Executive Summary
Safety and security work hand in hand in the manufacturing automation arena. However, despite more and more sophisticated, frequent and costly cyber attacks, security still does not receive the same attention as safety. There is a growing need to elevate security awareness to the same level as safety – ensuring not only a safe, but also a secure manufacturing environment.

This paper explores the current differences in treatment of safety and security, discusses reasons for the different treatments and necessary steps to make security an equal player to safety in manufacturing automation.
Table of Contents

Executive Summary ................................................................................................................................................................1

Security Awareness ..........................................................................................................................................................3

Stronger Safety Emphasis .......................................................................................................................................3

Lagging Security Adoption .......................................................................................................................................4

Culture Mindset ..........................................................................................................................................................4

Standards Set the Tone ..............................................................................................................................................5

Government Involvement ..........................................................................................................................................6

Raising Awareness ....................................................................................................................................................7
Security Awareness

Let’s face it - security awareness today suffers from an identity crisis at manufacturing facilities across the globe. Big, small or anything in between, there is a general lack of understanding of security best practices.

With reported cyber attacks growing by 600 percent since 2010, according to NSS Labs, security awareness amongst manufacturing organizations needs to grow to the point where best practices end up ingrained in workers’ minds. That only makes sense as safety protects man against machines, while security protects machines against man.

Well-known within security circles, cyber security awareness in the manufacturing enterprise remains nascent and needs to bust out and go mainstream within each organization.

But where does that awareness begin and how can a manufacturer get started on the journey toward security?

A decade ago when most systems and business networks remained isolated from one another security was relatively simple. The enterprise stayed connected to the Internet, but focused on keeping its network up, running and protected, while process control and safety systems remained isolated and really did not have to worry about web connections. However, in the name of progress and efficiency, over time the two networks became interconnected – a true sensor to boardroom communication. By the early 2000s, and especially after September 11, 2001, security professionals saw that safety systems and the control network, previously unguarded from any kind of security measures, needed protection. But getting industry leaders to understand and grasp that concept was akin to rolling a boulder up hill.

Stronger Safety Emphasis

The idea of safety, on the other hand, generated a strong following especially after the disaster in Bhopal, India when a methyl isocyanate gas leak occurred on the night of December 2 and early in the morning December 3, 1984 at the Union Carbide India Limited pesticide plant leaving 3,787 dead and 558,125 injured, according to the India government.

In the years since Bhopal, process safety gained corporate importance and all manufacturers understood and respected all safety initiatives. Yes, manufacturers had to look at cost, but it was imperative that companies targeted safety. “Safety First” initiatives began in full force.

Process safety programs focus on design and engineering of facilities, maintenance of equipment, effective alarms, effective control points, procedures and training. It was, and still remains, a vital area to protect a company, its people and the surrounding area from any kind of potential disaster.

When it comes to safety, in order to contain a complex process (such as an oil/gas operation, refinery, chemical plant, steel plant, and automobile manufacturing to name a few), a manufacturer must design and implement management systems to:

- Understand the risk, which involves predicting problems, including predicting the risk of possible accident/loss scenarios, establish the appropriate design and the right layers of protection to control risk to a tolerable level
- Control risk factors every day, which involves controlling the original design by maintaining the established layers of protection and managing changes to the design using integrated management systems
- Analyze actual problems and determine weaknesses in the system, which involves identifying weaknesses in design and management systems and weaknesses in risk understanding through root cause analysis of actual problems (losses and near-losses)
Lagging Security Adoption

At a basic level, security follows those same set of guidelines. Why, then, are more organizations not implementing security into their daily mindset as they are safety? Some of the top internal reasons are: People, training, no real corporate mandate, and no business return on investment.

With security being the new kid on the block for process control, getting people to embrace how to integrate security into their everyday work life is an ongoing education process. Teaching workers to not plug a thumb drive into a computer before checking to make sure it is free of any virus is just one example.

In essence, the lack of ongoing training is also a culprit of not having automation professionals think of security on an every day basis. In safety, manufacturers have ongoing training and standard operating procedures, but in security, there is not enough emphasis placed on total security worker education.

To talk security, there must be a solid business proposition behind why a manufacturer would decide to make the investment. Bringing the idea up to the executive suite that security is more of a business enabler that keeps the network and system up and running and productive and not just an insurance policy is important to generate awareness and send a strong message out to the company. After all, security is going to be an ongoing expenditure, not a one time expense. Initially, there needs to be a risk analysis; what do you need to protect, what is the cost, what is the risk? Then there needs to be a way to quantify those numbers to assess the true benefit.

