INL/JOU-23-72997-Revision-1

Interdisciplinary Approaches to Cyber-vulnerability Impact Assessment for Energy Critical Infrastructure

May 2024

Andrea NMN Gallardo, Robert J Erbes, Katya L Le Blanc, Lorrie Faith Cranor, Lujo Bauer

Changing the World's Energy Future

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/JOU-23-72997-Revision-1

Interdisciplinary Approaches to Cyber-vulnerability Impact Assessment for Energy Critical Infrastructure

Andrea NMN Gallardo, Robert J Erbes, Katya L Le Blanc, Lorrie Faith Cranor, Lujo Bauer

May 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517, DE-AC07-05ID14517

Interdisciplinary Approaches to Cybervulnerability Impact Assessment for Energy Critical Infrastructure

Andrea Gallardo
Carnegie Mellon University
Idaho National Laboratory
Pittsburgh, PA, USA
agallar2@andrew.cmu.edu

Robert Erbes
Idaho National Laboratory
Idaho Falls, ID, USA
robert.erbes@inl.gov

Katya LeBlanc
Idaho National Laboratory
Idaho Falls, ID, USA
katya.leblanc@inl.gov

Lujo Bauer
Carnegie Mellon University
Pittsburgh, PA, USA
lbauer@cmu.edu

Lorrie Cranor
Carnegie Mellon University
Pittsburgh, PA, USA
lorrie@cmu.edu

ABSTRACT

As energy infrastructure becomes more interconnected, understanding cybersecurity risks to production systems requires integrating operational and computer security knowledge. We interviewed 18 experts working in the field of energy critical infrastructure to compare what information they find necessary to assess the impact of computer vulnerabilities on energy operational technology. These experts came from two groups: 1) computer security experts and 2) energy sector operations experts. We find that both groups responded similarly for general categories of information and displayed knowledge about both domains, perhaps due to their interdisciplinary work at the same organization. Yet, we found notable differences in the details of their responses and in their stated perceptions of each group's approaches to impact assessment. Their suggestions for collaboration across domains highlighted how these two groups can work together to help each other secure the energy grid. Our findings inform the development of interdisciplinary security approaches in critical-infrastructure contexts.

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**.

ACM Reference Format:
Andrea Gallardo, Robert Erbes, Katya LeBlanc, Lujo Bauer, and Lorrie Cranor. 2024. Interdisciplinary Approaches to Cybervulnerability Impact Assessment for Energy Critical Infrastructure. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24), May 11–16, 2024, Honolulu, HI, USA.* ACM, New York, NY, USA, 24 pages. https://doi.org/10.1145/3613904.3642493

1 INTRODUCTION

Knowledge sharing and collaboration between energy operators and computer security professionals is needed to understand risks to and potential impacts on energy production systems. The protection of energy infrastructure is an immensely critical computer security problem. Disrupting energy grid operations can have particularly severe consequences for society, with loss of power potentially causing a ripple effect that impacts other critical sectors and services, such as hospitals [47, 66, 79, 83], financial services [37, 65, 73, 84], agriculture [19, 23, 44, 67, 68], and energy production and distribution [24, 42, 58, 70].

However, while these two groups of experts need each other in order to secure energy systems, they come from different disciplines, operational cultures, and sometimes have competing motivations and approaches (e.g., block connections vs. keep connections open for remote maintenance, patch immediately vs. schedule downtime to patch). In energy operational contexts, the security of electric-grid equipment has often been considered in terms of equipment failure or misuse, as energy systems were traditionally independent of information technology (IT) or relied on barring connections to external networks [11, 45]. IT security approaches and frameworks are often inadequate for energy operational contexts, which face challenges such as legacy systems that run on old operating systems and the need to operate continuously, which can delay patching and updates. Additionally, the security of energy-grid operational technology requires an understanding of how this technology is responsible for the generation, transmission, and distribution of energy and how computer vulnerabilities can impact these energy-production processes.

Nevertheless, the operational technology (OT) used in such critical infrastructure increasingly relies upon computers and computer networks to operate, as systems like power grids become integrated with networked Internet of Things devices and require maintenance through connected devices or remote workers. Thus, energy OT infrastructure becomes increasingly vulnerable to attacks through exploitation of computer vulnerabilities [70].

However, there is a well-documented shortage of computer security professionals [6, 31, 38, 39, 59, 64], and smaller energy facilities and utilities may lack resilient defenses and recovery plans [78] due to limited economic, staff and computer security resources [34]. Finding ways to build cross-domain knowledge will allow low-resourced utilities to help their staff make better-informed decisions about how to address risks posed by computer vulnerabilities, and also help computer security experts, whether on-site or designing industry-wide standards, develop security measures that are

CHI '24, May 11–16, 2024, Honolulu, HI, USA

ACM ISBN 979-8-4007-0330-0/24/05
https://doi.org/10.1145/3613904.3642493

suitable for energy environments. While it may not be reasonable to expect OT engineers to perform the roles of computer security professionals or vice versa, building each group's awareness of risk factors in the other group's domain could help them seek appropriate resources to address risks to the energy grid.

Given this disciplinary divide between energy operational engineering and computer security and the need to develop cross-domain considerations, we situate our work around 18 employees of an energy-sector organization from these two domains, to compare their approaches to assessing the impact of computer vulnerabilities on energy OT. By computer vulnerability (hereon, vulnerability), we mean an exploitable weakness in a computer system, system security procedures, internal controls, or implementations that could be exploited or triggered by a threat source [56]. More specifically, these subject matter experts (SMEs) were: 1) computer security experts who primarily perform research in industrial control system security (cyber SMEs) and 2) operational technology experts with experience in engineering and operation of energy systems (energy OT SMEs). Our research questions are as follows:

- RQ1: What information do cyber SMEs and energy OT SMEs need when assessing the potential impact of computer vulnerabilities? Are there notable differences between the groups (i.e., cyber SMEs and energy OT SMEs)?
- RQ2: What do these experts consider to be the differences between the two groups' approaches to impact assessment and understanding of vulnerabilities?
- RQ3: What insights or suggestions do these experts provide that directly address collaboration between the two groups or building cross-domain understanding?

When self-reporting their approaches to impact assessment, both groups responded similarly at a general level, with roughly the same number of experts per group discussing each vulnerability impact assessment topic we coded. Both groups displayed knowledge about both domains, perhaps due to their interdisciplinary work at the same organization.

Nevertheless, we observed notable differences in the details of their self-reported considerations, as well as in their perceptions and suggestions regarding both groups' impact assessment approaches. These differences regarding each group's domain-specific focus and understanding were particularly interesting given that all participants had cross-domain work experience. Differences that shone through despite interdisciplinary backgrounds, such as cyber SMEs' more adversarial focus on gaining access and modifying device capabilities or energy OT SMEs' holistic considerations about connections across the system and potential disruptions in operations, highlight some domain-specific aspects that could be harnessed in complementary ways for critical infrastructure security. Indeed, many participants emphasized the value of cross-domain dialogue and exposure to the other group and had several suggestions for collaboration, building mutual understanding, and improving usability and security in energy OT contexts.

Our findings inform design for interdisciplinary security in critical infrastructure contexts by characterizing experts' approaches to impact assessment and highlighting differences in focus, mindset and understanding. Echoing suggestions made by participants, we recommend bringing experts together to foster cross-domain exchanges, developing training, tools, and educational interventions to help interdisciplinary practitioners build cross-domain understanding, and implementing usable security solutions in energy OT contexts.

2 RELATED WORK

Our work provides insight into key issues in interdisciplinary impact assessment in energy OT contexts, focusing on the differences in approaches, professional motivations and skills of two groups of experts: computer security researchers whose work primarily focuses on vulnerability analysis and energy operational technology engineers. Below we discuss prior work establishing differences between OT and IT security, including perceptions and biases. We also note some existing frameworks and prior work on assessing risk or impact in computer security and energy OT contexts, as well as studies regarding cyber SMEs' and non-experts' mental models and perspectives in computer security contexts.

2.1 Contrasting OT and IT Security

Prior work has shown there are major differences between security approaches in IT and OT contexts, including differences in workers' training, knowledge, and culture, regulations for IT security versus OT safety, and conflicts between IT policies and OT continual operations. Studies have considered differences or conflicts between security approaches to IT and OT systems [15, 22, 27], as well as differences between considerations for operational safety and computer security in critical infrastructure OT systems [28, 41, 45, 81].

Wolf et al. identify key differences between traditional IT security and physical industrial control systems (ICS) computer security problems and make recommendations for remediation during design and runtime. For example, they discuss the potential for false data injection to cause harm to physical systems by creating unsafe operational conditions despite not traditionally being considered by cyber security threat models [81].

Prior work has noted historical and cultural differences between OT engineers and IT workers, suggesting that mindset, training, and epistemological approaches differ considerably [45, 49, 61]. Studies on collaboration and communication in security contexts have established a disconnect between IT security professionals and non-security professionals [63]. Michalec et al. highlight the historical differences between security incidents in IT and OT systems, given that "these systems were traditionally built for different purposes," and argue that there are "epistemic and material differences between legacy OT environments and big data practices." In their study interviewing 30 critical infrastructure OT professionals, they show that security risk management practices in critical infrastructure, which often relies on "old world" legacy systems, "cannot be directly transplanted from the safety realm, as cyber security is grounded in anticipation of the future adversarial behaviours rather than the history of equipment failure rates" [45]. The authors highlight three collaborative aspects critical to risk management across security and safety: access to diverse expertise and professional practices, trust and engagement between IT and OT workers, and the collective development of "risk thinking hiveminds," i.e.,

sharing expertise and best risk management practices across the sector via working groups.

While prior work has considered differences between IT and OT workers' security management practices, e.g., what mitigations are acceptable, how often to patch, and who has responsibility, our work considers how risk or impact is understood and assessed by experts working with OT systems. Rather than focusing on IT security professionals whose job responsibilities may include setting organizational IT security policies or monitoring networks for anomalous behavior, we consider cyber SMEs whose work identifying and analyzing vulnerabilities is distinct from energy operations and yet increasingly necessary to prevent, mitigate, and resolve computer security problems in energy OT equipment and systems.

2.2 Risk or Impact Assessment

The most commonly used framework for assessing the severity of vulnerabilities is the Common Vulnerability Scoring System (CVSS) [53, 57, 82]. Hollerer et al. attempted to merge CVSS and two safety and security frameworks to develop a "risk evaluation methodology to prioritize and manage identified threats considering security, safety, and their interdependencies" [28]. Prior work has also looked at ranking vulnerabilities in critical infrastructure [3, 21]. Some research has considered impacts or risks of interdependencies in critical infrastructure systems [50, 75]. Prior research has also provided suggestions for how to determine cyber security risk for energy sector infrastructure [2, 9, 29, 32, 36, 85] and OT systems, such as supervisory control and data acquisition (SCADA) systems [12, 20, 28, 60, 71]. While there are industry-wide reliability standards, such as the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards [51], there is no industry standard for assessing risk for OT systems that is as widely adopted as CVSS is for scoring the severity of vulnerabilities.

2.3 Subject Matter Experts

Our study is concerned with the opinions of experts and how those opinions can be used to inform the vulnerability impact assessment process. Prior research has studied the mental models and skills of cyber SMEs and their perspectives on certain problems [1, 4, 5, 25, 30, 43, 72, 74, 76, 77, 80], suggesting that the perspectives of cyber SMEs can be valuable in outlining issues for certain tasks and that knowledge required for understanding vulnerabilities can often be specialized and varied. For example, in 2018, Votipka et al. showed that there is a divide between how two domain experts, "testers" and "hackers," think about software vulnerability discovery, and explored differences in factors such as training and motivation. They found that "hackers" were better able to spot vulnerabilities than testers [77]. Botta et al. and Hawkey et al. interviewed IT security professionals to characterize their responsibilities, goals, tasks, and skills, as well as difficulties collaborating within organizations [10, 26]. Reinfelder et al. interviewed seven IT security managers and found that IT security managers had difficulty receiving adequate feedback regarding usability of security features [63].

Comparative studies between experts and non-experts have also helped identify gaps in security approaches [8, 30]. Prior work has also considered the computer security perspectives of other kinds of subject matter experts, such as network administrators [35], Internet Service Providers (ISPs) [69], data scientists and data engineers [48], and cryptographic library developers [33].

Some qualitative studies have provided insight into practitioner perspective on critical infrastructure computer security. Line et al. assessed preparedness through interviews about situation awareness and incident response [40]. Michalec et al. interviewed 30 cyber security practitioners for their views on directives standardizing computer security for critical infrastructure [46]. Reilly et al. conducted interviews with 31 relevant stakeholders, including critical infrastructure operators, regarding how crisis information is communicated in critical infrastructure settings [62]. Yet, as far as we know, prior work does not provide detailed insight into the perceptions, experiences, and suggestions of energy OT SMEs and cyber SMEs regarding cross-domain collaborations assessing the potential impact of vulnerabilities on energy OT systems.

3 METHODS

Below we describe our participant selection and recruitment process, our interview protocol, how we analyzed data, and limitations of our study.

