A RIPE Implementation of the NIST Cyber Security Framework

Adding the How-To to the NIST CSF

Perry Pederson

October 2014

The Langner Group

Arlington | Hamburg | Munich

Contents

EXECUTIVE SUMMARY **3**

THE NIST CSF GOALS **4**

PRODUCING A CYBER SECURITY PROGRAM **4**

THE NIST CSF FRAMEWORK CORE **5**

FUNCTIONS 5
NIST CSF CATEGORIES 7
NIST CSF SUBCATEGORIES 7

THE NIST CSF IMPLEMENTATION TIERS **8**

TIER 4: ADAPTIVE 9
HOW RIPE EXPRESSES TIER 4 CHARACTERISTICS 9

THE CSF CYBER SECURITY PROFILE **10**

IMPLEMENTATION CONSIDERATIONS **11**

IMPLEMENTATION USING THE CSF 11
IMPLEMENTING A CSF CONFORMANT PROGRAM USING RIPE 11

SECURITY CONTROLS AND CYBER SECURITY CAPABILITY **12**

CONTINUOUS IMPROVEMENT AND INFORMATION SHARING **13**

CONCLUSION **13**

APPENDIX **15**

RIPE TEMPLATES AND GUIDELINES OVERVIEW 15

About the author

Perry Pederson is co-founder and managing principal of The Langner Group. He began protecting critical infrastructure against cyber attacks with the US Department of Defense and continued that effort as the Director of the Control Systems Security Program (CSSP) at the US Department of Homeland Security. At DHS, he managed the Aurora project where it was demonstrated that electrical generators can be destroyed by a cyber attack. Pederson then moved to the US Nuclear Regulatory Commission where he helped build the regulatory framework for cyber security at US nuclear power reactors and has consulted with the International Atomic Energy Agency on applying security controls to digital instrumentation and control systems globally. Before joining The Langner Group, Pederson held the position of Senior Cyber Threat Analyst for the Nuclear Regulatory Commission.

Executive Summary

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) was published February, 2014. An apparent problem with the framework is the chasm between the CSF as a framework and the details of "how-to" actually implement the CSF on the plant floor. This paper posits a solution on how The Langner Group's Robust Industrial Control Systems Planning and Evaluation (RIPE) Program solves the problem and can even be used a means to demonstrate compliance with the CSF.

The CSF provides high-level taxonomy and a common way to talk about cyber security, but RIPE provides the detailed step-by-step guidance on how to actually achieve the promise of the CSF's intended goals. The RIPE Program provides owners and operators of critical infrastructure[1] with the skills, tools and templates to meet the goals outlined in the CSF and thereby meet the stated policy objective of President Obama's Executive Order (EO 13636) *"It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."*

[1] EO 13636 Sec. 2. Critical Infrastructure. As used in this order, the term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

The NIST CSF Goals

In summary, the CSF provides a common taxonomy and mechanism for organizations to leverage existing standards, guidelines, and practices, to achieve the following:

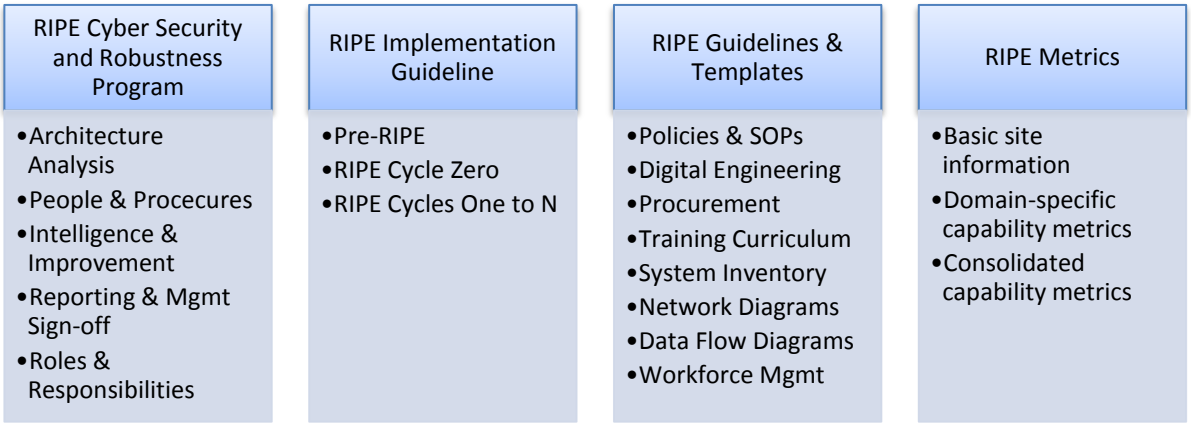
1) Describe their current cybersecurity posture;
2) Describe their target state for cybersecurity;
3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
4) Assess progress toward the target state;
5) Communicate among internal and external stakeholders about cybersecurity risk.

