- It is clear that SIA Standards needs to begin preparing for participation in TC 79 should it be re-activated.

- Currently the U.S. TAG to TC 79 is the NFPA.
- CENELEC's EN 50131 Standard suite will be brought into this international arena for consideration as an International Standard.

#### 4.9 National Burglar & Fire Alarm Association [<http://www.alarm.org>]

*Scope:* The standards activities undertaken by the NBFAA standards committee will encompass the development and maintenance of American National Standards regarding residential and commercial electronic home and building systems including, but not limited to: electronic security and life safety systems, entertainment (audio/video), environmental control (automation/energy management), lighting, and the integration thereof. These standards shall include terms, definitions, requirements, procedures and methods that apply to installation, maintenance, testing and the ongoing operation of systems. Standards activities will not be restricted to specialized sections of the industry, but rather will represent an effort to produce standards that are harmonious with the industry as a whole, and do not duplicate any widely accepted and applied pre-existing standards

#### 4.10 National Electrical Manufacturers Association (NEMA) [<http://www.nema.org>]

*Scope:* NEMA, created in the fall of 1926 by the merger of the Electric Power Club and the Associated Manufacturers of Electrical Supplies, provides a forum for the standardization of electrical equipment, enabling consumers to select from a range of safe, effective, and compatible electrical products.

#### 4.11 National Fire Protection Association [<http://www.nfpa.org>]

*Scope:* These Regulations cover the process of developing and revising NFPA Documents and the role of the Board of Directors, Standards Council, Technical Correlating Committees and Technical Committees in this process. Procedures for establishing and operating these Committees are included as are requirements for processing Tentative Interim Amendments and Formal Interpretations

The 2002 *NFPA 72®: National Fire Alarm Code®* provides the most advanced requirements for all aspects of protective signaling systems and their components. Trust this comprehensive document to support your work with the design, application, installation, performance, testing, and maintenance of these vital early warning systems.

In addition, NFPA has also moved into the physical security space and requirements on manufacturers through the creation of *NFPA 730: Guide for Premises Security* and *NFPA 731-200x - Standard for the Installation of Electronic Premises Security Systems*.

**See Appendix D for a further Summary of NFPA Standards Activities**

#### 4.12 NIST [<http://www.nist.gov>]

*Scope:* NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life.

#### 4.13 PSEAG – SEIWIG [<http://herbb.hanscom.af.mil>]

*Scope:* The Physical Security Equipment Action Group (PSEAG) is the central manager for Physical Security Equipment (PSE) Research, Development, Test and Evaluation (RDT&E) funding within Department of Defense (DoD). The Security Equipment Integration Working Group (SEIWG) is a standing subcommittee of the PSEAG. SEIWG membership includes US Air Force (USAF), US Army (USA), US Navy (USN), and US Marine Corps (USMC) as shown in Figure 1.

The SEIWG mission is to coordinate and influence system architecture, technical design, and systems integration of all Physical Security Equipment (PSE) to be used within the DoD. One of the SEIWG

initial efforts is to begin the process of developing a joint PSE technical architecture for application to all DoD PSE design and acquisition efforts.

**TV-1** [[http://herbb.hanscom.af.mil/esc\\_opps.asp?rfp=R1264](http://herbb.hanscom.af.mil/esc_opps.asp?rfp=R1264)]

*Scope:* The AT/FP TV-1 is a listing of standards and protocols currently used by the USAF, USN, USA, USMC, security vendors, and program managers in the development and procurement of physical security systems, equipment and components within their domain and those proposed by the Services for current and use prior to 2007. Also included are descriptions of options and parameters associated with each standard. This TV-1 is the culmination of joint activities among the Services and Industry to bring forward recommended standards and protocols to the SEIWG for adoption as DoD-wide standards for AT/FP systems and equipment.