3.1 Participant Selection

Study participants consisted of two kinds of experts: power systems experts ("energy OT SMEs") and computer security experts ("cyber SMEs"). The energySMEs were mostly engineers who maintain or manage energy systems. The cyberSMEs were researchers who utilize their deep understanding of how vulnerabilities work, harnessing skills like reverse engineering, to discover and analyze vulnerabilities in devices or systems they assess on a workbench.

We recruited participants from lists developed by colleagues (who were SMEs themselves) at Idaho National Laboratory, a U.S. Department of Energy national laboratory that conducts research on energy and national security. Each list consisted of people who qualified as one of the two types of experts based on their current professional responsibilities and department, i.e., their current work took place primarily in one of the two fields of expertise. We did not share the list of suggested potential participants beyond the two authors who conducted interviews. Most participants responded directly to a recruitment email, and a few responded to follow-up emails from these two authors, who were not managers and did not work directly with participants. Managers were not involved in the recruitment process to avoid any sense of coercion. Participants were informed in recruitment materials and the consent form that the study was voluntary, and they had several opportunities to decline to participate or request that their data be deleted. They participated during work hours, and their employer paid them their normal salaried rate for the time they spent on the study. Only the two authors who conducted interviews had access to the deanonymized videos and transcripts. The only data and findings shared with the employer were anonymized results. All study protocols were approved by both the Carnegie Mellon University and Idaho National Laboratory institutional review boards.

Code	Description	Example
Accessibility	Information on the reachability of the vulnerable system.	Can I talk to the system from the internet? Is there an attack vector that can reach the system?
Attack	Understanding of adversarial threat, consideration of attacker, attacker motive, or actions.	How appealing is the system to an attacker? Who is the attacker?
Connectivity	Information on what the system is connected to.	Is the system connected to more important systems? What does the vulnerable system talk to?
Consequence	The result or possible result of malicious action upon the vulnerable device.	How long will it take to recover from an attack? Who would an outage affect? At what cost?
Consult other SME	Seeking external expertise outside of the participant's domain.	I would need to ask a power engineer to understand what would happen.
Device Information	Information about the system or device the vulnerability was identified within.	What does the system do? Where is it typically used? How common is it?
Vendor	Information on or about the company that builds the vulnerable system (unprompted).	Does the vendor provide support? What is their track record for fixing vulnerabilities?
Vulnerability	Information about the vulnerability itself.	Severity rating (e.g., CVSS). Can it be exploited?

Table 1: Definitions and examples of top-level strategy codes. Subcode definitions can be found in Appendix D.

3.2 Interviews

We conducted semi-structured interviews to capture the nuanced thought processes of experts as they considered their approaches to vulnerability impact assessment. Each interview lasted between 60 and 90 minutes and took place via Microsoft Teams between November 2021 through April 2022. All but one interview were recorded, and all interviews were automatically transcribed by Microsoft Teams software (including the non-recorded one). Transcripts were subsequently reviewed and corrected by the first author, based on recordings and notes. Our interview questions are included as Appendix C.

We began each interview by collecting general information, such as occupational background, years of experience, and experience conducting impact assessments. To better protect the identities of participants, we did not collect gender, age, income, or education level, though to the best of our knowledge, every participant had at least a bachelor's degree.

We then elicited and discussed the individual SME's general strategies for assessing the impact of a cyber vulnerability, what information they would need, and how subsector, context, vendor, and other factors might influence their approach. We also asked questions to elicit the SME's perceptions of differences between the two SME groups, i.e., differences in approaches to assessing the impact of vulnerabilites and differences in understanding of vulnerabilities.

3.3 Data Analysis

We structured our analysis around strategies, perceptions, and suggestions. We developed two codebooks for this analysis: one contained a list of *a priori* codes for impact assessment strategy topics that was refined throughout the coding process. The other codebook contained codes that emerged from review of the transcripts.

3.3.1 Impact Assessment Strategy Topics. The first three authors developed an initial list of codes based on their technical and research experience in computer security and vulnerability analysis. These codes were intended to help us categorize and track the participants' stated approaches to vulnerability impact assessment by honing in on whether they discussed particular topics. For example, did they mention understanding of vulnerabilities, potential consequences like loss of power, or how the system in question connected to or controlled other things?

We then coded a few of the responses for self-reported approaches to assessing the impact of vulnerabilities, iteratively returning to the codes to discuss disagreements, refine or consolidate the codes, and add any codes we felt captured concepts not covered by the initial list. This helped us further develop main codes and subcodes. We used the code book developed in this process to code all responses to the open-ended strategy questions as well as the questions that elicited participants' perceptions of their own expert group and of the other expert group. Our final list of codes for strategies or approaches to assessing the impact of vulnerabilities are described in Table 1. We also developed subcodes to capture more details about each category, described in Appendix D.

For each question, the first or second author assigned codes to the responses (coder), and the other author reviewed the codes, noting any disagreements or adding new codes (reviewer). We tallied final code counts separately for self-reported responses and perception responses. Each sub-code was counted only once per participant, even if it was mentioned repeatedly, to allow for clearer group comparisons. We also coded each response with a perception valence of positive or negative, where the term "positive" means that the described group would consider the factor, or would be effective at considering the factor, and "negative" to signify the converse. Since the two groups had consistent positive and negative views of

their own and the other groups (see Appendix B), we report results for positive and negative perceptions in aggregate.

3.3.2 Group Perceptions and Suggestions. The first author, either as a coder or reviewer, also used the following codes to characterize participants' responses to the perception questions, developing codes in a bottom-up coding process by first identifying detailed themes and subsequently reviewing the responses to thematically group them into three categories: 1) Stereotype: the SME group tends to do certain things or see things a certain way; general characterizations. 2) Occupational Motivation: habits, mindset or approaches based on training or job; what they are expected to do. 3) Suggestion: a recommendation regarding interdisciplinary work or collaboration. Another researcher reviewed these codes to verify their appropriateness and to suggest changes or additional codes. All codes are included in Appendix D.

3.4 Limitations

Our team is composed of computer security researchers and one human factors researcher. One limitation of our work is that our development of thematic codes was informed primarily by a computer security perspective. There may be additional codes that could have been included, had an energy OT SME been on the research team.

Another limitation is our small sample size of experts, which limits the generalizability of the results. While we sometimes report counts to make it easier to understand whether opinions were unique or more widely held, we don't imply any further quantitative characterization of the responses.

Additionally, all participants came from the same organization and may share overlapping or similar interdisciplinary experiences that could inform their responses and thus diminish notable differences for each group. Finally, questions about their own and other SMEs' understanding and abilities may have lead to responses with social desirability bias.

4 RESULTS

We first provide background information about participants' professional and interdisciplinary experience (Section 4.1). We then present results for participants' self-reported impact assessment approaches (Section 4.2) and results for responses to questions about their perceptions of SME groups' strategies and understanding (Section 4.3). Finally, we relay their suggestions directly addressing interdisciplinary collaboration in energy OT security contexts in Section 4.4.

4.1 Participants

We interviewed 18 participants including nine cyber SMEs and nine energy OT SMEs from the same organization. We provide background information by participant number in Table 2 and additional details below about prior experience in impact assessment and cross-domain experience. When we provide numbers of participants in parentheses to characterize the responses, we use "Cyber" to indicate cyber SMEs and "OT" to indicate energy OT SMEs.

Four participants had 1–5 years of experience, five had 11–15 years of experience, and five had 16–20 years of experience. The remaining four had over 20 years of experience. Seven participants (1 OT, 6 Cyber) joined the organization directly after finishing higher education, and 11 (8 OT, 3 Cyber) had work experience prior to joining the current organization.

Participant	SME Group	Experience	Prior Job
E1	Energy OT	11-15	Y
E4	Energy OT	11-15	Y
E6	Energy OT	21-25	Y
E7	Energy OT	16-20	Y
E8	Energy OT	11-15	Y
E10	Energy OT	26-30	Y
E15	Energy OT	31-35	Y
E16	Energy OT	16-20	N
E18	Energy OT	11-15	Y
C2	Cyber	16-20	N
C3	Cyber	1-5	Y
C5	Cyber	1-5	N
C9	Cyber	1-5	N
C11	Cyber	16-20	N
C12	Cyber	11-15	Y
C13	Cyber	16-20	N
C14	Cyber	21-25	Y
C17	Cyber	1-5	N

Table 2: Summary of participants, showing participant number, expert group, total years of work experience (including prior experience), and whether or not they had work experience prior to working at the current organization.

4.1.1 Impact Assessment Experience. Nine participants (7 OT, 2 Cyber) had prior experience conducting impact assessments, and when asked if their work "focused on the impact of cyber vulnerabilities," four additional participants (all Cyber) said yes, and one energy OT SME with impact assessment experience said no.

When asked about standard impact assessment procedures, participants noted that there was no standard impact assessment procedure for energy OT environments, but they mentioned some standard tools that could be used for impact assessment: the CVSS scoring system [53, 57] (3 Cyber, 1 OT), Common Vulnerabilities and Exposures (CVE) [17, 54] or Common Weakness Enumeration (CWE) [16] reports (2 Cyber), the NIST Cybersecurity Framework [55] (1 Cyber, 1 OT), the MITRE ATT&CK framework [18] (1 Cyber), a methodology developed at the organization (2 OT), as well as North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards [51], US-CERT and ICS-CERT (now CISA) alerts and advisories [13, 14], and the CARVER methodology [7, 52] (each 1 OT).

4.1.2 Cross-domain (Computer Security and Energy OT) Experience. All participants had some cross-domain experience. Of the energy OT SMEs, all nine had on-the-job exposure to computer security, and seven had some exposure to vulnerability analysis. Of the cyber SMEs, all nine had on-the-job exposure to energy OT systems. All 18 participants had worked on the same team as the other kind of SME and had also either worked on the same project or did work that overlapped with the other SME group's work, requiring coordination or complementary approaches. Such an interdisciplinary group is not typical in energy OT contexts. We thus want to emphasize that our reporting of differences and similarities is not meant to generalize to trends in the energy OT industry. Rather, our results provide details about responses from experts in a particularly interdisciplinary group. We hope their responses will provide insight valuable for future work on developing cross-domain knowledge both among interdisciplinary experts and in environments where working together is less common.

4.2 Self-Reported Impact Assessment Strategies (RQ1)

We report how participants responded to questions about what information they would need to assess the impact of a vulnerability in an energy OT system, highlighting similarities (Section 4.2.1), differences (Sections 4.2.2–4.2.3), and interdisciplinary knowledge (Section 4.2.4). Despite bringing up similar high-level topics, there were notable differences in participants' stated approaches to vulnerability impact assessment, indicated by the level of detail participants provided, such as how cyber SMEs had more specific considerations about gaining access to networks, or how energy OT SMEs spoke more about connections to the overall system and potential disruption of operations. While we include numbers in some of the results below and in Table 9 in Appendix E to characterize this particular participant pool, we note again that these are not generalizable results.

4.2.1 Similarities in Self-Reported Impact Assessment Strategies. We expected cyber SMEs and energy OT SMEs to show a stark imbalance in their stated approaches to vulnerability impact assessment, based on prior work (Section 2.1), but we did not find this to be the case. Experts across both groups raised similar vulnerability impact assessment topics relating to Accessibility, Connectivity, Consequence, Device Information, and Vulnerability (described in Table 1), as shown in Figure 1 and Appendix E. Responses to questions about whether subsector and vendor would influence their approach were also similar. We hypothesize this may have been due to all participants having interdisciplinary experience. We describe these similarities below.

Accessibility. Both groups of participants spoke generally about how to gain access (remotely or physically), who might have access, and access controls.

Consequence. Both groups were aware of possibilities for large-scale impact, emphasized understanding systemic and broader scale implications, and offered general considerations about the potential impact on human life, damage to equipment, financial or business impact, remediation or recovery time, and whether it would affect critical systems.

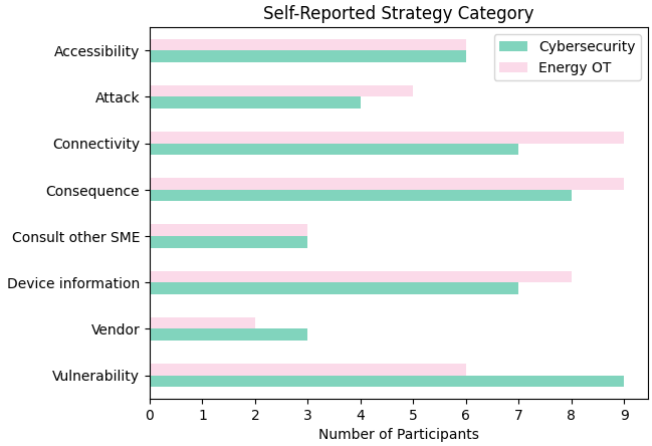

Figure 1: Top-level impact assessment topics considered relevant by participants in their self-reported impact assessment approaches, showing count of unique participants by SME group. We did not observe a stark difference between the two groups, which may have been due to the interdisciplinary background and experience of all participants.

