The RIPE Framework

A Process-Driven Approach towards Effective and Sustainable Industrial Control System Security

Ralph Langner

Abstract

This paper outlines a novel approach towards industrial control system (ICS) security that is focused on effectiveness, scalability, and sustainability. Based on proven concepts from quality management, it is pointed out that risk management decision making is often mislead by insufficient cyber system understanding and lack of cyber governance, resulting in ineffective mitigation strategies. The foundation of an ICS framework is elaborated, consisting of eight different domains. This framework is called the RIPE Framework, for Robust ICS Planning and Evaluation. It is shown how such a framework lays the ground both for measurable cyber security capability and for identifying weak spots by establishing benchmarks and scorecards. It is also highlighted that such a framework-based approach to ICS security provides economies of scale that can result in significantly improved efficiency compared to risk management exercises that approach every single plant as a completely unique universe.

The Inconvenient Truth behind Unsuccessful Cyber Security Campaigns

Cyber security campaigns by and large can be characterized by the biblical phrase "the spirit is willing, but the flesh is weak". Despite outspoken political will to protect national critical infrastructure against cyber attacks[1], the private sector's response leaves many observers frustrated. Though representative surveys are not publicly available, this author estimates that more than 95% of asset owners in critical infrastructure don't have a single dedicated full-time staff member responsible for the cyber security of industrial control and safety systems, and have a budget for ICS security that is less than one percent of the overall budget for process IT and industrial control system equipment and services. For the private sector at large, ICS security is not a priority[2].

It's not difficult to explain why. Cyber attacks against industrial control system installations are extremely rare, making it appear like a waste of company resources to protect against them. The generally accepted policy is to accept the risk and only after having seen a significant successful attack at home within the same industry, then figure out how to protect[3].

In the control system space this is a risky gamble. If any nation suffers a significant cyber attack against its critical infrastructure, or a large corporation against one of their multiple plants, recovery will be much more difficult than from physical attacks where damage may be severe, but contained. In contrast, cyber attacks are scalable; they can trigger follow-up and copycat attacks. Whereas explosives can only be used once, digital weapons can be copied and re-used, and a single breach head such as a contractor's remote access can be exploited to compromise multiple targets[4]. For the cyber-physical domain, the lead time to protect against such

[1] As an example, the Obama administration repeatedly identified the cyber security of critical infrastructure as a top national priority. To quote executive order 13636: "The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront." (http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity)

[2] This statement should not be misunderstood to suggest that things are any better in the public sector; indications are that they are not.

[3] A variation of this attitude is to turn to the government for help in case of disaster. The CEO of a large electrical utility once expressed the expectation to the author that the government should implement some kind of cyber Delta Force team that can be called to the rescue.

[4] Infiltration of a high-profile vendor got in the spotlight after the reported breach of Telvent, a company selling SCADA software to the energy sector (http://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent/). Remote access by a single vendor may expand to well over 1,000 systems in critical infrastructure; for an example see http://www.garymintchellsfeedforward.com/feed-forward/2012/3/26/whats-up-with-ge-intelligent-platforms-1.html.

ripple effects will be way too short. In control system environments that usually run 24/7, configuration changes can only be applied during maintenance outage windows, which often occur only once per year for a limited number of days. Any effort to expedite matters would involve extra downtime, thereby advancing an attacker's intentions. This would suggest that a useful contingency plan is a priority, enabling control system installations on a large scale to prepare against predictable attacks in ample time. Unfortunately, generally accepted methods for such contingency planning, along with appropriate resource allocation for execution, are missing on a large scale. A related deficiency is the lack of forensic readiness; presuming that a failure will happen, its root cause may require prolonged forensic efforts, and ultimately even be lost for the sake of re-establishing operations in a rush.

If this seems shortsighted, it shouldn't come as a surprise. The objective of corporate risk management is not to minimize risk, it's to minimize cost. The default reaction of the security industry, the media, or government officials to witnessing critical infrastructure operators widely ignoring cyber insecurity was to revert to scare tactics and doomsday scenarios[5]. But if the prospect of cyber attacks against industrial control and safety systems becomes confusable with science fiction, spiced up with drama and exaggeration, one should even less expect it to be discussed in board meetings. This paper advocates a different course of action that is centered on effectiveness, scalability, and sustainability. It also argues that it is a waste of resources to invest in security controls without having established security capability first. It is detailed how security capability can be achieved and sustained, and how such capability can be turned into results, leveraging economies of scale.

How Ineffective Risk Management Decisions Are Made

From a business perspective, the rationale for risk management is to minimize the overall cost associated with cyber risk. In this framing, risk exceeding accepted risk (= excess risk) should only be reduced to the extent that mitigation cost remains lower than the projected cost of consequence associated with excess risk, moderated by likelihood of occurrence. Projected cost of mitigation has a direct effect on risk management decision making – it's the focal point where return on investment (ROI) comes in. Anything on top of that would appear as a waste of company resources; at least in a short-term perspective. The solution is then to raise the level of accepted risk, either by explicit decision or by conclusive behavior, sometimes even blithely as accepting risk appears to be an immediate cost-saver[6]. The basic subject that is managed by risk management is not risk itself but the organization's perception of risk worth mitigating. Risk management can ultimately turn into risk ignorance as accepted risk doesn't cease to exist; it's just that based on more or less complex math, the organization has decided to no longer worry about it.