While this brief outline of goals sounds reasonable, there is scant information in the CSF or any of the reference standards on precisely how to implement a *process* to consistently achieve measureable progress toward these goals. This is where RIPE can be brought in to fill the gap between the aspiration of those who want to improve their cyber security posture and a fact-based, verifiable and measurable demonstration of improved security posture.

Producing a Cyber Security Program

Although the CSF mandates (as much as a voluntary program can mandate) that critical infrastructure owners implement a cyber security program, the CSF does not specify to any extent what such a program should look like or entail. This is not a problem unique to the CSF as many existing industry standards lack such guidance. Some would say that this is feature rather than a shortcoming. However, process engineers are left scratching their heads and hoping for some more detailed guidance.

This is exactly where RIPE steps-in to provide a template for the program as well as a template for all of the component parts of the program such as policies and procedures, database schema, and a complete set of metrics to measure current state as well as progress toward a desired state. In RIPE, a high-level cyber security and robustness program that must be signed off by management is the principal template for initiating a governance process. It lists activities in eight domains that can be mapped to NIST CSF Categories and Subcategories. The specifics of these eight domains are then presented in more detail in guidelines that may and will change annually. Last but not least, there is an implementation guideline and a metrics document. As the name suggests, the RIPE Implementation Guideline provides step-by-step guidance for introducing RIPE to a production facility.



A cyber security program – as the high-level policy document that clearly states activities and expected goals – is the central document of any cyber security effort that intends to avoid being random and anecdotal. In RIPE, an actionable program is provided as a template, which is supported by all other RIPE documents and tools.

The NIST CSF Framework Core

Functions

Functions as defined by the CSF organize basic cybersecurity activities at their highest level, forming the *CSF Framework Core*. Functions used within the CSF are *Identify, Protect, Detect, Respond,* and *Recover*. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities.

The following table addresses each of the NIST CSF Functions from the perspective of the RIPE program. RIPE encompasses all the activities associated with each of these functions, and also goes beyond just a high-level description of goals to include specific step-by-step guidance and templates.

Where the NIST CSF is intended to provide a language or means of expressing cyber security requirements to partner and customers alike (i.e., a cyber security protocol), RIPE provides the specific and detailed content, ready for implementation on the plant floor.

NIST CSF Function & brief description	The RIPE Perspective
Identify Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.	Before anyone can even begin to understand risk, let alone talk about it in the context of a particular plant, they must first know what they have. This is, without a doubt, the most often overlooked yet critical foundational step to getting control of the digital plant ecosystem. How can anyone be expected to provide any reasonable level of cyber risk management layered over the top of systems that that they do not understand, and of procedures (such as contractors' use and abuse of laptop computers) that they do not control? It is equally important that not just the plant engineers know what they have, but that decision makers share this understanding in a way that facilitates effective cyber security governance. Cyber security risk is not manageable in the traditional sense, but there are activities that if practiced diligently will improve robustness as well as security across the digital ecosystem.
Protect Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.	Users of the NIST CSF or other standards are still burdened with determining "appropriate safeguards." With the information that RIPE is designed to capture and present to plant management, this decision is made routine. Furthermore, because of the rigorous governance process and routine compliance checking, critical infrastructure service delivery are assured. In RIPE, appropriate safeguards are provided in the form of reference architectures, best practices as identified among the RIPE user base (information sharing), and as individual advice contained in the annual RIPE report that The Langner Group provides to every RIPE user.