**4.14 RTCA** [<http://www.rtca.org>]

*Scope:* RTCA, Inc. is a private, not-for-profit corporation that develops consensus-based recommendations regarding communications, navigation, surveillance, and air traffic management (CNS/ATM) system issues. RTCA functions as a Federal Advisory Committee. Its recommendations are used by the Federal Aviation Administration (FAA) as the basis for policy, program, and regulatory decisions and by the private sector as the basis for development, investment and other business decisions.

**4.15 Underwriters Laboratories, Inc.** [<http://www.ul.com>]

*Scope:* Standards for safety. UL also has major standards activities that support listings for a variety of Burglar Alarm hardware. UL has a number of Standard Technical Panels (STP's) to supervise their ANSI –accredited standards efforts. Many of SIA members have UL listings for these Burglar Alarm standards.

**See Appendix E for a Summary of UL Standards Activities**

**5 Other Issues**

**5.1 Global Markets**

In the current climate, an increasing number of governments and businesses are realizing the economic interdependence of markets and the importance of standards to the success of the international business. The European Community has already acknowledged the benefits of consistency on standards issues and the Asian markets are also increasingly using standards in their products to compete in the U.S. and around the world.

The emergence of new national participants and powerful regional alliances may increase the resources available for the creation, implementation and testing of international standards. However, U.S. standards developing entities need to recognize that regional alliances will become an important factor in standardization. It is therefore, necessary to monitor the activities of these groups and cooperate with them in international activities.

**5.2 Consortia**

There is a growing concern about the various types of "industry" standards on which a consortium has reached agreement. Customers and consumers of all types of standards face additional confusion as to what to use, when, and how to select the proper "standards" for their needs. It is incumbent upon SIA to proactively interact with consortia in order to make the most effective use of consortia and formal standards activities.

**6 Standards Tactics**

Despite the increasing economic importance of standards, there is widespread ignorance about how the process works, what it does, and the advantages (and disadvantages) of the system, as it exist today. This is also a growing level of misinformation in the literature available on the subject, which causes confusion and

delay. If the standards processes and products are not understood then it is likely that they will be less effective.

## **6.1 Marketing**

There is a need to develop a marketing strategy overall that will provide for broad participation at both the End User and SIA Member levels. There is a large opportunity in SIA Standards that is unrecognized. The SIA Standards program is an extremely useful tool for members to develop technologies from which feedback can be obtained as well as a venue from which user requirements can be obtained. An infrastructure that lends itself to short time to market would also be of value to the SIA members.

The overall push should show the “profit relevance” of these activities to all participants. This would require some things such as:

- Develop a SIA Standards General Marketing Brochure that appeals to:
  - Government / End User
  - SIA Member
  - CEO/CTO/CFO Executive Summary (Roadmap would be additional collateral) – this piece would be the short enough and provide peer to peer pitches with additional quotes from customers
- Develop a similar information piece that could be picked up by the trade press.

