2

RESTORING TRUST

Cyber-Informed Engineering

Successful strategies must proceed from the premise that cyberspace is continuously contested territory.

—Former Secretary of the US Navy, Richard Danzig[1]

In a world of increasing connectivity and cyber threat innovation, it must be assumed that our computing environments have been compromised and that we cannot certify any system fully secure. It is reckless to presume historical analytical assumptions and approaches … can cover the unique nuances of the cyber threat.

—INL's Bob Anderson and Joseph Price[2]

Where Probabilistic Risk Assessment (PRA) or Probabilistic Safety Assessment (PSA) analysis utilizes equipment failures or human error as initiating events for a hazard, cyberattacks use the historical framework and functionality of a trusted system to perform operations outside the intended design and potentially without the operator's knowledge.[3]

—INL's Bob Anderson and Joseph Price

SIDEBAR: THE MYTH OF AIRGAPS

"We're air gapped" used to be the right thing to say to auditors. After all, if there's no network connection between the important system or data in question, there must not be a way for hackers to reach it … right? In the earliest days of mainframes and terminals, and later local area networks with servers and PCs, the only way for computers to share data or instructions was if they were connected by a copper wire or fiber optic cable. Cut the connection, and you had complete isolation. That is, if you forgot about the other ways to move data among machines, like floppy disks, USB sticks, and other removable storage devices.

Even someone as brilliant as Maine Senator Angus King, a Rhodes Scholar and one of the most cyber savvy Senators, once recommended air gapping the grid as a strategy to thwart advanced cyber adversaries. (He doesn't anymore.)

Only problem is, the term long ago ceased to signify anything of substance, with the exception of revealing the ignorance or naiveite of the person who still believes it has value. In fact, it was never an accurate way of delivering or thinking about cybersecurity, and folks on both sides of the auditor's question were sharing a mutual delusion. Talk about a false sense of security.

Here's why there are no air gaps:

- In recent years with the rise of ubiquitous cell coverage, Wi-Fi, Bluetooth, and other wireless communication technologies, the absence of a physical communications conduit means nothing in terms of network isolation.

  Imagine a PC or other computer-based system (e.g., all "smart" devices—Figure 2.1) was entirely un-networked, with no wired connections, and all wireless connectivity not just set to off in options, but with communications physically disabled or removed. In this mode, is it useful?

Figure 2.1 Smart Wireless and Networked Devices.

- Another system or network might be configurated to be, relatively speaking, "air gapped" by a particular administrator for a period. Personnel turn over, as do policies, and it's often the case that a system that was previously configured in a more secure way becomes much less so when a new leader takes charge or new initiative is undertaken.

The requirements of operating a plant or other engineering-heavy organization often demand actions that further service to undermine the concept of air gapping, including:

- Corporate networks connected through firewalls to operational networks
- Remote access into field devices (often with little or no authentication) by engineering stations or for vendors' remote diagnostic support
- Removable media (e.g., flash drives, CDs, external hard drives, etc.) used to perform patches, upgrades, and backups or to pull data from a device
- Having common buses control systems and safety systems

On the positive side, if attempting to build and maintain air gaps means there are fewer ways to reach a system or network, then that is a good thing.

SIDEBAR: NUCLEAR DESIGN BASIS THREAT

INL's Bob Anderson and Joseph Price gave a long hard look and the cybersecurity threat to nuclear power plants (NPPs) and found potential blind spots via adherence to a design basis threat (DBT) that hasn't kept up with the times. They noted:

> The IAEA publication INFCIRC/225/Rev.4, also known as Nuclear Security Series #13, "*Recommendations for Physical Protection of Nuclear materials and Nuclear Facilities*," states that a DBT is a description of the attributes and characteristics of potential insider and/or external adversaries who might attempt unauthorized removal of nuclear material or sabotage against which a physical protection system is designed and evaluated. DBT considers insiders, external adversaries, malicious acts leading to unacceptable consequences, adversary capabilities, and an evaluation of protective designs. Historically, DBT did not address cybersecurity concerns. With the cyber threat demonstrating its ability to influence physical protections systems including blended attacks, digital components and systems must now be considered as either part of the existing DBT or part of a separate cyber threat assessment. Either way, cyber-informed engineering must contribute to the analysis of credible scenarios that include the adversary compromising computer systems at nuclear facilities that lead to sabotage or the blended attack to remove nuclear material. Incorporation of the cyber threat must carefully consider new technologies, use of mobile computing, social media, and many more tactics, techniques, and procedures (TTPs) of the adversary. As these threats are considered, the engineer must design systems that reduce or remove these threats.

SOFTWARE HAS CHANGED ENGINEERING

Software arrived in our world, practically speaking, in the 1950s with the development of the Fortran programming language.[4] It took several more decades before computers and computer networks became affordable and commonplace enough to play a helpful role in the engineering-design process, as well as in the operation of computer-assisted process control functions. Previously, engineering was principally a realm of mathematics and physics, and until the arrival of the digital calculator in the 1970s, the slide rule was the engineer's constant companion.[5]

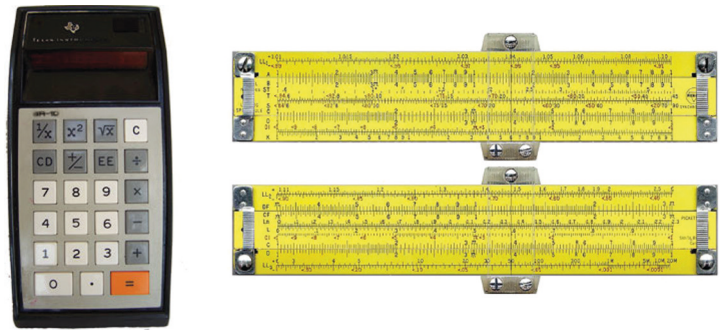

Figure 2.2 Software-driven Planning and Design Tools Develop Software-intensive Products and Systems. Calculator (left) and slide-rule (right).