One of the advantages safety has that is not as prevalent in security is the concept of levels. With safety you have a very clear definition of a safety integrity levels. A system must meet SIL 1 which there is safety, but at a basic level, through SIL 2, SIL 3 and SIL 4, which would be the most dependable. While with security, there is the security assurance levels (SL) but it is not as prevalent and not commonly used throughout the industry. Manufacturers are not yet demanding a security protection that guarantees a SL 3.

Essentially, SL 1 would protect against a casual or coincidental attack and SL 4 would protect against an intentional attack using sophisticated means and extended resources. There are several values of SL within a solution. There is a targeted SL, which is where the user wants to be. Then there is an actual SL which is the user’s current status based on the existing implementation. There is a maximum attained, which is the maximum attainable SL with your current technology. The ideal situation is your targeted SL and your actual SL end up equal. SL levels are a part of the ISA99 security standard specification, which the international industrial control committee defined and accepted.

The problem is a SL is harder to determine than a SIL because of the ever changing threat scenario. The idea of a SL could be a positive in that it can make a security program much simpler. SL remains relatively new, however, and there will need to be some time for industry to let it marinate have it become part of its imbedded culture.

Culture Mindset

Technology will not fix a problem unless the right processes and the right best practices are in place. Technology will help enable people to make the right decision. But the security culture has to be on a par with the safety culture in order to protect against a cyber attack. Even with multiple technology protective layers, users need to enforce a strong security culture that reaches every level – and it has to start at the top.

That is evolving. In the early 2000s, people were starting to become aware of the entire idea of security and by around the 2005 timeframe, people talked about devices like firewalls that could protect them. But from that timeframe until now, there has been an increase in awareness. The thought process is changing about installing applications and users are starting to think more about security. Within the rank and file, you are starting to hear more about security. But is that happening quick enough?
It is easy to understand that manufacturers’ mindset is one of “we were never hit with a security breach before, so why should I install this complicated solution?” That mindset, while still common today, is starting to change - the idea of security being complicated and confusing is evolving into users knowing they need to learn the basics to protect themselves without breaking the bank.

One of the basic areas of uncertainty is manufacturers not understanding what they need to protect. While safety is very specific in what needs protecting, security has vast areas to safeguard. Attackers today are not necessarily looking for destruction. In quite a few cases, they were working in stealth mode in an effort to steal a company’s intellectual property.

Take “Night Dragon.” For well over two years, hackers were surreptitiously able to access oil companies’ systems and steal information including financial documents related to oil and gas field exploration and bid negotiations, in addition to operational details on oil and gas field production Supervisory Control and Data Acquisition (SCADA) systems. That attack emphasized security needed to be strong from the field all the way through the enterprise.

In Night Dragon, attackers compromised the perimeter security through SQL injection attacks on extranet web servers; targeted spear-phishing attacks aimed at mobile workers’ laptops, and took control of corporate VPN accounts. Several major oil companies were exploited by Night Dragon.

**Standards Set the Tone**

While it did take a long time to finalize them, safety often relies upon adhering to a company’s standards or industry standards like IEC’s 61508 and 61511. What is interesting to note and something most manufacturers should keep a vigilant eye on is just about 66 percent of safety instrumented systems in use today predate these standards. The same is true about security, as most control systems on the plant floor today were in existence long before cyber security became an issue.

While the U.S. implementation of IEC 61511 includes a “grandfather clause” for older systems, its insistence that operating companies ensure safety systems end up “designed, maintained, inspected, tested, and operating in a safe manner” leaves no room for less-than-rigorous safety system discipline. The same needs to be true for cyber security.

Even though the IEC Safety Instrumented Systems (SIS) standards are not legal requirements, their growing acceptance as descriptors of industry best practices means that non-compliance may have very real liability implications in the event of an incident. And in some regions and industries, compliance already carries the force of law.

Purposely non-prescriptive in nature, the IEC safety standards outline a holistic methodology for managing every stage of a safety systems' lifecycle from risk analysis and design engineering through operations, management of change and decommissioning.

Elements relevant to safety systems performance assessment include adherence to accepted risk evaluation and mitigation methodologies such as process hazards analysis (PHA), hazards and operability (HAZOP) analysis, and layers of protection analysis (LOPA).

Industry and government absolutely mandate safety. Practitioners have to adopt safety under penalties or potential fines if they don’t. In addition, in most cases standards are international, so in a global manufacturing environment manufacturers have to adhere to them. In theory, that means solid safety practices should be the same in the U.S. as they are in Europe, Asia, Australia, South America and Africa. Everyone understands the standards and everyone ends up measured against the same standards and there are penalties if they don’t meet those standards.
These types of standards for cyber security could help drive awareness and implementation. Security standards are a big deal. In a world where attacks are fluid and changing, standards give a level of consistency. They are something you can measure against, especially if they undergo an external verification and end up certified.