NIST CSF Function & brief description	The RIPE Perspective
Detect Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	Increasing cyber security capability using RIPE can increase an organization's ability to monitor its environment and strictly enforces policies and procurement guidelines. As one example, a complete and accurate system inventory as mandated by RIPE is a prerequisite for identifying rogue hardware and software. This leads to a higher security posture compared to an organization bereft of a repeatable and sustainable process. Expenditures for extensive security controls and real-time monitoring for events above the achievable level of security, as determined by existing cyber security capability, are a waste of money. A conceptual shift of focus worth pointing out is that RIPE not only develops the capability to identify the occurrence of cyber security events, but – maybe more importantly – flaws in design and procedures that make such events possible in the first place.
Respond Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	The RIPE Policies and Standard Operating Procedures document lists detailed advice for contingency and reporting procedures. The RIPE Training Curriculum teaches how to apply such procedures. At a strategic level, cybersecurity events are addressed in the annual analytics, reporting and improvement process.
Recover Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.	While metrics-based sustainability is at the heart of RIPE, the necessary system criteria for sustainability and recover must be included in the procurement process. If this is not done consistently then resilience cannot be sustained. A software and configuration backup plan is part of the system documentation, identifying recommended backup intervals, data files to be backed up, and restoration of data. Some key features of the RIPE procurement guidelines for purchasing new systems that support effective recovery planning includes; Backup of runtime data is supported during normal system operation, i.e. on a “live” system, automatic backup and restore of all software components and data files is possible, and a full operational system restore on a new hardware installation is supported.

In summary, it is clear that RIPE not just implements the NIST CSF Functions but exceeds those functions’ objectives by adding sustainability and root cause analysis of potential cyber security events that the NIST CSF’s concept is built around. In a way one could say that while the NIST CSF is focused on symptoms, RIPE delivers a cure for the underlying disease. In environments that rely on industrial control systems, such an approach is a necessity because of the drastically longer timeframes involved for any updates of systems, architectures and procedures as compared to IT environments.

NIST CSF Categories

The subdivisions of a CSF Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities. Examples of Categories include “Asset Management,” “Access Control,” and “Detection Processes.”

In the following table the CSF Categories are aligned with the various elements of the RIPE Program to illustrate that RIPE indeed covers all of the topics. Furthermore, in addition to providing high-level guidance for each of the categories, RIPE also provides the step-by-step guidance and templates as needed to immediately implement the goals therein.

NIST CSF Function	NIST CSF Category	Reference RIPE Program Element
Identify	• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy	• Architecture Analysis • People and Procedures • Intelligence and Improvement • Reporting and Management Sign-Off • Roles and Responsibilities
Protect	• Access Control • Awareness and Training • Data Security • Information Protection Processes and Procedures • Maintenance Protective Technology	• Architecture Analysis • People and Procedures • Roles and Responsibilities
Detect	• Anomalies and Events • Security Continuous Monitoring • Detection Processes	• People and Procedures • Intelligence and Improvement
Respond	• Response Planning • Communications • Analysis • Mitigation • Improvements	• Architecture Analysis • People and Procedures • Intelligence and Improvement • Reporting and Management Sign-Off • Roles and Responsibilities
Recover	• Recovery Planning • Improvements • Communications	• People and Procedures • Intelligence and Improvement • Reporting and Management Sign-Off • Roles and Responsibilities