"Illustrated Self-Guided Course on How to Use the Slide Rule." Web page, accessed January 4, 2020. www.sliderulemuseum.com/SR_Course.html.

"Calculator Museum." Mr. Martin's Web Site. Web page, accessed January 4, 2020. www.mrmartinweb.com/calculator.html.

While the first computer-aided design (CAD) programs emerged in the 1960s, it took until the arrival of applications on Unix workstations in the 1980s and Windows PCs in the 1990s for these capabilities to hit the mainstream and start making very large impacts in aerospace, automotive, and other industries.[6]

Imagine attempting to sabotage an engineered creation by hacking a physical slide rule (in use for centuries) or an early digital calculator (appeared circa 1970) (see Figure 2.2). To modify a single unit would require physical access to that unit and then some nifty craftwork to subtly change the devices without detection by its owner. Modifying a calculator might prove even more challenging and would require a skillset including precision soldering. To affect multiple units of either would force strategies targeting the manufacturers and/or their supply chain. While one can imagine any of these approaches employed by spy organizations, there's simply no comparison to the effects possible today at great distances and with great stealth.

INL and Engineering

Officially designated by the US Department of Energy as an applied engineering lab, INL's charter is to bring its enormous depth in engineering

to solve the hardest problems of the near and mid-term future. This distinguishes it from other labs, the "science labs" that work on technical challenges of the more distant future.

There's a stereotype of inquisitive young engineers, inventors, and tinkerers who can't help themselves; they're compulsively driven to learn by taking things apart. Whether by unhurried and careful dissection, or else via sledgehammer, explosives, or other less meticulous means, there's an instinct to see how things are made by opening them up, and in so doing, determine whether they can be made better.

For the thousands of engineers and scientists at INL, better might mean a number of things, including safer, more efficient, simpler to operate, less expensive to build and/or maintain, etc. And in the twenty-first century, an increasingly essential attribute is more secure. The Idaho National Lab is an expansive government-funded test bed and playground for these types of folks. A sampling of their activities over the years would include:

- Running nuclear test reactors to the point of failure
- Calibrating battleship guns by firing Volkswagen Bug–sized projectiles at buttes dozens of miles away
- Electric grid testbed
- Water testbed
- Wireless communications range
- EMP/GMD testing
- Aurora: convincing a large electric generator to tear itself apart via a few strokes on a keyboard
- Creating extremely high-tech armor for the US Army's main battle tank
- Following the physical attack on the Metcalfe Substation serving Silicon Valley, designing and building a prototype of practical low-tech substation armor
- Operating the National SCADA Test Bed (NSTB) to take apart and find exploitable weaknesses in grid infrastructure components
- Voting machine security analysis for Department of Homeland Security (DHS)[7]
- Hosting elements of DOE's Cybersecurity Testing for Resilience of industrial control system (ICS) (CyTRICS) program today, an NSTB follow-on[8]

There's another word used to convey a constructive urge to disassemble, rearrange, or otherwise simply mess around with things: Hacking. To be called a hacker was and still is a source of pride among technical types,

including but not limited to software developers, as hardware and all manner of machines can also be hacked. And biological organisms too. More recently, though, the definition of the word has skewed to include malicious intent. That's a trend that often offends the original cohort who hacked to understand and improve things, but as we all know, definitions can shift over time and no one, not even the folks in Oxford, can control them.

ENGINEERS STILL TRUST THE TRUST MODEL

Unverified Trust

In the digital world, to include almost all internetworked computing and communicating devices, the term "trust model" has signified the collective confidence derived from mutually agreed processes and protections achieved via broad conformance to standards (e.g., Secure Socket Layer [SSL], Certificates, HTTPS, password conventions, IP4, IP6, etc.). In the enterprise context, these, along with an ever-increasing arsenal of security technologies that began with antivirus tools and network firewalls, served ostensibly to protect systems and data by keeping the bad guys out. Best practices promulgated by NIST, ISA, and other standards bodies–guided organizations, but it has always been the case that targeted attacks can penetrate defenses that appear stout to their owners. With so much uncertainty, it's easy to see why the trust model has been pronounced dead by security professionals for quite a while.

Trust is more about psychology and human behavior than technology. INL's Curtis St. Michel almost always laces the opening segments of the CCE training sessions he conducts with ruminations on the dangerous position we've put ourselves in via "unverified trust." And ICS Cybersecurity educator and cyber threat analyst Sean McBride puts it this way:

> At the convergence of information technology and industrial control is a rat's nest of unseen, unknown, and unverified relationships—that for convenience and expediency we have "trusted away." Trust simplifies our decisions and puts our minds at rest: we anchor on the past to predict the future; we look for brand names; we stay in the center of the herd. But unseen, unknown, and unverified trust has immensely destructive potential. Modern societies have come to trust a convergence

> of operational technologies—sensors, motors, valves, programmable controllers, and communications networks—to provide electricity, water, and manufactured goods. But the design and integration of these industrial operations are largely unverified. As a result, we have opened the door to cyberattacks intended to cause devastating physical consequences at a time of the adversary's choosing.[9]

Engineering is a different animal with a foundation built on the immutable laws of physics, more specifically in well-worn theorems from aerodynamics, fluid dynamics, thermodynamics, electrical engineering, and materials science.

