chapter twelve

Securing supervisory control and data acquisition control systems

Nathan Lau, Hao Wang, Ryan Gerdes, and Chee-Wooi Ten

Contents

12.1 Security of critical infrastructures ................................................................. 237
12.2 SCADA systems ........................................................................................................ 239
  12.2.1 Nature of SCADA cybervulnerabilities ................................................... 241
12.3 HCI issues in the cyberkill chain ................................................................. 242
12.4 Promising research and design directions ......................................................... 246
  12.4.1 Individual users and components ............................................................... 246
  12.4.2 User interface design ............................................................................... 247
  12.4.3 Teamwork and resilience .......................................................................... 248
  12.4.4 Risk assessment and resource allocation ................................................ 248
  12.4.5 Attacker attribution, intelligence coordination, and deterrence (geopolitics)...249
12.5 Conclusions ............................................................................................................. 250
References ..................................................................................................................... 250

12.1 Security of critical infrastructures

National physical infrastructures are often operated by industrial control systems (ICSs) that heavily rely on information and communication technology (ICT). Specifically, industrial control systems of many sectors are built around the supervisory control and data acquisition (SCADA) architecture, consisted of communication network connecting servers, clients and embedded computer devices for automation, and operators to monitor and control the physical equipment. For example, water treatment, petrochemical, agriculture, and critical manufacturing facilities all adopt SCADA technology [1–3]. SCADA systems contribute to efficient operations of many critical infrastructure sectors. For example, the smart grid has increased prediction accuracy in loading shedding (i.e., matching generation to demand), which reduces 10% costs for utilities and consumers [4].

The significance of SCADA systems in operating critical infrastructures has made them prime targets of cyberattacks to inflict major disruptions on our society. As of 2015, the Repository of Industrial Security Incidents database contained over 250 SCADA incidents in the past two decades globally [5]. Table 12.1 [6–10] outlines the most prominent attacks on SCADA systems highlighting some worrisome cybersecurity trends. First, these prominent cyberattacks inflicted severe physical damages and service disruptions, indicating that malware are no longer only targeting traditional information technology systems. Second, the attacks targeted diverse infrastructure sectors, suggesting that all major systems are likely vulnerable to cyberintrusions. Third, the malware were unique and sophisticated, highlighting the skills of the attackers. For example, the most infamous
<table>
<thead>
<tr>
<th>Target organization</th>
<th>Time</th>
<th>Delivery method</th>
<th>Malware or exploits</th>
<th>Target device</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australian Maroochy Shire Sewage System</td>
<td>Feb.–Apr. 2000</td>
<td>Insider with identical radio system</td>
<td>Insider</td>
<td>Pumping stations: RTUs</td>
<td>Overflow of over 800,000 liters of untreated sewage</td>
</tr>
<tr>
<td>Davis–Besse Nuclear Power Plant</td>
<td>Aug. 2003</td>
<td>E-mail attachments</td>
<td>Slammer worm: SQL server worm</td>
<td>Network hosts</td>
<td>(DOS) Disable monitoring system and control network communications</td>
</tr>
<tr>
<td>Iranian Natanz nuclear facility</td>
<td>?–Jul. 2010</td>
<td>Removable drives (USB), suspected insiders</td>
<td>Stuxnet</td>
<td>Gas centrifuges: PLCs</td>
<td>Destroyed gas centrifuges in Iranian nuclear facilities</td>
</tr>
<tr>
<td>Saudi Aramco Oil Refinery</td>
<td>Aug. 2012</td>
<td>N/A</td>
<td>Shamoon virus/ Ransomware</td>
<td>Oil refinery workstations</td>
<td>(DOS) Affecting global energy sector, such as Saudi Aramco (oil refiner)</td>
</tr>
<tr>
<td>US Power Utility intrusion</td>
<td>Oct. 2012</td>
<td>Removable drives (USB)</td>
<td>Mariposa virus</td>
<td>N/A</td>
<td>(DOS) Plants shut down for 3 weeks</td>
</tr>
<tr>
<td>German Steel Mill cyberattack [8]</td>
<td>Dec. 2014</td>
<td>Phishing with e-mail attachments</td>
<td>Unknown</td>
<td>Work station PLCs and plant network</td>
<td>Blast furnace explosions</td>
</tr>
<tr>
<td>Ukrainian power grid cyberattack [8]</td>
<td>Dec. 2015</td>
<td>Phishing with e-mail attachments</td>
<td>BlackEnergy 3 malware</td>
<td>Workstation RTUs</td>
<td>(DOS) Disconnect seven substations for three hours</td>
</tr>
</tbody>
</table>

Note: DOS, denial of service.
malware is Stuxnet, which employed four unique vulnerabilities to inflict damage on the gas centrifuges in the Iranian uranium enrichment facility [11].