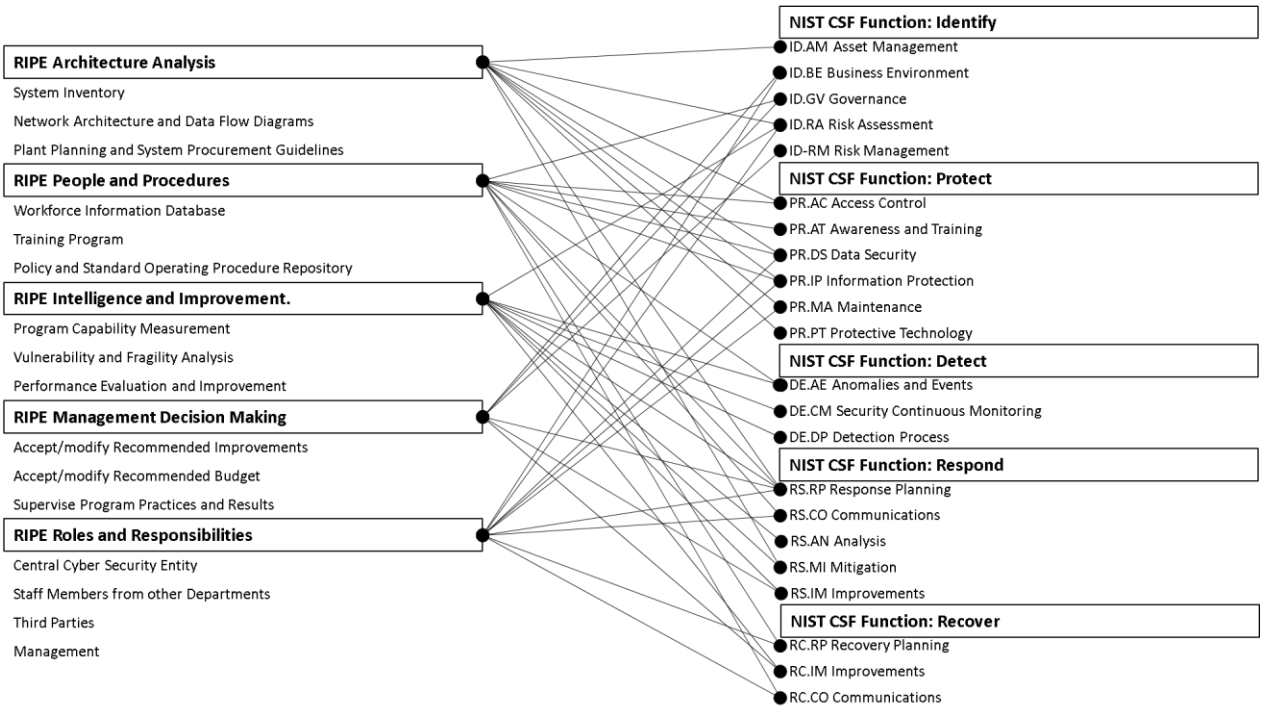
NIST CSF Subcategories

Subcategories further divide a CSF Category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category. Examples of Subcategories include “External information systems are catalogued,” “Data-at-rest is protected,” and “Notifications from detection systems are investigated.”

Although the Subcategories are not addressed in the above table, each Subcategory that might be selected by an organization, based on their Target Profile, is addressed with the RIPE Program. Again, in addition to providing the conceptual level guidance, RIPE provides detailed guidance and templates for implementing even the lowest level Subcategory.

For every Function, Category, Subcategory, process or element within the CSF you find a corollary within the RIPE Program. The following chart provides a visual mapping of the various RIPE program elements to the CSF at the Function and Category level, as going down another level would make the chart unreadable. The bottom line is that every possible combination of Function, Category, and Subcategory that an organization might choose within the CSF as part of a given Profile, there is an element with RIPE that will address the intent.

Although RIPE does not attempt to independently measure risk per se, every activity within the RIPE program, in a similar way as every activity within the CSF, is intended to reduce or at least identify overall cyber risk to the organization. The flexibility remains, again in a similar way to the CSF, that an organization can decide their so called "risk appetite."



The NIST CSF Implementation Tiers

The CSF states that "The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk. The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4)."

Although the language in the CSF suggests Tiers are not to be thought of as strictly levels of maturity because in some instances, Tier 1 may be sufficient for the assets being protected. However, in keeping with the stated goals of EO 13636 (i.e., protecting the most critical of all critical infrastructure), it does not seem reasonable to expect anything less than a Tier 4 approach.

Although RIPE could be implemented to operate at any Tier within the CSF, for the purpose of this paper the notional implementation is at Tier 4 which illustrates how RIPE meets the most stringent requirement of the CSF (but could be implemented at any Tier based on business requirements). Additional capabilities not addressed by the CSF, but nonetheless necessary for effective program management, such as compliance metrics, are also provided by RIPE.

Tier 4: Adaptive

The CSF describes some characteristics of a Tier 4 (adaptive) cyber security program:

- ***Risk Management Process*** – The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.
- ***Integrated Risk Management Program*** – There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks.
- ***External Participation*** – The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs.

How RIPE Expresses Tier 4 Characteristics

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. The RIPE Program was designed to meet this challenge head-on by providing a practical and cost-efficient cyber security method to confront a problem that keeps getting bigger and bigger with every new network connection. Following are some of the characteristics of RIPE that address the issues of unmanageable risk in ICS environments and simultaneously match the characteristic of a Tier 4 ICS cyber security program:

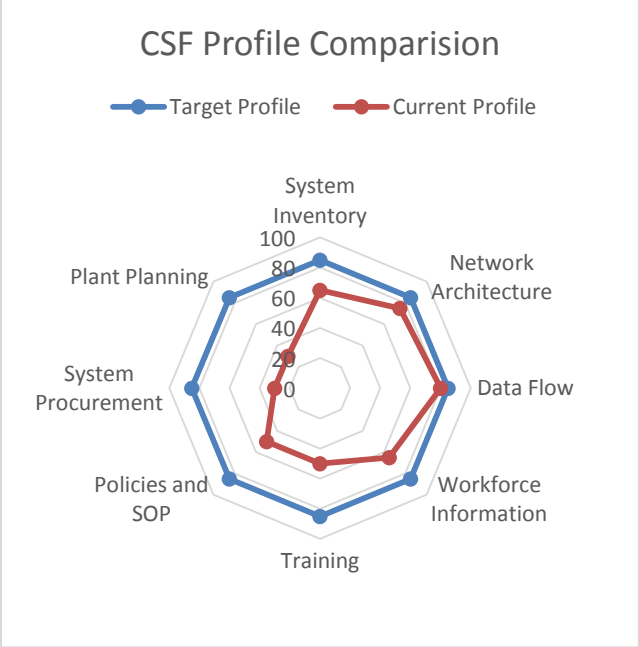
- Risk management is a fairly advanced concept and most agencies, organizations (including standards development organizations) don't have a firm grasp on the necessary foundational requirements to support risk management. The purpose of RIPE is to establish a governance process that evaluates and continuously improves the cyber security and robustness of digital systems used in process control in a systematic manner. Their reliability, security, and safety characteristics cannot be left unplanned and unchecked.
- The governance process covers all major factors that have an impact on the cyber security and robustness of industrial control systems and their functionality. It covers technical system attributes, activities of personnel (employees and third-party staff members) that need to interact with such systems in a live production environment, and also staff members who plan, procure, and commission such systems.
- The governance process involves distinct activities that are grouped in three major categories:
    - Architecture Analysis
    - People and Procedures
    - Intelligence and Improvement.
- Practices categorized in Architecture Analysis and People and Procedures comprise the execution part of the process, whereas practices categorized in Intelligence and Improvement provide a meta-level of compliance checking, performance evaluation, and program improvements. Intelligence and Improvement practices are introduced to verify that other program activities are executed to specification – i.e. that the process is performed in empirical reality rather than on paper only – and to evaluate performance, providing the opportunity to introduce improvements to program practices.

- A Reporting program activity provides the link to management, enabling informed oversight and decision making, and assessment of progress and cost-efficiency. Program improvements signed off by management are pushed back into the process. Reporting and management sign-off is executed periodically once per year.

The CSF Cyber Security Profile

The NIST CSF states that a Framework Profile is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state).

- With input from appropriate stakeholders, the Central Cyber Security Entity (CCSE) develops the CSF Profiles of the current state (as obtained from annual verification) as well as the target state (as a result of analytics and improvement). Typically, within the RIPE Program the current state and any indicators for possible improvement are encompassed with the RIPE Metrics. The RIPE program itself does not mandate any specific target levels for cyber security capability and performance; it is up to the asset owner (or a regulatory authority) to set such targets, thereby defining a target profile.
- Metrics play a central role within RIPE because they associate framework artifacts with empirical reality, and provide a means for scoring and benchmarking. Scores and benchmarks help an organization to rate if cyber security capability within a specific RIPE domain is sufficient or not. In addition, RIPE sub-metrics provide insight on potential reasons why capability scores are above or below expectations, thereby highlighting areas that might need improvement.
- 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 a sustainable cyber security and robustness program that provides for resilience and reliability even with further integration.

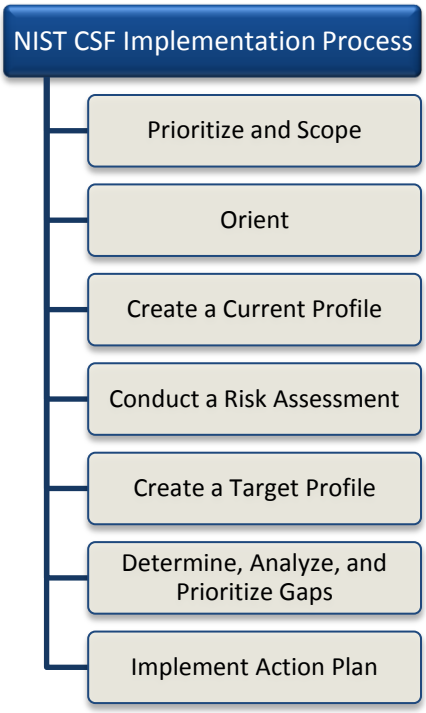


- Compared to the NIST CSF, RIPE is more stringent in the respect that it mandates annual verification and measurement of the actual cyber security and definition of a new target security profile for the next RIPE cycle.