In the "Old Days," the tools were physical:

- Calculations: slide rule
- Drafting medium: pencil and paper
- Storage medium: paper
- Security mechanism for sensitive intellectual property (IP): a safe protected by an analog combination lock
- Communications: via private branch exchange (PBX)/landline phone, ground, and air mail
- In Engineering (2020), the laws of physics and specific engineering disciplines are captured and reflected in software. Now the tools are:
- Calculations: software
- Drafting medium: software
- Storage medium: various digital media
- Security mechanism for sensitive IP: various software security products
- Communications: digital over fiber, wireless (and ground and air mail still)

SIDEBAR: INL'S CHUCK FORSHEE ON CYBER-INFORMED ENGINEERING (CIE)[10]

I was just talking to Bob Anderson about CIE-CCE. Bob and I go way back, designing and installing digital ICS at the Advanced Test Reactor (ATR) in the early 1990s. I believe that we are trying to make a cultural change with respect to the digital world we all live in, and the engineering challenges associated with this new reality. All new

technology brings with it some new problems or faults (e.g., airbags and the warning stickers all over the inside of our cars).

In the 1990s we were just focusing on making digital ICS work. We knew components were going to fail, and there might be bugs in software, as evidenced by the ubiquitous blue screen of death. We weren't even thinking about how an adversary might use our systems against us.

We had to answer engineering design questions from a safety analysis perspective, all fault or failure based. We did not consider sabotage. When you approach a safety analyst now and tell him to design a new fault tree considering all the possible vectors a hacker might explore, you meet resistance. We try to overcome this in our CCE projects by developing sobering, sometimes shocking, but always realistic scenarios, showing the art of the possible and help them get to an epiphany.

Engineers will need to accept this new reality and develop a new culture that understands cyber vulnerabilities and employs cyber shields in all new engineering designs.

It's unfortunate that we are on our heels in a wait-and-see posture. Hoping that a new hacker doesn't exploit the holes we know exist in our systems. The hackers are getting smarter, and we are playing catchup trying to prevent their attacks. "This approach is not going well in the ransomware IT world we now live in. It's just a matter of time before the IT hackers get bored and really start to focus on OT systems. The IT stuff is most often an easy pathway to our OT systems."[11]

The C-suite knows that there are insufficient resources to patch all the holes because the OT systems were not designed with cyber vulnerabilities in mind in the first place.

TRUSTING WHAT WORKS: CIE IN DETAIL

There are a few prominent thinkers poised at the intersection of cybersecurity and physics. In the early days, circa 2003, concerned that there was too much marketing in the cybersecurity solution space, Allan Paller, the founder of the SANS Cybersecurity Training Institute, used to evaluate security tools on the basis of "What Works." Not long after he commissioned Mike Assante to build SANS ICS Security Summit and begin development of an ICS cybersecurity curricula, which now

includes four different courses and certifications, from introductory level to advanced.

Richard Danzig, cited earlier, also had this to say about trimming technology down to its minimum functional requirements, so as to reduce the size of the playing field attackers have to navigate.

> Pursue a strategy that self-consciously sacrifices some cyber benefits in order to ensure greater security for key systems on which security depends. Methods for pursuing this strategy include stripping down systems so they do less but have fewer vulnerabilities; integrating humans and other out-of-band (i.e., non-cyber) factors so the nation is not solely dependent on digital systems; integrating diverse and redundant cyber alternatives; and making investments for graceful degradation. Determining the trade-offs between operational loss and security gain through abnegating choices will require and reward the development of a new breed of civilian policymakers, managers and military officers able to understand both domains.[12]

And my INL colleague, Virginia "Ginger" Wright, who played a critical role in the initial development of CIE, captures this sentiment with great concision when she says "We may not be able to engineer out all risk, but there are choices we can make during the design to simplify the cybersecurity process."[13]

While INL performs research and other initiatives as tasked by multiple DOE offices (and DHS, DoD and more), the lab's primary sponsor is the Nuclear Energy (NE) office of DOE. Until recently, NE-funded efforts were primarily in materials and process research, but in 2017 it commissioned the lab to perform potentially ground-breaking research in cybersecurity challenges and opportunities facing those who own and operate nuclear plants, using CCE as its primary lens.[14]

INL researchers examined the systems engineering process across the entire lifecycle and identified 11 areas where key engineering decisions could substantially impact the cybersecurity of the operational technology:

1 **Consequence/Impact Analysis**
2 **Systems Architecture**
3 **Engineered Controls**
4 **Design Simplification**
5 **Resilience Planning**
6 **Engineering Information Control**

7 **Procurement and Contracting**
8 **Interdependencies**
9 **Cybersecurity Culture**
10 **Digital Asset Inventory**
11 **Active Process Defense**

Let's take a look at each of these:

1 **Consequence/Impact Analysis**
The first element of CIE, consequence analysis, is concerned with the challenge of scarcity. Given finite money, time, and attention, how can limited resources be optimized to avoid the worst outcomes? The first task is to identify high-impact consequences and the actions that separately or together could bring them about. Mitigations that could prevent those results from occurring are generated. But in case mitigations are incorrect or incomplete, it's imperative to identify protections that diminish the consequences themselves. Consequence analysis can increase security simply through design decisions. Ideally, mitigations can be put in place early in the design cycle, well before the first procurement actions. To begin, identify
- the bounded set of high-impact consequences.
- the situations that must not be allowed happen.
- systems that could contribute to or enable the negative consequence.
- associated digital and communications assets.
- protections for the system that greatly diminish negative consequences.

2 **Systems Architecture**
With the rarest of exceptions, it's not much of an overstatement to say that all of our systems and products were designed foremost for functionality, not security. However, when a team wants to undertake a project to build something that both fulfills its functional and performance requirements, and that is intrinsically secure as well, there are several points to keep in mind:
- Design requires collaboration to ensure design is functional and secure. So the design team needs cyber expertise to ensure appropriate security technology (such as data diodes, virtual local area networks [VLANS], network access lists, firewalls, etc.) is used to support the architecture. And system engineering experts

are required to fully explore and select the best approaches for meeting functional requirements.

