SIA STANDARDS ROADMAP 2015

The SIA Standards Committee's Plan for Security Standards and Emerging Technologies

SIA
SECURITY INDUSTRY ASSOCIATION

Mission Statement

The mission of the Security Industry Association (SIA) Standards Committee is to develop and promote the use of technology and application standards for the security industry; provide education and publication services for standards; and work with other standards organizations to promote interoperability for the overall benefit of industry stakeholders and customers.

The *SIA Standards Roadmap* describes the strategies for achieving the mission and enhancing stakeholder participation.

Foreword

Much has changed in the security industry since the SIA Standards Committee published Roadmap 2.0 in 2011. To cite but a few of the most significant developments:

- The industry is the midst of a wholesale embracement of IP technology.
- As a result of the “new convergence” brought on by the Internet of Things, the industry faces new standardization challenges related to connectivity and security.
- Industry specifications continue to develop new profiles with different standardized integration paths for manufacturers, integrators and end users.

Roadmap 3.0 addresses these realities, reaffirms the SIA Standards mission and more closely ties the efforts of the committee to the constantly emerging technology landscape.

In Case You Missed It

In 2011, SIA adopted a new strategic plan which included a focus on increased resources and member engagement. Under new leadership, the Standards Committee elected chairs and introduced Standards Subcommittees to enhance the opportunities for members to engage and interact within the security industry. SIA Standards is not only known as a developer but also known for its contributions in the industry to advocate, educate, and to be a harmonizer of standards and interoperability.

The following year marked the release of the Open Supervised Device Protocol (OSDP^{TM}) version 2.1.5 specification. OSDP^{TM} is a communications protocol that allows card readers and devices to interface with control panels and other security management systems. Other benefits of OSDP^{TM} include interoperability and solution capabilities for high-end encryption as required in federal applications.

One of the priorities of the committee in 2011 was to release actionable standards that were implementable and widely embraced by the industry. Progress would be measured through effective demonstrations of interoperability or "plugfests." In 2012, the OSDP^{TM} Interoperability Demonstration showed how an early version of OSDP^{TM} promoted interoperability between multiple access control vendors—and in 2014 this exercise morphed into the first SIA OSDP^{TM} Plugfest at ISC West. Hundreds observed the growing number of manufacturers that utilize SIA OSDP^{TM}. Adding even more business value, this event also showcased the SIA Open OSDP^{TM} Test Tool, a piece of software which emulates an OSDP^{TM} peripheral device or control panel. This allows manufacturers of OSDP^{TM}-compatible equipment to test their products against the specification for compliance and facilitates integration of equipment between different vendors.

Over the past three years, the SIA Standards Committee has developed a number standards and application papers dedicated to standards and technology, including the SIA Cloud and Mobility Whitepaper and the SIA Digital Video Handbook. The Cloud and Mobility Whitepaper created by the Cloud and Mobility & Internet of Things Working Group serves as a vision blueprint to provide definition, to model reference architecture for the cloud-based security application, and to outline several cloud and mobility candidates for standardization. Meanwhile, the Digital Video Handbook serves as a guide to practitioners looking to achieve maximum video quality for various applications of digital video through proper system design.

Standards harmonization efforts resulted in a signed memorandum of understanding with ONVIF in 2014, a collaboration toward further development of IP-based interoperability standards. SIA Standards also remained well-aligned with long time partners such as the Central Station Alarm Association (CSAA) and the Electronic Security Association (ESA), and contributed to various standards programs. Other industry efforts included a collaboration with *Security Systems News* to provide webinars on emerging technologies impacting the security industry. SIA also collaborated with the Smart Card Alliance on projects relating to federal standards and guidelines for physical access control systems.

While SIA Standards has not yet created a formal Standards Education program, we have taken advantage of the SIA Education @ISC program to deliver numerous standards-driven sessions. The Committee continues to strengthen the use of sponsors and deliver educational sessions on interoperability nationwide through travel roadshows and educational seminar like those of IP Video Surveillance Academy.

Our Continued Industry Standards Roles

In every standards community, there are many roles and stakeholders: authors, publishers, educators, testers, manufacturers, integrators, users—and, not least, a public forum in which dialogue can take place. Building off of the success of the SIA Standards program since 2011, SIA will continue to lead the industry in the following standards activities:

Authoring new standards will continue to be a primary activity of the Standards Committee. We embrace both formal processes (ANSI, ISO/IEC, etc.) as well as informal or *de facto* standards recognition. As the industry and technology evolve, there will always be a need for new standards development, and we will remain at the forefront of this effort.

Publishing can be conducted apart from authorship and provides an independent value to the stakeholders, particularly when coupled with a review process that brings informal or *de facto* specifications to a wider audience. The prevalence of current *de facto* standards argues for a clearinghouse for industry norms that have no clear provenance. Publishing such standards under SIA auspices provides similar value to first-hand authorship.

Education is a constant need in our industry, and one that SIA recognizes as one of the "pillars" of value that we bring to our members. Many users, integrators and manufacturers have expressed the need for structured information on how to use and apply industry standards

Harmonization Advocacy among standards bodies is an important activity, both to the industry and its customers. Harmonization is about encouraging cross-participation by constituents of different standards bodies, where there are commonalities, to avoid unnecessary and burdensome conflicts in resulting standards. With multiple organizations now providing overlapping standards for security products, vendors and buyers must often make difficult choices between "families" of compatible products. Harmonizing standards would allow users to choose the products best suited to their needs. SIA will continue to advocate that standards be harmonized to the extent possible under their respective charters and do our part to ensure that information about all standards activities that affect our industry is disseminated through our outreach.