The objective of corporate risk management is not to minimize risk, it's to minimize cost

An evident problem is that the cost of mitigation is known and the consequence from failure to mitigate is speculative – it is a cost that could theoretically materialize in an undetermined future, assuming worst-case scenarios[7]. A closer look at cost estimates for cyber attacks shows that cost of consequence tends to be overblown, sometimes driven by interest[8]. Other shortcomings of risk management fidelity are home-made. If major *internal* factors affecting risk assessment and the fidelity of risk mitigation are unknown, undocumented, ignored, ungoverned, or carry a high degree of variability, it may even turn into black magic which is how it is

[5] An example is US Department of Homeland Security Secretary Janet Napolitano's assertion that *a "cyber 9/11" could happen imminently* when talking at the Wilson Center on January 24, 2013 (http://www.reuters.com/article/2013/01/24/us-usa-cyber-threat-idUSBRE90N1A320130124).

[6] Corporate decisions to raise accepted risk in respect to ICS security are rarely overt and documented, which can cause concern because they often stay under the radar of corporate oversight.

[7] The concept of risk implicates a predictive timeframe. See Langner, R. & Pederson, P.: *Bound to fail: Why cyber risk cannot simply be "managed" away.* Washington/DC, 2013 (http://www.brookings.edu/~/media/research/files/papers/2013/02/cyber%20security%20langner%20pederson/cybersecurity_langner_pederson_0225.pdf)

[8] See Florencio, D. & Herley, C.: *Sex, lies, and cyber-crime surveys.* (http://research.microsoft.com/apps/pubs/default.aspx?id=149886) Also: Lewis, J. & Baker, S.: *The economic impact of cybercrime and cyber espionage.* (http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf)

perceived by many process and control system engineers anyway[9]. Unfortunately, that's the reality on most plant floors: Cyber system attributes, component interaction, and configuration practices are rarely documented, repeatable, addressed with measurable concepts and procedures, or even verifiable. This is the major reason for the well-known philosophy "*never touch a running system*"[10]. It is sometimes complemented by a testing regime based on the idea *"never test for an error condition that you can't handle"*.

To the extent that the accuracy of ICS risk assessments can be challenged because of incomplete and inaccurate information on system configuration details, and risk mitigation efforts are positively known to be limited because of a lack of capability to control essential parameters of internal procedures such as remote access or use of removable media, risk management can turn into self-deception. Such considerations, not necessarily conscious, contribute to predominant risk management decisions to fix only the bare minimum, which often is, ironically, the biggest waste of time and money. Sporadic and anecdotal deployment of security controls tends to be completely inefficient[11] and manifests an approach of moving from crisis to crisis, fighting the last war rather than the next one, to use a simile from the military domain[12]. Risk management as a method to *prioritize* mitigation efforts and budget allocation will necessarily fail in cyber environments that are poorly documented and loosely governed. Factoring in only acquisition cost of security controls rather than overall lifetime operational cost, and assuming perfect performance of such controls, is a common pitfall that further contributes to poor effectiveness. In order to prioritize security efforts for maximum effectiveness, one must first have established a baseline cyber security capability.

Sporadic and anecdotal deployment of security controls tends to be completely inefficient

Applying the Simple Rules of Quality Management

Fortunately, the seeds of an improved cyber protection lie close at hand. In the very same environments where cyber security is slighted, it is not uncommon to see quality management being practiced with skill, passion, and determination. What applies to a production process' output can also be applied to its cyber security posture, thereby laying the foundation for a systematic cyber security governance process with measurable effectiveness.

A first lesson from quality management is that process capability[13] is a prerequisite for product quality. It is pointless to aim at any product quality level, no matter how high or low it may be, until process capability has been established – the capability to arrive at the target quality level repeatedly and reliably. The path to get there is well established: First, document system properties and procedural guidance. Then implement a governance process for determining the accuracy of system documentation, and for the compliance of procedural execution. An analogy can even be found in control system 101 by referring to the accuracy of sensor input and reliability of actuator output.

---

[9] Engineers usually are not sympathetic to regarding propositions as real that involve prediction but cannot be proven by experiment.

[10] The state of affairs as depicted here is common knowledge on the plant floor. A common excuse by control systems engineers is "historical growth" – which seems to have become the accepted technical term to express that software and network traffic have turned into quite an undocumented mess. "Growth" is a synonym for unstructured development; it suggests a transcendental power (like nature or stochastics) as a driving force rather than planning and governance. On many plant floors, and even in the development department of some vendors, cyber is thought of as a non-essential add-on to "real" (analog) process functionality. This has resulted in an attitude where the biggest concern about cyber is that it could somehow "get in the way" of the control system or process engineer. Predictably, the resulting mental blockade impairs judgment: "This is impossible to understand, so it must be impossible for it to happen."

[11] For example, it can be debated if investments in industrial firewalls buy their money's worth of risk reduction for installations where perimeter perforation by remote access and/or contractors' laptops remains uncontrolled, or where the ruleset configuration of such firewalls is left to guesswork and idiosyncrasy rather than consistent policy and verification.