The perpetrators for most cyberattacks on critical infrastructures are nation states motivated by complex, geopolitical objectives. This stands in contrast to traditional cybercriminals interested in financial incentives only. For example, the 2015 Ukrainian power grid cyberattack that caused power outages affecting over 225,000 customers [8] was followed by the 2017 Petya ransomware attacks, which affected multiple state-owned enterprises including the Boryspil International airport and the Chernobyl nuclear power plant [9]. Russia was the alleged attacker reacting to the ousting of former President Viktor Yanukovych (who favors ties with Russia) and the possibility of joining the European Union and North Atlantic Treaty Organization [12,13]. Further, as part of their military strategies, many governments operate state-of-the-art facilities and employ highly trained professionals to create and stockpile zero-day exploits—undisclosed vulnerabilities exploited by attackers for system access and control. For example, the 2017 global ransomware attack was allegedly enabled by stealing exploits created by the US National Security Agency [9]. Nation states can also employ other methods, including insider and supply chain attacks. These attacks can be difficult to defend due to the number of components and personnel involved in the design, operations, and maintenance of SCADA.

The cybersecurity of our critical infrastructures requires sociotechnical solutions to defend against highly sophisticated cyberattacks on SCADA systems. Human–computer interaction (HCI) plays a central role in these sociotechnical solutions. This book chapter provides an overview of research and challenges in the human factors of SCADA cybersecurity. The remainder of this chapter is organized as follows: The next section begins with a description of SCADA technology pervasive in critical infrastructures and highlights attack targets and security issues that put functions of many critical infrastructures at risk. Following the next section, HCI issues are identified by examining the seven phases of the cyberkill chain, the process by which adversaries stage their attacks. Lastly, we conclude with potential research directions in HCI that can strengthen the defense of SCADA platforms.

### 12.2 SCADA systems

SCADA is a control architecture adopted by most industrial control systems that enable human and automation in monitoring and controlling industrial processes [14,15]. SCADA systems usually contain three segments of ICT—field devices, the SCADA/control network, and the corporate network—connected as in Figure 12.1 [16].

Referring to Figure 12.1, networking devices, such as switches, cables, and wireless radios, provide communication services to the SCADA components. These networking devices are mainly Ethernet-based [17], which supports the communication protocols commonly adopted by field devices. Common protocols implemented in SCADA include distributed network protocol (DNP3), modbus, and fieldbus that are not adopted by the corporate network or the World Wide Web. Computer servers and clients host supervisory control applications, a historian, and the human–machine interface (HMI). Supervisory control applications process the sensor data and configure control loops executed by the field devices. The historian logs all process data that can provide a basis for plant engineers to diagnose anomalies and develop new control algorithms. Finally, the HMI provides the means for control room operators to monitor the industrial processes and assume manual control as necessary.
Authorized licensed use limited to: 10.3.97.143. Downloaded on: 05/17/2023 05:17:20 AM. Redistribution subject to license terms at https://www.cambridge.org/core/terms. Connected to the SCADA network are field devices that include remote terminal units (RTUs), programmable logic controllers (PLCs), and intelligent electronic devices (IEDs) for processing sensor data and issuing control commands [18]. PLCs and RTUs are digital computers customized for executing control and safety functions of industrial processes. IEDs are sensors and actuators with microprocessors for collecting plant data and changing equipment settings, respectively. The common communication protocols are DNP3 (IEEE 802.3) and modbus [14,19]. In other words, PLCs and RTUs process sensor data to issue control commands according to control loops configured by process engineers through supervisory control applications hosted by SCADA network computers. Further, PLCs and RTUs relay sensor data and actuator settings to computers hosting the historian and HMI via fieldbus protocols specified by IEEE 7-4.3.2 [20,21].

The corporate network is a common information technology (IT) network found in most businesses. Corporate networks typically consist of Ethernet-based network devices, servers, and desktop computers for carrying out business and engineering activities such as marketing, e-mails, engineering design, data analysis, and cloud-/Internet-based services. Traditionally, the corporate and SCADA networks are completely isolated from each other; however, recent implementation mediates the connection between the two networks through a demilitarized zone, firewalls, and/or additional routers [22]. This mediated network connection enables users to access data or update the configuration of SCADA components while performing other tasks only available on the corporate network (e.g., e-mail access).

Figure 12.1 Generic implementation of SCADA.
services). The corporate network adopts the more common communication protocols (e.g., user datagram protocol) and connects to the Internet.

