Functional Analysis of Cyber-Physical Systems for Confidentiality Quantum Resilience

Conference Paper · August 2024

DOI: 10.1115/DETC2024-142349

2 authors:

Douglas Lee Van Bossuyt
Naval Postgraduate School
135 PUBLICATIONS **937** CITATIONS
SEE PROFILE

Britta Hale
Naval Postgraduate School
21 PUBLICATIONS **167** CITATIONS
SEE PROFILE

Proceedings of the ASME 2024
International Design Engineering Technical Conferences & Computers and Information in Engineering Conference
IDETC/CIE2024
August 25–28, 2024, Washington, DC

IDETC2024-142349

FUNCTIONAL ANALYSIS OF CYBER-PHYSICAL SYSTEMS FOR CONFIDENTIALITY QUANTUM RESILIENCE

Douglas L. Van Bossuyt[1,*], Britta Hale[2],

[1]Naval Postgraduate School Department of Systems Engineering, Monterey, CA
[2]Naval Postgraduate School Department of Computer Science, Monterey, CA

ABSTRACT

The pending development of a cryptographically relevant quantum computer (CRQC) puts cryptographic security relying on public key cryptography at risk. Such cryptography can be found throughout systems today, including cyber-physical systems, which raises a question on when to transition security to quantum resistant alternatives, i.e., post-quantum cryptography. Criticality of transition timeline and planning can be non-trivial for system managers and the cybersecurity risk of transition delay is often opaque. This paper investigates functional system modeling techniques for planning and risk mitigation against quantum threats to confidentiality in cyber-physical systems. The research in this paper applies systems engineering and design engineering tools such as Functional Modeling in the form of Functional Failure Identification and Propagation (FFIP) and Flow State Logic (FSL) to analyze flow paths and provide quantum vulnerability metrics for cyber-physical systems. Using this insight, this work further provides guidance on how such metrics can be used to plan system transition for quantum resistance. Timeline upgrade prioritization of functions and their component solutions to prepare for the threat of a CRQC is possible with the method proposed in this paper. A simplified case study of a polar research facility is presented to demonstrate the method. This paper introduces the concept of Quantum Vulnerability Information Timeline (QVIT) in the context of system modeling and demonstrates within the case study how QVIT values can be calculated for various system components to estimate preparation timelines against quantum threats.

Keywords: Functional analysis, post-quantum, quantum computer threats, cyber-physical systems, systems engineering, design engineering

1. INTRODUCTION

The ongoing revolution in quantum computing promises to greatly increase computing power especially in ways that are relevant to decryption, encryption, and cyber-security. However, quantum computing also brings with it the threat of breaking traditional public-key cryptography that is not Post Quantum (PQ)-ready. Most currently deployed complex cyber-physical systemss (CCPSs) and many under development CCPSs could be vulnerable to an attacker equipped with a cryptographically-relevant quantum computer cryptographically-relevant quantum computer (CRQC), which could allow the adversary to access and modify information, including controls and safety overrides. Consequently, transition to appropriate PQ security solutions is a necessity. System complexity means that transition is non-trivial. Ultimately, a risk-mitigation and transition plan has the desirable benefits of protection against the worst cases as well as cost balancing for overall system maintenance.

Functional modeling enables fault tracing throughout a system. This research introduces functional modeling in the context of post-quantum security which provides insight into the effects of quantum adversarial compromise of a particular system aspect, including dependencies of that. In cyber-physical systems, functional modeling of quantum security risks can demonstrate propagation of a threat throughout the complex system. This in turn highlights points of high criticality for protection using post-quantum methods.

Impacts of a quantum threat extend to both confidentiality and authenticity [1]. A CRQC is not yet available under the current quantum computer state-of-the-art and the exact timeline of having a CRQC available is unknown. However, store-now-decrypt-later attacks [2], also known as backtracking attacks, allow adversaries to gather information now, even if encrypted, to break confidentiality at a later date once a CRQC is available. This is particularly relevant for cyber-physical systems, which frequently cannot update or replace cryptographic ciphersuites with post-quantum ones on demand; system functionality and availability; acquisition and funding timelines; and niché system needs that require specific testing pre-deployment all contribute to a longer security transition timeline than may be typical in standard networks. These pre-deployment testing and planning

*Corresponding author: douglas.vanbossuyt@nps.edu

considerations also apply to authenticity. If a CRQC becomes available within e.g., 10 years, where the system specification requirements are described now in terms of traditional cryptography, the lead time for hardware design and testing may well lead to deployment of a system that meets specifications but is almost immediately vulnerable to quantum threats.