Because any individual element cannot be trusted, the design

- avoids assumed trust.
- uses defense-in-depth principles.
- supports least privilege.
- ensures architectural boundaries are instrumented and monitored.
- documents communication flows.
- uses both horizontal & vertical network protections to enforce communication flows.

3 Engineered Controls

Engineers usually have two and sometimes several different options when making functional design decisions, and the same is true for security professionals. In a perfect and therefore unrealistic world, most security problems would be addressed through the top one or two control strategies in the list that follows. In reality, most solutions require use of some of the approaches drawn from the following list (also in Figure 2.3):

1 Elimination: Design the system to NOT have the potentially hazardous capability (often through simplification; disablement of broad "general purpose" functionality).
2 Substitution: Design the system to use a less dangerous capability (e.g., input/output information through other means).
3 Engineering Controls: If there is no way around a hazardous element in the process, then work to keep it as far away from human operators as possible. Or vice versa (e.g., use port blockers to prevent unauthorized access).
4 Administrative Controls: Develop and enforce policies and procedures that support security (e.g., structured and enforced kiosk check-in and check-out to secure mobile storage devices).
5 Personal Protective Equipment (PPE): The last line of defense. Implement cybersecurity controls. Must implement and configure correctly, patch quickly, and administer properly. (e.g., implement technical cyber controls to block unauthorized mobile devices)

In all of this, it's important to consider both IT and engineered controls as early in the design lifecycle as possible. In legacy OT systems it is often the case that patching must wait for a preplanned maintenance activity, sometimes only on a yearly or twice-yearly basis. To take some of the pressure off of patching, investigate how vulnerabilities can be designed out or mitigated

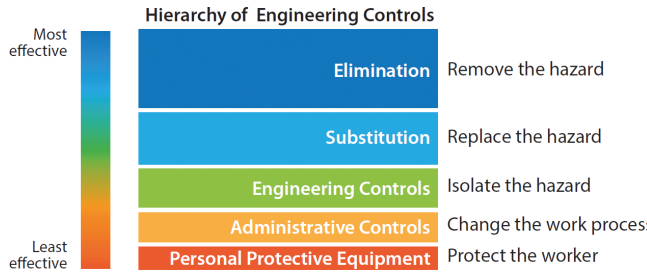

Figure 2.3 Hierarchy of Engineering Controls.

through additional engineered controls, and lastly, note that engineered controls will almost always provide more robust and dependable protection than add-on IT controls.

4 Design Simplification via ALARA

Ever-increasing system complexity is one of the trends that make defenders' lives difficult and confer advantages to attackers. ALARA—As Low as Reasonably Achievable—is a concept born from a program initially developed to reduce engineer and operator exposure to radioactivity. In the IT and OT context, it translates to reducing the functionality to only what is absolutely necessary.

A couple of cybersecurity maxims apply here. First, you can't secure what you don't even know you have. This is a comment on asset management, and the fact is that most larger critical infrastructure organizations don't achieve and maintain a comprehensive record of their assets to include the hardware, software, firmware communications, and the policy-driven and/or ad hoc processes used to operate them.

Here's another: Complexity fights security, or stated another way, you can't secure what you don't understand. An almost gratuitously high levels of complexity are what we've achieved and continue to layer on with applications and services riding on top of generous purpose operating systems undergirded by general-purpose hardware. Windows 10, while demonstrably more secure in many ways than its many generations of predecessors, includes many tools that can be turned against its users (see PowerShell, web servers, etc.). Current generation automobiles are now being recalled for patching, with multiple wired and wireless networks with processors running hundreds of millions of lines of code. All this latent functionality is a gift to attackers; it often comprises the primary playing field

adversaries will traverse to get where they need to go and accomplish what they seek to accomplish.

Ideally, from a cybersecurity viewpoint, a specific function is supported by a system, digital, or otherwise, customized to enable and support that function, and that function only. And if that cannot be achieved, it nevertheless can be aimed for, and the resultant reduction in complexity and therefore in attack surfaces will only serve to aid the defenders.Lastly, simplification is a specific aspect of resilience. In contrast to the massively complex and interdependent systems we have now, a better future lies in decomposing these into distributed and fundamental operations with simplified interactions, for instance, a distributed grid with primary responsibilities for local power support with microgrids and the bulk grid for supplemental needs only. Sharing or isolation can occur if the bulk grid is lost, but also, if a microgrid is compromised its effects remain localized.[15]

5 The Importance of Resilience Planning

Resilience is the ability to sustain or bounce back when stressed or compromised … to continue operating at a minimum useful level even when impaired. There is a connection between design simplification and resilience. There is a happy medium for any system between the two.

Why is resilience necessary?

- Any digital component or system may be compromised.
- Vulnerabilities always exist, known or unknown.
- Can't always stop the process and reboot.

  Current critical infrastructure and safety-critical control system designs are not able to handle multiple and coordinated malicious cyberattacks, and new failure modes from emergent properties of complex interdependencies and interactions. These systems are extremely brittle, and their operators, when faced with cascading failures and/or cyber effects, are unable to team up with the control system infrastructure engineers to achieve effective and timely resiliency responses. A more adaptive approach is needed, and this calls for new design approaches based on systems thoroughly vetted via engineering foundations.[16]

6 Engineering Information Control

Organizations and individuals should strive to make a prospective hacker's job as difficult and, therefore, as costly as possible. One way of doing this is by limiting the amount of technical information

about the product or process they can find online. While documents will be created and shared as part of every engineering design and development effort, there are things one can do to reduce their accessibility and minimize the spread of this sensitive information. For example, organizations should be prepared to protect the following types of information throughout the life of a project:

- Engineering records
- Drawings
- Requirements
- Specifications
- Designs
- Analysis
- Testing
- Detailed supplier-specific technical experience listed in job postings

While every employee has a role in this, responsibility for controlling these details falls in large part to procurement offices and departments. Social media, vendor websites, press releases, conference talks, etc., any and all of these have the potential to exposure unnecessarily detailed information to the wider world. Human Resources too has a large part to play, for instance, in developing policies related to reviewing, modifying, or terminating access when authorized users or key partners leave the organization.