12.2.1 Nature of SCADA cybervulnerabilities

Cybersecurity is essential for maintaining operations of our critical infrastructures. However, SCADA implementations in most critical infrastructures are extremely difficult to defend due to legacy, functional, and system design reasons [16].

SCADA technology evolves from the gradual deployment of embedded computers and microprocessors primarily designed to enhance the efficiency of supervisory control. Modern SCADA implementations increase connectivity among internal components and to other networks for maximum automatic and distributed process control [23], dramatically increasing the likelihood of intrusions [22]. Meanwhile, many SCADA technologies with virtually no security foundation in their design have become open standards and heavily deployed for their supervisory control functions. For example, commonly used industrial protocols such as modbus and DNP3 often do not support information integrity checking or authentication mechanisms between master and slave devices, resulting in potential risks in the corruption of control commands. Publicly known information of SCADA systems also allows attackers to gain in-depth system knowledge and access to technology [24]. Typically, critical infrastructure sectors are capital intensive and long-term investments and are likely to operate with either older equipment built with minimal security features or new equipment built on a relatively poor security foundation.

Besides legacy design issues, functional requirements place additional constraints on security. The control of physical processes can be highly sensitive to time lags prohibiting computationally intensive encryption or other mechanisms. For example, the nuclear industry gives high priority to the response time of safety systems [25]. SCADA systems also tend to run on out-of-date software that contains known, or probable, vulnerabilities. Prior to any software patching, validation activities must be conducted to ensure all control and safety functions must remain intact. Otherwise, the security updates would introduce undue risk into operations of the physical process [26,27]. This delay in patching software extends the time for attackers to deploy known exploits.

Finally, general system design characteristics may also constrain the cybersecurity of SCADA. These systems are inherently complex sociotechnical systems relying on many different types of components and professionals working internally and externally to their organizations [28]. Consequently, the attack surface for all system is immense. The individual components as well as the interfaces between the wide spectrum of technologies need to be secured. Also, connectivity is likely to increase for cloud-based services [29]. For example, smart grid systems will likely operate in a more decentralized paradigm, in which distribution network operators will need remote access to many geographically distributed and small-scale power generators, such as solar and wind [30]. As a result, many workers, or simply users such as homeowners, are necessary to operate and maintain SCADA components, thereby increasing the possibility of credentials being leaked through access control mismanagement (i.e., careless handling of passwords) or phishing (i.e., fraudulent e-mails resulting in malware infection that steals credentials). There is also the prospect of insider attacks, in which employees with system access can circumvent technological preventions [31].

The weak security foundation has resulted in SCADA systems being the prime targets for cyberattackers to inflict damages on physical infrastructures without any use of force [32]. Security measures guarding these cyberthreats must account for the two
unique aspects of cybersecurity in SCADA systems. First, security efforts must consider how SCADA devices for controlling physical processes/equipment are designed, configured, operated, and maintained differently from conventional computer network systems. Equally important, cyberattacks on SCADA systems are best characterized as a part of warfare given their geopolitical motivations, as opposed to cybercrimes driven by financial incentives. These two essential aspects suggest that a military perspective on disrupting the cyberattack process would be appropriate for identifying and developing security mechanisms for the design, implementation, operation, and maintenance of SCADA devices. The next section examines the security mechanisms and HCI issues pertinent to thwarting adversaries’ attack process, commonly known as the cyberkill chain [33]. We also relate each phase of the cyberkill chain to the infamous Stuxnet cyberattack on the Iranian enrichment facility to exemplify this approach for identifying HCI issues.

12.3 HCI issues in the cyberkill chain

The cyberkill chain refers to “a systematic process to target and engage an adversary to create desired effects.” [33, p. 4]. The cyberkill chain consists of seven phases: reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), and actions on objectives [34].

The first phase is reconnaissance, during which adversaries identify, select, and profile targets through legal and illegal means. In other words, this is an information-gathering activity about the targets for developing custom cyberthreats. Many of these activities can be legal, such as gathering information on specific employees for targeted phishing [35] or studying the vulnerabilities of SCADA devices [36], while others, such as industrial espionage, may be illegal [37]. Adversaries may automate part of this process with web crawlers that generally do not pose any serious security threats [38]. For example, the Stuxnet attack in 2011 likely involved some form of espionage. It is now surmised that the alleged attackers were the American and Israeli governments, interested in obstructing Iran’s progress toward developing nuclear weapons [39]. During this phase, the attackers became knowledgeable about personnel and details of the SCADA system configurations in Iranian nuclear facilities.