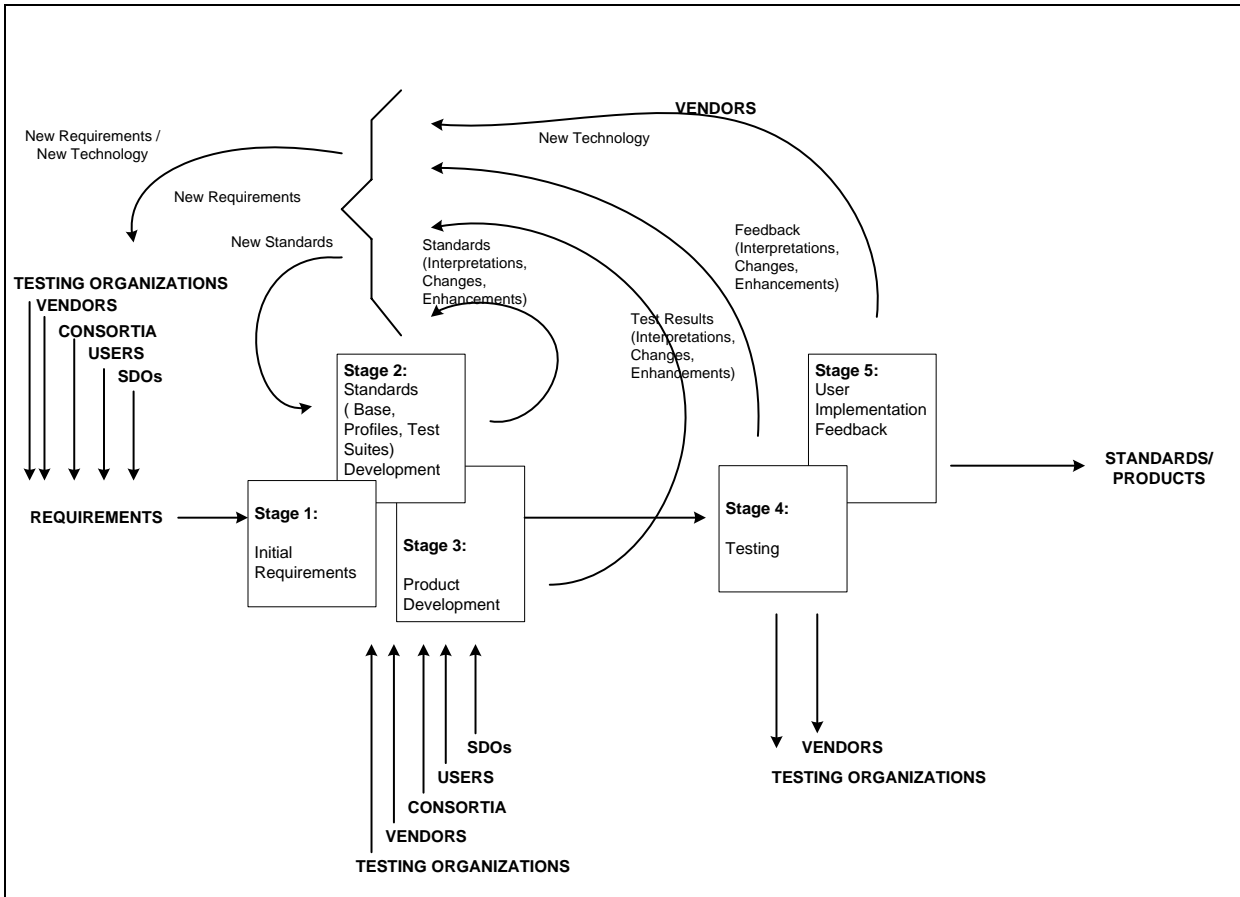
## **6.2 Government Affairs**

There is a need in SIA Standards for knowledgeable people from multiple agencies to represent their agencies' (DOD, DOE, DHS, DOS, DOC) requirements in SIA Standards development activities. SIA's Government Affairs can build awareness in the SIA Standards activities as well as aid agencies in identifying their needs and requirements. The awareness should be raised at a high level to address the concepts of standards and the value proposition for the end user as well as at the lower levels; such as the application specific area. Another area in which SIA Standards will be of value is with the growing demands of procurement and procurement via standards.

## **6.3 SIA Industry Groups**

The proposed reorganization of the SIA Industry Groups and the formation of the IAC are viewed favorably. Mechanisms have been in place for the sharing and initiation of activities.

# Appendix A - Standard Life Cycle



## Appendix B - ASIS Guideline Summaries

**Business Continuity Guideline:** A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery: A guideline outlining a series of interrelated processes and activities, including readiness, prevention, response, recovery/resumption, testing and training, and evaluation and maintenance, that will assist in creating, assessing, and sustaining a comprehensive plan for use in the event of a crisis that threatens the viability and continuity of an organization.

**Chief Security Officer Guideline:** A guideline that addresses the key responsibilities and accountabilities, skills and competencies, and qualifications for an organization's senior security executive.

**General Security Risk Assessment Guideline:** A seven-step process that creates a methodology by which security risks at a specific location can be identified and communicated, along with appropriate solutions.

**Private Security Officer Selection and Training Guideline:** A guideline that sets forth minimum criteria for the selection and training of private security officers, which also may be used to provide regulating bodies with consistent minimum qualifications.