[12] It has even been argued by Jason Healey that cyber defense activities at a nation-state level are event-driven rather than proactive. See Healey, J. (ed.): *A fierce domain: Conflict in cyberspace, 1986 to 2012.* CCSA, 2013

[13] Process capability is a basic concept of quality management, or Statistical Process Control (SPC) to be more specific, and is used on an everyday basis on thousands of plant floors around the globe. The basic idea is that the statistical variance of measured quality output must be reduced to a certain extent in order to reliably arrive at a product of a given quality, no matter how high or low that quality may be. – A more fundamental paradigm from Total Quality Management (TQM) that is applied in this paper is to view quality – and cyber security – as a process rather than a system state.

If accurate documentation of system properties is not available, then system understanding is blurred, and the result is unreliable risk assessment. If procedural guidance is implemented only partially or incorrectly, the effect of security controls is lost. Blur and loss can easily combine to form a situation where actual security posture is much lower than the assumed -- and paid-for -- security posture. To use an analogy from building security, one should imagine a security expert who has to work with an incomplete and inaccurate site plan, and who has no means of checking if any demanded fences, gates, locks, and surveillance cameras are actually implemented and operated properly. Everybody recognizes that for the building security expert, security cannot be achieved. For ICS security, we expect the people in charge to cope with very similar constraints.

No system or procedure can be verified against itself. Just like measurement, verification involves comparison. In the process of verification, which may include walk-down inspections, lab experiments, and audits, documentation content is checked against empirical reality in a procedure that must deliver observer-independent results[14], making sure that security concepts and controls are more than wishful thinking. Of course, even fully accurate documentation may present a misleading picture if it is incomplete, and documentation on all specific aspects of a given system is of little value if it is inaccurate. Table 1 lists the basic quality attributes that can be used to measure cyber security capability[15] and notes how these are commonly blurred.

Attribute	System Properties (Think: Sensors)	Procedural Guidance (Think: Actuators)
Verifiability	Documentation on system properties is verifiable by walk-down inspection or experiment Blur example: System documentation claims that a component (such as a PLC, or software application) is "secure" without detailing why and how	Conformity to procedural guidance documents is verifiable by audit Loss example: Security policies that contain language such as "as soon as possible" or "as appropriate", resulting in unpredictable execution that cannot be audited
Completeness	System architecture models are complete, verified by walk-down inspection or experiment Blur example: Systems used on the plant floor (including mobile devices), or software applications running on computers, are not listed in the system inventory	Written procedural execution items (policies, SOPs, guidelines) are provided for all procedures that otherwise leave room for variation that could affect the cyber security posture Loss example: Security policies are produced and enforced for employees, but not for contractors
Accuracy/ Compliance	Walk-down inspection or experiment verify that documentation of system properties is accurate Blur example: A system is configured differently than documented, for example in respect to network connectivity, software version, security patch level etc.	Audits verify that procedure execution is compliant with written policy Loss example: Mobile devices are configured or used in a manner that violates policy; backups are not performed according to policy; network segregation (firewall rules) is not configured according to policy

Table 1: Cyber Security Capability Attributes

Documentation is of little use as a static artifact; it only provides a transitory snapshot of system state as it once was, and of intended policies and guidance that may well have been ignored for a long time. Documentation within the context of quality management is only useful if it is embedded in a continuous governance process that determines the accuracy and completeness of system documentation, and measures and enforces compliance to procedural directives. Such a basic cyber governance process is illustrated in figure 1.

[14] This approach is also used in well-established conformity assessment standards such as ISO 9001.
[15] Other requirements or principles from quality management, such as consistency, could be referenced as well, but they don't play the essential role that the three attributes mentioned here do.

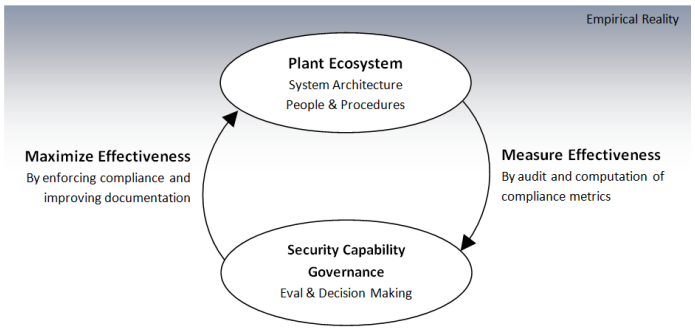

Figure 1: Basic Cyber Governance Process

Different from existing capability maturity models where the characteristic that a process is "managed" is identified as a top-end activity[16], in the approach outlined in this paper cyber governance is a foundational principle that must be mastered before it makes sense to start improving other activities such as deciding on appropriate mitigation strategies.

Exactly What Needs To Be Governed?

There are eight domains of the plant ecosystem where variability undermines immunity to threats, threat response agility, and even the capability to survive legitimate configuration changes without major problems[17]. Each domain has an analog in the realm of process operations and control of the physical plant. To varying degrees of detail, each of the domains and associated documentation can be related to similar items that should already be in use for sustainable plant operations. The eight domains are:

1. System Population Characteristics

- *Operational analog:* Equipment and instrument list.[18]
- *Documentation:* A cyber system inventory, manifested as a database, stores information on hardware systems, the software running on those systems, network association, and configuration details.[19]
- *Impact on effectiveness:* A missing, incomplete, or inaccurate system inventory will result in insufficient system understanding, in being unable to identify systems that need security configuration changes, rogue systems etc. It will also render the network architecture model and dataflow model (see below) incomplete and inaccurate.