7 **Procurement and Contracting**

Approximately half of the burden of containing or limiting open source exposure can be resolved via policies followed by the organization and its employees, with the rest falling to partners, integrators and suppliers. Contracts are the first and one of the best vehicles for beginning to lock down sensitive engineering information and should begin right at the RFP/tender/requirements stage.

Procurement language must specify the exact requirements a vendor must comply with as part of the system design, build, integration, or support. Depending on the product or service being procured, some of the cybersecurity capabilities and characteristics to consider include:

- Software Security and Secure Software Development Lifecycle (Secure SDLC)
- Access Control
- Account Management
- Session Management
- Authentication/Password Policy and Management

- Logging and Auditing
- Communication Restrictions
- Malware Detection and Protection
- Heartbeat Signals
- Reliability and Adherence to Standards

These requirements can raise procurement costs, but without them, caveat emptor. Costs related to bolting security on post procurement may be many times greater than if these functions were designed and built in the first place. Other points to consider relate to contractors and subcontractors who are allowed entry into your facilities:

- Be aware of what a subcontractor leaves behind on your network. You don't know where subcontractor devices were before today.
- Vendor tools such as calibration equipment or diagnostic equipment, which, unbeknownst to the vendor, may harbor malware (if digital).

Here are a few vetted resources for including cybersecurity concerns in the contracting process:

- Department of Homeland Security's DHS—Cybersecurity Procurement Language for Control Systems
- Energy-Sector Control Systems Working Group (ESCSWG)—Cybersecurity Procurement Language for Energy Delivery Systems
- Electric Power Research Institute (EPRI)—Cybersecurity Procurement Methodology Rev. 1 2013 Technical Report

8 Interdependencies

Few if any modern systems are 100% free of dependencies on other systems or processes. Complex digital systems have inputs from, connections to, and protections from other systems, and it is essential that system engineers understand the people and systems on which they depend and that these interdependencies may enable cyberattacks.

While engineering design builds on experiences from multiple disciplines, (including safety, quality, maintenance, chemical, etc.), all disciplines that share information between them have to gauge how a cyberattack would affect their primary areas of concern. Questions to begin with may include:

- On what people, services, or systems do you and your product/system rely?
- What services, systems, and people rely on your product/system?

Case in point: At the sector level, US legislators have come to realize that the reliable generation of electricity now depends upon the well-being of natural gas distribution pipelines. With a full third of US electricity now coming from natural gas, should key compressor station controls be sabotaged by either cyber or physical means, the impacts to the US grid could be substantial. Efforts are underway to tighten up cybersecurity policy and oversight for the natural gas distribution companies.

Similarly, thermal electricity generation plants (e.g., coal, natural gas, nuclear) require reliable water sources as coolant and to drive the turbines that produce electricity. And the complex modern grid completely depends upon robust communications capabilities for operator and reliability coordinators to do their jobs. And then there's financial markets, another sector without which the grid cannot function for long.

9 Cybersecurity Culture

It has become increasingly clear that damaging cyber breaches (see: NotPetya's $10 billion worldwide costs[17]) can impact the bottom line in ways similar to large safety failures.

A cyber-informed organization will ensure that while concerns with managing cybersecurity risk reduction factors will not entirely remake the way it does business (e.g., design discussions, partnering selections, M&A criteria, etc.) it will insist that a cyber professional has "a seat at the table" when any decision of consequence is being made.

But it's not just the inclusion of cybersecurity professionals in decisions they were once removed from, it's also the inculcation of a shared awareness of cyber risks in every part of the organization. All staff are part of the organization's cyber defense team and must understand, at a basic level, how damaging cyberattacks are made easier as more digital technologies (e.g., IoT, 5G, AI) are brought into everyday activities. From an engineering perspective, a cybersecurity culture must be formalized to include requirements that all interactions with digital elements receive adequate scrutiny.

As cybersecurity becomes increasingly involved into engineering process decisions, the engineering disciplines must be included in cybersecurity curricula. The Internet of Things will continue to stress organizational infrastructure while mobile technology will continue to add digital attack pathways.Bringing cybersecurity to the same level of acceptance and practice as safety would have an immense effect on the organization's defensive security posture.

And as in mature safety cultures, in cybersecurity spaces, a perpetual questioning attitude should be encouraged.

10 The Centrality of Digital Asset Inventories

For an enterprise, maintaining a comprehensive and accurate inventory of all digital assets is somewhere between a Russian nested doll, a labyrinth, and a marathon. But for an engineering firm designing a product or a system to be comprised of elements from multiple suppliers, the challenge can be similarly daunting. A digital inventory includes all hardware, software, and firmware, plus the policies and processes used to maintain it all. It drills down into the software to determine whether it's part of a packaged commercial application or platform, open source, or custom code. It needs to address whether cloud services are being used, and if so, the details of those services including how security is achieved and maintained by the cloud partners. Operating system version, patch-level, device drivers, dynamic load libraries (DLLs), and more must be annotated and tracked, for they constitute the environment adversaries will learn and leverage on the pathway toward achieving their goals.