Past work has looked at the risk of aggregate delays to acquisition of post-quantum systems and security risks from difficulties in providing software updates for post-quantum ciphersuites to some systems, given component lifespan and cost management [2]. The risk for cyber-physical systems, in particular, stems from the complexity of such systems. Unlike a smartphone application, updates to a cyber physical system must take into account an interdependent overall functionality. Furthermore, security updates may be weighed against other priorities and costs by system managers. In some cases, where cryptographic mechanisms are encoded in hardware, the security component may not be replaced or updated with one that is post-quantum until the entire system is updated or replaced, an approach that could put confidentiality and authenticity vulnerability well into a very realistic time-frame for a CRQC [2].

Consider a case of an implantable medical device on a high profile individual, X. The medical data from the device is sensitive, not only from a personal information perspective but in that any news of a medical status change for X could e.g., impact the stock value of X's company or be a national security risk if X held a senior government position. Given this, X is a target for data collection. Currently, such data is encrypted using traditional methods; however, if the security on the implanted device cannot be updated without surgery – potentially high-risk surgery – the device could be left without updates for many years. Thus, using store-now-decrypt-later attacks, an adversary that later gains access to a CRQC can publicly share information on significant past events in X's medical history, breaking the intended confidentiality. Using a CRQC, the adversary may also break the traditional authenticity algorithms, leading to an ability to inject false medical data or even manipulate the implanted medical device remotely, leading to threat to life.

The exact timeline and risk window posed by CRQC for a given system is dependent on how the system is used and its ability (and probability) to be updated later with post-quantum algorithms and protocols [2]. Further, the sensitivity and duration of sensitivity of the information aboard the system complicated the timeline. In particular, certain components, subsystems, or systems within a CCPS may each have their own timelines and risk windows. Additionally, some cyber-physical subsystems such as motor drivers and associated software can often be overlooked in analysis.

When calculating the quantum vulnerable information timeline ($QVIT$) for a system, one must first consider the type of threat model being considered. For instance, in some systems store-now-decrypt-later attacks will put confidentiality as a main consideration priority while in others authenticity and data forgery will be a focus. Some systems may consider both, or both but at different timescales. Quantum threats apply across the security spectrum. Suppose, for example that we focus on the threat of store-now-decrypt-later attacks for a case system. In the case system we have that (A) data is sensitive for 5 years and (B) it will take 2 years to test new algorithms after waiting (C) 2 years for suitable digital certificates and matching algorithms are approved. It takes (D) an additional year for planning and (E) the planning process has determined that cryptographic hardware components that hold the ciphersuites will not be replaced for 3 years due to cost of accessing the system funding balancing with other priorities. This leads to a basic $QVIT$ calculation of $A + B + C + D + E = 13$ years. Thus by extension and Mosca's equation, if a CRQC is available in 13 years or less, the confidentiality would be lost for the system. Similar calculations can be considered for authenticity or various timeline combinations of confidentiality and authenticity. For simplicity, this work focuses on modeling in $QVIT$-confidentiality issues.

This research presents a method of conducting functional analysis of CCPS for quantum resilience where functional analysis is used to identify vulnerable components, subsystems, or systems within a CCPS. The vulnerabilities are then analyzed from a function-flow perspective and using CRQC timeline and risk window information to ascertain overall system risk. This allows for a timeline to be established that systems engineers must meet in order to ensure PQ security.

2. BACKGROUND AND RELATED WORK

This section provides an overview of several topics used in the research including PQ, design engineering and systems engineering, risk and failure analysis, and functional failure identification and propagation (FFIP).