Device Information. Participants from both groups said they would need information about what the system or device is, what its function is or how it is typically used, how it is configured, who uses it, where it is located and situated within the OT system, how widely it is deployed in the overall environment and in the country, and how well it is protected from a physical and network standpoint. One participant, E7, called for a software bill of materials (SBOM) to better understand where a vulnerable component exists and what the "most granular indivisible element that this vulnerability impacts" is.

Vulnerability. Participants from both groups said they would consider what the vulnerability was, the area or systems affected by the vulnerability, proof of concept, and exploitability.

Subsector. In response to questions prompting participants to tell us whether the energy subsector (e.g., generation, transmission, or distribution) would influence their vulnerability impact assessment approach, all but one participant felt that considering subsector was important for impact assessment, with one cyber SME saying the subsector would not impact their assessment at all (C3). In all cases where subsector was described as being important, it was due to the scale of the potential impact. Some participants ranked subsectors by importance, named the one they thought was most critical, or stated that all subsectors were equally important.

Vendor. Five participants (2 OT, 3 Cyber) listed vendor as a factor they would consider before being prompted to discuss how a vendor would influence their vulnerability impact assessment approach. In response to our question, four participants (2 OT, 2 Cyber) stated that the vendor doesn't matter at all. All other participants stated that the vendor did matter. Some participants said different vendors had different track records with computer security, specifically with how open and communicative each vendor was with their

customers regarding vulnerabilities, emphasizing the importance of strong lines of communication and relationships. Two participants discussed the difficulties of trying to report vulnerabilities to different vendors (E10, C12).

4.2.2 Differences in Cyber SMEs' Self-Reported Impact Assessment Strategies. Cyber SMEs' responses were distinguished by a more adversarial focus on gaining access, identifying connections, and imagining device capabilities and exploits.

Gaining Access. Cyber SMEs spoke in more detail about gaining access to a system's networks or devices than energy OT SMEs, saying they would want information about an attacker's ability to move around within an OT environment (C13) or a company's networks, including SCADA or control system networks (C12), or the potential for an attacker to access "additional resources that you can chain to get there or tie in with other controllers" (C11).

Identifying Connections. Cyber SMEs also emphasized identifying connections across networks and systems, imagining paths to hard-to-reach devices:

> *I would try to trace a path to this piece of equipment to try to understand how easy it is to get there. Some equipment is designed to be on a network that is more likely to have malicious traffic. Other equipment is not designed for that, and it's expected that it's going to be behind several firewalls. (C12)*

C11 said, "Often, end devices are not very reachable. So you'd have to have access to several other networks or a different entry point to get to them." Others asked questions such as "Does it cross the boundaries between different networks?" (C5) and "Can you go to the next system over?" (C15).

Device Capabilities. Cyber SMEs provided more examples about what affected devices or systems might be capable of doing. Three cyber SMEs suggested devices could be modified to perform unintended actions or be mis-programmed by abusing a given functionality. C5 wanted to know potential impact "if it was to be modified and if the vulnerability allows the code to be changed and just run something arbitrary instead." C5 also considered the possibility of modifying a device or system that is "just supposed to be gathering data" to "send commands to something" on the same network. C12 considered looking for potential capabilities of hardware components:

> *Sometimes we think about a device as a single device, but if you open it up under the hood there might be two or three or four different devices inside with distinct functionality. And maybe one portion of that device is built to be more trusting, and so you have to look and do a divide and conquer approach. (C12)*

C12 also contrasted the idea of looking for a "novel exploit, which you should definitely search for," with an unintended or "insecure implementation" of a provided functionality. C17 considered the potential impact of "issues with the device," such as an "accessible debug shell" that could be made to "continually crash and restart, taking up resources."

In contrast, three energy OT SMEs spoke more generally about understanding what affected devices or systems were capable of doing, with E16 also considering the ability to change things "within the product to be used inappropriately."

Exploit details. Cyber SMEs also considered details regarding potential exploits. C5 wanted to know if there were "creative" ways to modify the device or change the system's code and if this could take the system offline. C9 said they would consider what kind of data could be released by the vulnerability, as well as its severity. C11 said they would be more concerned if it were possible to "chain" the vulnerability with knowledge about other vulnerabilities to create a larger impact. C12 expressed concern about older systems being exploited with published "off-the-shelf" vulnerabilities. C14 asked whether the vulnerability was persistent or temporary and whether it could spread to other things.

All five cyber SMEs who raised the topic of exploitability asked how "easy" it would be to exploit the vulnerability, while energy OT SMEs asked whether it was "actually" exploitable (E7, E16) or would require remote access (E10). The cyber SMEs' responses implied that compromise was possible but that their consideration depended on difficulty, highlighting factors like how reachable the system is and the attacker's skill level.

4.2.3 Differences in Energy OT SMEs' Responses. Overall, energy OT SMEs conveyed a more holistic view of the system and provided more concrete examples of parts of systems and how systems might be affected.

Connections to the larger system. Energy OT SMEs provided more details about how connections between devices and systems relate to the overall system. For example, E1 considered an engineering workstation as "something with a pretty low impact for safety or operations" but with high potential security impact because "it touches everything" and might contain credentials and configuration files. E7 and E15 were concerned about whether the vulnerability was "on something centralized that controls a lot of different things, like my SCADA or EMS" (E7). E8 expressed concerns about distribution systems "becoming more integrated," saying, "Historically, a distribution system was one radial feed. Now it's starting to talk to all the meters out in these residential areas." E16 was concerned about effects on "the downstream load."

In contrast, cyber SMEs asked general questions such as what it means for devices connected to the system (C17), "what equipment is being used and what ties they have to the outside world or to any type of network" (C3), what the system communicates with, controls, or monitors (C5), and what the dependencies on the system are (C14), not providing potential answers themselves, as some energy OT SMEs did, implying that they would obtain this information from another source, such as an energy OT SME.

Disrupting operations. Energy OT SMEs also spoke in more detail about potential disruptions in operations. For example, E15 considered whether the location might be a "high priority site" that needs to "maintain critical loads" and whether it would thus be among the last users to lose service and the first users returned to service after an interruption. E16 wanted to understand how much power or the "amount of megawatts and gigawatts" that might be "turned off" and what point in power distribution was disrupted: a meter at a residence or a transmission substation.

Differences	Description
Cyber Focus:	
Gaining access	Cyber SMEs discussed ability to move around within environments/networks and access additional resources to chain together
Identifying connections	Cyber SMEs wanted to trace paths across networks and systems, determine boundaries
Device capabilities	Cyber SMEs imagined potential capabilities such as mis-programming or modifying systems for different functionality, running arbitrary code, sending commands, or exploiting unused parts of hardware
Exploit details	Cyber SMEs considered exploit methods and also considered exploitability in terms of difficulty, not as a binary
Energy OT Focus:	
Connections to larger system	Energy OT SMEs were concerned with how the affected system connected to the larger system in terms of operations, important files, centralized SCADA/EMS systems, and downstream devices like smart meters
Disruption in operations	Energy OT SMEs specified considerations about disruptions in operations, such as whether the site was a high priority site, the amount of power at stake, and the severity of disruption
Risk mitigation	Energy OT SMEs emphasized containing the risk, ensuring operational integrity and investigating residual impact on the system

Table 3: Summary of differences in vulnerability impact assessment strategies.

Energy OT SMEs also wanted to understand what kind of disruption might occur. For example, E18 wanted to distinguish between whether the vulnerability would "completely shut us down" or "only slow us down temporarily." E7 suggested that temporarily mitigating a threat by "physically remov[ing] some kind of communication channel" might cause people to complain that they "need the data," but suggested that the potential impact might not be great: "But do you really need it? Are you billing from it? Is it a regulatory thing, or is it just something that you'd like to have?" Thus, for E7, potential impact on business processes might be higher impact than lacking nice-to-have information.

Risk mitigation. When discussing vulnerabilities, energy OT SMEs also focused more on stopping or mitigating the vulnerability, containing the risk, patching, ensuring operational integrity, and understanding the residual impact or risk of the vulnerability for the larger system and operations. For example, E15 said that after stopping an attack, they would verify "the integrity of operational functions" and if they had control of all equipment and operational status, and then "find what was potentially accessible to the attack" and confirm protection systems were still functional and working "as designed" and "that my rules haven't been changed on my communication devices."

4.2.4 Cross-domain Knowledge. Some participants displayed cross-domain awareness in their responses or said they would seek out such knowledge as part of their impact assessment strategies. C17 made a distinction between whether a system could be accessed by customers at their homes or by engineers at a generation plant:

> *If there's an exposed port that you can connect to that gives you debug access or a shell, that would largely be an issue with a consumer device, because that means your consumer could do whatever the heck they want to with your device. But in the case of a high reliability system in generation, it might be significantly more important to have that as a means of debugging any issues that do occur with the device. (C17)*

C12 said they would not consider a cabinet containing "a bunch of ethernet ports that you could connect to," to be "very high impact" if it were inside "a facility with 10 layers of physical security." Additionally, E6 considered the cyber hygiene of portable media and mobile devices accessing the system: "What do you do for maintenance? Do you bring a laptop over? Do you sanitize all of your portable media?"

Additionally, C14 and E7 conveyed cross-domain knowledge when speaking about isolating systems containing the vulnerability. E7 mentioned the "occasional" situation in which they are able to "wall off" a vulnerability "that's not actually used for the functionality of that product":

> *It is incredibly difficult and maybe in a few cases straight up impossible to actually exploit, and then that lets me back off and step back from the ledge a little bit and say "OK, this is important," but it's not like, "Oh my God," the end of the world here. (E7)*

C14 evoked concepts from a recent training on safety risks:

> *Going through lab training the other day, there's a whole, when you have a safety risk or safety issue, the best thing to do is to eliminate it. The second thing to do is to have controls that contain it. The third thing to do*

> *is to tell people not to use it. … So I guess that applies also in this kind of system. (C14)*

This suggests that C14 was applying knowledge from an energy OT safety training to a computer security context.

Additionally, one energy OT SME and one cyber SME participant suggested methods for obtaining interdisciplinary insight, emphasizing how they would consult the other expert group once they had seen proof of concept for the given vulnerability. E16 said they would consult a "product SME" and cyber SME to collaboratively understand what the vulnerability was capable of doing. C17 said they would "lean on the energy SMEs" to gain insight into potential implications for the system, how easy it would be to replace the device, if the device could be "ruined" by the vulnerability, or what kind of impact it might have "in terms of environmental impacts or larger societal impacts."

4.3 Perceptions of SME Groups (RQ2)

We first present recurring generalizations or perceived tendencies about each group, in Sections 4.3.1–4.3.2. Because we didn't spot any particular difference between the characterizations advanced by the two groups of SMEs, we present the stereotypes by the group who is the target of the stereotypes. Then, in Section 4.3.3, we convey what participants said were the occupational motivations, or driving factors, of the expert groups. Participants' positive or negative perceptions of both expert groups' vulnerability impact assessment strategies are included in Appendix A.

4.3.1 Stereotypes of Cyber SMEs. Some stereotypes about cyber SMEs were that they understand vulnerabilities, misunderstand energy OT systems and impact, reduce systems to computers, pay attention to details, overestimate impact, and cut off access to protect systems. Cyber SMEs were also seen as representing "IT" people or departments.

Cyber SMEs' understanding of vulnerabilities and systems. Cyber SMEs were characterized as understanding exploits and vulnerabilities (3 OT, 4 Cyber), e.g., being able to tear devices apart to do things like extract firmware or find vulnerabilities. Ten participants said that cyber SMEs lacked understanding of energy OT systems (4 OT, 6 Cyber). Eleven participants said that cyber SMEs lacked understanding of impact or overestimated impact (5 OT, 6 Cyber), while only one said they underestimate impact (1 Cyber). C12 suggested that cyber SMEs "are more likely to think the sky is falling when it's not." E7 also suggested they may incorrectly think a vulnerability could crash the grid:

> *The cyber security folks tend to think of it as: "This is exploitable, and if you can do this, you can crash the grid with it." Whereas the electric folks are like, "OK, no. You can maybe knock off that one generator, but in reality, you can just knock off the controller for that induced draft fan, and that means I would have to derate my generator. … I'm not making as much money that day. But it's not the end of the world. (E7)*

Thus, this overestimation could be due to not understanding redundancies in place and safeguards that prevent a vulnerability from impacting systems.

Cyber SMEs see computers. Cyber SMEs were depicted as treating OT systems as computer systems that can be manipulated as such (1 OT, 3 Cyber). E7 conveyed how systems perceived by engineers in terms of their function could be reduced to modifiable computers. "From the perspective of the maker, the people who install it, [and] the protection and controls people," a protective relay is a device that quickly and reliably "reads electrical voltage and current," then "does some math on them" to determine whether or not "to send a trip signal to a breaker." Yet, they added:

> *From the adversary, cyber security perspective, this thing is a computer. It's got a full-blown operating system. It's running Yellowstone Linux or Windows 8.1 embedded or something else. And if I have the right passwords or I can figure out how to bypass the different protections on it, I can make this thing do anything that a computer could do. (E7)*

Cyber SMEs focus on details. Four participants emphasized cyber SMEs' attention to detail (1 OT, 3 Cyber). C11 and C12 said they go into "rabbit holes" and that this could be both a good and bad thing, with C11 suggesting the importance of "reigning yourself in" when focusing too much on one type of analysis, and C12 acknowledging that some things may be interesting from a cybersecurity standpoint but may end up being low risk. Yet, they said, it is not always clear whether it is low or high risk until it is fully tracked. E1 said cyber SMEs spend months on device vulnerability analysis doing a full evaluation of a device. C13 suggested that cyber SMEs underestimates impact because they focus on "the here and now" details about the immediate environment rather than thinking about implications and how something might "cascade" through a system.