Here's how the Atlantic Council described four types of complex software supply chain issues for suppliers and their customers alike[18]:

1 Supplier-Facilitated Risk: This refers to the cybersecurity of third-party partners who can influence energy-sector operations. For instance, systems integrators who design and implement products into energy-sector (and other industrial) operations environments, as well as other vendors who have physical or network access.
2 Counterfeit Goods: Components that come through an unauthorized channel are not authentic and would fail a sufficiently rigorous validation. Counterfeiters are typically motivated by financial gain, buying inexpensive components, and passing them off as more expensive ones. Negative impacts on operations are often an unintended consequence.
3 Malicious Taint: Components that often come through authorized channels are authentic and pass highly rigorous validation. Nonetheless, these components have some unintended functionality when placed intentionally by an adversary, which has negative implications on reliability, security, and safety. Typically,

introducing malicious taint requires very high-level capabilities and resources, such as those a nation-state may possess.

4 Unintended Taint: Components that come through authorized channels are authentic and pass highly rigorous validation. Nonetheless, these components contain quality defects in the form of software flaws or vulnerabilities, which may be known or unknown to the producer at the time of implementation.

Identification of counterfeit hardware also requires a more granular analysis that may not be readily apparent, including at the level of boards and chips. And not just for logic and memory but for I/O, interfaces, power supplies, cooling fans, and more. And as with software, the questions of provenance matter: Who made what, and when and where? And did any other third parties handle the hardware as it traversed other supply chains?

Organizations must also recognize the sensitivity of their inventories. Once collected, this information must be carefully protected, as it would be a "gold mine" for attackers. And despite the difficulties of this endeavor, this adage applies: You cannot protect what you don't know you have. And to protect it you've got to know it as least as well as your would-be adversaries.

11 Active Process Defense

Active defense is an advanced concept and requires highly skilled defenders to make it work. But as soon as resources and schedules allow, it behooves every engineering organization to begin to migrate from a purely passive cyber defense posture (e.g., network firewalls, antivirus, intrusion detection systems, etc.) to active defense. Technology researcher and writer Dan Woods describes five options available to active cyber defenders[19]:

1 Control the Scope of Damage: Quarantine the known infected systems and contain the attack in an isolated environment. This is a judgment call, often driven by the depth of expertise of the security team. The analyst may decide to watch the attacker or simply shut down the attack ….

2 Perform Forensic Analysis: Perform forensic analysis to better understand the attack. Once an attack is detected, the learning process can begin …. What does the adversary want to do next based on what they've done before? What network traffic is being generating? What payloads are they dropping? What processes are they loading? What data are they accessing?

3 Execute Standard Countermeasures: Execute playbooks for automated or manual responses in the event of a cyberattack. The ability to analyze the nature of an attack can in part be automated and made into playbooks to execute at the time of an attack. This type of automation can take the form of programs that find out everything about the traffic that came from a certain IP address or that crossed boundaries that no normal traffic should ….
4 Perform Threat Detection and Hunting: Search for evidence of similar attacks. Once you understand how an attack is working and what the adversary wants to do next, you can use that insight to search methodically through your IT and OT landscape to find similar infections that may not have been detected and fully remediated.
5 Gather Threat Intelligence: Record and share the nature of the attack with others. Native integrations between vendors and actively remove internal information silos and improve productivity. As part of the cybersecurity community, companies often share intelligence about attacks they have detected and understood. Active defense gives an opportunity to provide deeper and richer threat intelligence so that other cybersecurity practitioners can make both their own and industrywide defenses more powerful.

SECURITY AS A CO-EQUAL VALUE TO SAFETY

Though there's no such thing as (and there never will be) a completely secure system, some degree of cybersecurity will be built into every product and featured in every service when both sellers and buyers are fully "cyber-informed." That day will come as part of a culture shift comparable to what senior INL engineer Curtis St. Michel witnessed over the first half of his career at the lab. He recalls that when he started work in Idaho in the 1980s, safety incidents at the lab and across the country (in steel mills, in mines, in coal generation plants, on oil rigs and in refineries, in heavy manufacturing, and for telephone and electric linemen) were still somewhat common. Evidence suggests that while these types of jobs were dangerous everywhere, the United States was among the most dangerous places to work in the early-mid-twentieth century.[20]

Most accounts describe a slowly evolving safety awareness campaign that began with Massachusetts passing safety laws in 1887 and which gained traction with the rise of industrial manufacturing processes,

and the associated deaths and injuries in the early twentieth century and reaching a peak around World War II (WWII). Even though injuries tapered after the war, robust economic expansion in the 1960s saw safety incidents rise again. The Occupational Safety and Health Act (OSHA) was signed by President Richard Nixon in 1970, following attempts by his predecessor, Lyndon Johnson, two years prior to get the bill through Congress.[21] Sentiments for OSHA became further entrenched following the worst industrial accident in history. The 1984 Union Carbide chemical plant explosion in Bhopal India was a watershed: It killed 3,800 immediately with thousands more dying within months, injured tens of thousands, and exposed hundreds of thousands to the harmful effects of methyl isocyanate.[22]

So what St. Michel initially observed was the tail end of a process that had been in motion for a century, but that had not arrived at the mature state in which we find it today. As processes became more and more governed by new safety rules, he recalls, in an echo of how many chafe against security policies in 2020, "crusty" INL engineers complaining in the 1980s that they'd never get any work done if they had to perform their tasks with so much attention to safety.[23] Skeptics notwithstanding, work got done then and is getting done today. And safety culture is now so entrenched, so thoroughly codified in organizations performing potentially dangerous functions, that St. Michel says it would be extremely difficult for him to design and build an inherently unsafe system.

Yet the arrival of connected digital technologies in the inner sanctum of safety, Safety Instrumented Systems (SISs), shows that there is a looming blind spot in safety culture. It also shows that companies are willing to trade risk for cost savings and convenience, although perhaps they have been fooled by the vendors into thinking they're not taking on any additional risk when they connect their SIS to their control systems.