Implementation Considerations

Implementation Using the CSF

Implementation is a key issue in any new program. There is a lot at stake and there are multiple stakeholders. The CSF provides an outline of the implementation process, however, there is little guidance beyond the high-level concepts such as: Prioritize and Scope, Orient, Create a Current Profile, Conduct a Risk Assessment, Create a Target Profile, Determine, Analyze, and Prioritize Gaps, and Implement Action Plan.



The diagram to the right is not meant to imply nor does the CSF suggest that these are sequential steps in a process. Many of these steps are performed in parallel by various elements within the organization and in many cases it is an iterative process.

The underlying assumption is that if these steps are completed by an organization, then they have made the first steps toward implementing the CSF. Unfortunately, there is little else to base a robust cyber security program upon. Much more detail is needed and this is where the RIPE Program can be used to fill the gap in assisting the efforts of diligent practitioners in implementing the intent of the CSF.

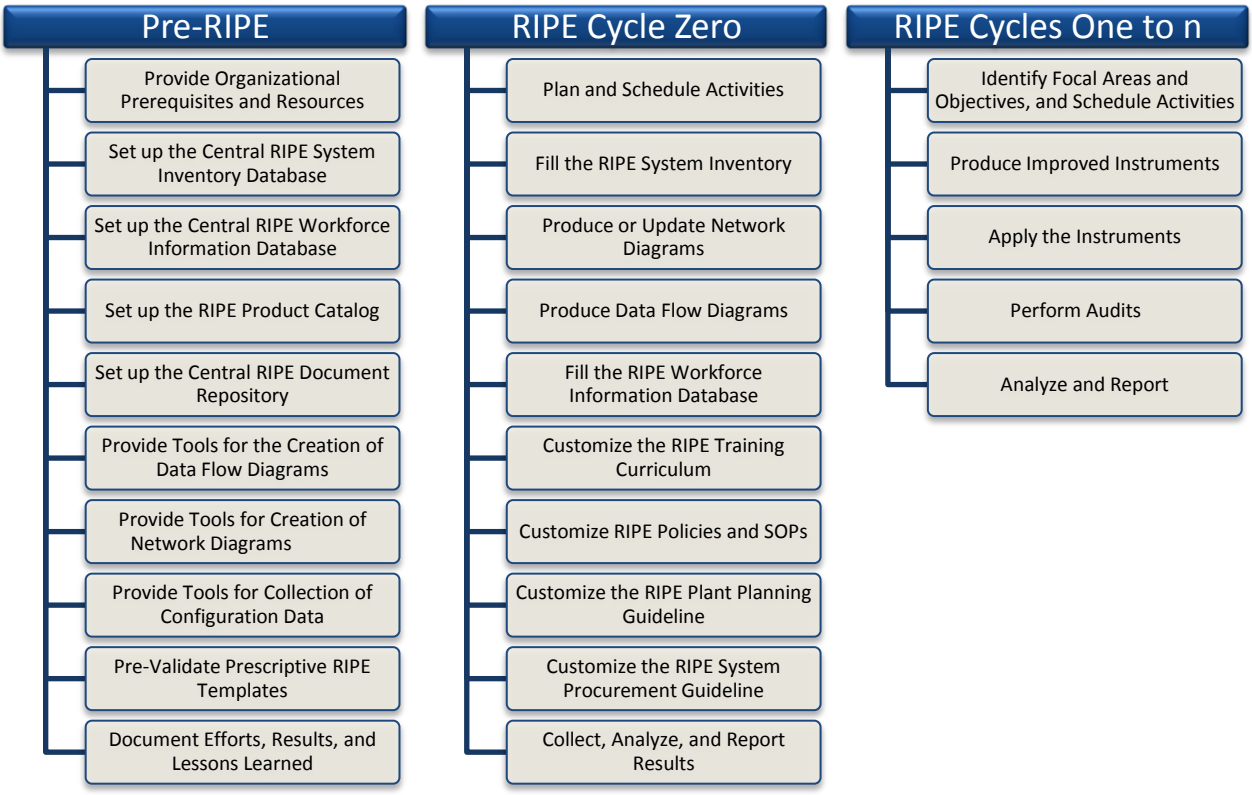
Implementing a CSF Conformant Program Using RIPE