2. Network Architecture

- *Operational analog:* Piping and instrumentation diagrams.
- *Documentation:* A network architecture model, manifested as a set of diagrams with accompanying detail information for reference, identifies the connectivity options for specific endpoints and groups of endpoints.[20] It identifies which network-connected systems can talk to which other network-connected systems (without necessarily having a requirement to do so). An accurate and complete network architecture model is also an essential prerequisite in determining potential rogue or otherwise undesired network access options.
- *Impact on effectiveness:* Missing, inaccurate, or incomplete network architecture models obscure the risk of unauthorized network traffic, for example from systems in the office network, or through wide-area connections.

---

[16] Process capability as applied to software development and cyber security has sometimes been put into the context of maturity, resulting in capability maturity models. The most prominent example is the *Cybersecurity Capability Maturity Model (ES-C2M2)* by the Carnegie Mellon University (http://energy.gov/sites/prod/files/Electricity%20Subsector%20Cybersecurity%20Capabilities%20Maturity%20Model%20%28ES-C2M2%29%20-%20May%202012.pdf). This model uses *Maturity Indicator Levels* (MIL) to express the maturity of cyber security practices (incomplete, initiated, performed, and managed). Any MIL below "managed" would be considered "pre-RIPE".

[17] Unintended side-effects of well-meaning actions by authorized personnel account for the majority of cyber incidents on the plant floor. A prominent example is the 2008 cyber incident in the Hatch nuclear power plant in Baxley, Georgia where a legitimate software update of a computer system residing in the plant's business network by an authorized administrator caused a reactor scram (emergency shutdown). See the discussion of the incident in Weiss, J.: *Protecting industrial control systems from electronic threats.* Momentum Publishing, 2010

[18] Equipment and instrument lists sometimes include cyber systems, for example in the nuclear industry where such listing is mandatory, but often list only physical system attributes such as dimensions and weight.

[19] While the context is different, it should be pointed out that the latest version of the SANS Top Twenty Security Controls, Version 4.1, lists hardware inventory and software inventory at the very top. (http://www.sans.org/critical-security-controls/guidelines.php) It should be noted that producing and maintaining system inventories in the ICS space is much easier than in IT because the component density is an order of magnitude or two lower, and because system configuration stays comparatively static.

[20] Network architecture is usually documented in form of network diagrams. However, such diagrams often lack information on logical networks, VLANs, VPNs, firewall rules, network switch ACLs etc.

3. Component Interaction

- *Operational analog:* Process flow diagrams.
- *Documentation:* A dataflow model, manifested as a set of diagrams with accompanying detail information for reference, identifies the interfaces of digital components. For interfaces that have dedicated communication counterparts, such association is identified. Interfaces extend to non-IP networks, fieldbus, RS-232, and proprietary.
- *Impact on effectiveness:* Missing, inaccurate, incomplete dataflow models will inevitably result in failure to identify malicious compromise options and dependencies on other system components.

4. Workforce Roles and Responsibilities

- *Operational analog:* Workforce records of operations and maintenance personnel.
- *Documentation:* A workforce information database storing the identities, affiliation (staff or contractor), role-based physical and logical access and execution privileges, applicable policies and SOPs, and competence (training requirements, respectively) of all individuals that legitimately interact with industrial control and safety systems or process IT equipment. Interaction does not only cover operations as an end-user, for example in the control room, but extends to maintenance (including re-configuration), commissioning, and de-commissioning, and extends to remote workers and third parties.
- *Impact on effectiveness:* Poor workforce management will result in policies that are unknown to their addressees or cannot be enforced, users not having appropriate training, and contractors not being bound to policy.

5. Workforce Skills and Competence Development

- *Operational analog:* Training curriculum and records of operations and maintenance personnel.
- *Documentation:* A structured cyber training program (manifested in form of training manuals, presentations, or videos) is a requirement for staff members and contractors to perform their interactions with industrial control systems professionally and meeting the provisions of policies and SOPs. Training extends to the appropriate application of plant planning guidelines and system procurement guidelines (see below).
- *Impact on effectiveness:* Poor training will result in staff and contractors interacting with systems inappropriately and potentially insecurely.

6. Procedural Guidance

- *Operational analog:* Standard operating procedures used by operations and maintenance personnel.
- *Documentation:* Policies and Standard Operating Procedures for cyber, manifested as written documents, structure the activities that comprise legitimate and appropriate interaction with plant floor systems. Typical policy items are use of mobile devices (if any), mobile media, remote access procedures, and performing backups.
- *Impact on effectiveness:* Non-verifiable or non-audited policies will result in computer systems not being patched, staff and contractors using insecure mobile devices, mobile media, etc.

7. Deliberate Design and Configuration Change

- *Operational analog:* Plant planning and change management procedures.
- *Documentation:* Plant planning guidelines for cyber, manifested as written documents. Such guidelines contain advice on the topology and architecture of process networks, configuration of essential infrastructure services such as DHCP, NTP, and central backup sinks, authorized remote access options and products, or proper configuration and usage of virtualization technology.
- *Impact on effectiveness:* Poor quality or absence of plant planning guidelines will result in retrofits, reconfigurations, and new designs not meeting a unified, best-effort level of cyber security and robustness, thereby invalidating any previously achieved level of risk.

