NAME: Djenana Campara	GROUP REF.: D2
COUNTRY: Bosna & Herzégovine / Canada	PREF. SUBJECT: PS2 A
REGISTRATION NUMBER: 200	QUESTION N°: 2.2

Question 2.2: What are the future needs of cyber security regulations, standards, protocols, or procedures for the power industry?

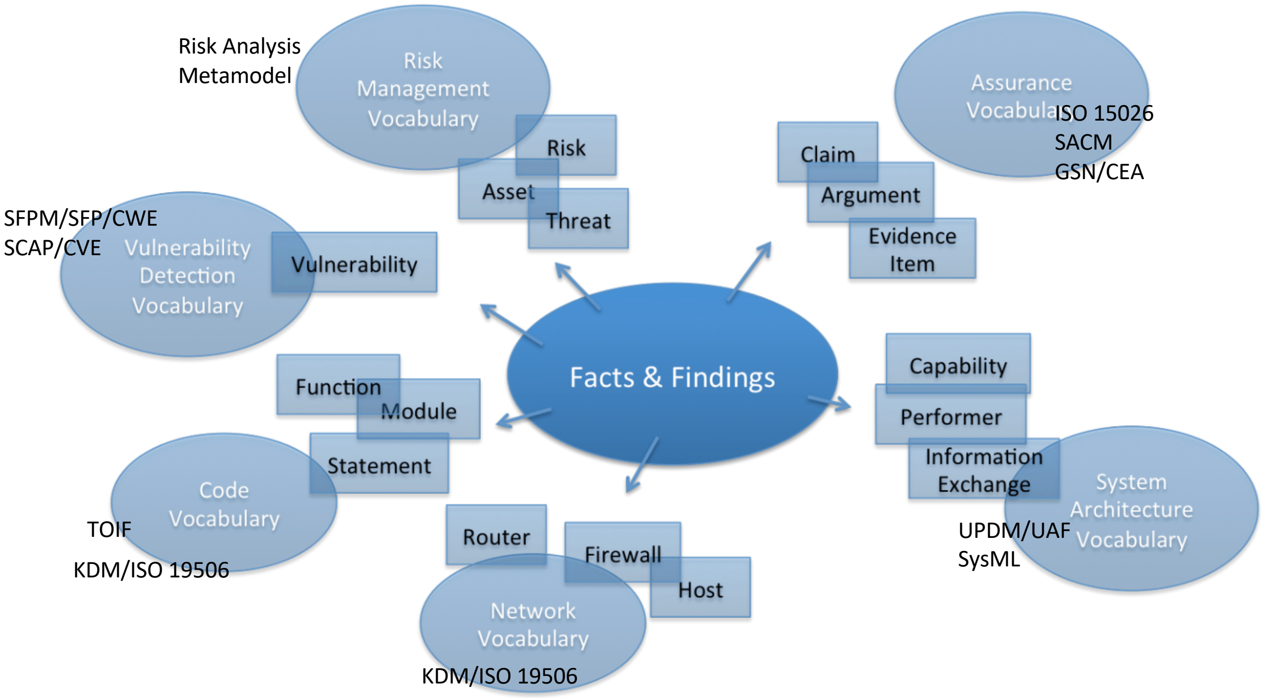
Have you ever wondered why attackers are repeatedly successful and defenders are constantly in reactive mode, trying to catch up? One of the reasons is a common understanding that attackers need to be "right one time" to break into a system while defenders need to be "right 100%" every time to defend the system. However, there is another reason, much more cynical: what makes attackers extremely efficient is extensive knowledge sharing while defendants are more focused on protecting their IP. In other words, attackers are willing to share not just their knowledge but also their tools and "weaponries", which become available to the individuals who are willing to launch attacks. As a result, an efficient ecosystem emerges, which amplifies the results of a few highly skilled attackers, and feeds larger number of less skilled but highly motivated criminalized attackers. Attackers may not be systematic in what they do, but they succeed in making their knowledge repeatable and shared. On the other hand, the defender community lacks efficiency in their knowledge collaborations due to too many barriers such as using and packaging knowledge in an effort to retain competitive edge, expand market space, enhance offerings, etc.

The only way for defenders to overcome this roadblock is to become more proactive and create an efficient technological ecosystem for collaboration where units of knowledge are formally presented in machine consumable and exchangeable form. The purpose of the ecosystem within the cybersecurity community is to facilitate the collection and accumulation of cybersecurity knowledge needed for assurance, and to ensure its efficient and affordable delivery to the defenders of cybersystems, as well as to other stakeholders. This way more systematic and comprehensive knowledge which is necessary for defence can be built in a timely manner via automation. The key to the creation of such an ecosystem is standardized open technical specifications. Many different security activities and disciplines can benefit from standardized expression and reporting.

Many current standards in the cybersecurity space are mostly process oriented, informal, relying upon subjective interpretation. As such, it is almost impossible to compare and accept results amongst organizations utilizing those standards (one example would be a risk assessment in cross-border power grid systems). Also, it needs to be pointed out that some of regulations are based on these informal standards. There are a very few exceptions where a standard is backed by a technical specification, one of them is The Technical Specification for the Security Content Automation Protocol (SCAP) (NIST SP 800-126) – very successful community driven technical specification that enables security automation from monitoring for and discovering known vulnerabilities to automatically issue remediation if a patch is available.

The need for highly automated solutions is recognized, however for successful acceptance and wide deployment of such solutions across the energy sector many challenges need to be addressed by the energy sector community – these challenges are centred around establishing a culture of security, assessing and monitoring risk, developing and implementing protective measures to reduce risk, managing incidents, and providing resources necessary to continuously sustain security improvements as new threats emerge and operating environments advance. In other words, the community needs to establish a set of technical standards in this field that organizations could utilize and certify their systems' compliance against. This mutually agreed to security requirements would ensure a consistent approach to confidence level measures for power systems of different origin/pedigree (e.g., organization, countries …) enabling utilities to quickly understand where to focus cyber-risk mitigation resources.

Instigating a paradigm shift in an industry is not a trivial undertaking. Technical standards are a good place to start. One community understands this – the Object Management Group (OMG) consortium develops standards as machine-consumable specifications. OMG System Assurance Task Force has been working on defining one of the cybersecurity ecosystems that is focused on risk and vulnerability analysis of OT/IT systems, and it could be further extended from a breadth and depth perspective.



However, one of the key requirements to any of these technical ecosystems is a better management of the engineering description of systems - as automation is often possible in the context of managed descriptions of systems as machine-consumable input.

Therefore, as a starting point some effort needs to be made across the community of equipment suppliers, utilities, transmission operators and regulators on the following:

- Standard set of Information and the corresponding templates documenting the system including OT and IT components,
- Common approach to impact characterization of the system
- Catalogue of Security Controls to choose from based on system-impact characterization and their individual effectivbnes/strength.