The Industrial Internet’s Achilles’ Heel: Unmanageable Cyber Risk

Digital technology, IT, and the Internet have revolutionized process and factory automation, and industrial production at large. Whether the anticipated benefits of this development will outweigh its inherent risk will depend on how well cyber security and fragility issues are addressed. This is why we developed RIPE – a practical and cost-efficient cyber security program for industry to confront a problem that keeps getting bigger and bigger with every new network connection.

YESTERDAY
• IT is nothing but a nice to have add-on to automation technology. The major IT application on the plant floor is standalone PC-based SCADA.
• “Openness” of software interfaces is a declared design objective in order to facilitate easy integration with office applications. A textbook example is OPC.
• Targeted and complex cyber attacks against industrial facilities are unknown.

“Let’s be crystal clear: the worries over vulnerabilities in critical infrastructure to cyberattack have real validity. From 2011 to 2013, probes and intrusions into the computer networks of critical infrastructure in the United States went up by 1700 percent.”
P.W. Singer and Allan Friedman

TODAY
• Ethernet is the new fieldbus standard. Field devices are configurable via Web browser. Remote maintenance and condition monitoring via the Internet are ubiquitous.
• The modern factory depends on digital data flow. Digital technology and networks have become an enabling technology without which efficient production is no longer possible.
• Plant extensions and retrofits regularly get more expensive than planned – due to uncontrolled digital “growth” that can be understood and untangled only with unscheduled, painstaking effort.
• IT security controls such as antivirus and security patches fail in production environments. Almost every asset owner has experienced malware in the process network. Cyber attack campaigns like Stuxnet and Energetic Bear highlight the dimensions of a problem that continues to be neglected thoroughly.

TOMORROW
• Analog sensors and actuators are no longer available.
• By implementing the “Industrial Internet”, complete supply chains get digitally integrated. Digital super structures dominate the landscape from Smart Grid to manufacturing. The reliability and security aspects of the continuously “growing” (= disorderly rambling) structures are no longer fully understood by anyone.
• Customers, insurance companies, investors and government agencies demand verifiable cyber security in production environments. Cyber sabotage risk is regarded at least as important as privacy.

“Essentially all current digital designs in widespread use are far less dependable than almost any analog system of 50 years ago. We have made a giant leap backwards in surety while making a giant leap forward in controllability and function.”
Fred Cohen
It has become common knowledge: Flexibility and comfort of modern cyber technologies come with a security risk, and this risk increases proportionally with networking and the degree you depend on it. Everything that can be monitored and re-configured comfortably via the network can be compromised as easily. The impact is then not restricted to isolated automation cells because more digital integration also means more dependencies, more potential sources of trouble, and more widespread consequence in the event of failure or compromise.

“Cyber systems’ responsiveness to instruction makes them invaluably flexible; but it also permits small changes in a component’s design or direction to degrade or subvert system behavior.”

Richard Danzig

Technical point solutions like firewalls, antivirus and security patches don’t solve the problem. They fight symptoms but don’t cure the disease. Protecting single assets is not sufficient; at the end of the day it must be assured that the enterprise can leverage the full potential of its cyber ecosystem while minimizing systemic risk. The prerequisite for achieving this is a governance process featuring proactive planning and supervision — this is what the “planning and evaluation” stands for in RIPE.

This insight isn’t new. It is embedded in various cyber security frameworks such as ISO 27001, ISA-99/62443, and the NIST CSF. However all of these frameworks lack concrete, practical procedures that implement governance. These standards expected that asset owners invent individual cyber security plans rather than following a standard guideline. This is counterproductive for several reasons. You re-invent the wheel, because no matter which industry you are in, others have solved your problem already. You also forego comparability and scalability. But if you are responsible for multiple plants you will hardly prefer individual custom-built solutions over proven and efficient standards.

This is where the RIPE program comes in. It comes with standardized and concrete templates, checklists and reference architectures, developed and annually updated by internationally respected experts with decades of experience. Implementation may either be achieved by internal staff or external service providers. Introducing RIPE to a plant environment occurs step-by-step, reflecting given resources and security requirements.
RIPE Control Variables: Technology and System Architecture

**System inventory.** It’s a building block of every cyber security program, yet few enterprises have it. RIPE teaches how a solid hardware and software inventory can be produced and maintained.

**Network and data flow diagrams.** If you haven’t documented your network to the detail, you don’t really know it – and can’t protect it efficiently. RIPE shows how standardized, meaningful network and data flow diagrams can be produced without which full system understanding isn’t achievable.

