A Lifecycle Framework for Self-sustaining Implementation of Smart Grid Interoperability and Cyber Security Standards

Introduction

Advancing Smart Grid interoperability and security through standards adoption fosters innovation and accelerates robust, secure and reliable Smart Grid deployments. This is achieved by lowering the barriers to entry for vendors; accelerating secure and interoperable product time to market; and ultimately lowering costs for consumers. With all the potential benefits associated with broad standards adoption it seems reasonable to institute a standards lifecycle framework to ensure the deployment of a robust and interoperable Smart Grid. Unfortunately, realizing the benefits of standardization requires more than just selection of a standard.

Several papers in circulation including papers developed by EnerNex[1] and EPRI[2] show that there are plenty of standards available. With so many available standards, why has the pace of adoption been slow? The answer is that the selection of a standard is but one aspect of a greater product lifecycle. Full realization of the benefits will require a shared government and industry focus on a common set of Smart Grid functions, and a standards lifecycle framework supporting those functions. The goal of this standards lifecycle framework is to align policy, standards development, product development and procurement actions to create a self-sustaining Smart Grid market. A successfully operating, self-sustaining Smart Grid product market is defined by public policy supported by standards that are rapidly adopted by product vendors seeking certification, and driven by utility procurement agents only buying products certified to those standards. The effect in the market place is that product vendors are incented to compete against each other to create products that are increasingly interoperable and secure. Within this context, it is clear that any approach needs to be comprehensive and cohesive.

Beyond the creation of a standards lifecycle framework, it should also be noted that the associated effects of validation, enforcement, certification and accreditation are missing or in need of additional support. Certification and enforcement are critical elements of the lifecycle. Certification defines test cases that clarify standards interpretation in products by vendors. In this manner, any ambiguity in standards interpretation is quickly identified and remedied in such a closed loop process. Without such a process, vendors will interpret standards differently and interoperability will not be achieved.

This holistic approach to standards adoption allows for a more inclusive stakeholder representation. Achieving increasing levels of interoperability and robustness will require a concerted effort by all stakeholders including regulators, government agencies, utilities, vendors, commercial organizations and standards development organizations. These interests can be represented through a look at the applicable development and adoption lifecycles and how these lifecycles intersect. Two of the most relevant lifecycles are the procurement lifecycle and the

---

[1] Smart Grid Standards Assessment and Recommendations for Adoption and Development, draft v0.82, Enernex for California Energy Commission, February, 2009

[2] EPRI Technical Report: Integration of Advanced Automation and Enterprise Information Infrastructures: Harmonization of IEC 61850 and IEC 61970/61968 Models, EPRI, Palo Alto, CA 2006. Product ID 1013802.

standards development lifecycle. These two lifecycles are significant in that they cover both the development of the products and standards and the adoption and enforcement of the standards.

Standards Development Lifecycle

The standards development lifecycle is the realization of an operational need through the articulation of the need, followed by the development of standards, certification processes, and implementation validation. The standards process is better served when the organizations needing to procure the products are involved in this needs development. In the case of Smart Grid, these organizations are mostly utilities. Needs are typically represented through business objectives, use cases and requirements. These needs should be the basis for both platform agnostic and platform specific standards development. The process for establishing and representing the needs through standards is well established and actively practiced in the utility industry.