The RIPE Implementation Guideline is a central document within the RIPE Program as it outlines the recommended approach to implementing RIPE for a given site. It also details the technical and organizational prerequisites that must be in place before it makes sense to seriously start with the RIPE process. There are three phases to a full RIPE implementation that mirror the essence of the CSF process, but include an order of magnitude more detail:

- Establishing the organizational and technical prerequisites for RIPE in the Pre-RIPE (Phase I);
- Adjusting and validating the RIPE instruments in the RIPE Cycle Zero (Phase II);
- Moving to a continuous RIPE process that focuses on improvement (Phase III).

The various tasks detailed in this document include a section on respective responsibilities, which may span across the organization and extend to third parties. Certainly the exact identification and assignment of responsibilities depends on organizational specifics, so any listing of responsibilities should be understood as a suggestion. For example, the bulk of activities for the Pre-RIPE and RIPE Cycle Zero phases can be outsourced to a contractor such as the dedicated RIPE implementation partner, or even a general IT service provider.

The following table provides an overview of the three phases of a CSF compliant RIPE implementation. As you can surmise by looking at this chart, RIPE is a front-loaded activity. There is a lot of work necessary to develop and implement a robust ICS cyber security program. However, once an ICS cyber security capability is established, a decreasing amount of time and effort are required to sustain the program. Nonetheless, the benefits to the organization are cumulative as the investment yields increased value over time.



Security Controls and Cyber Security Capability

The CSF lists many existing cyber security standards and asset owners are left to their own devices just how to approach the implementation of security controls. Most of the existing guidance for ICS security place unsubstantiated faith in the mere presence of security controls, which is commonly expressed in a checklist where the presence of specific security controls is judged as an indicator of cyber security posture. However, security controls are not magic properties that, if allegedly present, would provide security assurance in a guaranteed manner. In reality, any typical security control provides not much more than a grey zone which must be carefully examined in order to establish the factual value of such control.

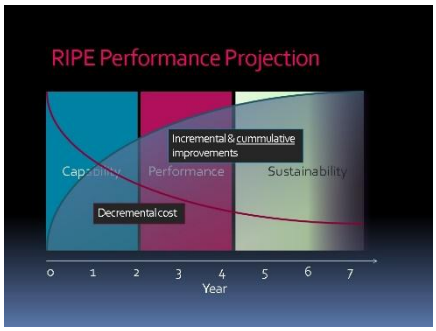
Unlike the CSF, RIPE covers this grey zone extensively and is known as *cyber security capability*. The term reflects the gap between a conceptual security control and its actual de-facto implementation, configuration, and behavior. For example, regimes for the application of security patches or anti-virus updates regularly are not executed per policy in real-life plant environments. The same is true for behavioral controls such as policies where audits regularly show that security policies are either not known to their intended audience, not practicable (such as non-comprehensive, non-memorizable, or simply non-executable for practical reasons), or simply not followed for convenience.

The establishment of security controls without the implementation of a governance process to achieve and verify cyber security capability leaves cyber security to wishful thinking. For this reason, the RIPE Framework places the emphasis on implementing such a governance process. Although the CSF touts governance as an important aspect of any cyber security program, there is little information on how to actually establish and operate an active ICS cyber security governance process. Another point of contrast between the CSF and RIPE is that RIPE favors design change over bolt-on security controls, if only to eliminate the need for installing ever more devices and software

that can be misconfigured or fail, or mandating new procedures that require staff time which must be subtracted from other tasks.

Continuous Improvement and Information Sharing

The CSF suggests that once an organization has adopted the framework and used various Profiles to identify areas for improvement, then the security posture will improve over time. However, in many organizations, the cyber security of ICS is viewed as a task that can be mastered on the side by notoriously overburdened control system engineers, with no specific budget. The CSF and RIPE are very much alike in this regard, nothing really gets done without good planning, management commitment, and resources. The real difference is in that RIPE Program provides all the parameters for resource planning and for monitoring of progress. At the core, the RIPE Program represents a continuously improving process focused on the cyber security and robustness of digital industrial control systems regardless of the current state Profile as might be described under the CSF.