SIDEBAR: THE EVOLUTION OF SAFETY SYSTEMS[24]

1960s–1970s: Mechanical Simplicity

Safety systems were called emergency shutdown devices (ESDs). They were electromechanical relay circuits with discrete inputs (e.g., pressure, temperature, vibration, etc.). When inputs went outside pre-set parameters, logic would trip pumps, motors, valves, etc., preserving them in a safe state while diagnostics were performed.

1980s: Initial Arrival of SIS Complexity

Along with the arrival of microprocessors and PCs, process engineers began switching out mechanical relays for programmable logic circuits (PLCs). As relays were prone to frequent failure, the primary drivers for this were reliability improvements and attendant cost savings. (relays were) always configured to fail in an open position, which interrupted processes and that downtime cost the asset owners money. During the transition, though, some recognized dangerous PLC failures and failure modes. Specialty vendors (e.g., August, Triconix, ICS Triplex) emerged and created "triple modular redundant (TMR)" PLC solutions with three of everything (sensors, IO's, logic cards). Two out of the three systems had to agree to cause an interrupt. Systems included firmware on PLCs and stand-alone DOS-based programming terminals, which later switched to Windows.

1990s: Open Systems and the First Moves Toward Integrating ICS and SIS

Mirroring developments in the IT world, the 1990s saw a big push for "Open" SIS solutions, including:

- Windows APIs for programming
- Ethernet
- Modbus, OPC, and others vs. proprietary protocols

Open architectures allowed asset owners and their integrators to contemplate efficiency in addition to the other benefits they might gain by connecting control and safety systems. Standards-based architectures also made it possible to move away from the vendor lock-in that came with proprietary systems. At about this time, many asset owners found themselves maintaining different providers for ICS and SIS but noticed that each company would blame the other when something went wrong, and the customer was often left in the lurch, trying to mediate the dispute and arrive at a workable solution. But one company, Exxon, placed a high value on maintaining separation for vendor independence, and of course, safety reasons.

2000–2015: ICS and SIS Integration Stampede

Asset owners now sought to avoid the finger pointing and cost, devalued independence of control & safety vendors, and didn't

seem to notice that they were accepting cybersecurity trade-offs they might later come to regret. This decade and a half saw companies embrace integrated communications, HMIs, and common configurations too. Most chose to ignore the potential safety downside to the loss of independent systems, but when some asked, their vendors told them their internal development teams were independent, so not to worry.

2016–Present: TRISIS gives some Pause

As of early 2020, the roster of vendors selling integrated ICS and SIS solutions included:

- ABB
- Emerson
- Siemens
- Schneider
- Honeywell
- Rockwell
- Yokagawa

Asset owners concerned with safety are comforted by compliance to updated safety standards that are beginning to add security language to the mix, including IEC 61508 for suppliers and IEC 61511 for asset owners, the latter which added a security assessment requirement. Initially, very few did the assessments. But some, as they've become aware of the implications of 2017's TRISIS attack on an SIS in Saudi Arabia, have started to move in this direction. Still fewer than 25% do anything of substance beyond generating paper to document an assessment was performed. And everyone needs to be aware that now that safety systems are made of software and networked or integrated with other systems, like software-based control systems, safety systems themselves now have the potential to be threat vectors.[25]

Failure Mode, Near Misses, and Sabotage

Historically and still, the vast majority of working engineers, and the engineering school professors that help produce them, think of machine failure as something that happens when parts wear out. They do not consider that a machine might fail because an external actor was manipulating it or one of its supporting systems or processes.

In the software application world, in the early requirements and design stages, use cases help to establish and clarify desired functionality, look and feel, and more. Developers generate the different categories of users (e.g., administrators, customers, partners, HR professionals, etc.) and build the functionality needed for each. Access to different elements and capabilities is managed by authorization controls. One category of user rarely if ever considered by developers and their project managers (PMs) is the malicious cyber attacker. Assuming they can achieve access (and we should) the question is: What kind of experience do we want that person to have?

As every physical product is software-enabled, aka made "smart," in every engineering discipline, engineers must ask themselves what kind of experience they want criminals and other bad actors to have, then they arrive to intentionally misuse their creation. Data theft is one thing, misuse intended to cause damage or destruction, injury or death, is the province of modern cyber saboteurs.

Failure Mode and Effects Analysis

Begun in the 1940s by the US military, failure modes and effects analysis (FMEA) is a step-by-step approach for identifying all possible failures in a design, a manufacturing or assembly process, or a product or service.

- "**Failure modes**" means the ways, or modes, in which something might fail. Failures are any errors or defects, especially ones that affect the customer and can be potential or actual.
- "**Effects analysis**" refers to studying the consequences of those failures.

Failures are prioritized according to how serious their consequences are, how frequently they occur and how easily they can be detected. The purpose of the FMEA is to take actions to eliminate or reduce failures, starting with the highest-priority ones.