In the security environment, there are a number of evolving standards with some more prevalent than others like IEC 62443 (ISA99) and the WIB standard. The IEC 62443 (ISA99) series of standards has been in development for over 10 years and some parts are final. But there are other parts that are still a work in progress. The WIB standard, approved in 2010 is a standard that outlines a set of specific requirements focusing on cyber security best practices for suppliers of industrial automation and control systems.

Unlike safety, penalties for not adhering to security standards are non-existent, nor are there rewards for following them. Right now, with the exception of the North American Electric Reliability Corporation (NERC) in the power industry, there is no real reporting requirement for security as there is for safety. NERC requires companies to follow their standards and if not, there can be significant financial penalties for noncompliance.

**Government Involvement**

An overall movement toward reporting requirements could be coming in the form of the Executive Order 13636—Improving Critical Infrastructure Cybersecurity signed by President Barack Obama in February 2013. The Executive Order calls for the government to develop a voluntary framework to reduce cyber risks, recognizing U.S. national and economic security depends on the reliable functioning of critical infrastructure.

The National Institute of Standards and Technology (NIST) is in the process of drafting the framework and collecting comments to incorporate into the final draft to come out in February 2014.

In the end, just how can the government end up helping ensure the critical infrastructure remains secure?

Other than the framework, legislation has failed in the past. As a matter of fact, the Executive Order was in response to failed legislation. Government does have some options like not renewing operating permits until companies meet the requirements.

One fear from all ends of the manufacturing automation industry is there has to be some major incident, much like what happened in Bhopal, which will force companies to focus on and ensure their systems remain secure.

There have been quite a few incidents since 2010 – Stuxnet, which brought down an Iranian nuclear facility; Night Dragon; Flame, which was a cyber espionage malware program targeting Middle East countries; Duqu, a computer worm discovered in September 2011 and related to Stuxnet, and Shamoon, a virus that wiped out 40,000 hard drives at one oil company last August – that have come in and knocked off various networks and inflicted damage. While those incidents are just a few that raised awareness, the level of urgency to get manufacturers thinking about security on the same level as safety is lacking.

**Security Best Practices**

- Assess Existing Systems: Understand what you have and your exposure
- Document Policies and Procedures: Know what you have to do and when you have to do it
- Train Personnel and Contractors: Everyone has to be on the same page
- Segment the Control System Network: Zones and conduits
- Control Access to the System: Allow certain access privileges
- Harden the Components: Lock down functionality of components
- Monitor, Maintain System Security: Remain vigilant
Raising Awareness

Security protection is still in its infancy. But that does not mean the industry gets a free pass to ignore or hold off on securing their systems. The list of attacks and potential exposure goes on. Corporate data losses hit the highest levels this year since 2008 as companies need to improve data security strategies against a greater variety of more sophisticated IT attacks, according to one KPMG report.

Former Homeland Security Department Director Michael Chertoff told oil and gas industry executives in Houston this fall the top threat their businesses face is from cyber attacks. Most companies, he said, experienced some type of cyber security event whether they know it or not. Energy companies are clearly in the cross hairs of cyber criminals as more than 40 percent of all reported malicious cyber attacks in 2012 ended up directed at them.

The risk is there for everyone, but by following a guide of best practices, mandatory personnel training and starting the task of undergoing risk assessments, manufacturers big and small can ward off intruders to keep their systems up and running so they can remain a profitable enterprise.

The basic need for security is to:

- Increase plant safety
- Reduce downtime
- Reduce environmental and financial risk
- Meet regulatory compliance
- Connect the plant to the enterprise

In the end, manufacturers’ main goal is to make product and not deal with anything that throws them off track. That is why they have to demand security in the products they buy. They have to make those demands to force vendors to certify the products in an accepted standard, but be willing to pay extra for a more secure solution. After all, if a vendor invests in security for their products and no one will pay for it, then it will be a slow roll out. In safety, it is clear manufacturers will invest in higher safety compliant systems that have a SIL certified rating.

Security, like safety was, is a culture change. Technology must include security and people have to embrace it. Security must start at vendors and work its way through the product lifecycle and it has to continue once it gets up and running at the manufacturer. It is a huge job and the industry is moving in a positive direction, but there is a long way to go.

As Mike Baldi, chief cyber security architect at Honeywell Process Solutions said, “Safety requires investing in resources to achieve it. Security is exactly the same. Security takes money and people to manage it, to implement it and to verify it is working. It is an accepted practice for safety. It is becoming an accepted practice for security.”