8. System Acquisition

- *Operational analog:* System procurement guidelines specifying physical and functional system attributes and properties.
- *Documentation:* System procurement guidelines, manifested as written documents, that specify which cyber security and robustness attributes industrial control and safety systems, industrial network gear, and process IT systems must have in order to meet an organization's quality criteria. Typical attributes covered are network resilience, access control and account management, system hardening, prevention of unauthorized software, and documentation quality. The idea is to turn cyber security and robustness into quality criteria that must be documented and met by vendors just like IP code[21]. The major challenge for a system procurement guideline is that it must be verifiable for compliance objectively and easily (i.e. by trained non-experts)[22].
- *Impact on effectiveness:* Failure to use system procurement guidelines, or using improper (non-verifiable or irrelevant) system procurement criteria, will result in systems getting procured and commissioned that don't meet an organization's cyber security and robustness posture and must therefore be supplied with add-on mitigation.

These eight domains can be modeled in a cyber security framework that I call the RIPE Framework. RIPE is an acronym for Robust ICS Planning and Evaluation. By integrating the domains and procedures of the RIPE

[21] IP code is an international classification identifying a hardware component's capability to withstand dust and humidity. It has nothing to do with networking and the IP protocol. IP code is specified in virtually any system requirement for the plant floor.

[22] This requirement is not fulfilled by the major published procurement guidelines, such as the *Cyber Security Procurement Language for Control Systems* by the Department of Homeland Security (http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/SCADA_Procurement_Language.pdf).

Framework into mainstream plant operations it is possible to emphasize the importance of effective cyber security to a well running facility, and to establish accountability for ICS security and robustness.

How To Use Framework-Based Metrics for Security Planning and Optimization

Measuring and maximizing security capability is a prerequisite for getting to the point where assessing the cyber security posture of a given installation is no longer rough guesswork that struggles with categorizing subjective assessment results as high, medium, or low, and where effectiveness of security controls is no longer wishful thinking. The following examples illustrate what RIPE metrics look like and how they can be used for planning and optimization.

RIPE System Inventory Quality	
SI.Quality:	Completeness and accuracy of the system inventory Computation: SI.Accuracy * SI.Completeness / 100
SI.Completeness:	Percentage of components listed in the system inventory based on total number of components as identified by walk-down inspection
SI.Accuracy:	Percentage of components listed accurately in the system inventory as identified by walk-down inspection

RIPE System Procurement Quality	
SP.Quality:	Completeness of system procurement guideline application and compliance of acquired systems Computation: SP.Completeness * SP.Compliance / 100
SP.Completeness:	Percentage of system acquisitions during last audit interval for which system procurement guidelines have been applied
SP.Compliance:	Percentage of system acquisitions during last audit interval for which systems proved to be compliant with system procurement guidelines

RIPE Training Program Quality	
TP.Quality:	Completeness of training program and compliance with training obligations and offerings Computation: TP.Completeness * TP.Compliance / 100
TP.Completeness:	Percentage of user roles relevant for industrial control systems and process IT, including contractors, for which a formal training program beyond awareness is established
TP.Compliance:	Percentage of users, including contractors, eligible or obligated for training actually finishing respective training sessions during the last audit interval

Metrics like these provide useful benchmarks and scorecards. For example, an organization with multiple plants will be interested in scoring their individual RIPE capabilities in the eight domains. The same can be done on a larger scale within and even across specific industries, resulting in empirical data that provides valuable insight in how different regions, organizations, or even industries approach ICS security and robustness. Figure 2 illustrates what such a comparison may look like. It compares two hypothetical plants within one organization. Two performance differences stand out: Plant B achieves a much higher score on system inventory quality, whereas Plant A scores much higher on plant planning guidelines. Since both plants are operated by the same organization, this would trigger questions about what causes the differences and if and how the outperforming strategies can be mapped to the respective sister plant.

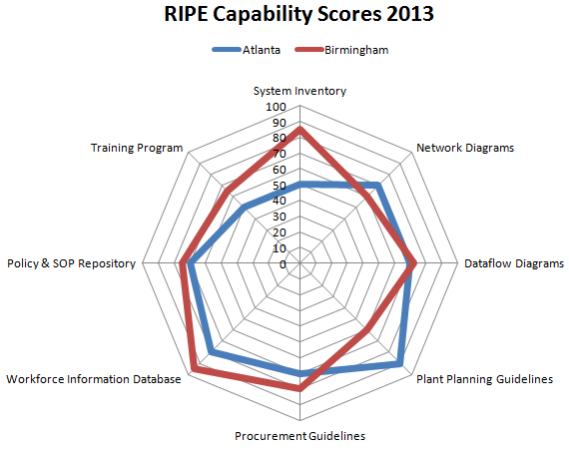

Figure 2: Comparing two plants in a spider web diagram

Aiming at higher RIPE scores in any domain establishes a direction for structuring ICS architectures and procedures, and also for allocating efforts and budgets. Beyond this, RIPE capability scores can be used for prioritization of efforts and budget simply by looking at specific domains that score low, and/or by looking at benchmarks derived from other plants or other organizations within the same industry (if available). Besides that, capability as reflected in RIPE scores can be put to other good uses that may not obviously be related to cyber security. One is to assure that cyber on the plant floor is governed and subject to compliance verification like other business processes[23]. Another is to provide operations and maintenance with the transparency needed to keep up with system understanding in an environment that's progressively more reliant on abstract digital technology.