FMEA also documents current knowledge and actions about the risks of failures, for use in continuous improvement. FMEA is used during design to prevent failures. Later it's used for control, before and during ongoing operation of the process. Ideally, FMEA begins during the earliest conceptual stages of design and continues throughout the life of the product or service.[26]

The existing Safety Analysis and Probabilistic Risk Analysis (PRA) models were created with safety and failure mode analysis as its basis and design principles with electromechanical/analog technology in mind. With the now abundant use of digital systems for both safety and non-safety functions, this model must incorporate cybersecurity concepts and methodologies. Safety analysis should now consider previously analyzed unlikely or highly unlikely events that could potentially change those probabilities based upon an intelligent cyber aggressor. Revised analyses may yield different outcomes. Although malicious cyberattack methods may or may not change previously analyzed safety events, the potential for reactor sabotage or damage may increase.[27]

Inter-chapter Transition Thoughts and Questions

If this chapter tells you anything, it's that if we want to live in a more secure world with more secure products and services, we must have security subject matter experts (SMEs) involved in almost every decision in a product's or project's lifecycle. We're probably also going to want fewer folks in the workforce who are completely naïve about how their decisions and actions contribute or detract from the overall risk posture of their organization. So artificially marking 2020 as a starting point, here are a few things to consider:

- How do we increase the cyber IQ (if you'll pardon that term) of every member of our organization, top to bottom, without affecting adversely impacting productivity?
- Is it too early to include requirements for basic cybersecurity knowledge in every job description, with more advanced knowledge and/or skills mandatory for certain positions, and with extra consideration given to applicants who meet threshold criteria?
- Incentives for professional development in cybersecurity beyond the annual refresher training?
- How can we get more cybersecurity content into K-12 schools but especially in graduate and post-graduate engineering curricula?
- If it's going take a decade or more to include minimum cybersecurity requirements at the earliest stages of the design and acquisition processes, what can we do to better secure what we've already got? That means legacy: the industrial processes, fleets, buildings, we depend on right now and in the near-medium term.

NOTES

1 Richard Danzig. "Surviving on a Diet of Poisoned Fruit." Center for New American Security. July 21, 2014. www.cnas.org/publications/reports/surviving-on-a-diet-of-poisoned-fruit-reducing-the-national-security-risks-of-americas-cyber-dependencies.

2 Bob Anderson and Joseph Price. "Cyber-Informed Engineering: The Need for a New Risk Informed and Design Methodology." Page 1. www.osti.gov/biblio/1236850-cyber-informed-engineering-need-new-risk-informed-design-methodology.

3 Ibid., page 2.

4 Sarah Jensen. "How Did People in the Olden Days Create Software without Any Programming Software?" MIT School of Engineering, accessed April 3, 2012. https://engineering.mit.edu/engage/ask-an-engineer/how-did-people-in-the-olden-days-create-software-without-any-programming-software/.

5 "Side Rule." Wikipedia. Page accessed January 4, 2020. https://en.wikipedia.org/wiki/Slide_rule.

6 David Cohn. "Evolution of Computer-Aided Design." DE247, accessed December 1, 2000. www.digitalengineering247.com/article/evolution-of-computer-aided-design/.

7 "ES&S Sets High Standard in Elections Industry with Independent Third-Party Testing." Election Systems & Software web site, accessed April 30, 2019. www.essvote.com/blog/our-customers/idaho-national-lab-performs-independent-third-party-testing-of-voting-machines/.

8 Paul Stockton. "Securing Supply Chains." The EIS Council. Page 20. www.eiscouncil.org/App_Data/Upload/8c063c7c-e500-42c3-a804-6da58df58b1c.pdf.

9 Sean Mcbride. Written correspondence, May 2019.

10 Via email, June 2019.

11 Perspective from INL's Sarah Freeman: There's actually a ton of specialization these days in hacking …, so mostly people who learned to hack java websites are not going to become OT hackers (overnight or ever). The OT hacking space has gotten crowded not because more people are hacking OT but because there is more IT being implemented on the OT side. If you're curious about a person's background, just ask them if it's possible to hack a serial connection. The IT-focused among us will say no, that's not digital. The OT-focused hackers, however, will recognize that it's just another communication mechanism, like the rest, and capable of being manipulated like all the others.

12 Danzig, Ibid..

13 One of the lab's principal cyber and energy researchers, Virginia Wright, often kicks off her CIE talks with this statement.

14 Bob Anderson et al. "Cyber-Informed Engineering." Accessed March 1, 2017. www.osti.gov/biblio/1369373-cyber-informed-engineering.
15 INL's Dr. Craig Rieger in correspondence, January 7, 2020.
16 INL's Dr. Craig Rieger in correspondence, January 7, 2020.
17 Andy Greenberg. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired Magazine* online, accessed August 22, 2018. www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
18 Beau Woods and Andy Bochman. "Supply Chain in the Software Era." The Atlantic Council, accessed May 30, 2018. www.atlanticcouncil.org/publications/issue-briefs/supply-chain-in-the-software-era.
19 Dan Woods. "5 Ways to Fight Back against Cybersecurity Attacks: The Power of Active Defense." *Forbes* online, accessed June 27, 2018. www.forbes.com/sites/danwoods/2018/06/27/5-ways-to-fight-back-against-cybersecurity-attacks-the-power-of-active-defense/#1cbe940646d7.
20 "History of Workplace Safety in the United States, 1880–1970." EH.net web page, accessed January 4, 2020. https://eh.net/encyclopedia/history-of-workplace-safety-in-the-united-states-1880-1970-2/.
21 Ibid.
22 "On 30th Anniversary of Fatal Chemical Release that Killed Thousands in Bhopal, India, CSB Safety Message Warns It Could Happen Again." Chemical Safety Board website online, accessed December 1, 2014. www.csb.gov/on-30th-anniversary-of-fatal-chemical-release-that-killed-thousands-in-bhopal-india-csb-safety-message-warns-it-could-happen-again-/.
23 Curtis St. Michel, in conversation, February 2019.
24 Interview with John Cusimano of aeSolutions on the evolution of safety systems, June 24, 2019.
25 Paul Stockton, in conversation, February 12, 2020.
26 "Failure Mode and Effects Analysis." American Society for Quality website, accessed January 4, 2020. https://asq.org/quality-resources/fmea.
27 Bob Andersen et al. "Cyber-Informed Engineering." Page 2. March 2017. https://inldigitallibrary.inl.gov/sites/sti/sti/7323660.pdf.