**Threat Advisory System Response Guideline:** A guideline to provide private business and industry with possible actions that could be implemented based on the Alert Levels of the Department of Homeland Security.

**Workplace Violence Prevention and Response Guideline:** A guideline to offer useful ways to maintain a safe and secure work environment through such means as identifying, evaluating, and controlling potential hazards and conducting employee informational training.

### **In Progress:**

**Pre-employment Background Screening Guideline:** A guideline to aid employers in understanding and implementing the fundamental concepts, methodologies, and related legal issues associated with the pre-employment background screening of job applicants.

**Information Asset Protection Guideline:** A guidelines to offer general protection advice (collection, storage, dissemination, and destruction) for an entity's information assets, including proprietary, classified, and marketing materials, etc.

**Physical Security Measures Guideline:** A guideline to assist in the selection of appropriate physical security measures including defining risk levels, implementing an integrated set of physical security measures, and devising policies and procedures related to security incidents, access control, monitoring systems, lighting, security personnel, audits and inspection, etc.

## Appendix C - CSAA Standards Activities

### ***ANSI/CSAA CS-V-01-2004.XX Alarm Verification and Notification Procedures (version July 16, 2004)***

This standard has been prepared under the direction of the Security Industry Standards Council (SISC) members with the participation of Central Station Alarm Association (CSAA) members, Security Industry Association (SIA) members, National Burglar & Fire Alarm Association (NBFAA) members, ASIS members and Canadian Alarm Association (CANASA) members. This standard is to be used by alarm monitoring facilities and by state and local units of government in their development of consistent administration criteria for alarms. New technologies and successful efforts to reduce false alarms have led to this standard. This standard, adopted by the various states and local units of government, recognizes the life saving benefits monitored security and fire alarm systems provide. The intent of this standard is to achieve increased efficiencies by reducing costs and eliminating wasteful efforts associated with potential false alarms.

***(CSAA.GOT1) - Glossary of Terms (January 1996)*** The Central Station Alarm Association (CSAA) has created this Glossary of Terms used in the alarm industry as an aid to avoiding confusion because many terms are misused or may be confusing. The definitions reflect the meanings of the terms used in the CSAA Standards that have been developed, that are in the process of being developed, and that are in the process of being pre-pared to become ANSI standards by the CSAA.

## Appendix D - NFPA Standards Activities

### ***BSR/NFPA 730-200x - Guide for Premises Security***

The industry's first-ever guide for exterior and interior security features, *NFPA 730: Guide for Premises Security* addresses security in all occupancies from residential dwellings to large industrial complexes. Uniform guidelines help you assess vulnerability and design appropriate security plans.

Provisions describe construction, protection, and occupancy features and practices intended to reduce security risks to life and property. Topics covered include:

- General requirements and facility classifications
- Security vulnerability assessment
- Exterior security devices and systems
- Physical security devices
- Interior security systems
- Security planning
- Measures to control security vulnerabilities in educational, healthcare, and other facilities

The Guide also addresses protocols for special events, and the responsibilities of security personnel. (Approx. 88 pp., 2006)

### ***BSR/NFPA 731-200x - Standard for the Installation of Electronic Premises Security Systems***

*Installation of Electronic Premises Security Systems* is the first Standard developed primarily to define the means of signal initiation, transmission, notification, and annunciation, as well as the levels of performance and the reliability of electronic security systems.