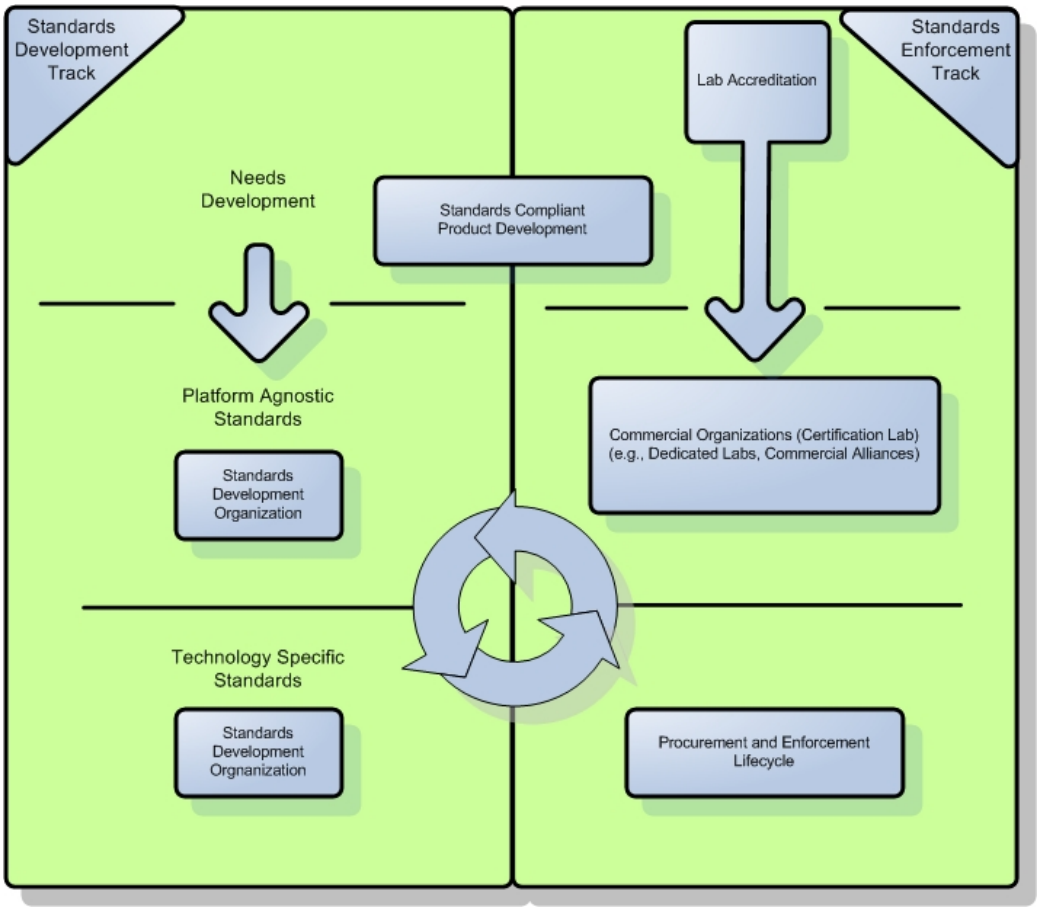


Figure 1: Standards Development Lifecycle

As shown above in Figure 1, the standards development lifecycle does not end with the development of the standard; this is simply the starting point. The standard needs to be implemented, validated and adopted. In most cases where standards are available but not widely used, the fault is not with the development of the standard but rather with the enforcement of the standard. Fortunately, normal competitive market drivers can be used to enable this piece.

Commercial organizations chartered to validate vendor implementations claiming to be compliant with a given standard are needed. These organizations play a critical role in the overall adoption of a standard. There are several commercial organizations currently providing certification services including ZigBee, HomePlug, Wi-Fi, and WiMAX. While the communications space is well served by these organizations, other domains have no commercial equivalent. As an example for the electric grid, there are no commercial security certification organizations. Utilities and other organization have developed security related needs statements and there are many security standards. Again, because there is no certifying organization the lifecycle is broken and the standards adoption becomes ad-hoc. Closing the loop with a certification process is a key to accelerating mature standards. In doing so, interoperability issues are discovered and regressed into the standards and the technologies. Without this closed loop process, interoperability is almost impossible to achieve on a broad system spanning multiple vendors.

Ultimately, adoption is achieved through the procuring organization. The utilities procure devices which extend and enhance the capabilities of the electric grid. Using security as an example, devices which are certified as more robust or more secure will be procured over competing devices offering less robustness or security. In this way, both the utilities and the vendors have the necessary incentives to foster a sustainable Smart Grid ecosystem.

Procurement-driven Standards Lifecycle Framework

The standards development process relies on the utility procurement lifecycle for enforcement. This lifecycle also provides other key touch points with the standards development lifecycle beyond the final enforcement of a given standard. These touch points give visibility and provide context for participation of various stakeholders. The utility procurement lifecycle, at its core, is concerned with procuring products which meet a given set of criteria. These criteria include regulatory policy, operational needs and business functionality as well as any standards compliance requirements. Regulators and standards organizations support the utility procurement process at several points in the lifecycle.

Regulators at both the state and federal level can provide four key roles in the lifecycle.