Thwarting reconnaissance, then, like that described earlier against Iran, clearly requires tight information control to prevent adversaries from acquiring personnel and technical information to devise cyberattacks [5]. However, tight information control presents major issues for employees striving against deadlines to complete their work or achieve other system goals. For example, roles and contacts of key employees (or their relatives and friends) are meant to be communicated freely, but this information is sufficient for adversaries to identify phishing targets for spreading malware to obtain credentials for access to SCADA networks [40]. Technical and configuration information about the SCADA system such as control application software is equally difficult to conceal, as it may be sufficient to be used by adversaries to infer system vulnerabilities [22]. Therefore, the central HCI issues would be how technical and personnel information can be communicated among authorized persons in a manner that would hinder reconnaissance while not affecting work efficiency.

The second phase is weaponization, during which adversaries employ information from reconnaissance to design and develop a malware or the payload—a binding software application with remote access that supports C2 by the attackers. The attackers set up clients and servers to support C2 and develop malware relying on exploits in the operating systems, software applications, communication protocols, and firmware of SCADA
devices. The most infamous cyberweapon is Stuxnet, a malware that is capitalized on four zero-day exploits to self-install and self-destruct, replicate across removable drive and networks, communicate to external servers, and manipulate supervisory control software while bypassing any detection.

Weaponization technically does not involve any interaction with SCADA components or personnel, so thwarting this phase requires overall security improvements in the design, implementation, and operations of SCADA systems such that “hacking” becomes more difficult. Unfortunately, limited funds or research efforts are committed to secure SCADA-oriented software development, although hackers frequently take advantage of bugs in existing software for intrusion [41,42]. SCADA systems often employ commercial off-the-shelf (COTS) hardware and software to be cost-effective; however, COTS components permits adversaries to access the SCADA technology and discover exploits more easily than they can with custom “obscure” components [43]. Risk analysis is needed to clearly justify the return on the required investment For this reason, the main HCI issue concerning weaponization is developing “usable” cyberrisk analysis that can communicate to the decision makers about the investments needed to integrate upgrades to cybersecurity as part of the system design rather than as after thoughts [44,45].

The third phase is delivery, during which the cyberweapon is transmitted to the target network or computer system. Interestingly, cyberweapon delivery to SCADA relies on common and traditional methods: e-mail attachments [46], forced download [47], removable media [e.g., universal serial bus (USB) drives, [48]], and domain name system spoofing [49]. These delivery methods mostly intrude the corporate network that turns out to be a convenient stepping stone into the SCADA network. Delivery can be much simpler, with insiders who have sufficient privilege to install the malware or assist with the delivery in some other way. Insider delivery may also occur in the SCADA system supply chain, involving component manufacturers or transporters [50]. Stuxnet is infamous for deploying the payload on USB drives inserted into some SCADA system computers and spread to other computers through self-replication in the network of the system [51]. Although some types of generic malware can spread on its own through a network and removable drives, the Stuxnet attack was suspected to have involved insiders because the deep knowledge of the SCADA systems in the Natanz facility appeared necessary in order for this attack to have been carried out so successfully [52].

Thwarting delivery can be achieved by isolating system components, networks, and users to prevent exposure to cyberweapons. This approach has become the dominant strategy to cybersecurity. Specifically, cybersecurity has focused on perimeter-based solutions [53], including firewall, antivirus, access policy (e.g., disabling all USB ports), and authentication to block or identify suspicious traffic from entering into the system. Similar to preventing reconnaissance, isolation easily conflicts with productivity or other business objectives [53]. Application-oriented access control, including sandboxes, is also fraught with usability issues [54]. HCI issues in thwarting delivery involve developing perimeter-based solutions that are inherently flexible to accommodate a wide range of worker activities involving frequent communication with external networks or systems that can contain threats. For example, operations of many companies rely on cloud computing and the Internet of things that potentially expose the corporate and thus SCADA networks to much more malware. Further, these perimeter-based solutions must include user friendly interfaces for supporting appropriate configurations with considerations to cyberrisks.

The fourth phase is exploitation, which refers to leveraging the exploits in the software, communication protocols, or even workers to trigger the execution of malware code without detection. For example, a PDF attachment in a phishing e-mail that appears to be
sent from a friend may be sufficient to elicit a click to initiate the installation of malware [55]. Further, sophisticated cyberattacks often employ multiple exploits to trigger installation (i.e., both human and software/protocol). Besides efforts in their discovery during weaponization, exploits engineered into the cyberweapon at the time of the development must remain effective against the operating systems and intrusion detection software after delivery. Otherwise, malware installation would be detected leading to removal or some cyberresponse. Stuxnet likely exploited both human and software vulnerabilities in that workers were successfully tempted to plug USB flash drives of unknown origin into a SCADA computer, and the infected USB drives took advantage of Windows “autorun” vulnerabilities (i.e., LNK and autorun.inf) to initiate self-install.