One way to boost continuous improvement in RIPE is information sharing. In the process of analyzing architectures, procedures, and mitigative strategies for producing annual reports for RIPE users, The Langner Group accumulates information about security strategies that practically work, and about those that don't. Such information is reflected in RIPE reports and forms a basis for improved templates, procedures, and reference architectures. Where conventional IT security wisdom focused on threat intelligence and incident data when thinking about information sharing, in RIPE the focus is on vulnerabilities and how to fix them in the most reliable and cost-efficient manner.

The chart at left provides an example of the cumulative cost reduction and cumulative improvement that would result from any quality managed process. Pre-RIPE is estimated to require about 3-6 months of effort to ensure the technological capability is in place to build a RIPE program. This Pre-RIPE phase is then followed by RIPE Cycle Zero and includes a full iteration of the RIPE Program to include the generation of performance metrics. At the end of RIPE Cycle Zero, the primary inputs to improve the next iteration are the results of the first and thus begins a process of continuous improvement in the overall security posture.

Conclusion

It seems that everything is being connected to everything at an ever increasing frequency. This is driven by several factors such as economics and convenience. However, 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.

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 – and while the CSF purports to embody such features, this is what the "planning and evaluation" stands for in RIPE.

The concept of a governance process for ICS cyber security is embedded in the NIST CSF as well as other cyber security frameworks such as ISO 27001 and ISA-99/62443. However, all of these frameworks lack concrete, practical procedures that implement governance. These standards expect that asset owners invent individual cyber

security plans on their own rather than follow a standard guideline or template. 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 a problem that the NIST CSF cannot solve alone. However, the RIPE Program has already solved this problem and is already in practical use to protect the most critical of critical infrastructures: nuclear power plants.

Unlike the CSF, the RIPE Program comes with standardized and concrete templates, checklists and reference architectures. It replaces the obscure art of assessing risk by methods and procedures that will yield results and don't require cyber security experts to execute. Implementation may either be achieved by internal staff or external service providers. Introducing RIPE to a plant environment occurs step-by-step depending on resources and security requirements in the same way that implementing the CSF depends on resources and requirements.

While the NIST CSF provides a good first step, there is a wide chasm between the high-level concepts outlined in the CSF and the reality of implementing a sustainable ICS cyber security program on the plant floor. The RIPE Program provides the bridge from a meager beginning to a sustainable, predictable, and continuously improving cyber security posture at the least possible cost.

The burden on the owners and operators of critical infrastructure cannot be overstated. They are in a constant balancing act between the need for increased security in a world of evolving threats while maintaining shareholder value. The NIST CSF was designed to assist those asset owners achieve the cyber security posture appropriate for a given situation and while it does provide a taxonomy to facilitate the discussion, many plant engineers may need more detailed guidance. This is where RIPE can step-in to fill the gap and help asset owners achieve the promise of the CSF. The CSF, as a voluntary program is the opportunity for industry to say "we can do this" and the RIPE Program provides the tools to actually make it happen.

Appendix

RIPE Templates and Guidelines Overview

- **The RIPE Cyber Security and Robustness Program** is the high-level policy document that describes the various activities that the organization performs to manage cyber security and robustness.
- **The RIPE Implementation Guideline** documents favored approaches how to implement the RIPE Framework and assists in resource planning.
- **The RIPE Policies and Procedures** document specifies how activities with an impact on cyber security (but unrelated to system configuration) shall be performed.
- **The RIPE System Procurement Guideline** addresses characteristics of cyber systems that are planned for acquisition. The Procurement Guideline also affects systems (including software systems) that are developed in-house by staff members.
- **The RIPE Plant Planning Guideline** specifies how to integrate and configure cyber systems in order to meet conformance with the organization's cyber security criteria.
- **The RIPE System Inventory Database Architecture Guideline** details how the System Inventory should be structured and integrated with other RIPE instruments.
- **The RIPE Network Diagram Style Guide** suggests how network diagrams shall be designed for best readability and easy comparison with network diagrams created by others.
- **The RIPE Data Flow Diagram Style Guide** specifies what data flow diagrams should look like.
- **The RIPE Workforce Information Database Guideline** specifies which information should be in a workforce information database in order to map functional roles to training requirements, system responsibilities, and applicable policies and standard operating procedures.
- **The RIPE Training Curriculum** lists training modules that address the training requirements for the various stakeholders that are expected to apply dedicated tasks within the RIPE Framework.
- **The RIPE Metrics** document specifies metrics that can be used to measure and document status and progress in each of the eight RIPE domains.