Cyber SMEs cut off access to protect systems. Five participants said that cyber SMEs cut off access to protect system (3 OT, 2 Cyber). Several responses indicated that cyber SMEs were perceived as restricting access to systems in order to protect them. Indeed, some participants provided anecdotes or made suggestions that evoked frustration with a lack of usable solutions.

> *There needs to be open communication between certain applications, certain devices. And completely locking those down, to the level that a lot of cyber security experts would like to see, just isn't feasible. …A lot of times the OT, I think, just kicks out cyber security and says "Get out of my hair." (E8)*

Cyber equals IT. Four participants (3 OT, 1 Cyber) discussed cybersecurity and IT departments in the same statements, suggesting an association between the two. When responding to a question about cyber SMEs, E6 suggested that "IT people" don't understand how controllers work and how they communicate, and thus they "think that they can just go onto the OT side and do the same thing and then they have they find out the hard way":

> *They don't have the understanding of how controllers work and how they communicate, so if you run certain things to do analysis, you could potentially take out your production system, where on an IT system, it wouldn't matter (E6)*

C14 suggested working with IT teams to develop authentication solutions, since if "the IT Department is enforcing things without actually talking to the people who have to use it, then you never figure out that you can come up with different authentication systems." E15 also evoked IT being an enforcer when, for example, "IT says we've got to make a firewall or system" to avoid public access to the grid.

Other Perceptions. Less common perceptions included that cyber SMEs overemphasize the following: complicated exploits when simpler ones achieve same effect (1 OT), IP-level communications (as opposed to serial and proprietary level communications) (1 Cyber), patching (2 OT, 1 Cyber), and software (1 Cyber). Two energy OT SMEs said that cyber SMEs underestimate the importance of continuous operations and keeping things functioning (1 Cyber) and underestimate or fail to consider misuse of technology (2 OT). One participant suggested that cyber SMEs lack funding or resources (1 OT).

4.3.2 Energy SME Stereotypes. Energy OT SMEs were represented as understanding systems and impact, not understanding vulnerabilities or exploits, lacking imagination, and taking shortcuts.

Energy OT SMEs understand systems. A repeated opinion was that energy OT SMEs understand the design, maintenance, and operation of energy systems, energy OT equipment and capabilities, and how system components are connected. E15 also said energy OT SMEs know how to install equipment, maintain it correctly by making sure it integrates well with other equipment that's coming in, and replace old equipment. C11 highlighted how energy OT SMEs' input about systems helps them understand impact:

> *Usually the people that are talking about it and introducing us to it are quite honest about, "And if this part goes down, it's gonna be a huge pain." They may not be thinking about it in risk, but they usually point out parts that are difficult to replace or computer systems that are very key to keeping up and running. (C11)*

E4 also spoke specifically about asset owner operator energy OT SMEs, saying that they "will know their systems better than anyone else on the planet."

Energy OT SMEs do not understand vulnerabilities. Energy OT SMEs were characterized as lacking understanding of exploit capabilities, attacks, vulnerabilities, technical details, and network communications. Regarding overestimating and underestimating, seven participants suggested that energy OT SMEs underestimate the ease with which vulnerabilities could be exploited (1 OT, 6 Cyber). C5 suggested that people who set up the OT systems may not think about how easy it is for the different systems to be compromised and not consider lateral movement across different parts of the network and creative ways of gaining access. Relatedly, three participants said that energy OT SMEs overestimate protections (1 OT, 2 Cyber).

Other things that participants said energy OT SMEs underestimate include: access & connectivity (2 OT, 2 Cyber), hardware attacks (1 Cyber), impact (2 OT), misuse (1 OT), and risk (1 Cyber). Participants also suggested that energy OT SMEs overemphasize the following: network security (1 OT), physical security (1 OT), prior vulnerabilities (2 Cyber), system resilience (1 OT), vulnerability score (1 OT), what a device is supposed to do (1 Cyber), and software (1 Cyber).

Energy OT SMEs lack imagination. Eight participants suggested that energy OT SMEs find it difficult to think of possibilities outside of what they already know (2 OT, 6 Cyber), i.e., are not able to imagine vulnerabilities or potential exploits or harms beyond what they already know.

> *Some of that stuff is not readily clear just by say reading about something or walking through its configuration, which is typically what an OT SME might do, where they don't go to that layer below, they really just look at what's there and kind of accept that that's how it is. (C13)*

E7 suggested that energy OT SMEs fail to see computers in OT devices: "It's not a protective relay. That's a computer. It can do computer stuff." C11 suggested that some energy OT SMEs needed convincing or explanations when told that a device had to be replaced due to a severe vulnerability.

> *Some OT SMEs do not believe you, they're like, 'Oh no, you just reboot it. It's made to be reliable.' . . . They have worked with systems for a long time, and they are used to things breaking and being good after a reboot or two. They think that's the same thing for someone actively trying to exploit or damage a system. . . . They're so used to it just being able to recover because it's made to have high reliability for the types of things that happen accidentally, that having someone purposely damage it is a completely foreign idea. (C11)*

Additionally, E16 suggested that energy OT SMEs might not consider "the potential downstream" impact of a highly motivated and resourceful attacker exploiting a relatively minor vulnerability on a large scale, e.g., rather than simply opening one switch, creating a scenario with "hundreds of or thousands of switches that are opened and then you can't re-close them because communication lines have been taken out." C17 suggested that energy OT SMEs see some systems as always failing into a known state or behaving in known and proven ways, and that they do not consider vulnerabilities that can change how the system behaves. E18 suggested that how specific responsibilities are distributed amongst personnel in an organization could influence energy OT SMEs' understanding of vulnerabilities: "You may have one person that is responsible for aspects of the operations on a daily basis. They need to make sure that the facility is functioning and might have less of a concern about quote unquote potential risk."

Energy OT SMEs take shortcuts. Six participants warned about energy OT SMEs taking shortcuts, thus leaving vulnerable defaults open, in order to work around restrictive policies put in place by IT or cybersecurity departments (3 OT, 3 Cyber). E1 said that engineers circumvent or work around security policies if they're too restrictive so that they can access the system, for example, by putting in a back door. C14 said "at some point you're a little bit looser on your security because you need to get stuff done and there's other defenses."

Stereotype	Definition
Cyber does not understand energy OT systems	Cyber SMEs do not understand how energy OT systems work and may overestimate impact on overall system
Cyber sees computers	For Cyber SMEs, energy OT devices can be reduced to computers
Cyber is detail-oriented	Cyber SMEs pay attention to details, go into rabbit holes, spend a long time on analysis
Cyber cuts off access to protect system	Cyber SMEs place protections on the system that prevent or make it difficult for Energy OT SMEs to access or operate systems
Cyber equals IT	Cyber security and IT staff/departments are the same
Energy OT understands systems	Energy OT SMEs are skilled in the design, maintenance, and operation of energy systems
Energy OT does not understand vulnerabilities	Energy OT SMEs do not understand exploit capabilities, attacks, and details about vulnerabilities and may underestimate ease of exploit
Energy OT lacks imagination	Energy OT SMEs do not or cannot think of technical possibilities outside of what they already know, e.g., an adversary changing a device's functionality
Energy OT takes shortcuts	Energy OT SMEs leave access open, create backdoors, or otherwise allow vulnerabilities to remain, for convenience or increased usability

Table 4: Specific stereotypes from responses comparing the two expert groups' strategies for vulnerability impact assessment and understanding of vulnerabilities. See Appendix D for more thematic codes.

Other perceptions. Energy OT SMEs were also depicted as lacking funding or resources (2 OT, 1 Cyber) and "mistak[ing] safety systems being certified safe or a security certification with securing a system from hacking" (1 Cyber).

4.3.3 Occupational Motivations. Regarding impressions about cyber SMEs' occupational mission, ten participants suggested that cyber SMEs identify exploits, vulnerabilities, and flaws (4 OT, 6 Cyber). Three participants said that cyber SMEs tear apart or dissect systems (1 OT, 2 Cyber), and three said they focus on protecting computer systems (3 OT).

The most common impressions about energy OT SMEs' motivation were that they focus on making sure the system works and ensuring power delivery (5 OT, 3 Cyber). One or two participants also suggested that energy OT SMEs focus on the following: operational efficiencies such as maximizing reliability, minimizing costs, and saving time (2 OT), development or design (2 OT), protecting systems (1 OT, 1 Cyber), and human safety (1 OT).

4.4 Participants' Suggestions (RQ3)

Throughout our interviews, participants shared insights about their collaborative experiences working with other type of experts and made many suggestions for how collaboration, usability, design, and education could be improved. Indeed, when discussing their own strategies for impact assessment, six participants suggested they would consult a SME from the other group themselves (3 OT, 3 Cyber), and when discussing perceptions of group strategies, eight said that they expected SMEs to consult the other group (4 OT, 4 Cyber) in certain situations.

Overall, eleven participants made suggestions about collaboration and communication (6 OT, 5 Cyber), emphasizing bringing together the two SME groups to work on the same team or collaborate in shared work settings, opening up communication and listening to each other, and understanding the goals and areas of the other SME group.

4.4.1 Integrate OT Environments to Include Both Experts. Participants suggested integrating energy OT operational environments by having conversations that build mutual understanding, creating overlap in operational teams, and conducting red-team simulated attack exercises.

E15 suggested that one cross-domain problem is that the two groups have different conceptions of what it means to protect a grid: "I can talk to you about protection and line current differentials …, but to a cyber security person, it's not going to make any sense. But that's how I protect my grid. And they can talk to me in other terms about how they can protect the thing, that I'm not going to understand." E7 suggested that a way to build mutual understanding is to have a discussion between the two groups that "resembles a lot of the same processes that an adversary would need to go through to develop a targeted capability to create a specific impact" and which requires both sides to go back and forth:

> *They're going to converge towards a point of understanding in … that back and forth of, "What do you mean somebody exploiting this couldn't crash the grid?" Well, because that piece of equipment, no matter what you do with it, can't cause an electrical cascading event. "OK, I don't know what that means, but it makes me glad that you can't crash the whole grid. What can you*

> *do?" Well, here's all the things you can do with this equipment, if you had total control over it. And the cyber guy is like, "Here's what I would need to do to have total control over it." (E7)*

Thus, approaching issues "from different sides of the center" allows the interdisciplinary team to iteratively build understanding of potential impacts on the system.

E1 highlighted the importance of overlap in operational teams to securing critical infrastructure and said that "operational groups" should work with "the security side" in an integrated matter to understand risk and avoid "breakdowns" in operational contexts:

> *Why do I care if a cyber researcher understands power equipment, and why do I care if a power SME understands cyber? The only time I really care about that is implementing it in the actual operating utilities. If [those groups] can work in a more integrated manner, then they are going to do a better job. And engineers, if they understand the risks and the hazards, are very good at using that in their designs. But if they don't understand that risk, then they're going to exclude that. And that's what I think happens in a lot of places, that you don't have enough overlap, so even if your power SME wants to do things correctly, they don't understand how to do it correctly. (E1)*

E1 thus emphasized integrating energy OT operational teams to include cyber SMEs to help "utilities protect their systems operationally."

C12 said that in their experience, the situations where "knowledge tends to go back and forth" were exercises that brought the groups together and assigned them roles to attack and protect the system.

> *You have a group of people that will be focused on trying to break something, and then you would have a group of your OT experts that are there to manage the system and restore and reign in the other team from going too far and damaging everything. (C12)*

C12 said that through these exercises, "the cyber people would become more knowledgeable about the system, and the [energy] OT SMEs would become more knowledgeable about the cyber aspect and what could break."

4.4.2 Consult Other SMEs for Domain-Specific Knowledge. Participants emphasized the importance of consulting and listening to people who understand the other domain very well. Some cyber SMEs suggested that talking to energy OT SMEs who understand specific systems would help them understand how systems are set up or implemented, how they are supposed to work, how they actually work, and what they are connected to. C11 said that energy OT SMEs can identify which systems are key to keep up and running and thus difficult to replace, as well as provide advice for how to replace such systems when they are no longer operational or should be put out of service due to vulnerabilities.

E8 suggested that they gained knowledge from cyber SMEs and said they now assume an air gap is already compromised: "I'm more cautious [about air gaps], but that's because I've worked with cyber security researchers and cybersecurity experts that told me otherwise. But that's not the commonly accepted practice, from my experience."

