Foundations of the Survivability and Information Assurance Curriculum

Survivability and Information Assurance (SIA) Curriculum Development Team
CERT® Program
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA

Introduction

The Survivability and Information Assurance Curriculum was designed and implemented to address several issues and concepts that form its foundation. This document highlights the foundations of the SIA Curriculum.

Foundation 1: The Principles

Successful system administrators must have sufficient training so that they know how to use specific instances of technology to accomplish tasks in support of their goals. Whether they receive that training on the job or through technical training courses is less important than is the notion that they have learned how to use the tools available to them.

A much more interesting question arises when either the selected technology changes or when it does not work as expected–does the system administrator really *understand* what they are doing? If they do understand, they can continue to increase their operational skills when using a changed or new instance of technology. They know what they are trying to accomplish, so it is just a matter of making the technology do what needs to be done.

However, if the system administrator does not really understand the problem they are trying to solve, then they are often lost and the steps toward a solution appear random. Perhaps through trial-and-error they will eventually arrive at an acceptable result, perhaps not. And if they are successful in making the technology do what needs to be done, what knowledge have they gained for the next time when technology changes, as it inevitably will?

This foundation focuses on ten principles that guide the system administrator toward the root issues and techniques of survivability and information assurance. They provide an organized thought process for decision-making using conceptual understanding, checks and balances, methods, guidelines, rules and regulations, roles and responsibilities, and a strategy for collaboration with others.

System administrators who understand these principles stand a much better chance of controlling a specific instance of technology and will be better able to achieve their goals through controlling the technology available to them. The principles are the firm educational foundation upon which today's enterprise networks are built and sustained.

® CERT is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

Foundation 2: The Enterprise Network Supports the Mission of the Business

The computer systems and network infrastructure components[1] in an enterprise network exist to support the mission of the business. System administrators must recognize that the success of the business mission is crucial to their success and that the computer systems and network infrastructure components they control greatly impact that success. Technology for technology's sake is no longer practical in today's business environment.

To be successful, system administrators must make the connection between technology and business mission. They must understand how a specific piece of technology fits into the overall business, its contribution to that business, and its importance.

System administrators must also know risk management concepts and philosophies because the management and mitigation of risk will impact technology choices. They must also know the concepts and philosophies of policies and procedures, how to live within in them, how to affect change, and their roles and responsibilities in their formulation and operation.

Not only is it important for system administrators to know what their job is, but also what their job is not. With respect to policy, procedures, and risk management, system administrators do have a role in these activities but they are not in charge of them. They need to know this and how to professionally convey their level of responsibility to management.

Similarly, system administrators' direct management needs to know the roles and responsibilities of system administrators and the principles of survivability and information assurance. Through a mutual and realistic understanding of each other's jobs, roles and responsibilities in supporting the mission of the business, each, and the business as a whole can be more successful.

Foundation 3: Survivable Functional Units (SFUs)

Every enterprise network today consists of functional units[2] but their existence and lines of demarcation may not be clear to the system administrator. These functional units also have a degree of survivability that might not be clear to the system administrator. Through a rigorous assessment of the enterprise, these functional units and their relative degrees of survivability can be discovered and their relative importance to the mission of the business more properly evaluated using an in-depth application of **Principle 6: SFUs are a helpful way to think about an enterprise's networks**.

Principle 6 provides a conceptual method for system administrators to reduce the complexity of the enterprise network to a more manageable level. Instead of seeing a network with 10's or 100's of computer systems and network infrastructure components, by using SFUs the system administrator need only see 10 to 15 entities in the network. Their intra- and inter-relationships are subject to investigation and analysis only when necessary: likely much less than all of the time, as is the case when seeing individual computer systems and network infrastructure components. When visualizing the enterprise network as a set of cooperating SFUs, each SFU's contribution to the mission of the business is clearer. Also, the nature of the cooperation between SFUs becomes clearer.