Mitigating exploits requires timely actions that eliminate human and machine vulnerabilities on which cyberweapons capitalize [56]. In general, software patching and updating can thwart some exploitations of the technology, but extensive functional testing is required to ensure safe and efficient operations of physical equipment [36]. Meanwhile, human vulnerabilities can be reduced with training and cognitive aids (e.g., spam or malware alerts). HCI issues related to human vulnerabilities and solutions are extensively examined for IT systems (see Iachello and Hong [57] and Sasse et al. [58]); however, both training and cognitive aids must be augmented to include materials specific to SCADA components and configurations. For example, SCADA employees must be trained to guard against latest infection methods that could jump the “air gap” (i.e., not connected to the Internet) such as removable drive infection after the forensics of Stuxnet was published. In general, essential HCI research includes effective training methods on information privacy and security and intuitive cognitive aids to reduce the likelihood of human exploitation [59]. Further, developing usable tools for testing software patches and tracking vulnerabilities for threats related to patching delays is needed.

The fifth phase is the installation of the malware that inject codes into the operating systems and software applications for adversaries to gain remote access and persistence (including some functional controls of the software) inside the target environment. This installation phase is intricately linked to exploitation (previous) and C2 (next). Installation is thus very complex because the exploits must target software applications specific to controlling SCADA components and the operating systems, to temporarily bypass security software and system authority. Then, installation needs to reoccur during C2 when attacker servers discretely update the malware. For Stuxnet, after the initial exploitation, the malware first gathered host information [e.g., operating system (OS) version and antivirus] to match targets. The actions are followed by either self-removal or installation/code injection to leverage the necessary exploits for authority escalation. Stuxnet has a two-part code injection. Common to most cyberattacks, the first part of code injection targeted background processes of the Windows OS that could obfuscate its traces, infect removable drives, and communicate with other resources in the network. Unique to attacks on SCADA systems, the second part of code injection targeted the supervisory control application (i.e., Siemens Step 7) to gain access and control of PLCs that gather sensor data and issue a command to centrifuges for enriching the uranium.

Thwarting the malware installation and code injection essentially requires the same security mechanisms for mitigating exploitation that provides authority escalation and vector obfuscation. In other words, mitigating exploitation with software updates or worker aids can directly hamper installation. When systems fail to prevent exploitation and installation, security would need to rely on scanning the network for malicious code and testing software for integrity. Although useful, both mechanisms cannot guarantee security, as signatures of malicious codes are often well hidden [60] and software integrity is
testable only for well-defined criteria, such as safety-critical events that should never occur [61]. Further, the characterization of detected malicious codes or software compromises in the system is necessary to support security and operations personnel in assessing potential cyberimpacts and physical impacts to inform intervention (e.g., degraded operations versus shutdown). Hence, HCI issues concern developing tools that help workers identify and characterize compromises to support decision-making. Further, HCI research should support creating effective forensics tools for detecting points of delivery and exploitation that would require monitoring and subsequent elimination [62] and developing usable alarm systems for prioritizing attention toward high-risk areas.

The sixth phase is C2, during which the malware establish a communication channel to attacker servers to transmit information, receive updates, and execute commands. C2 can be particularly lengthy because adversaries must time their strikes based on the dynamics of geopolitics. An unnecessary strike could result in an extremely undesirable effect, including unwanted retaliation against the attackers. Forensics of the Stuxnet indicated a lengthy C2 phase as suggested by the registration of the very first server to be five years prior to action on objectives or physical damage to the centrifuges. During those five years, more C2 servers were registered to gather information on the operating system, the SCADA software configuration and network traffic [11].

The C2 phase can be foiled with advanced network intrusion and traffic monitoring that can aid workers in tracking and acting on malware infection. C2 can be like a lengthy game between attackers and defenders. Attackers can gather information and update the malware, while defenders can detect foreign intrusion and neutralize cyberweapons. HCI issues include developing visualization and expertise that help identify suspicious network traffic, with consideration to the geopolitical climate. Further, HCI research should help develop usable tools for the manual inspection of communication paths between SCADA network and untrusted areas.