4.4.3 Make OT Systems More Usable. Seven participants suggested making energy OT systems more usable (5 OT, 2 Cyber). As discussed above, some participants conveyed the impressions that energy OT SMEs take shortcuts or leave vulnerable defaults open and that cyber SMEs cut off access to protect systems. E1 said that cyber SMEs "should not have it be so locked down that the operational side can't do their job," emphasizing that energy OT SMEs needs easy access to systems to do their job. C5 specifically spoke about usability, making the following suggestion:

> *If something is extremely difficult to do, but it has to be done all the time, then people are going to try to find shortcuts or ways around it, so [try] to work with the people who are using something to design solutions that will work for them. (C5)*

E8 said that there needs to be more open communication and more collaboration on how to accomplish securing devices and applications while allowing them to communicate as needed. C14 suggested tailoring or simplifying "cyber requirements" for the OT environment. E15 said, "You can't have them putting so many layers of protection that you can't use the system or operate it" and suggested "minimiz[ing] the complexity of cyber protections to avoid not being able to restore power due to cyber protections." They added:

> *To keep power flowing I have to do maintenance, operation on these devices, and replace equipment. [Cyber protections] can't be so difficult on the SCADA or communications sides that I'm unable to perform maintenance, repairs, replacements, and get the grid up. The system should not be so complex that we can't make it work with [them]. (E15)*

E16 said that a system or product might still "work very well" despite "poor code quality" and cyber SMEs' disapproval, suggesting that there could be more flexibility in restrictions for products that continue to work well.

C14 provided some insight into the technical problems of applying recommendations, such as installing Microsoft updates "in a plant kind of environment" or in "the electric sector":

> *They [energy OT SMEs] can't reboot their systems all the time. … But if you want to change your authentication on one system, you have to update all the other systems that talk to it, in order to continue talking to it. … The redundancy is more costly than in like a server farm. (C14)*

This suggests that they were familiar with how typical security measures like updates might disrupt operations.

4.4.4 Security by Design. Four participants (2 OT, 2 Cyber) recommended that OT systems be initially designed with computer security in mind, rather than focusing primarily on the operational functionality and addressing security flaws later on. C3 recommended bringing cyber SMEs into the development process at the software or board level, as security consultants, saying that some problems may be "a lot easier to fix in the beginning than to try

and go back and patch it." E16 suggested that software developers "clean up the code" while considering risks and "abuse cases" when developing a product:

> *There's a whole concept of product secure development cycle, and if developers were just to understand and follow the principles within the secure product development lifecycle, then 99% of the issues that we have today would go away because the developers weren't just trying to make things work. They were trying to make them work securely, using good coding practices, looking at risks. (E16)*

E10 made the design recommendation for equipment companies to make "the right choices at the very beginning of their design process" such as putting in "hardware protection that protects their software."

C14 expressed skepticism about revising design processes, suggesting that both expert groups might stick to old habits or mental models, saying, "We would hope to do a better job of it, but … we're going to go back to what we know also when we redesign it." They also noted that some OT systems are "obsolete" and difficult to understand even for energy OT SMEs, and yet that "trying to set up the infrastructure from scratch" would be very costly.

4.4.5 Educating SMEs. Participants made suggestions for things to teach cyber SMEs (4 OT, 5 Cyber) and energy OT SMEs (1 OT, 3 Cyber). Topics suggested for cyber SMEs include: context, energy infrastructure, functional purpose, intended use, configuration, what it controls and is connected to, system requirements, energy OT need for access, maintenance and operation, that some devices are not practically exploitable in OT contexts, what is being targeted, what to prioritize (avoid rabbit holes), and impact on controls. Topics suggested for energy OT SMEs include: hardware and software vulnerabilities, risks and attack vectors, system capabilities, how to monitor what's happening and detect anomalous behavior, and what red teams or attackers are looking for.

Some participants specified that even within their expert group, certain skills were needed. C14 suggested that curiosity and willingness to learn were prerequisites for vulnerability researchers. C12 also said that even among cyber SMEs, it was rare to find people who were exceptional at finding meaningful exploits, saying, "Being able to find exploits is a skill, and not everyone has it. … And I would probably put myself in that category." C13 suggested that a "good cyber security person" should have experience exploiting vulnerabilities." E4 said energy OT SMEs should be familiar with things like technology misuse, vulnerabilities and historical exploits for OT equipment.

5 DISCUSSION

Our research provides empirical insight into self-reported strategies, perceptions and suggestions of a group of interdisciplinary cyber SMEs and energy OT SMEs regarding vulnerability impact assessment in energy OT contexts. While we found that responses about information necessary to conduct an impact assessment (RQ1) were broadly similar across both groups of participants, some responses suggested major differences in the ways cyber SMEs and energy OT SMEs think about risks posed by vulnerabilities in energy OT systems. Differences appeared in their discussions of certain topics, like cyber SMEs' more adversarial and detailed considerations about access and exploits, and energy OT SMEs' holistic considerations about the overall system and disruptions in operations (Section 4.2). Differences also appeared in their perceptions of the two groups (RQ2), which align with prior work on differences between critical infrastructure security and traditional IT security approaches (see prior work in Section 2.1).

We first discuss the significance of the differences (RQ1 and RQ2) we found between the two groups (Section 5.1). We then discuss the interdisciplinarity of this group of participants and how their responses highlight the need for cross domain exchanges (Section 5.2). We also offer ideas for potential follow-on work related to cross-domain collaboration and for future work given the limitations of this study (Section 5.3). Finally, we make recommendations echoing the suggestions of participants (RQ3) to make systems more usable, and to develop more effective communication and collaboration across domains in critical infrastructure security (Section 5.4).

5.1 Harnessing Differences in Approaches

Participants' self-reported strategies, perceptions, and suggestions convey some relative differences in approaches to vulnerability impact assessment between energy OT SMEs and cyber SMEs. Finding differences within this interdisciplinary group is particularly insightful, as the differences highlight emphases and mindsets that can persist despite cross-domain experience. Considering that the goal of cross-domain interaction is not necessarily a complete skills transfer but rather to seek benefits from exposure to other methods and ways of thinking, the differences addressed in our work draw attention to approaches and perceptions that can potentially complement each other in building overlap in understanding risk for energy OT systems. Below we consider a few differences conveyed in participants' responses.

First, our study provides examples of cyber SMEs' considerations about gaining access to networks and resources, tracing paths across boundaries, modifying devices and their functionality, and exploitability. The overlap between these more adversarial considerations and energy OT systems may be useful for energy OT SMEs to understand.

Our study also revealed the more holistic emphases of energy OT SMEs on the overall system, potential disruptions in operations, and risk mitigation, which aligns with prior work suggesting that "OT practitioners" are primarily concerned with physical resilience and safety aspects such as "equipment damage and continuous supply of 'essential services' " [45]. Educating cyber SMEs about the overall system and their redundancies could help them avoid problems suggested by participants such as overestimating potential impact.

We encourage professionals and researchers to work to ensure that important aspects relating to risk and impact are transferred across domains.

5.2 An Interdisciplinary Group

Participants in our study had repeated exposure to the other discipline and worked with the other group at a research organization focusing on the energy sector. Given the interdisciplinary background of all participants and their similar broad-level responses, it appears that many participants had already built cross-domain

awareness that allowed them to consider both computer security and energy OT issues when assessing impact.

In our interviews, some participants made clear references to experiences where they gained understanding from the other kind of SME. These experiences likely helped them develop a model for each group's skills, occupational motivations, and weaknesses, and we therefore hypothesize that many of their considerations sprang out of exposure to the other discipline.

While we expected the groups to diverge in their perceptions of each other, we were surprised to find that they had consistent views of both groups. Even when speaking of their own group, participants shared critical views of limitations or weaknesses. We did not see many instances of resentment or annoyance (the only times we noted this was when energy OT SMEs spoke about security policies that prevented them from working or slowed them down). Rather, negative perceptions usually indicated recognition of particular tendencies.

Yet, interdisciplinary experience did not appear to have equalized their knowledge base; they did not replace each other. Participants were aware of their own gaps in knowledge and where they might need to consult the other type of expert, and they recognized the strengths of the other experts. This was consistent with prior work conveying differences between operational and security professionals (Section 2.1).

Indeed, the two groups' specializations appear distinct enough to imply that experts will continue to need to come together to contrast their perspectives and build cross-domain understanding. The problem remains that interdisciplinary security in critical infrastructure contexts is not the norm; it is uncommon for energy OT SMEs and cyber SMEs to have access to each other. Resource constraints may also prevent companies from being able to build interdisciplinary teams or bring people together. Our study suggests that discussions or exercises across groups working in the same context will provide valuable insight. Researchers and industry professionals must seek ways to facilitate cross-domain exchanges.

5.3 Future Work

Below we describe potential future work building on this study, addressing its limitations, and expanding into other infrastructure contexts.

First, following our discussion above about interdisciplinarity, we encourage future work that develops ways to foster effective and scalable cross-domain knowledge transfer in energy OT contexts. For example, such work could consider vulnerability impact assessment approaches of energy OT SMEs lacking computer security experience and test the influence of interventions, such as exposure to training, educational materials or interdisciplinary interactions with a cyber SME, on participants' risk assessment considerations.

Additionally, given our small sample size, we encourage future work that investigates whether our hypothesis that the interdisciplinary nature of the group leads to similar general approaches to impact assessment holds at a larger scale. It is possible that our thematic strategy codes were not able to sufficiently capture differences in impact assessment approaches for this limited number of participants. Future work could address these limitations by conducting a larger-scale study with these two kinds of experts to test whether there is a difference in approaches between the two expert groups, as well as between interdisciplinary and non-interdisciplinary experts.

Future work could also conduct interview studies with similarly sized interdisciplinary groups to see if differences are more pronounced when discussing different topics, such as what mitigations are acceptable, when to accept certain levels of risk, best patching practices, or who is responsible for given aspects of energy OT security.

Finally, we also recommend researchers explore building cross-domain understanding in different infrastructure contexts, such as healthcare, water, and transportation. Such contexts similarly require professionals to learn to operate highly specialized and complicated systems, such that adding computer security understanding to their job requirements can pose training and educational challenges.

5.4 Recommendations Building on Suggestions

There is a dire need for cross-domain collaboration in energy OT operational, training, and educational contexts, as it is not the norm for energy OT SMEs and cyber SMEs to work together, especially given the short supply of computer security workers. In their suggestions addressing collaboration between the two groups (RQ3), cyber SMEs and energy OT SMEs emphasized the continuing need for cross-domain communication and knowledge sharing among people who understand vulnerabilities and energy OT systems, as well as usable security and security by design. We echo participants' suggestions in our recommendations below.

First, we reiterate participants' suggestions to make energy OT systems more usable. As conveyed by participants, low usability security requirements can prevent engineers from effectively doing their work, or worse, encourage engineers and operators to use shortcuts that leave open vulnerabilities to be exploited. Usable solutions could include collaboratively developing security policies or designs that take into account operational needs such as continuous operations and the ability to restore power, simplifying or reducing human-in-the-loop computer security requirements that are too complex or burdensome for energy OT SMEs, and finding ways to update systems with minimal downtime.

Since one of the roadblocks to cross-domain exchanges may be organizational structure and assignment of roles, we also echo participants' suggestions to integrate teams. We recommend that companies and researchers investigate potential benefits of unsiloing workers and encouraging cross pollination of ideas. Walking through interdisciplinary contexts from multiple angles can help stakeholders develop holistic solutions that integrate diverse considerations.

As it may not always be realistic to integrate teams, given limited resources and labor supply, we also encourage the design and development of tools and interventions to help avoid wasting limited resources of potentially overextended operational engineering and cyber security staff. In addition to our call above for researchers to develop effective ways to acquire and apply cross-domain knowledge, we recommend that utilities and energy operators educate cyber SMEs and energy OT SMEs on the other group's objectives, how they think about a system or context, and information they

might consider critical to understanding risk in operational contexts and computer security.

In particular, such training would provide energy OT SMEs with additional information on how to think about energy OT systems by considering different perspectives. Cross domain understanding could act as a companion to industry risk assessment standards, helping operators and other energy OT SMEs interpret standards with more nuance, rather than mechanically following checklists or output from automated systems, thus building resiliency in the human operators of energy OT systems.

6 CONCLUSION

We interviewed two groups of subject matter experts, energy OT SMEs and cyber SMEs, to explore and compare the two groups' self-reported impact assessment strategies, perceptions of differences between the groups, and suggestions for working together. We find that while their impact assessment considerations were generally similar, the details of their considerations and their discussions of their perceptions of each group revealed major differences in mindset and understanding. We recommend following participants' suggestions to foster interdisciplinary collaboration and integrate usable security into operational contexts, and we call for researchers and companies to develop tools and interventions that will enable cross-domain knowledge sharing in critical infrastructure security.

ACKNOWLEDGMENTS

This work was supported in part by the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response. We also wish to acknowledge the thoughtful feedback from the anonymous CHI'24 reviewers that helped us strengthen this paper.