Emerging Technologies – Looking Ahead

The 2011 *Roadmap* served as a policy and planning document that described how we intended to execute our mission moving forward. The *Roadmap* guided the SIA Standards process as a whole as well as the activities of its subcommittees.

We found it important to look ahead again in the 2015 version of the roadmap at technologies for which the SIA Standards Subcommittees will provide guidance over the next few years. The insert maps these technologies with the activities planned within the SIA Standards subcommittees.

The Value of Standards

The ultimate value of standards is to improve the customer experience. This can mean many different things. A short list of benefits might include:

- More features, better competitive positioning
- Easier to use and install
- Simpler to integrate
- Easier to produce and maintain
- More reliable, less support
- Less expensive, better margins
- Nonproprietary, open architecture
- Better compliance with regulations

In addition to these particular benefits, standards also create "meta-benefits" for the industry as whole. The most important of these is the overall market growth that we believe is fostered by product interoperability and simplified integration. We also believe that these industry benefits include reducing barriers to entry and promotion of competition by establishing a level playing field for new product innovation.

The Value of Participation

The best way to realize these values is to participate directly in the standards process. Companies that take an active role in standards development are able to:

- Shape standards to make sure they meet customers' needs.
- Influence technology choices to ensure product compatibility.
- Understand the long-term direction of the industry.
- Learn what your counterparts are advocating.
- Avoid obsolescence.
- Gain credibility with partners and customers.
- Enrich careers through visible industry participation.

Being an active part of the standards process is an increasingly necessary aspect of global competitiveness, both for individual companies and the U.S. security industry as a whole. As a leading representative of the security industry's interests, SIA encourages all stakeholders to take an active role in achieving the goals of this *Roadmap.*

For more information on how to participate in SIA Standards, please visit us at http://www.securityindustry.org/Standards.

SIA STANDARDS
EMERGING TECHNOLOGIES ROADMAP

FirstNet

For more effective communication during times of crisis, the U.S. plans to launch an interoperable public safety broadband network dedicated to first responders. To ensure adequate spectrum, the FCC granted a single license use of 700MHz D block based on the wireless standard, Long Term Evolution (LTE). It will be imperative for the security industry to aid first responders with their mission critical tasks by ensuring installed technology can successfully access and operate on this dedicated frequency.

360 Degree Surveillance

Applications are available for certain use cases that stitch together multiple video sources to provide one panoramic view. The technology brings the same standardization issues as traditional digital video surveillance, the expanded field of view has ramifications in the field of video analytics, both for rules based and behavioral analytics.

The Internet of Things

The Internet of Things (IoT) will have a revolutionary impact in the physical security industry. Within a few years, this "new convergence" will drive big change in both physical and cyber security, along with a profound impact on automation. With IoT devices being network-capable, this means that they can be compromised if standard identity and authentication controls are not in place.

4K /Ultra HD Surveillance

4K cameras based on the Ultra HD standard with a resolution of 3840 x 2160 are deployed in media and entertainment. This 8MP format commonly referred to as the sweet spot for low-light performance and high resolution. The security industry should not only be prepared to address standardization issues for the camera technology but also those issues relating to data storage and deployment.

Frictionless Access Control

As enterprises continue to move towards efficiency, access to controlled areas, naturally without the user having to break gait will be an increased area of focus. Particularly in the emerging area of school security, where a high-level of security is vital. This can be achieved with long range biometrics, short-range radio frequency technology and mobile application systems interoperating.

Social Secure Spaces

Combining identities through social, business and enterprise networking platforms along with mobile technologies buildings can know who we are, why we are there and how to manage security practices based on standard rules about the identity of people and NPEs.

Emerging Technologies

Greening of Security – Sustainable Security Technology (POE, smart sleep technologies, reducing data proliferation).

2015 — 2016 — 2017 AND BEYOND

Intrusion – Security panels inside commercial and residential buildings already communicate to central stations using wireless networks; SIA Standards will ensure this equipment is capable of working in the designed network.

Cloud, Mobility and IoT – Data from connected devices could prove vital to first responders in emergency situations.

Digital Video – It is key to provide standards guidance for proper equipment performance. Another related standardization topic is how 360 camera feeds are handled through various video management systems.

Perimeter Security – 360 degree cameras can be useful for some large perimeter applications. SIA will work to ensure best practices and deployment standards are available. SIA will work to ensure best practices and deployment standards are available.

Cloud, Mobility and IoT– This subcommittee will explore the standardization challenges as cloud services and mobile devices are part of this larger IoT ecosystem. SIA Standards can work to ensure security devices provide the identity controls for connected devices are beneficial.

SNMP

SNMP – As these IoT devices are all network-capable, monitoring their services and health through a standard set of SNMP MIBs will be of importance to the security industry and network administrators that need to monitor all of these devices.

Digital Video – The digital video subcommittee can provide guidance on the deployment of 4K surveillance as well as become involved in development of standards for storage and tagging of this high resolution video.

Access Control and Identity – Leveraging their work with OSDP, this group can develop extensions to the standard which enables this end point of secure frictionless access control.

Cloud, Mobility and IoT – Due to the computing power and features available on such devices, the smartphone will become the credential. Ensuring that tried and true security standards are adaptable to this new environment of apps and secure elements on smartphones and harnessing all the capabilities of the devices (camera, motion sensor, fingerprint reader, etc…) will be a focus for this group.

Access Control and Identity – Identity is key to social spaces; the subcommittee will monitor collaborate with other organizations developing identity solutions. Additionally, this group will explore next-generation identity solutions and how they can be foundational for secure social spaces.

Cloud, Mobility and IoT – In these scenarios, the mobile device will likely be the device holding the identity credential or running the social application that the connected secured space is using.