The final phase is actions on objectives, when data exfiltration, network spreading, and system disruption occur. Attacks on SCADA typically begin with data exfiltration to acquire additional information on targets that could lead to malware updates for more targeted code injections to exact the physical sabotage of interest. Thus far, the phases of the kill chain are presented as sequential for simplicity. In reality, attackers persistently advance all phases to maintain access in the target environment because system updates or security responses could thwart one part of the kill chain and thereby neutralize the cyberweapon. This phase interacts with earlier phases through network communication and malware updates/installations. The alleged attackers of American and Israeli governments began developing Stuxnet in the early 2000s. American–Israeli attackers acted on their objective to obstruct the development of nuclear weapons when a series of International Atomic Energy Agency reports presented evidence of Iran’s progress toward uranium enrichment in late 2010s [63–65]. To inflict physical damage on Iran’s enrichment facility, Stuxnet injected codes into the supervisory control software (i.e., replaced the s7otbxdx.dll) that rewrote the control algorithm of the PLCs to issue commands of erratic rotational speeds to centrifuges and transmit misleading speed information to the operator displays.

Actions on the objectives of an adversary are not preventable if a defender cannot thwart earlier phases of the kill chain; however, the impact of cyberattacks can be reduced with resilient systems operation design. That is, the workers should be ready to respond to cyberevents by executing alternative procedures or adaptive work-arounds to operate through compromises or to shut down safely. HCI issues in this area require workers to engage in creative problem-solving supported by training and effective user interface
design (e.g., Cone et al. [66] and Wei et al. [67]). Further, the response to cyberthreats aimed at inflicting damages to physical process also means that teamwork between security and operations personnel is essential [68]. Consequently, another HCI issue is developing intuitive collaboration user interfaces that illustrate how the compromised SCADA or cyber-components interact with equipment to affect the physical process. Finally, additional workforce may need to mobilize depending on geopolitical situations like how airports or other public areas increase physical security.

12.4 Promising research and design directions

As illustrated through the cyberkill chain and exemplified by the Stuxnet attack, the complex and evolving nature of cyberattacks on SCADA components present increasing challenges in the design, implementation, operations, and maintenance of current and future SCADA systems. SCADA systems must have the quality of preventing and adapting to successful cyberattacks. Thus, generally, human workers with better adaptive capabilities than machines are central to sociotechnical solutions for securing SCADA systems. However, HCI research on SCADA technology, let alone the cybersecurity challenge, is limited in the literature. The examination of the cyberkill chain, nevertheless, alludes to a multitude of interdisciplinary security approaches to thwarting cyberattacks. This section presents promising and emerging HCI research for securing SCADA, ranging from the perspectives of educating individual workers to shifting the asymmetric nature of cybersecurity.

12.4.1 Individual users and components

Much of current cybersecurity attention has been aimed at mitigating flaws in individual users and SCADA components. Common users are typically uneducated about cybersecurity for both IT and SCADA systems. They tend to place blind trust on the security features of the product to thwart malicious materials that could lead to cyberintrusion [69]. For example, researchers have been examining human susceptibility pointing out that males are more susceptible to phishing [70]. In addition, research has also discovered vigilance increments driven by incentives and diligence with appropriate trust on security functions [70,71]. Effective methods of minimizing common and naive human exploits include embedded training; contextual training; and online education against fraudulent e-mails, website, or attachments [72]. HCI efforts have been applied to studying different aspects of user authentication, such as password compositions [73] and two-factor authentication [74,75]. Regarding SCADA network security, research has shown narrative-based training to be more effective than tool-based training or other combinations of training methods [76]. Additional research and development on training tools is particularly necessary to address the risk associated with cloud services in SCADA technology. In general, much of the research and education effort focuses on the corporate network, neglecting the risk of SCADA components being compromised and potential impact on the physical processes.

An impending research area is a human-centric perspective of cybersituation awareness (cyber SA). Current research on cyber SA mostly adopts a data modeling perspective that focuses on what and how data in the system can be fused to identify activities of attacks. The literature contains virtually no empirical studies examining the cognitive work of how security analysts achieve cyber SA or acquire knowledge about attacks. Similarly, research formulates several key measurement dimensions of cyber SA: how well systems hypothesize true attack tracks (confidence), quality of evidence for the hypothesized tracks
Chapter twelve: Securing supervisory control and data acquisition control systems

(purity), cost associated with signaling true and false positives, timeliness in detecting an attack for meaningful response, and the effectiveness in supporting cyberresponse [77]. Although theoretically applicable, measurements of these SA dimensions have not been investigated for assessing security personnel. The literature on cyber SA of the human workers is in paucity, representing a significant knowledge gap for designing optimal training programs and user interfaces.