REFERENCES

[1] Bushra A. Alahmadi, Louise Axon, and Ivan Martinovic. 2022. 99% False Positives: A Qualitative Study of SOC Analysts' Perspectives on Security Alarms. In *31st USENIX Security Symposium (USENIX Security 22)* (Boston, MA). USENIX Association, 2783–2800. https://www.usenix.org/conference/usenixsecurity22/presentation/alahmadi

[2] Mohammed Alghassab. 2022. Analyzing the Impact of Cybersecurity on Monitoring and Control Systems in the Energy Sector. *Energies* 15, 1 (Jan. 2022), 218. https://doi.org/10.3390/en15010218

[3] George E. Apostolakis and Douglas M. Lemon. 2005. A Screening Methodology for the Identification and Ranking of Infrastructure Vulnerabilities Due to Terrorism. *Risk Analysis* 25, 2 (2005), 361–376. https://doi.org/10.1111/j.1539-6924.2005.00595.x

[4] Miriam E. Armstrong, Keith S. Jones, Akbar Siami Namin, and David C. Newton. 2018. The Knowledge, Skills, and Abilities Used by Penetration Testers: Results of Interviews with Cybersecurity Professionals in Vulnerability Assessment and Management. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 62, 1 (2018), 709–713. https://doi.org/10.1177/1541931218621161

[5] Miriam E. Armstrong, Keith S. Jones, Akbar Siami Namin, and David C. Newton. 2020. Knowledge, Skills, and Abilities for Specialized Curricula in Cyber Defense: Results from Interviews with Cyber Professionals. *ACM Transactions on Computing Education* 20, 4 (Nov. 2020), 29:1–29:25. https://doi.org/10.1145/3421254

[6] Kate Behncken. 2022. Closing the cybersecurity skills gap – Microsoft expands efforts to 23 countries. https://blogs.microsoft.com/blog/2022/03/23/closing-the-cybersecurity-skills-gap-microsoft-expands-efforts-to-23-countries/.

[7] Luke Bencie and Sami Araboghli. 2018. A 6-Part Tool for Ranking and Assessing Risks. *Harvard Business Review* (Sept. 2018). https://hbr.org/2018/09/a-6-part-tool-for-ranking-and-assessing-risks.

[8] Veroniek Binkhorst, Tobias Fiebig, Katharina Krombholz, Wolter Pieters, and Katsiaryna Labunets. 2022. Security at the End of the Tunnel: The Anatomy of VPN Mental Models Among Experts and Non-Experts in a Corporate Context. In *31st USENIX Security Symposium (USENIX Security 22)* (Boston, MA). USENIX Association, 3433–3450. https://www.usenix.org/conference/usenixsecurity22/presentation/binkhorst

[9] Seppo Borenius, Pavithra Gopalakrishnan, Lina Bertling Tjernberg, and Raimo Kantola. 2022. Expert-Guided Security Risk Assessment of Evolving Power Grids. *Energies* 15, 9 (Jan. 2022), 3237. https://doi.org/10.3390/en15093237

[10] David Botta, Rodrigo Werlinger, André Gagné, Konstantin Beznosov, Lee Iverson, Sidney Fels, and Brian Fisher. 2007. Towards Understanding IT Security Professionals and Their Tools. In *Proceedings of the 3rd Symposium on Usable Privacy and Security* (Pittsburgh, Pennsylvania, USA) *(SOUPS '07)*. Association for Computing Machinery, 100–111. https://doi.org/10.1145/1280680.1280693

[11] Eric Byres. 2013. The air gap: SCADA's enduring security myth. *Commun. ACM* 56, 8 (Aug. 2013), 29–31. https://doi.org/10.1145/2492007.2492018

[12] Yulia Cherdantseva, Pete Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, and Kristan Stoddart. 2016. A review of cyber security risk assessment methods for SCADA systems. *Computers & Security* 56 (Feb. 2016), 1–27. https://doi.org/10.1016/j.cose.2015.09.009

[13] CISA. 2023. US-CERT and ICS-CERT Transition to CISA | CISA. https://www.cisa.gov/news-events/alerts/2023/02/24/us-cert-and-ics-cert-transition-cisa.

[14] CISA. 2024. Cybersecurity Alerts & Advisories | CISA. https://www.cisa.gov/news-events/cybersecurity-advisories. Accessed February 22, 2024.

[15] Wm. Arthur Conklin. 2016. IT vs. OT Security: A Time to Consider a Change in CIA to Include Resilience. In *2016 49th Hawaii International Conference on System Sciences (HICSS)*. 2642–2647. https://doi.org/10.1109/HICSS.2016.331

[16] The MITRE Corporation. 2024. CWE - Common Weakness Enumeration. https://cwe.mitre.org/. Accessed February 22, 2024.

[17] The MITRE Corporation. 2024. Home | CVE. https://www.cve.org/. Accessed February 22, 2024.

[18] The MITRE Corporation. 2024. MITRE ATT&CK. https://attack.mitre.org/. Accessed February 22, 2024.

[19] Julie Creswell, Nicole Perlroth, and Noam Scheiber. 2021. Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business. *The New York Times* (June 2021). https://www.nytimes.com/2021/06/01/business/meat-plant-cyberattack-jbs.html.

[20] Alvaro A. Cárdenas, Saurabh Amin, Zong-Syun Lin, Yu-Lun Huang, Chi-Yen Huang, and Shankar Sastry. 2011. Attacks against process control systems: risk assessment, detection, and response. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS '11)*. Association for Computing Machinery, 355–366. https://doi.org/10.1145/1966913.1966959

[21] K Davis, R Berthier, S Zonouz, G Weaver, R Bobba, E Rogers, P Sauer, and D Nicol. 2016. Cyber-physical security assessment (CYPSA) for electric power systems. *IEEE-HKN: THE BRIDGE* (2016).

[22] Patrick Denzler and Wolfgang Kastner. 2023. *Reference Architectures for Closing the IT/OT Gap*. Springer, 95–123. https://doi.org/10.1007/978-3-662-65004-2_4

[23] Payal Dhar. 2021. Cybersecurity Report: "Smart Farms" Are Hackable Farms. *IEEE Spectrum* (March 2021). https://spectrum.ieee.org/cybersecurity-report-how-smart-farming-can-be-hacked.

[24] Chandelis Duster. 2021. Energy secretary says adversaries have capability of shutting down US power grid | CNN Politics. *CNN* (June 2021). https://www.cnn.com/2021/06/06/politics/us-power-grid-jennifer-granholm-cnntv/index.html.

[25] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. 2020. Ask the Experts: What Should Be on an IoT Privacy and Security Label?. In *2020 IEEE Symposium on Security and Privacy (SP)*. 447–464. https://doi.org/10.1109/SP40000.2020.00043

[26] Kirstie Hawkey, David Botta, Rodrigo Werlinger, Kasia Muldner, Andre Gagne, and Konstantin Beznosov. 2008. Human, Organizational, and Technological Factors of IT Security. In *CHI '08 Extended Abstracts on Human Factors in Computing Systems* (Florence, Italy) *(CHI EA '08)*. Association for Computing Machinery, 3639–3644. https://doi.org/10.1145/1358628.1358905

[27] Siegfried Hollerer, Bernhard Brenner, Pushparaj Rajaram Bhosale, Clara Fischer, Ali Mohammad Hosseini, Sofia Maragkou, Maximilian Papa, Sebastian Schlund, Thilo Sauter, and Wolfgang Kastner. 2023. *Challenges in OT Security and Their Impacts on Safety-Related Cyber-Physical Production Systems*. Springer, 171–202. https://doi.org/10.1007/978-3-662-65004-2_7

[28] Siegfried Hollerer, Thilo Sauter, and Wolfgang Kastner. 2022. Risk Assessments Considering Safety, Security, and Their Interdependencies in OT Environments. In *Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES '22)*. Association for Computing Machinery, 1–8. https://doi.org/10.1145/3538969.3543814

[29] Huma Imran, Mohamed Salama, Colin Turner, and Sherif Fattah. 2022. Cybersecurity Risk Management Frameworks in the Oil and Gas Sector: A Systematic Literature Review. In *Advances in Information and Communication (Lecture Notes in Networks and Systems)*, Kohei Arai (Ed.). Springer International Publishing, 871–894. https://doi.org/10.1007/978-3-030-98015-3_59

[30] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "...No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)* (Ottawa, Canada). USENIX Association, 327–346. https://www.usenix.org/conference/soups2015/proceedings/presentation/ion

[31] Inc ISC2. 2023. *ISC2 Cybersecurity Workforce Study 2023.* https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf.

[32] Suhaila Ismail, Elena Sitnikova, and Jill Slay. 2014. Using integrated system theory approach to assess security for SCADA systems cyber security for critical infrastructures: A pilot study. In *2014 11th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD).* 1000–1006. https://doi.org/10.1109/FSKD.2014.6980976

[33] Jan Jancar, Marcel Fourné, Daniel De Almeida Braga, Mohamed Sabt, Peter Schwabe, Gilles Barthe, Pierre-Alain Fouque, and Yasemin Acar. 2022. "They're not that hard to mitigate": What Cryptographic Library Developers Think About Timing Attacks. In *2022 IEEE Symposium on Security and Privacy (SP).* 632–649. https://doi.org/10.1109/SP46214.2022.9833713

[34] Derek B. Johnson. 2023. Department of Energy opens $9 million in competitive cyber funding to small electric utilities. *SC Media* (Aug. 2023). https://www.scmagazine.com/news/department-of-energy-opens-9-million-in-competitive-cyber-funding-to-small-electric-utilities.

[35] Sara Kraemer and Pascale Carayon. 2003. A Human Factors Vulnerability Evaluation Method for Computer and Information Security. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 47, 12 (2003), 1389–1393. https://doi.org/10.1177/154193120304701202

[36] Josephine Lamp, Carlos E. Rubio-Medrano, Ziming Zhao, and Gail-Joon Ahn. 2019. ExSol: Collaboratively Assessing Cybersecurity Risks for Protecting Energy Delivery Systems. In *2019 7th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES).* 1–6. https://doi.org/10.1109/MSCPES.2019.8738791

[37] Roslyn Layton. 2021. Hackers Are Targeting U.S. Banks, And Hardware May Give Them An Open Door. *Forbes* (Feb. 2021). https://www.forbes.com/sites/roslynlayton/2021/03/17/hackers-are-targeting-us-banks-and-hardware-may-give-them-an-open-door/.

[38] James Andrew Lewis and William Crumpler. 2019. The Cybersecurity Workforce Gap. *Center for Strategic and International Studies* (Jan. 2019). https://www.csis.org/analysis/cybersecurity-workforce-gap.

[39] Martin C. Libicki, David Senty, and Julia Pollak. 2014. *Hackers Wanted: An Examination of the Cybersecurity Labor Market.* https://www.rand.org/pubs/research_reports/RR430.html.

[40] Maria B. Line, Ali Zand, Gianluca Stringhini, and Richard Kemmerer. 2014. Targeted Attacks against Industrial Control Systems: Is the Power Industry Prepared?. In *Proceedings of the 2nd Workshop on Smart Energy Grid Security (SEGS '14).* Association for Computing Machinery, 13–22. https://doi.org/10.1145/2667190.2667192

[41] P. Litherland, R. Orr, and R. Piggin. 2016. Cyber security of operational technology: understanding differences and achieving balance between nuclear safety and nuclear security. In *11th International Conference on System Safety and Cyber-Security (SSCS 2016).* 1–6. https://doi.org/10.1049/cp.2016.0856

[42] Lloyd's. 2015. Business Blackout: The insurance implications of a cyber attack on the US power grid. https://www.lloyds.com/news-and-insights/risk-reports/library/business-blackout/.

[43] Alessandro Mantovani, Simone Aonzo, Yanick Fratantonio, and Davide Balzarotti. 2022. RE-Mind: a First Look Inside the Mind of a Reverse Engineer. In *31st USENIX Security Symposium (USENIX Security 22)* (Boston, MA). USENIX Association, 2727–2745. https://www.usenix.org/conference/usenixsecurity22/presentation/mantovani

[44] Claire Marshall and Malcom Prior. 2022. Cyber security: Global food supply chain at risk from malicious hackers. *BBC News* (May 2022). https://www.bbc.com/news/science-environment-61336659.

[45] Ola Michalec, Sveta Milyaeva, and Awais Rashid. 2022. When the future meets the past: Can safety and cyber security coexist in modern critical infrastructures? *Big Data & Society* 9, 1 (2022), 205395172211083. https://doi.org/10.1177/20539517221108369

[46] Ola Aleksandra Michalec, Dirk van der Linden, Sveta Milyaeva, and Awais Rashid. 2020. Industry Responses to the European Directive on Security of Network and Information Systems (NIS): Understanding policy implementation practices across critical infrastructures. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020).* USENIX Association, 301–317. https://www.usenix.org/conference/soups2020/presentation/michalec

[47] Maggie Miller. 2022. The mounting death toll of hospital cyberattacks. *POLITICO* (Dec. 2022). https://www.politico.com/news/2022/12/28/cyberattacks-u-s-hospitals-00075638.