The root problem of cyber insecurity and fragility is that more things can happen than planned

As with many other organizational processes, there is a risk that religious but thoughtless execution ultimately results in self-servicing bureaucracy that does anything but achieve its original goal. It would be quite counter-productive to focus the Basic Cyber Governance Process on continuous compliance assessment rather than on continuous improvement. The way to prevent this is to validate and improve the various items of cyber security documentation. For example, security policies and standard operating procedures must be validated and improved to better meet the minds and needs of the people who have to use them, without lowering security posture. System attributes in the system inventory must be validated and improved to delete attributes that proved without practical value, and to include new attributes that become necessary due to technical change.

Why Security Capability is a Precondition for Security Assurance

Security is a function of the degree of control that is exercised on the given system and its environment[24]. "Control" is expressed in the various technical and procedural restrictions that are enforced to limit manipulation of industrial control and safety systems to what is planned. In a system-centric view, without looking at externalities like threats, the root problem of cyber insecurity and fragility is that *more things can happen than planned* – i.e., unintended consequence can result from unplanned and unfavorable, and even from planned and well-intended events[25].

Control of a plant's cyber ecosystem has two dimensions: First, the extent to which ICS designs, configurations, network access options, operator procedures etc. are substantively restricted (= *substantive control*), and second, the extent to which such intended restriction is actually enforced and monitored (= *procedural control*, or program governance). The latter is expressed as security capability. Both dimensions taken together form a domain-specific security posture for every of the eight security domains mentioned earlier.

Security capability is a precondition for any reasonable level of security assurance[26]. For example, when looking at perimeter defense, in theory a firewall can offer more control than a router, a data diode[27] can offer more control than a firewall, and an air gap can offer more control than a data diode. All these progressive restrictions of network connectivity represent progressive levels of substantive control. But in real life, a firewall does not necessarily make an installation more secure than a router or a network switch if procedural control, or security capability, is ignored. It may have been (a) configured improperly without anybody -- other than potential attackers -- recognizing, (b) the organization might have missed one or more "hidden"

[23] If the general approach looks similar to Sarbanes-Oxley (SOX) compliance processes, this is not an accident. Whatever the reason for SOX may be, it can and should certainly be questioned why to have it for a lot of other areas but not for ICS security.
[24] To quote the definitive book on IT security metrics: "As nearly any serious security publication will tell you, *security is about control*" (italics in the original). Jaquith, A.: *Security metrics. Replacing fear, uncertainty, and doubt.* Pearson, 2007
[25] The same applies to safety.
[26] In the context of this paper, cyber security assurance is defined as protection against specific identified cyber attack vectors. Cyber security assurance does not claim to offer protection against novel, unidentified attack vectors. This is a difference to the concept of cyber robustness. See Langner, R.: *Robust control system networks. How to achieve reliable control after Stuxnet.* Momentum Publishing, 2011
[27] A data diode is a piece of network equipment or special-purpose gateway computer system with the capability to enforce unidirectional flow of information. For example, FTP file transfers can be limited to outbound-only.

connections between the process and business networks[28] that can invalidate the whole concept and utility of the firewall, or (c) the firewall may have been silently decommissioned by a control system engineer who experienced trouble when trying to remotely access systems in the process network for maintenance purposes[29]. It is discouraging to see how many asset owners (from management down to control system engineers) are satisfied with the idea to "have addressed the problem" of ICS insecurity by having invested in firewalls, anti-virus solutions, security patching regimes etc. without ever bothering to check their effectiveness. Perhaps the best example of illusionary security assurance is the popular misconception that an air gap per se would make an installation almost perfectly secure[30].

The relationship between substantive control and procedural control is illustrated in figure 3. An increase in security capability does not necessarily result in a proportional increase in security assurance (blue triangle). However, increasing capability can increase security assurance to some extent because an organization that monitors its environment and strictly enforces policies and procurement guidelines will automatically have a higher security posture compared to one that doesn't. On the other hand, any security assurance above the blue triangle is illusionary; expenditures for tight security controls above the achievable level of security assurance as determined by existing cyber security capability are a waste of money.

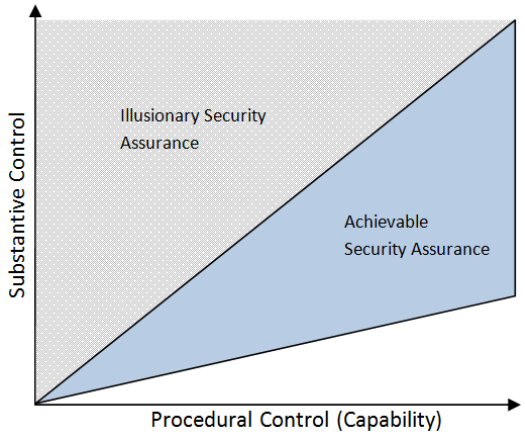

Figure 3: The relationship between procedural and substantive control

The amount of substantive control planned for a given environment is determined by a deliberate decision on the appropriate degrees of freedom in every given ICS security domain. Usually this decision is based on the idea of achieving a balance between convenience and cost vs. desired (or required, in case of regulatory pressure) level of security assurance. For example, many employees have already experienced the inconvenience associated with rigid password regimes, usually resulting in loosened security policies that aren't as restrictive but don't prompt employees to search for creative ways to circumnavigate security policy either. Procedural control, on the other hand, doesn't offer any operational advantage if loosened; it doesn't do any good if the accuracy, compliance, and completeness of procedural control is degraded.