**Plant planning and system procurement.** RIPE comes with detailed reference architectures for the design and configuration of networks, conduits, IT end devices etc. It also lists concrete cyber security criteria for system procurement that are essential to make cyber security sustainable.

RIPE data flow diagrams help plant engineers to understand the digital dependencies of system components

RIPE Control Variables: People, Policies, Training

**Policies and standard operating procedures.** Let’s face it: Security policies from IT don’t work on the plant floor. In consequence, everybody may do what they want to do – an untenable situation. RIPE comes with concrete policies and standard operating procedures for different user roles.

**Training.** Humans can only perform professionally if they know what they’re doing. RIPE comes with a comprehensive training curriculum that centers on efficiency.

**Workforce management.** Policies can only be audited if their target audience is personally known. The same is true for conducting training. Yet most businesses don’t keep a record of their contractors. RIPE includes procedures and concepts for establishing an effective workforce management process that solves the problem.
Do you have reservations about cyber security because too much hot air was produced under this label? We too! That’s why we based RIPE exclusively on verifiable and measurable facts and circumstances. As practiced in quality management for decades, periodic verifications and audits along with appropriate corrections are at the core of RIPE. Unless regulations require otherwise, you decide by yourself if audits shall be conducted by a third party or by internal staff.

“Moving beyond the Hamster Wheel requires practitioners to think about security in the same ways that other disciplines do – as activities that can be named, and whose efficiencies can be measured with key indicators.”
Andrew Jaquith

Based on annual audit results, The Langner Group produces an analytic report. The report includes an analysis of emergent vulnerabilities and their potential physical effects. The efficiency of the cyber security program is measured with performance indicators that can be compared to other plants and to an industry-wide benchmark. In regulated industries such as nuclear, RIPE reports also form the basis for documenting compliance.

The objective of RIPE is the implementation of a continuous improvement process as it is known from quality management. Current achievements form the basis for further improvement.

The result is sustainable cyber security and robustness that provides for resilience and reliability even with further integration and growing sophistication of threats. Not just as a bold yet unsubstantiated promise, but as demonstrated system capability. As an asset owner you get the confidence that your investment in modern automation technology won’t turn into an Achilles’ heel that puts business continuity and competitiveness at risk, and it allows you to face the prospect of future cyber regulation calmly.

“Security involves making sure things work, not in the presence of random faults, but in the face of an intelligent and malicious adversary trying to ensure that things fail in the worst possible way at the worst possible time... again and again.”
Bruce Schneier

Performance indicators measure the maturity of your cyber security program. They allow for comparison with other plants.
About Langner

The Langner Group is a cyber defense consultancy founded by Ralph Langner and Perry Pederson. Its European sister company (based in Germany) has a history of over 25 years.

Langner became globally known for a quick and detailed analysis of the Stuxnet malware. A summary that is regarded as the definitive reference on the subject is published as *To kill a centrifuge. A technical analysis of what Stuxnet's creators tried to achieve.*

Perry Pederson worked for the US Department of Defense, the Department of Homeland Security, and the Nuclear Regulatory Commission on cyber-physical security. In 2007 he lead the Aurora experiment where it was demonstrated by DHS that a cyber attack can destroy electric generators, threatening the reliability of the electric grid.

Langner’s several decades of international experience includes globally recognized milestone achievements in the analysis of highly complex malware and in identifying critical attack scenarios and the development of effective countermeasures. We have given advice to the White House, the US Senate, the Pentagon, the International Atomic Energy Agency, and many other organizations. We have designed secure industrial controllers and created process-based cyber security programs for asset owners.

In respect to the latter we focus on enterprises with multiple plants and facilities where scalability and comparability of cyber security programs are a priority. As strategic consultants our objective is not to sell as many man-days as possible but to establish effective collaborations with our clients’ internal teams.
To learn more about RIPE and The Langner Group
or to schedule a consultation appointment, get more information on the Web:

In the USA:
The Langner Group, LLC
1331 S. Eads Street #802
Arlington, VA 22202

phone:  +1 (571) 551 - 2998
mail: info@langner.com

In Europe:
Langner Communications GmbH
Kattjahren 4
D-22359 Hamburg

phone:  + 49 (40) 60 90 11 - 0
fax:  + 49 (40) 60 90 11 - 11
mail: info@langner.com

In the web >> www.langner.com <<

On Twitter >> www.twitter.com/langnergroup <<