The family car is a good example of an SFU. Most of the time, you view the family car as a monolithic entity servicing the mission of the family. While you were initially concerned with all of the intricacies and features of a new car such as gas mileage, cargo storage, and

---

[1] routers, hubs, etc.
[2] backup and recovery, user authentication, and file service

radio/CD/cassette options, over time your concerns changed to answering the question "can I carry two hockey bags, three suitcases, and four people to and from the hockey tournament next weekend in a reliable and safe way?" Its mileage, cargo capacity, and audio options are only a concern to you when you want and need those options (will two hockey bags, three suitcases, and four people fit?).

Similarly, the specifics of computer systems and network infrastructure components were of concern when these items where researched and purchased. But over time, they too fell by the wayside as the concern shifted to supporting the mission of the business, and rightfully so. Indeed disks do fill, processor speed is exceeded, and performance is limited by memory size. By and large, these details are in the background of a system administrator's thinking and only surface when they require attention.

Foundation 4: Inherit an Enterprise Network

While building a network from scratch represents a golden opportunity for system and network administrators, most administrators working in today's organizations are not often presented with this opportunity. Instead, they are more likely to join a team that already has management responsibility for a network believed to meet the needs of the organization in its present form.

It is important to educate system and network administrators about how to understand that network and positively participate in its management, all the while keeping the mission and constraints of the business in focus. The capstone course "Sustaining, Improving, and Building Survivable Functional Units (SFUs)" in the Version 3 family of the SIA Curriculum places students precisely in this role for these reasons.

From time to time, as a part of the capstone course, the enterprise requires new functionality to be added to the existing enterprise network. It is important for students to learn how to graft this functionality onto what is already there so that both the new and the old co-exist and the enterprise survives the integration operation.

The challenge is how to sustain and improve the enterprise's functionality and add new functionality as required. Once again, the ten principles can guide that decision-making process. The SIA Curriculum affords students the chance to experiment in this setting.

Foundation 5: Challenge Assumptions

System and network administrators are often confronted with data and information of unknown or questionable veracity. Style, appearance, or presentation issues frequently play an important role in accepting whether that data and information is correct and should be used as the basis for further assessments. This style, appearance, or presentation over substance, content or reality debate does not happen as often as it should and this can affect the ability of the business to survive.

Using **Principle 9: Challenge assumptions to understand risk** provides a method for system and network administrators to systematically evaluate the substance of assumptions regarding the validity of data and information. For system and network administrators' managers, it makes the case for letting their direct reports take the time to be thorough and complete in this analysis process supporting the business mission.

For example, the Address Resolution Protocol (ARP), part of the TCP/IP protocol suite, depends on the computer system or network infrastructure component that responds to a query to be truthful in that response. At this time, there is no widely-implemented authentication scheme whereby the response can be validated and used. Instead, with today's technology an ARP

response carries an inherent risk that must be recognized and its use compartmentalized appropriately.

The key is for the system and network administrators to understand the assumptions they are making and then make informed decisions based on challenging those assumptions. It is no longer appropriate to simply accept every piece of data and information as fact and use those "facts" as the basis for critical decisions in the enterprise network. By challenging assumptions to understand risk, system and network administrators are able to manage enterprise networks that are built on a firmer technological foundation. This leads to a higher degree of survivability of the enterprise network which is then better able to achieve the mission of the business.

Summary

The SIA Curriculum is based on five key foundations:

1. Principles of Survivability and Information Assurance - making decision through an organized thought process

2. The enterprise network supports the mission of the business - understanding how technology choices and applications impact the mission of the business

3. Survivable Functional Units - reducing the complexity of the enterprise to a manageable size

4. Inherit an enterprise network – managing the network, in a positive way, while keeping mission and constraints of the business in focus

5. Challenge assumptions - understanding first the assumptions and then making an informed decision

Each of these foundations pervades the courseware throughout the curriculum. Understanding them is a key part of successfully understanding and teaching the SIA Curriculum.