Requirements cover every step of security equipment installation, with provisions for the application, location, performance, testing, and maintenance of physical security systems and their components. Detailed chapters are included for:

- Intrusion detection systems
- Electronic access control systems
- Video surveillance systems
- Holdup, duress, and ambush systems
- Testing and inspection

Rules address the protected premises from the property line to the interior of the premises. *NFPA 731* also references or incorporates provisions from applicable UL, SIA, and other standards. (Approx. 43 pp., 2006)

## Appendix E - UL Standards Activities

UL-2034	Carbon Monoxide Alarms, Single & Multiple Station
UL-521	Heat-automatic fire detectors, Marine
UL-268	Smoke - Automatic Fire Detectors, Marine
UL-38	Emergency Alarm Manual Pull Stations
UL-2034	Gas and Vapor Detectors and Sensors
UL-1484	Gas Detectors, Residential and Recreational Vehicles
UL-1110	Gas and Vapor Indicators, Electric, Marine
UL-1110	Combustible Gas & Vapor Indicators, Marine
UL-268	Signal and Fire Equipment and Service
UL-521	Heat Detectors for Releasing Device Service
UL-464	Audible Signal Appliances, General Signal
UL-1480	Speakers
UL-1638	Visual Signal appliances
UL-464	Audible Signal Appliances
UL-38	Boxes, Manually Actuated
UL-38	Boxes, Coded
UL-38	Boxes, Non-coded
UL-268	Detectors, Automatic Fire
UL-268	Signal & Fire Alarm Equip. & Service Fire Gas Auto Det.
NFPA Stds.	Flame-automatic Fire Detectors
UL-521	Heat-automatic Fire Detectors
UL-521	Heat-automatic Fire Detectors accessories
UL-521	Tubing and Compartment units
UL-268	Smoke-Automatic Fire Detectors
UL-268	Smoke-Automatic Fire Detectors Accessories
UL-268 (A)	Smoke Detectors for Special Application
UL-346	Extinguishing Attachments
UL-539	Single and Multiple Station Heat Detectors
UL-217	Single and Multiple Station Smoke Detectors
UL-217	Commercial Residential Multiple Station Smoke Alarms
EN54	Fire Detectors & Alarm Equipment Classified International Req
UL-521	Heat Actuated Devices for Special Applications
UL-1971	Signaling Appliances and Equip. for the Hearing Impaired
UL-1638	Signaling Appliances for Fire Protective Signaling
UL-1468	Switches, Pressure
UL-1069	Hospital Signaling and Nurse Call Accessories
UL-1069	Hospital Signaling and Nurse Call Equipment
Main	Alarm System Units
Main	Alarm System Units Certified for Canada - Component
UL294	Access Control Units
UL294	Access Control Units-Component
UL294	Access Control Units

UL294	Key Management Systems
UL1610 & UL1635	Central Station Alarm Units
UL1610 & UL1635	Central Station Alarm Units-Component
ULC-S304-M88/UL1635	Central Station Alarm Units-Certified for Canada
ULC-S304-M88	Central and Monitoring Station Burglar Alarm System
UL634	Connectors & Switches
UL634	Connectors & Switches-Component
ULC/ORD-C634	Connectors & Switches-Certified for Canada
ULC/ORD-C634	Contacts & Switches
ANSI/SIA CP-01-2000	Control Panels, SIA False Alarm Reduction
UL636	Holdup Alarm Units
UL639	Intrusion Detection Units
UL639	Intrusion Detection Units-Component
ULC-S306	Intrusion Detection Units Certified for Canada
ULC-S306	Intrusion Detection Units Certified for Canada - Component
ULC-S306	Intrusion Detection Units
UL606	Linings & Screens
UL609	Local Alarm Units
ULC-S303	Local Alarm Units Certified for Canada
ULC-S303	Local Alarm Units
ULC-S304	Miscellaneous Burglar Alarm Devices
ULC-S306	Intrusion Detection Unit Component
ULC-S318	Power Supply Units
UL365/UL1023	Police Station Alarm Units
ULC-S303-M91/ULC S304-M88	Police Station Alarm Units Certified for Canada
UL603	Power Supplies for Use with Burglar Alarm Systems
UL603	Power Supplies for Use with Burglar Alarm Systems-Component
C603-M88	Power Supplies for Use with Burglar Alarm Systems-Certified Canada
UL1076	Proprietary Alarm Units
UL1076	Proprietary Alarm Units-Component
UL1076	Proprietary Alarm Units-Certified for Canada
UL1076	Proprietary Alarm Units
UL365/UL1023	Sounding Devices
ULC-S525/ULC-S303	Sounding Devices
Standard	Category
UL1037	Antitheft Alarms & Devices
UL1037	Retrofit Kits for Use with Specified Antitheft Alarms & Devices
Planning to Withdraw	Attack Resistant Doors, Type 1, 2, or 3
NIJ Standard 0108.01	Ballistic-Resistant Protective Materials
Federal Register	Breath Alcohol Ignition Interlock Devices
UL752	Bullet-Resisting Materials
NIJ Standard 0101.03	Body Armor
UL752	Bullet-Resisting Metals & Plastics