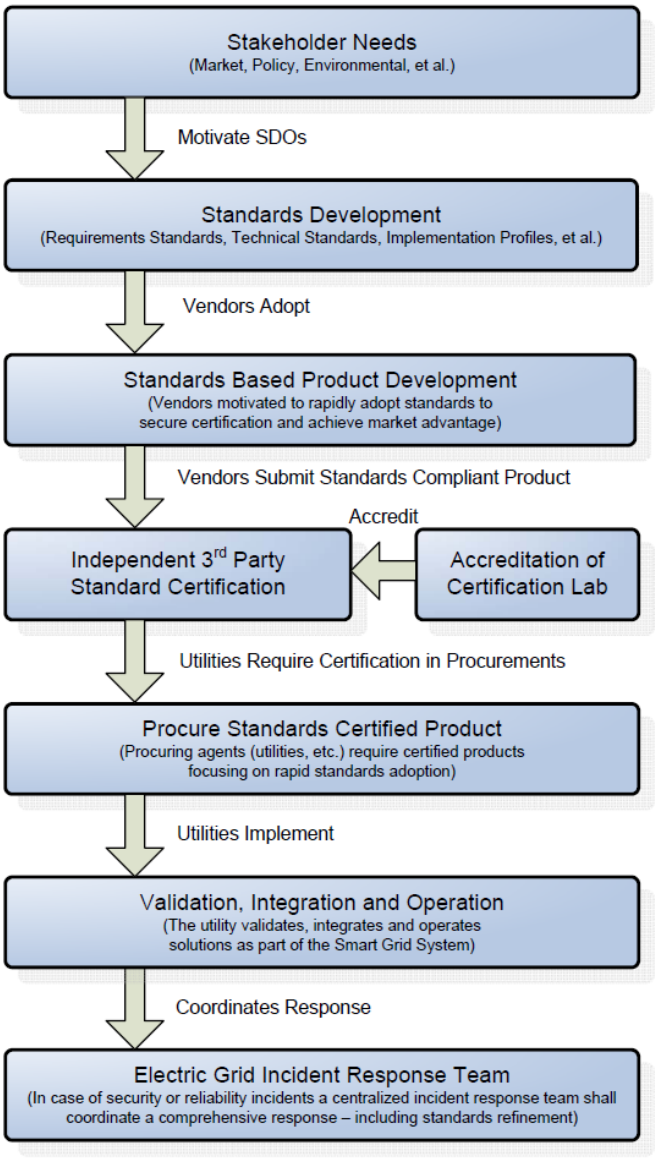
1. Define performance criteria in the context of meeting public policy objectives. California's "six criteria" for advanced metering is one example.
2. Provide oversight on utility expenditures and can enforce interoperability and cyber security standards adoption.
3. Ensure utility participation in a centralized incident response effort, and
4. Refine performance criteria based on continuous improvement.

Continuing with the security example, the procurement lifecycle merged with the standards development lifecycle to create a procurement-driven, cyber security standards lifecycle framework, as shown in figure 2 below, provides for a more consistent and more secure electric grid. In fact, enabling the entire lifecycle is the only way to increase security capability across the entire grid.

As part of this standards lifecycle framework, various industry stakeholders are able to define operational needs within the context of regulatory objectives. These needs are carried into standards development by utilities and vendors, evaluated for risk and used to seed various technology agnostic and technology specific standards development by standards development organizations (SDOs). The resulting standards can be recognized by federal and state regulators as meeting policy objectives. While standards development is often described as a long arduous

process, today Smart Grid development can benefit from the many existing standards available. The current potential to accelerate standards adoption is described in the "Smart Grid Standards Adoption - Utility Industry Perspective"[3] whitepaper.

Figure 2: Cyber Security Standards Lifecycle Framework



As this lifecycle framework continues, products are developed by manufacturers and software developers and evaluated for standards compliance certification by independent commercial labs, which have been accredited by a governmental agency such as NIST.

Devices/software are then procured by the utility for implementation. During the course of utility operations, performance information is gathered, new threats are identified, and knowledge is shared. Any security risk that is realized is responded to by a central incident response team which coordinates the response to the security event. Again, using the touch points across the standards lifecycle framework, the industry is able to transfer this security knowledge to the appropriate organizations.

Conclusion

Lower product costs, operational costs, and improved resiliency are significant benefits associated with standards adoption. In order to truly realize these benefits, the entire product lifecycle needs to be considered. There are two complimentary views of this lifecycle, the first view is the standard lifecycle, and the second is the procurement lifecycle. Certification is a key component of the lifecycle and without certification the cycle is broken and the ability to achieve broad interoperability is negated. These lifecycles should be unified by a comprehensive standards lifecycle framework described above. This more holistic view also clearly identifies the roles for key stakeholders' participation. For the energy sector, enabling and enhancing, this standards lifecycle framework should be the primary goal.

[3] Smart Grid Standards Adoption - Utility Industry Perspective v5.0, by Utility Smart Grid Executive Working Group and Open SmartGrid, March 23, 2009