High-Fidelity Identification of Vulnerabilities and Mitigation Options in Plant Context

As the examples given above illustrate, security assurance cannot be viewed as a property of a specific component or security control but must be viewed in context – in the context of the overall system design,

[28] "Hidden" connections are regularly discovered during thorough plant assessments. They are not limited to direct network access but can involve IPv4/IPv6 impedance mismatches, dual-homed computers, mobile media, and non-Ethernet connections.
[29] Network equipment that gets deliberately decommissioned (like firewalls) or spontaneously installed (like LAN, WLAN, and WAN interfaces) by authorized staff is a common problem on plant floors. It can be compared to intentional circumvention of safety mechanisms for better efficiency, which accounts for a substantial number of workplace accidents in industrial environments.
[30] Nobody learned that lesson better than the people responsible for the security of the Natanz Fuel Enrichment Plant in Iran during the Stuxnet attack. It can be speculated that when plant managers suspected a cyber attack at some point in time, they were assured by cyber security experts that this would be impossible because the facility was air-gapped.

configuration, and the people interacting with that system[31]. This is what makes vulnerability analysis challenging: High-fidelity vulnerability analysis cannot be limited to a component view but must use a system-centric approach, involving a synopsis of ICS security domains.

Discussion of ICS vulnerabilities is most often limited to the identification of buffer overflows in SCADA applications, deficient network resilience in PLC network interfaces, or lack of authentication features in industrial protocols. This component-level approach comes with the problem that the assessment of potential damage (if the vulnerability is successfully exploited) must rely on theoretical worst-case assumptions, which are often rejected as overblown by control system engineers who are intimately familiar with the specific purpose and function of such components. Leveraging the information from the system inventory, network architecture model, and dataflow models, a much more specific vulnerability analysis is feasible. This approach allows for the fact-based identification of *plant-level vulnerabilities*; vulnerabilities that will cause process disruptions, product manipulations, or destruction of equipment if exploited successfully. A major difference to component-level vulnerabilities is that while it is asserted that those *could* result in some kind of damage which is usually conceived referring to unlikely worst-case scenarios, exploitation of plant-level vulnerabilities *will* result in predictable damage that can be specified by referring to the characteristics of the given plant environment. Plant-level vulnerability analysis relates to potentially aggressive insider attacks because the insider threat is not just tied to legitimate system access but also to the deep system understanding that an insider may have. Proper system documentation makes such system understanding available for systematic analysis and thus for the design of advanced cyber defense solutions.

High-fidelity vulnerability analysis cannot be limited to a component view

Based on the RIPE Framework documentation, it is also feasible to determine which security controls yield the best mitigation for the cost – if implemented properly (as specified in mitigation advice). Mitigation advice will usually involve multiple security domains.

The decision which vulnerabilities require mitigation and which don't is the point where the concept of risk management may reasonably be applied – as a decision-making aid rather than a foundational methodology[32]. However, alternative strategies are possible and proven. For example, the decision how to mitigate identified vulnerabilities may also be policy-driven, as in the nuclear sector in the United States[33], or based on the concept of cyber robustness[34], or on the emerging science of cybersecurity[35]. No matter which security regime is preferred, within the RIPE Framework it is possible to arrive at generic protection profiles based on documentation templates that can be used to provide similar plant configurations with similar or almost identical cyber security assurance. Using such templates is feasible because of the static nature of typical ICS environments[36].

[31] This is a major difference to the safety realm where the safety integrity level (SIL) can be expressed for an isolated component using an ordinal scale from 1 (lowest) to 4 (highest).

[32] Contrary to common belief, the concept of risk is not the only paradigm for structuring cyber security efforts, and not even a particular attractive one. See Langner, R. & Pederson, P.: *Bound to fail: Why cyber risk cannot simply be "managed" away.* Washington/DC, 2013 (http://www.brookings.edu/~/media/research/files/papers/2013/02/cyber%20security%20langner%20pederson/cybersecurity_langner_pederson_0225.pdf)

[33] Cyber security for nuclear power plants in the United States is regulated by 10 CFR 73.54. It requires operators of US nuclear power plants to demonstrate that potential cyber attacks cannot result in radiological release – which basically requires asset owners to identify and fix plant-level vulnerabilities. The rationale behind this approach appears to be that no business-focused judgment about ROI of mitigation cost should interfere with the objective of arriving at installations where potential cyber attacks cannot result in disaster.

[34] Langner, R.: *Robust control system networks. How to achieve reliable control after Stuxnet.* Momentum Publishing, 2011

[35] Schneider, F.: *Blueprint for a science of cybersecurity* (http://www.nsa.gov/research/_files/publications/next_wave/TNW_19_2_BlueprintScienceCybersecurity_Schneider.pdf). It is worthwhile to point out that Schneider doesn't refer to the concept of risk in his groundbreaking paper.

[36] Compared to IT, ICS environments are extremely static since change takes place more within in a timeframe of years rather than months. The ideal configuration for ICS usually is the system state at commissioning time, throughout the lifecycle of the system, which often spans decades. This characteristic is consistent with the philosophy to *never touch a running system*: Systems that are never "touched" stay static throughout their lifetime.

