

# ICS/SCADA Cyber Security Requirements: A practical approach

Harsha Banavara, CSSLP  
Schneider Electric USA Inc.

According to Gartner Research, by 2020 about 25 Billion “things” will be connected to the internet (Internet of Things - IoT). This is a five-time increase from the 4.9 Billion “things” that were connected in 2015 [1]. With (Industrial Internet of Things) IIoT, the problems have just worsened as the threat surface area has increased exponentially. We in the ICS world have only been focused on performance and ease of use and knowingly or unknowingly compromising security.

## Security Requirements: The Why?

As we all know, there is nothing called ‘absolute’ security. However, building resilient systems and products is an effective way to mitigate a lot of these threats. One good approach is to incorporate Security Development Lifecycle (SDL) in an organizations offer creation process.

SDL was developed by Microsoft in early 2002. By 2004 they had made significant progress and decided to open it up to the outside world. In their own words, “SDL is a software development process that helps developers build more secure software and address security compliance requirements while reducing development cost. [2]”

There are 7 different phases in SDL as shown below: [3]



Training (blue in color) and Response (Orange in color) are more of supporting functions of SDL. Requirements through release (all green in color) can be described as the heart of the process.

Many people do not understand the need for security requirements or bypass them completely as they plan to conduct threat modeling, secure coding and pen testing of their product or application. Building a good product is like designing a house; both require a strong foundation. Good security requirements reduce the ambiguity for developers and ensure the results are consistent. It not only satisfies collecting needs of market place but also assist them in compliance.

## Security Requirements: The How?

We can broadly divide the process of coming up with security requirements into 3 stages;

1. Collection and Harmonization Stage
2. Filtering Stage
3. Prioritization stage

### 1. Collection and Harmonization Stage:

Inputs or sources of cyber security requirements can be classified into two types: Internal and External.

Under *internal sources* we may have:

- Voice of the customer (talking to internal teams, peers, customer facing representatives, customer engagement managers) - this can be very informal and subjective.
- Specifications and other invariants - more formal and objective in nature.

Under *external sources* we may have:

- Voice of customer (here we talk to the actual end user(s))
- External specification documents - generated by individual organizations
- Standards – generated by professional or industrial bodies
- Regulations – are mandated by law and can be both sector and country specific

One should also remember to take privacy requirements into consideration especially for those products or applications collecting personally identifiable information (PII) or protected health information (PHI).

Many Governance, Risk and Compliance (GRC) tools are available in the market that can be utilized to harmonize the standards and regulations. However, these tools are more catered to IT domain and highly regulated sectors such as finance, telecom and health care. It is rare to come across GRC tools with OT standards such as IEC 62443, 62351, NIST 800-82... already in them. This means we might have to manually import them into the tool thus adding extra time and resource to the project budget.

### 2. Filtering Stage:

All the standards that have been harmonized from the previous stage can be filtered based on the following criteria.

- Security Levels - We first need to understand where our product fits in the food chain. E.g. Is it a feeder meter? Is it a data logger? Is it a high end meter? Answering this question will help the organization understand what security level (such as low, medium, high) need to be assigned to it. If you are lucky, it might have already been decided in the standard itself!
- Regions, countries and sectors - If we know the region (such as EU, NA, APAC, EMEA) or country or sector that we plan to sell our product into, the organization can then concentrate its effort and resources on understanding the standards and regulations specific to those respectively.

However it so happens that most of the products these days are targeted to be sold in a number of countries. This is where the Pareto principle can be applied as the filtering criteria.

- Pareto Principle - Let's say a product is to be sold in 30 countries. If 80% of the revenues for this product is coming from just 20% of the countries (20% of 30 is 6), the organization can then focus on standards for only these 6 countries.

The output of this stage will be a master requirements specification document.

### 3. Prioritization stage:

Once we have the master requirements specification document (obtained at the end of previous stage) the organization needs to prioritize the requirements that can be implemented during the current release cycle/period. For this decision process to happen effectively, the organizations need to get a buy-in from all the relevant stakeholders. Prioritization can be done either by assigning high, medium and low with all the high priority requirements being implemented in the current release cycle OR Phase 1 requirements, Phase 2 requirements and so on.

The document that is obtained at the end of this cycle is the requirement specification document for that project and for that release.

### Conclusion:

Time has taught us over and over again (though we tend to repeat our mistakes) the earlier we introduce features to the development cycle, the more cost effective, and integrated are our results. Cyber Security definitely falls into this category. Secure requirements are a very critical part of the Security Development Lifecycle; it is essential to capture them upfront to ensure resilient products.

### References:

[1] <http://www.gartner.com/newsroom/id/2905717>

[2] <https://www.microsoft.com/en-us/sdl/default.aspx>

[3] <https://www.microsoft.com/en-us/sdl/process>