UL752	Miscellaneous Bullet-Resisting Materials
UL752	Bullet-Resisting Glazing Material
UL752	Bullet-Resisting Glazing Material-Component
UL752	Bullet-Resisting Tellers' Fixtures
Main	Burglar Alarm Systems
Main	Burglar Alarm Systems
Main	Burglary-Resistant Electric Locking Mechanisms
UL1034	Burglary-Resistant Electric Locking Mechanisms
UL1034	Burglary-Resistant Electric Dead-Bolts
UL1034	Burglary-Resistant Electric Door Strikes
UL1034	Burglary-Resistant Electric Door Strikes-Component
UL1034	Burglary-Resistant Electric Locking Mechanism Accessories
UL1034	Burglary-Resistant Electromagnetic Locks
UL972	Burglary Resistant Glazing Material
UL972	Burglary Resistant Glazing Material - Component
ULC-S332	Burglary Resistant Glazing Material
UL972	Impact Resistant Film
UL983	Camera Units, Surveillance
UL1981	Central Station Automation System Software
UL1981	Central Station Automation System Software
Main	Detention and Correctional Facility Equipment
Planning to Withdraw	Detention and Correctional Facility Electrical Equipment
ANSI/BHMA A156.23-1992	Electromagnetic Locking Mechanisms
UL294	Special Locking Arrangements
UL294	Special Locking Arrangements-Recognized Component
UL294	Special Locking Arrangements Certified for Canada
CAN/ULC-S533	Special Locking Arrangements Certified for Canada - Component
Main	Homeland Security Equipment
UL1037	Handgun Cases
UL1637	Home Health Care Signaling Equipment
UL1023	Household Burglar Alarm Units
Standard	Category
UL1023	Household Burglar Alarm System Units Certified For Canada
Subject-C1023	Household Burglar Alarm Units
Main	Locks
Main	Combination Locks
UL1034 & UL768	Combination Lock Accessories
UL768	Combination Locks, Group 1
UL768	Combination Locks, Group 1R
UL768	Combination Locks, Group 2
UL768	Combination Locks, Group 2 - Component
UL768	Combination Locks, Group 2M
UL768	Combination Locks, Group 2M - Component

Main	High Security Electronic Locks
Subject 2058	High Security Electronic Locks
Subject 2058	High Security Electronic Locks
Subject 2058	High Security Electronic Locks, Type 1F
Subject 2058	High Security Electronic Locks, Type 2
UL437	Security Container Key Locks
UL437	Locking Cylinders
UL437	Locking Cylinders - Component
ULC-S337 & ULC/ORD-C887	Time locks
UL437	Cabinet Locking
UL437	Door Locks
UL437	Door Lock Accessories
UL437	Locks for Safe Deposit Boxes
UL437	Locks for Safe Deposit Boxes - Component
UL887	Delayed Action Time Locks
UL887	Delayed Action Time Locks - Component
IEC 60900/ASTM F1505-94	Insulated & Insulating Hand Tools
Subject 1964	Fire Fighter Rescue Tools(Listing)
NFPA 1936	Fire Fighter Rescue Tools(Classification)
UL140	Relocking Devices
UL140	Relocking Devices for Safes
UL140	Relocking Devices For Heavy Vault Doors
UL140	Relocking Devices for Light Vault Doors
Planning to Withdraw	Repackaged Security Equipment
Main	Safes and Chests
UL291	Automated Teller Systems
UL291	Automated Teller Systems- Component
CSA No. 22.2 No 950-M89	Automated Teller Systems Certified for Canada
Standard	Category
UL786	Key-locked Safes, Class KL
UL687	Materials for Use in Burglary-resistant Safes and Chests - Component
UL771	Night Depositories
UL771 & UL687	Night Depository Systems
UL1037	Residential Security Container
UL687	Tool-resistant Safes, Class Deposit
UL687	Tool-resistant Safes, Class TL-15
UL687	Tool-resistant Safes, Class TL-15X6
UL687	Tool-resistant Safes, Class TL-30
UL687	Tool-resistant Safes, Class TL-30X6
UL687	Torch- and Tool-resistant Safes, Class TRTL-30
UL687	Torch- and Tool-resistant Safes, Class TRTL-15X6
UL687	Torch- and Tool-resistant Safes, Class TRTL-30X6
UL687	Torch- and Tool-resistant Safes, Class TRTL-60X6