How to Gain Cost-Efficiency from a Framework-Based Approach

A process-driven approach to ICS security will move asset owners from anecdotal and idiosyncratic risk management that restarts from scratch for every assessment, to systematically planned, measurable, and sustainable progress towards more secure and robust installations. From a business perspective, one of the most appealing aspects of the RIPE Framework is its emergent cost-efficiency. It is worth reflecting on why this is so.

RIPE improves all of the following:

Separating fact from interpretation. If security characteristics of a specific plant are documented properly and accurately, risk assessments and mitigation advice can be done on paper. This also means that third party experts can assess the security posture of a given plant without actually going there, by using the information that is documented and accessible. These external experts can be staff members in the company's headquarters, they can be independent consultants, or even members of a government agency. Depending on the size of the organization, independent entities staffed with domain experts and specialized advanced analytics capabilities may even be better qualified to analyze less obvious vulnerabilities and give advice on how to best mitigate them. Advanced analytics will also include less thrilling but equally important practical tasks of exploring correlations and dependencies between program practices and performance scores, such as between training and policy compliance, which can greatly help to further increase the effectiveness of a cyber security and robustness program[37].

Leveraging economies of scale, and moving from reactive to proactive tactics. Rather than approaching each plant as a unique universe with characteristics of its own, the generic approach of the RIPE Framework scales. For example, policies for one power plant will not be completely different from what is appropriate for another power plant -- especially if they are operated by the same utility, are of the same type (fossil, nuclear, hydro etc.) and/or use the same DCS. Procurement guidelines will be very similar, maybe even identical, for corporations within the same vertical. Dataflow diagrams and component inventories for standard DCS and SCADA products don't need to be produced from scratch over and over again. Instead, independent entities can provide prefabricated security documentation templates that only need to be adapted to a specific plant, organization, or country in respect to minor details. Industry-specific security profiles can be established based on such templates. – A related benefit is a shift towards a proactive approach. The application of technical security controls involves configuration change and is often objected by control system engineers just for this very reason. Rather than basing such configuration change on idiosyncratic and sporadic risk assessments it appears more reasonable to leverage thorough analysis of tens or hundreds of similar plants, and real-world operational experience with specific security controls. The obvious mid-term goal is to integrate cyber security features into reference architectures, ultimately resulting in appropriate cyber security and robustness being available at commissioning time.

If security characteristics of a specific plant are documented properly and accurately, risk assessments and mitigation advice can be done on paper by external experts

Enabling uncontroversial information sharing via independent third parties. Independent entities as mentioned above can act as information sharing brokers for RIPE users. Anonymized benchmarks, scorecards, and analytical results can be shared among participating organizations if they are willing to do so. Whereas many corporations show reservations about sharing cyber incident information, there is a chance that the opportunity to score cyber security performance and budget efficiency against peers and to benefit from advanced vulnerability analytics (via trusted communication channels) will encounter less hesitation[38].

[37] Analysis can be extended far beyond correlation to experimental settings in order to determine cause and effect, for example by comparing policy compliance between a trained and a non-trained group of users.

[38] A successful example of a similar metrics-based cyber security framework approach in the software industry is the *Building Security In Maturity Model*, or BSIMM for short. (http://www.bsimm.com/)

Conclusion

There is no magic to the approach presented in this paper. It's the application of insights that are known and have been practiced on plant floors around the world for decades. Management knows that nothing gets done without establishing a process that is driven by real people with accountability and real budget, subject to oversight. Employees know that selling management on addressing ICS insecurity requires a credible plan[39] with computable cost that can be put into a spreadsheet, and with fact-based performance indicators. Lawyers know that a cyber security plan along with fact-based performance indicators that cannot be disputed offer a strong defense in case of litigation. Quality engineers know that without having achieved measurable capability, reliable performance is illusionary. Control system engineers know that control is impossible if the accuracy of inputs and the reliability of outputs are questionable. ICS security experts know that the whole cyber security and robustness issue must be integrated with operations and engineering. All this has been known for a long time; it's "only" put together in the RIPE framework. If it looks obvious, it doesn't mean that it's a bad idea.

Acknowledgements

Eric Cosman, Richard Danzig, Perry Pederson, Dan Geer, Gary McGraw, Andreas Timm, Dale Peterson, Michael Assante, Leanne and Barry Kuehnle, Karl Brower, and Joe Weiss provided valuable feedback in the process of writing this paper.

About the Author

Ralph Langner is founder and director of Langner Communications GmbH, and a nonresident fellow with the Brookings Institution. He has accumulated over 20 years of hands-on experience in real-world plant environments and became globally recognized for cracking the Stuxnet malware. In addition to his consulting responsibilities, Langner is a frequent keynote speaker at international conferences on cyber security and national security.

About Langner Communications

Langner Communications GmbH is a cyber security consulting firm focused on industrial control system security. The company was founded in 1988 by Ralph Langner and is based in Hamburg and Munich (Germany). Langner Communications serves international clients in various verticals such as manufacturing, oil & gas, power generation, food & beverage, steel milling, and other industries. More information is available at http://www.langner.com/en.

[39] To quote the definition of "plan" from businessdictionary.com: "Written account of intended future course of action (scheme) aimed at achieving specific goal(s) or objective(s) within a specific timeframe. It explains in detail what needs to be done, when, how, and by whom". http://www.businessdictionary.com/definition/plan.html