2.1 Post-Quantum

Among their many uses, cryptographic algorithms and protocols provide the foundational mechanisms for securing data in transit in modern communications. This includes information security for data passed between sensors and components as well as for control in CCPSs. Cryptography provides confidentiality, usually with keys established through public-key based cryptographic protocols, and authenticity, frequently requiring digital signatures. Furthermore, digital certificates are currently the main backbone for distribution of such public keys, regardless of their use, and rely on digital signatures themselves. In short, modern cybersecurity is highly reliant on public key cryptography. However, traditional core building blocks of public key cryptography are vulnerable to certain quantum computers (i.e., CRQCs) using optimizations on certain algorithms such as Shor's algorithm [3]. This has lead to efforts by NIST to standardize post-quantum alternatives to the vulnerable algorithms that would be resistant to such attacks [4]. Progress has been made on the algorithm standardization front, but work is still ongoing for standardizing protocols and mechanisms for combining such algorithms [4–8]. Industry are in various stages of PQ transition, with some enterprising companies already deploying PQ algorithms in their solutions, but many still waiting for standardization efforts to finalize. This leads to a natural question: how long can a system manager afford to wait to transition their system to PQ?

2.2 Design Engineering and Systems Engineering

There are many similarities and overlaps between the design engineering and systems engineering domains. Indeed, the National Science Foundation (NSF) combined the two communities into the Engineering Design and Systems Engineering program a number of years ago. Of particular interest to this research is the system design process that is defined in both communities. Salient works such as Taguchi's House of Quality [9], Ullman's Mechanical Design Process [10], and Otto and Wood [11] share much in common with the system design process outlined by the International Council on Systems Engineering (INCOSE) community and realized through the "Vee Model," agile processes, and other system design process techniques [12–15].

Typically, the development of a new system or product starts with identifying customer needs and stakeholders. Then, requirements are distilled and elaborated on in a requirements definition and breakdown process. Next, functional models (discussed in the next subsection) are often created followed by identifying component solutions to the functions. Detailed design led by discipline-specific experts (e.g.: mechanical engineering, computer science, electrical engineering, etc.) occurs next. Systems manufacturing, integration, and testing follows along with verification and validation efforts to demonstrate that the system meets requirements. The system is then deployed to the customer and the operations and maintenance phase is entered. Many CCPSs go through upgrade and life extension phases before reaching the end of life and disposal [12, 13].

A number of requirements development techniques exist in the literature. The SMART requirements criteria includes specific, measurable, quantifiable, assignable, realistic, and time-related. Systems engineers commonly use the SMART requirements criteria to develop requirements [16, 17].

2.3 Functional Modeling

Functional modeling is a technique used by design and systems engineers to represent systems at the functional level. Generally, functional models are built to satisfy requirements that were developed as part of a system design process [18]. After a functional model has been developed, a variety of analyses can be conducted such as sustainability analysis [19], functional failure identification and propagation (FFIP) (discussed further below) [20, 21], and others[22–24]. In most system design processes including both in the systems engineering and design engineering communities, a component model is derived from the functional model where different component solutions to each function are examined to determine the most advantageous solutions. Information from functional analyses are used to help drive component solution decision-making.

A variety of ontologies exist to support functional modeling. The functional basis for engineering design (FBED) is a commonly used ontology in the design engineering community and is used in this research [25]. Using an established ontology or developing an ontology for a specific system development process is useful and helps to ensure consistency across modeling efforts conducted by different people and at different times.

2.4 Risk and Failure Analysis

Many risk and failure analysis techniques are in widespread use, are seeing limited adoption, or have been described in the literature but await adoption. Within the systems engineering and design engineering communities, techniques such as failure modes and effects analysis (FMEA)/failure modes effects and criticality analysis (FMECA) [26], probabilistic risk assessment (PRA), [27] reliability block diagrams (RBD) [28], and others are commonly used. These techniques can trace their origins back to developments coming out of World War II, National Aeronautics and Space Administration (NASA), and the civilian nuclear power industry among others [28]. These techniques are appropriate for hardware-dominant systems, and are also being used with increased frequency on CCPSs although work remains to ensure that cyber and cyber-physical issues are fully analyzed.