Research on advancing average users in security skills and knowledge is comparatively limited with respect to the effort on technical solutions in securing current SCADA components or system processes. Although not necessarily driven by a user-centric development process, these technical solutions are briefly described to provide the context for the subsequent discussion on HCI associated with those solutions. Technical solutions under investigation and deployment include the following:

1. **Protocol security advancement** enables authentication and encryption that were neglected in the initial development of communication protocol. The development of advanced protocols incorporates evolving security technologies such as hash-based message authentication and cryptographic primitives [78].

2. **Perimeter-based access control** regulates data/communication traffic to prevent unauthenticated data or restrict authenticated data into a selected part of the network. Recent advances include software-defined networking [79] that relies on centralized traffic controllers rather than configuring network policy for individual networking devices.

3. **Network intrusion monitoring** observes and records network data including packet signature, time stamps, origin and destination Internet protocol addresses of network attempts, types of network event, and frequency of attempts/events [80]. Since heuristics based on past events are typically ineffective against zero-day attacks, network intrusion monitoring shifts toward a signature-less approach, relying on machine learning to detect traffic anomalies [81].

4. **Cyberdenial and deception** employs decoys to collect data on behaviors and induces poor decision-making by the adversaries. The most established technical implementation is honeypot, which serves as a decoy network intended to be attacked and closely monitored to obtain valuable attacker information. Honeypot can produce an early warning call while slowing down an external cyberattack [82]. A SCADA version of honeynet is being developed to protect critical infrastructures (see Lukas. Rist [83]).

### 12.4.2 User interface design

Realizing the potentials of various security features requires that technical innovators give attention to HCI, particularly user interface design. User interfaces can play a vital role in configuring perimeter-based solutions and understanding the impacts (or controls) on traffic to enable effective communication between, and preventing intrusion into, SCADA components (e.g., Wool [84]). More importantly, user interfaces visualizing network traffics in relation to the physical process can enhance cyber SA required for the resilient response to cyberthreats. However, traffic monitoring systems require substantially more attention in research and development to support human intelligence in confirming the detection and evolution of suspicious traffic. Advanced methods relying on machine learning for design and evaluation of user interfaces are warranted [85]. Simple but mature cognitive aides, such as spam filters and warnings of a suspicious attachment, should not be
forgotten as they can improve user comprehension of potential risks of common intrusion vectors into IT systems or the corporate network [86].

HCI research is only recently attending to cyberdenial and deception. For example, One military exercise indicates the importance of adaptive problem-solving in human analysts when using honeynet for cyberdenial and deception [87]. The exercise also suggests that automation is currently incapable of sophisticated cyberdenial and deception, where the careful inference of adversarial behaviors, intents, and weaknesses is required. Thus, HCI research can play an important role in providing effective user interfaces for deploying advanced tools in SCADA systems to counterdeceive adversaries.

12.4.3 Teamwork and resilience

The technical and human response against SCADA attacks requires collective and coordinated efforts of employees with diverse interdisciplinary background to cover the vast attack surface of SCADA systems. The corporate and SCADA network staff must collaborate for system setup and threat diagnosis, as the two types of technology are converging. For example, many modern day control devices can likely connect to the Internet for cloud services to be offered by vendors [88]. Such trends present a trade-off between functionality and exposure that should be jointly examined by corporate and SCADA network personnel. Given confirmed intrusions, SCADA cyberresponders must collaborate with corporate administrators and control engineers to disconnect certain service paths for the prevention of further damage and review the restoration plans [8].

Cyberresiliency demands adaptive responses from many coordinated workers in SCADA [89,90]. For example, the financial cost and social impacts due to a temporary shutdown of a power plant must be considered with respect to the concerns in operational safety and compromises in security. That is, an effective cyberresponse not only demands security and operations staff to manage different technologies, but also challenges managers with financial and ethical dilemmas. There are many components to teamwork, as suggested a team effectiveness model for nuclear power plant cybersecurity [91] featuring communication, collective problem-solving, trust, shared knowledge of expertise, and adaptation. Further, government agencies can provide regular support by highlighting security solutions and alerts during times of high cyberthreats (cf., physical security level of public places). Each teamwork component can be enhanced with collaboration tools or computer-supported cooperative work. In the cyberdomain, large teams and massive information flow may also have drawbacks due to complexity with coordinating a larger number of people and the potential of propagating problems in the system [92]. In brief, research on multidisciplinary teamwork or collaboration between different personnel is pivotal to the robustness and resiliency of SCADA [93].