[48] Jaron Mink, Harjot Kaur, Juliane Schmüser, Sascha Fahl, and Yasemin Acar. 2023. "Security is not my field, I'm a stats guy": A Qualitative Root Cause Analysis of Barriers to Adversarial Machine Learning Defenses in Industry. In *32nd USENIX Security Symposium (USENIX Security 23)* (Anaheim, CA). USENIX Association, 3763–3780. https://www.usenix.org/conference/usenixsecurity23/presentation/mink

[49] Glenn Murray, Michael N. Johnstone, and Craig Valli. 2017. The convergence of IT and OT in critical infrastructure. In *Proceedings of the 15th Australian Information Security Management Conference.* 149–155. https://doi.org/10.4225/75/5a84f7b595b4e

[50] Cen Nan and Irene Eusgeld. 2011. Exploring impacts of single failure propagation between SCADA and SUC. In *2011 IEEE International Conference on Industrial Engineering and Engineering Management.* 1564–1568. https://doi.org/10.1109/IEEM.2011.6118180

[51] North American Electric Reliability Corporation. 2023. Reliability Standards. https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx. Accessed February 22, 2024.

[52] Federation of American Scientists Intelligence Resource Program. 1991. FM 34-36 Appendix D: Target Analysis Practice. https://irp.fas.org/doddir/army/fm34-36/appd.htm. Accessed February 22, 2024.

[53] Forum of Incident Response and Security Teams. 2023. CVSS v3.1 Specification Document. https://www.first.org/cvss/specification-document. Accessed February 22, 2024.

[54] National Institute of Standards and Technology. [n. d.]. NVD - CVEs and the NVD Process. https://nvd.nist.gov/general/cve-process. Accessed February 22, 2024.

[55] National Institute of Standards and Technology. 2018. Cybersecurity Framework | NIST. https://www.nist.gov/cyberframework. Accessed February 22, 2024.

[56] National Institute of Standards and Technology. 2019. Vulnerability - Glossary CSRC. https://csrc.nist.gov/glossary/term/vulnerability. Accessed February 22, 2024.

[57] National Institute of Standards and Technology. 2023. NVD - Vulnerability Metrics. https://nvd.nist.gov/vuln-metrics. Accessed February 22, 2024.

[58] U. S. Government Accountability Office. 2019. Preparing for Evolving Cybersecurity Threats Facing the U.S. Electric Grid. https://www.gao.gov/blog/2019/10/16/preparing-for-evolving-cybersecurity-threats-facing-the-u-s-electric-grid.

[59] Jon Oltsik and Bill Lundell. 2021. *The Life and Times of Cybersecurity Professionals 2021 Volume V.* https://www.issa.org/wp-content/uploads/2021/07/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Jul-2021.pdf.

[60] P. A. S. Ralston, J. H. Graham, and J. L. Hieb. 2007. Cyber security risk assessment for SCADA and DCS networks. *ISA Transactions* 46, 4 (Oct. 2007), 583–594. https://doi.org/10.1016/j.isatra.2007.04.003

[61] RP Reece and Bernd Carsten Stahl. 2015. The professionalisation of information security: Perspectives of UK practitioners. *Computers & Security* 48 (Feb. 2015), 182–195. https://doi.org/10.1016/j.cose.2014.10.007

[62] Paul Reilly, Elisa Serafinelli, Rebecca Stevenson, Laura Petersen, and Laure Fallou. 2018. Enhancing Critical Infrastructure Resilience Through Information-Sharing: Recommendations for European Critical Infrastructure Operators. In *Transforming Digital Worlds (Lecture Notes in Computer Science).* Springer International Publishing, 120–125. https://doi.org/10.1007/978-3-319-78105-1_15

[63] Lena Reinfelder, Robert Landwirth, and Zinaida Benenson. 2019. Security Managers Are Not The Enemy Either. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19).* Association for Computing Machinery, 1–7. https://doi.org/10.1145/3290605.3300663

[64] Justin Rende. 2023. Council Post: Why Overcoming The Cybersecurity Labor Shortage Matters To Company Success. *Forbes* (March 2023). https://www.forbes.com/sites/forbestechcouncil/2023/03/01/why-overcoming-the-cybersecurity-labor-shortage-matters-to-company-success/.

[65] Reuters. 2023. Bank of Canada says cyber attack could threaten overall financial stability. *Reuters* (May 2023). https://www.reuters.com/article/idUSBCLIGEJ5H/.

[66] David Rind, Sean Lyngaas. 2023. Apparent cyberattack forces Florida hospital system to divert some emergency patients to other facilities | CNN Politics. *CNN* (Feb 2023). https://www.cnn.com/2023/02/03/politics/cyberattack-hospital-tallahassee-memorial-florida/index.html.

[67] Paul F. Roberts. 2021. Under Scrutiny, Big Ag Scrambles To Address Cyber Risk. *Forbes* (June 2021). https://www.forbes.com/sites/paulfroberts/2021/06/20/under-scrutiny-big-ag-scrambles-to-address-cyber-risk/.

[68] Ax Sharma. 2021. $5.9 million ransomware attack on farming co-op may cause food shortage. *Ars Technica* (Sept. 2021). https://arstechnica.com/information-technology/2021/09/5-9-million-ransomware-attack-on-farming-co-op-may-cause-food-shortage/.

[69] Nissy Sombatruang, Tristan Caulfield, Ingolf Becker, Akira Fujita, Takahiro Kasama, Koji Nakao, and Daisuke Inoue. 2023. Internet Service Providers' and Individuals' Attitudes, Barriers, and Incentives to Secure IoT. In *32nd USENIX Security Symposium (USENIX Security 23)* (Anaheim, CA). USENIX Association, 1541–1558. https://www.usenix.org/conference/usenixsecurity23/presentation/sombatruang

[70] Tim Starks. 2023. Analysis | A presidential critical infrastructure protection order is getting a badly needed update, officials say. *Washington Post* (May 2023). https://www.washingtonpost.com/politics/2023/05/11/presidential-critical-infrastructure-protection-order-is-getting-badly-needed-update-officials-say/.

[71] Alexander Staves, Antonios Gouglidis, and David Hutchison. 2023. An Analysis of Adversary-Centric Security Testing within Information and Operational Technology Environments. *Digital Threats: Research and Practice* 4, 1 (Mar 2023), 14:1–14:29. https://doi.org/10.1145/3569958

[72] Timothy Summers, Kalle J. Lyytinen, Tony Lingham, and Eugene A. Pierce. 2013. How Hackers Think: A Study of Cybersecurity Experts and Their Mental Models. *The Third International Conference on Engaged Management Scholarship* (Sept. 2013). https://doi.org/10.2139/ssrn.2326634

[73] Gillian Tett. 2023. The financial system is alarmingly vulnerable to cyber attack. *Financial Times* (Feb. 2023). https://www.ft.com/content/03507666-aad7-4dc3-a836-658750b880ce.

[74] Mary Theofanos, Brian Stanton, Susanne Furman, Sandra Spickard Prettyman, and Simson Garfinkel. 2017. Be Prepared: How US Government Experts Think About Cybersecurity. In *Workshop on Usable Security (USEC)*. Internet Society. http://dx.doi.org/10.14722/usec.2017.23006

[75] Marianthi Theoharidou, Panayiotis Kotzanikolaou, and Dimitris Gritzalis. 2011. Risk assessment methodology for interdependent critical infrastructures. *International Journal of Risk Assessment and Management (IJRAM)* 15, 2/3 (2011), 128. https://doi.org/10.1504/IJRAM.2011.042113

[76] Daniel Votipka, Kelsey R. Fulton, James Parker, Matthew Hou, Michelle L. Mazurek, and Michael Hicks. 2020. Understanding security mistakes developers make: Qualitative analysis from Build It, Break It, Fix It. In *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, 109–126. https://www.usenix.org/conference/usenixsecurity20/presentation/votipka-understanding

[77] Daniel Votipka, Rock Stevens, Elissa Redmiles, Jeremy Hu, and Michelle Mazurek. 2018. Hackers vs. Testers: A Comparison of Software Vulnerability Discovery Processes. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, 374–391.

[78] Robert Walton. 2021. A month after "malicious" cyberattack, a small Colorado utility still doesn't have all systems back online. *Utility Dive* (Dec. 2021). https://www.utilitydive.com/news/a-month-after-malicious-cyberattack-a-small-colorado-utility-still-doesn/610983/.

[79] Nicole Wetsman. 2022. Cyberattack delays patient care at major US hospital chain. *The Verge* (Oct. 2022). https://www.theverge.com/2022/10/11/23398707/cyberattack-hospital-system-patient-care-issues.

[80] Flynn Wolf, Adam J. Aviv, and Ravi Kuber. 2021. Security Obstacles and Motivations for Small Businesses from a CISO's Perspective. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, 1199–1216. https://www.usenix.org/conference/usenixsecurity21/presentation/wolf

[81] Marilyn Wolf and Dimitrios Serpanos. 2018. Safety and Security in Cyber-Physical Systems and Internet-of-Things Systems. *Proc. IEEE* 106, 1 (Jan. 2018), 9–20. https://doi.org/10.1109/JPROC.2017.2781198

[82] Qiushi Wu, Yue Xiao, Xiaojing Liao, and Kangjie Lu. 2022. OS-Aware Vulnerability Prioritization via Differential Severity Analysis. In *31st USENIX Security Symposium (USENIX Security 22)* (Boston, MA). USENIX Association, 395–412. https://www.usenix.org/conference/usenixsecurity22/presentation/wu-qiushi

[83] Farah Yousry. 2023. Cyberattacks on health care are increasing. Inside one hospital's fight to recover. *NPR* (May 2023). https://www.npr.org/sections/health-shots/2023/05/08/1172569347/cyberattacks-on-health-care-are-increasing-inside-one-hospitals-fight-to-recover.

[84] Kim Zetter. 2021. Hacking Wall Street. *The New York Times* (July 2021). https://www.nytimes.com/2021/07/03/business/dealbook/hacking-wall-street.html.

[85] Ioannis Zografopoulos, Juan Ospina, Xiaorui Liu, and Charalambos Konstantinou. 2021. Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies. *IEEE Access* 9 (2021), 29775–29818. https://doi.org/10.1109/ACCESS.2021.3058403

A POSITIVE AND NEGATIVE PERCEPTIONS OF SME GROUPS

Below we present the positive and negative perceptions of both expert groups. Since the distribution of perceptions of both SME groups were very similar, as shown in Appendix B, we present results about the perception of SME groups in aggregate, not dividing perceptions according to the SME group to which the participant belonged but rather focusing on the target group of the participant's statements.

When discussing differences in the groups' approaches, more participants spoke positively about cyber SMEs than about energy OT SMEs for topics relating to Accessibility, Attack, and Vulnerability, but cyber SMEs were perceived more negatively for the topics of Consequence and Connectivity. Energy OT SMEs were depicted more positively regarding Connectivity and Consequence topics, and more negatively for Accessibility themes. The term "positive" means that the described group was perceived as adequately or effectively considering the factors relating to the topic, and "negative" signifies the converse.

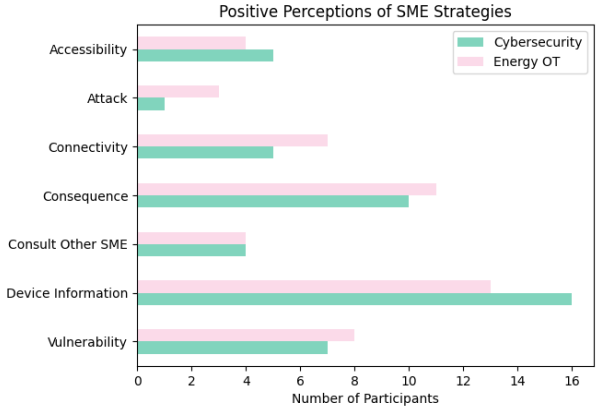

Figure 2: Positive perceptions of each SME group's impact assessment strategies and understanding, using top-level strategy codes and showing count per participant by target group.

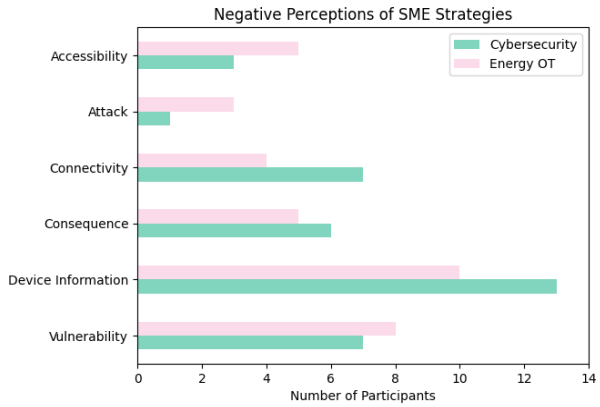

Figure 3: Negative perceptions of each SME group's impact assessment strategies and understanding, using top-level strategy codes and showing count per participant by target group.

B PERCEPTIONS BY PERCEIVING GROUP

The positive and negative perceptions offered by both SME groups about themselves and the other group were similar across each group, as can be seen in Table 5 and Table 6 below.