UL687	Torch-, Explosive- and Tool-resistant Safes, Class TXTL-60X6
Main	Household Fire Alarm Units
UL985	Household Fire Alarm Units
CAN/ULC S545	Control Units and Access-Household System Type Certified Canada
CAN/ULC S545	Household Fire Warning System Units
UL3044	Surveillance Closed Circuit Television Equipment
UL608	Vault Doors, Burglary Resistant
UL608	Vault Panels, Burglary Resistant
UL680	Vault Ventilating Ports
UL680	Vault Ventilators, Emergency
UL-2017	Emergency Alarm Equipment
UL-2017	Emergency Alarm System Accessories
UL-2017	Emergency Alarm System Control Units
UL2017	Process Management Equipment
UL864	Signal & Fire Alarm Equip & Service Accessories (Releasing Device Equip)
UL864	Signal & Fire Alarm Equipment & Service (Releasing Device CU.)
UL864	Signal & Fire Alarm Equipment & Service (Releasing Device)
UL60950	ITE Power Supplies for Alarm Systems
UL2017	Signal Appliances - Residential Water Hazard Entrance
UL2017	Signal Appliances - Signal System Units
UL1480	Speakers - General use
UL2017	Signal Appliances - Miscellaneous
UL464	Signaling Equipment
UL864	Signal & Fire Alarm Equip & Service (Control Unit, Systems)
UL864	Emergency Communication and Relocation Equipment
UL864	Signal & Fire Alarm Equip & Service (Control Unit Accessories, Systems)
NFPA72	Fire Alarm Replacement Parts
UL1481	Signal & Fire Alarm Equip & Service (Power Supply Units)
UL864	Signal & Fire Alarm Equip & Service (Smoke Control System Equipment)
UL1730	Signal & Fire Alarm Equip & Service (Smoke Detector Monitor & Accessories)
UL1711	Signal & Fire Alarm Equip & Service Component (Speakers and Amplifiers)
UL1711	Signal & Fire Alarm Equip & Service Component (Speakers and Amplifiers)
UL632	Signal & Fire Alarm Equip & Service (Transmitters, Elect Actuated)
UL864	Signal & Fire Alarm Equip & Service Magnetos
UL864	Signal & Fire Alarm Equip & Service - Portable Time Recorders
UL864	Signal & Fire Alarm Equip & Service - Miscellaneous Devices
UL864	Signal System Control Units and Accessories, Marine
UL681	Bank Burglar Alarm Systems
UL681, UL827	Central Station Burglar Alarm systems
UL681, UL2050	National Industrial Security Systems
UL681	Mercantile Burglar Alarm system
UL827, UL1076	Residential Monitoring Stations
UL827, UL1076	Proprietary Burglar Alarm Systems

ULWY	Residential Burglar Alarm Systems
UL681	Manual Holdup Alarm Systems
UL681	Semiautomatic Holdup Alarm systems
NFPA71, 72	Central Station Protective Signaling Services
NFPA 72, 72A	Local, Auxiliary, Remote Station & Proprietary

INTENTIONALLY BLANK