12.4.4 Risk assessment and resource allocation

The cybersecurity of critical infrastructures heavily depends on the commitment of upper management or leaders of organizations, similar to how safety must “begin from the top” [94]. Investment decisions or resource commitments are driven by the business case based on risk analysis rather than anecdotes of high-profile attacks and potential implications of SCADA attacks. For this reason, there has been substantial research in cyberrisk analysis [95], especially in quantitative modeling. Exemplary models include hierarchical models [87], attack trees or attack countermeasure trees [96], and graph theory-based models [97].
Much of the quantitative modeling work is built on machine-learning that is labor intensive with limited opportunities for empirical validation.

The complex nature of risk assessment methods can challenge practitioners who are continually performing analysis in response to constantly evolving threats. HCI research may ease the challenge by improving the usability of analysis tools and methods. For example, triage analyses (filtering for data of suspicious activities) requires more focused attention than escalation analyses [98]. This finding indicates that visualizations should differ between the two types of analysis. Meanwhile, incomprehensible risk assessment can challenge organizations in allocating resources and devising strategies (e.g., training) to defend different SCADA segments [99, pp. 41–80]. Risk analysis should thus be compatible with human reasoning or information processing. Recent work on work domain analysis presents one approach to building a psychologically relevant and physically faithful model of SCADA systems to highlight the risk of physical sabotage due to inadequate cybersecurity measures [100].

12.4.5 Attacker attribution, intelligence coordination, and deterrence (geopolitics)

The nature of cybersecurity and the business case for both defenders and attackers likely change with reliable attribution and retribution of the attackers. Attack attribution is defined as “determining the identity or location of an attacker or an attackers intermediary” [101]. Exposed identities can result in unwanted public spotlighting of the attackers, so other critical infrastructures sectors can become aware of the cyberrisks and begin tracking adversarial activities. Common attribution techniques mainly involves data traffic monitoring [101]. However, attackers are increasingly creative in distorting their traffic patterns with intermediate hosts/servers (i.e., “hops” [102]). Recently, security experts discovered merits in monitoring specific human behaviors in attributing attacks. Boebert [103] identifies critical human-related attribution characteristics including keystroke intervals; misspellings of command names; time of day references; and duration of intrusion to infer demographics of the adversaries, such as their language [104]. Web browsing behaviors can provide insights into an attacker’s behavioral patterns [105]. To enhance cybersecurity, HCI research can support the attribution of attacks in three ways—investigating how the attacker’s interaction behaviors with SCADA systems could potentially expose their identity, how the higher likelihood of identity exposure might alter the attacker’s behaviors (e.g., likelihood of a strike on SCADA systems), and how decision support systems can help cyberdefenders identify attackers.

Attribution enables retribution for attacks if nation states and international organizations are willing to pursue perpetrators. Retribution may shift the asymmetry of cybersecurity in that, without any retribution strategies, defenders bear most of the cost and consequence, while the attackers reap most of the rewards [106]. However, this asymmetry is reduced when consequences and monetary recuperation can be imposed on perpetrators who are caught. Legal ramifications, or simply retaliation postures, may deter attackers while financial recuperations may change investment decisions. Financial recuperations may drive new product markets in addition to the current cyberinsurance market, which provides financial security in a manner that draw investment away from permanent technical solutions [107,108]. However, details on retrributions for cyberattacks are limited, as only security and government agencies are privy to details of such knowledge. Future research in HCI can contribute to cybersecurity by studying how different rules of engagement and retribution methods can influence the security investment, the design and operations of different SCADA components, as well as the behaviors of attackers. Perhaps it is
only a possibility in the distant future can retribution be a significant factor in cybersecurity symmetry.

### 12.5 Conclusions

This chapter provides an extensive review of current and emerging SCADA security research related to human factors. A generalized SCADA architecture is presented along with the description of various components that can be targeted in cyberattacks. SCADA systems can suffer from security risks due to legacy design and functional complexity. The general IT solutions, such as vulnerability patching, are not always immediately applicable to securing SCADA/control network because some security mechanisms could interrupt real-time operations or degrade the reliability of the physical processes. The modern SCADA network often has firewall-mediated connection to the corporate network for exchanging information or accessing cloud services, presenting another risk factor. HCI research can enhance SCADA security through user interface design that supports workers in the effective configuration of security tools and acquisition of cyber SA. Further, research must begin to focus on teamwork starting with staff in security and operations for coordinating response to cyberattacks. Finally, HCI could examine how the attribution and retribution of attackers may shift the asymmetry of cybersecurity in favor of the defenders.

### References

Chapter twelve: Securing supervisory control and data acquisition control systems


Chapter twelve: Securing supervisory control and data acquisition control systems