Cyber Main Code	Positive		Negative	
	Cyber	OT	Cyber	OT
Accessibility	4	1	1	2
Attack	1	0	1	0
Connectivity	2	3	3	4
Consequence	4	6	5	1
Consult Other SME	2	2	0	0
Device Information	8	8	7	6
Vulnerability	6	1	1	6
Total	27	22	18	19

Table 5: Positive and negative valences for Cyber SMEs' narrated depictions of Cyber and Energy OT SMEs' vulnerability impact assessment approaches, using our top-level codes for impact assessment topics.

OT Main Code	Positive		Negative	
	Cyber	OT	Cyber	OT
Accessibility	3	1	2	3
Attack	3	0	1	2
Connectivity	4	3	1	3
Consequence	4	7	4	1
Consult Other SME	2	2	0	0
Device Information	5	8	8	8
Vulnerability	5	3	2	6
Total	23	21	16	19

Table 6: Positive and negative valences for Energy OT SMEs' narrated depictions of Cyber and Energy OT SMEs, using our top-level codes for impact assessment topics.

C INTERVIEW QUESTIONS

Below are the interview questions we used in our semi-structured interviews.

C.1 Background Questions

(1) What is your current job role?
(2) How many years?
(3) Previous relevant experience?
(4) What do you mainly work on? What is your broad area of expertise, for example, electric, ONG, computer security, or other?
(5) How familiar are you with energy sector operational technology (OT)?
(6) Do you have a background in or exposure to cybersecurity? *(If yes: In vulnerability analysis?)*
(7) Have you done impact assessments?
(8) Has your work focused on the impact of cyber vulnerabilities?
(9) Have you encountered or do you know of any standard procedures, strategies, or metrics for assessing the impact of cyber vulnerabilities?
(10) Have you worked on the same team as [energy OT/cybersecurity SMEs] before?
(11) Has your work overlapped with their work?
(12) In the context of OT security, have you collaborated across operational security and computer IT security teams?

C.2 Self-Reported Strategies

(1) How would you go about considering the potential impact of a cyber vulnerability in an OT system?
  (a) What information would you seek?
  (b) What questions would you ask?
  (c) How might the sub-sector in which the system is used influence your considerations, for example, generation, transmission, distribution?
  (d) How might the context or use-case of the system influence your approach?
  (e) How might the vendor of the system influence your approach?
  (f) Are there any other factors you would need or want to know about, to determine the impact, which we haven't already discussed?
(2) In your experience, how do energy OT SMEs' approaches or methods in assessing impact of cybervulnerabilites differ from cybersecurity SMEs' approaches?
(3) In your experience, how do energy OT SMEs' understanding of cyber vulnerabilities differ from how cybersecurity SMEs might understand cyber vulnerabilities?

C.3 Perceptions of SME Groups

(1) What are some gaps or differences in thinking or strategy that you have noticed in cybersecurity SMEs and energy OT SMEs that might be important to consider when conducting an impact assessment for an energy OT device or component?
(2) What are some specific things [energy OT/cybersecurity] SMEs are neglecting or perhaps overprioritizing at the expense of other things?
  (a) *(Ask for other SME type.)*
(3) What type of information needs to cross between the two domains to more accurately gauge cyberattacks' impact on energy OT systems?
(4) Based on your knowledge and experience, what cyber vulnerability impacts might energy OT SMEs tend to underestimate or overestimate?
(5) What cyber vulnerability impacts might cybersecurity SMEs tend to underestimate or overestimate?

D APPENDIX - CODE BOOK

We include our code book with the strategy codes we used to label response to all questions we analyzed in Table 7 and the perception

codes in Table 8, which we used to label responses about general skills, motivations, stereotypes of both expert groups.

E SUBCODES

Below are counts per participant for the subcodes described in Appendix D, which account for more detailed themes we encountered. Table 9 includes relevant information categories for participants' self-reported impact assessment strategies, counted per individual self-reported narrative. Table 10 includes all codes for perceptions of the SME groups, counted per participant (from either group) who expressed a negative opinion about cyber SMEs ("Cyber Negative"), a positive opinion about cyber SMEs ("Cyber Positive"), a negative opinion about energy OT SMEs ("OT Negative"), or a positive opinion about energy OT SMEs("OT Positive").

Main Code	Subcode	Definition
Accessibility	General	What type of access has to be necessary to get to it?
	Network Access	Can the network be reached? Does an attacker have to have a local presence on a network, behind several firewalls; via internet?
	Physical Access	Does reaching the system require physical access or contact with the system?
Attack	General	Consideration of adversarial threat, attacker and potential attack vectors
Connectivity	Communication Protocol	Specific protocol configuration and modules
	Logical Connectivity	How does this relate to, influence, or control other things in the system, beyond just physical or network connection? Follow-on effects. Dependencies.
	Network Architecture	Overall map that defines network on large scale
	Network Connectivity	How does it interact on the network? What connections are open?
	Physical Connectivity	What are the physical devices, ports, wires, etc. that it is connected to?
	Segmentation	How segmented is it from networks or the outside world? Boundaries.
Consequence	Cost/Financial Impact	Impact on costs, finances, business priorities
	Damage to Equipment	Physical damage to device/system/equipment
	Disrupt Operations	Disrupt operations, shut down power, cause outage
	Ecological Impact	Effect on the environment
	General	Consequences, implications, impacts, what could happen; includes concepts like data loss, criticality, critical infrastructure, severity of impact
	Human Impact	How many people might be impacted? Could there be injuries?
	Remediation	What will it take to restore service? How long will it take to fix things?
	Scale of Impact	How far does the impact spread, e.g., region, duration, number of systems
Consult other SME	General	Need or wish to consult the other kind of SME to seek their explanation, advice, or work on part of the problem
Device Information	Basic Information	What is the device or system? How is it installed, configured?
	Capabilities	What can be done on this device? Can it be used beyond intended function?
	Functional Purpose	What does the device or system do? What is it made to do? How is it used?
	Maintenance History	Details about when, how, how often the system is updated or maintained
	Physical Location	Where does it live? Physical location of device or system.
	Protections	How is the system protected? Includes physical and network protections
	System Architecture	Information about setup in relation to other things in a broader system
	Ubiquity/Deployment	How common or prevalent is this device in the system and generally?
	Users	Who uses the system or device?
Vendor	General	Unprompted mention of the vendor, before being prompted directly
Vulnerability	Affected Area	What places, systems, or devices have the vulnerability?
	Exploit Requirements	What is required to exploit the vulnerability? How long would it take?
	Mitigation	Can the vulnerability be mitigated: prevented, stopped, or patched?
	Residual Impact	An impact that causes adverse effects that remain after efforts to remediate
	Understanding of Vulnerability	How does the vulnerability work? What is the vulnerability supposed to do? How does it relate to system operation?
	Vulnerability Information	Basic information about the vulnerability, e.g., whether it occurs or not, CVE number, vulnerability score, what system it applies to

Table 7: Thematic codes developed for responses to questions about participants' self-reported strategies for vulnerability impact assessment.

Main Code	Subcode	Definition
Occupational Motivation	Cyber focuses on protecting computer systems	Cyber SME's goal is to protect computer systems, prevent intrusion
	Cyber identifies attack/exploit	Cyber SME looks for and identifies potential attacks or exploits
	Cyber identifies flaws or problems	Cyber SME seeks and identifies exploitable flaws or problems in software or hardware
	Cyber identifies things others haven't seen yet	Cyber SME identifies overlooked aspects of technology that could be exploited
	Cyber identifies vulnerabilities	Cyber SME identifies vulnerabilities, which could be exploited
	Cyber tears apart systems	Cyber SME takes apart systems to better understand them
	OT focuses on development/design	OT focuses on and prioritizes the development or design process
	OT focuses on making sure the system works	OT focuses on and prioritizes maintenance, operations, making sure devices work and power is flowing
	OT focuses on operational efficiency	OT focuses on and prioritizes reliability, minimizing or saving costs, saving time, operating at peak efficiencies
	OT focuses on protecting systems	OT focuses on keeping system and tools safe, keeping people out
	OT focuses on safety	OT focuses on and prioritizes human safety
Stereotype	Cyber cuts off access to protect system	Cyber SMEs place protections on the system that prevent or make it difficult for OT to access or operate systems
	Cyber is detail-oriented	Cyber SMEs pay attention to details, go into rabbit holes, spends a long time on analysis
	Cyber lacks funding or resources	There is a lack funding or resources to support cyber SMEs
	Cyber lacks understanding	Cyber SMEs don't understand some aspect
	Cyber overemphasizes	Cyber SMEs focus too much on some aspect
	Cyber overestimates	Cyber SMEs miscalculate or incorrectly consider some aspect as more important, severe, or consequential than it is or should be
	Cyber sees computers	For Cyber SMEs, OT devices can be reduced to computers
	Cyber underestimates	Cyber SMEs do not sufficiently consider some aspect
	Cyber understands	Cyber SMEs are knowledgable and skilled in some aspect
	OT conflates security and safety	OT SMEs mistake safety or reliability for security of computer systems
	OT lacks funding or resources	There is a lack funding or resources to support OT SMEs
	OT lacks imagination	OT SMEs do not, cannot, or find it difficult to think of possibilities outside of what they already know
	OT lacks understanding	OT SMEs don't understand some aspect
	OT overemphasizes	OT SMEs focus too much on some aspect
	OT overestimates	OT SMEs miscalculate or incorrectly consider some aspect as more important, severe, or consequential than it is or should be
	OT takes shortcuts	OT SMEs leave access open, create backdoors, or otherwise leave open vulnerabilities for the sake of having easy access
	OT underestimates	OT SMEs do not sufficiently consider some aspect
	OT understands	OT SMEs are knowledgable and skilled in some aspect
Suggestion	Collaboration	SME suggests how or whether SMEs should or can collaborate
	Make systems usable for OT	SME suggests that security design or policies should also ensure that systems can still be accessed and used by OT
	Teach Cyber	SME suggests that Cyber should know or learn something
	Teach OT	SME suggests that OT should know or learn something

Table 8: Thematic codes developed for responses to questions about participants' perceptions of the two SME groups' strategies for vulnerability impact assessment and understanding of vulnerabilities.

Main Code	Subcode	Cybersecurity	Energy OT	Total Count
Accessibility	General	6	6	12
	Network Access	5	1	6
	Physical Access	4	2	6
Attack	General	4	5	9
Connectivity	Communication Protocol	1	1	2
	Logical Connectivity	7	10	17
	Network Architecture	2	1	3
	Network Connectivity	4	3	7
	Physical Connectivity	1	1	2
	Segmentation	1	2	3
Consequence	Cost or Financial Impact	2	3	5
	Damage to equipment	2	1	3
	Disrupt Operations	2	4	6
	Ecological impact	1	0	1
	General	7	8	15
	Human Impact	5	2	7
	Remediation	1	4	5
	Scale of Impact	6	5	11
Consult other SME	General	3	3	6
Device information	Basic Info	5	7	12
	Capabilities	3	3	6
	Functional Purpose	4	5	9
	Maintenance	0	1	1
	Physical Location	2	3	5
	Protections	5	4	9
	System Architecture	4	5	9
	Type of Facility	0	1	1
	Ubiquity/Deployment	2	2	4
	Users	1	1	2
Vendor	General	3	2	5
Vulnerability	Affected area	1	2	3
	Exploit Technical Requirements	5	3	8
	Mitigation	1	4	5
	Residual Impact	1	3	4
	Understanding of Vulnerability	7	4	11
	Vulnerability Information	6	4	10

Table 9: Strategy subcodes applied to each individual's self-reported impact assessment strategies and considerations, showing count per narrating participant based on their expert group, and also showing total count.

Main Code	Subcode	Cyber Negative	Cyber Positive	OT Negative	OT Positive
Accessibility	General	3	7	3	2
	Network Access	0	0	2	0
	Physical Access	0	0	3	1
Attack	General	2	4	2	0
Connectivity	Communication Protocol	1	1	0	0
	Logical Connectivity	4	5	4	5
	Network Architecture	0	0	1	1
	Network Connectivity	0	1	1	1
	Physical Connectivity	0	0	2	0
Consequence	Damage to Equipment	1	0	0	1
	Disrupt Operations	1	0	0	2
	General	7	6	2	12
	Human Impact	0	0	0	1
	Scale	0	2	0	2
Consult Other SME	General	0	4	0	4
Device Information	Basic Info	1	1	1	4
	Capabilities	3	11	9	0
	Functional Purpose	5	4	1	12
	Maintenance History	1	0	0	1
	Physical Location	0	0	0	1
	Protections	2	0	1	0
	System Architecture	4	1	0	7
	Ubiquity/Deployment	1	0	0	3
Vulnerability	Exploit Technical Requirements	3	1	1	0
	General	0	3	3	1
	Mitigation	1	0	0	1
	Residual Impact	0	1	0	0
	Understanding of Vulnerability	0	9	10	0
	Vulnerability Information	0	2	1	2

Table 10: Strategy subcodes applied to participants' stated perceptions of the SME groups' strategies and understanding, showing counts per SME group being characterized (target of the comment).