The cybersecurity community has developed risk and failure analysis techniques. National Institute of Standards and Technology (NIST) recently released the Cyber Security 2.0 framework specifically to aid practitioners in dealing with cyber security threats [29]. More general guidance can be found in the NIST Risk Management Framework (RMF) citenistrisk. The NIST RMF describes guidance on preparation, categorization, selection, implementation, assessment, authorization, and monitoring. Both it and the Cyber Security 2.0 Framework focus on general system security (e.g., traditional confidentiality, access control, software life-cycles, etc.) rather than specific threats. Thus, frameworks such as the NIST RMF are frequently coupled with more specific cyber threat information for planning an system analysis, such as from the Common Vulnerabilities and Exploit (CVE) list [30], a daily point of reference for many organizations. In terms of quantum threats and cybersecurity risk management for them, there has been no guidance to date on aligning specific quantum concerns to risk management and planning frameworks.

2.5 Functional Failure Identification and Propagation

Within functional analysis, FFIP is of particular interest to this research and is described here. FFIP is a method of tracing how failures can propagate through a system at the functional level [20, 21]. It is similar in some respects to RBD although the failure can be explicitly transformed as it passes through a function. FFIP relies on the function-flow pairing found in FBED and other functional ontologies. Failures can be introduced into a system as either a failure flow or a functional failure. Then failures can move through a system at the functional level following flow paths or jumping between functions that are not normally directly connected via flow paths. This is analyzed using flow state logic (FSL) [31]. The FFIP research community has developed many augmentations to FFIP including and this list continues to expand [32–37].

Typically, FFIP is conducted by first developing a functional model of the system, then identifying potential failures (often called initiating events in some communities). Next, FSL can be used to analyze the potential flow paths through the functional model of the system that a failure might traverse. It is common to analyze the probability of a particular failure flow path occurring similar to how cut sets are analyzed in PRA.

3. METHODOLOGY

This section presents a proposed method to conduct functional analysis of CCPSs for quantum resilience on confidentiality. This method can be used either during conceptual system design or with an existing fielded system.

3.1 Step 1: Develop Functional Models of System

First, the system being analyzed must have a functional model. If no functional model currently exists, one must be developed. Often times, a functional model was developed during conceptual system design. If the analysis is being conducted on an under-development system, the functional model that was developed as part of the conceptual system design process can be used. Otherwise, if an existing fielded system is being analyzed, either a functional model will need to be developed if one does not already exist, or any existing functional models should be reviewed for accuracy. It is the authors' observation from professional practice that sometimes in system design, functional models are not kept up to date after the conceptual system design phase so it is important to verify that the functional model is accurate.

Regardless of the origin of the functional model of the system, it is of particular importance to this method that all cyber and cyber-physical functions and flows be represented. While in the authors professional experience, these representations are becoming more common in functional models, there are still many functional models for under development or operational systems that the authors have observed either not containing any cyber or cyber-physical functions or flows, or an incomplete set.

It should be noted that functional flow block diagrams or enhanced functional flow block diagrams are typically used in FFIP-related analysis methods. In this work, the authors recommend using either of these types of functional models or similar functional modeling techniques. Other types of functional models such as a functional decomposition diagram are not appropriate for this analysis.

3.2 Step 2: Develop Function Failure Identification and Propagation Models

Next, the FFIP models and analysis must be developed based on the system models from Step 1. This typically involves identifying both internal and external initiating events, analyzing the FSL, and developing cut sets of the failure scenarios that result. For quantum cyber threats against confidentiality, in practical terms such a failure event corresponds to a CRQC attack on public key encryption or key encapsulation mechanisms.

3.3 Step 3: Identify Cyber Functions

All cyber and cyber-physical functions in the functional model must now be identified explicitly. While this was already implicitly done in Step 1, this step and the subsequent sub-steps require explicit identification. Furthermore, such explicit identification should include the types of data confidentiality mechanisms currently employed. Here *type* refers to not simply the encryption ciphersuite, but is also taken to include protocols involved in key establishment that are relevant to data confidentiality.

3.3.1 Step 3.1: Determine Post-Quantum Transition Timeline of Each Function. Each cyber and cyber-physical function must now have the PQ transition timeline calculated, relevant for that component. For the purpose of this model, the timeline focuses on confidentiality-supporting components. This includes the function's lifespan based on the update frequency of cryptographic algorithms inside each cyber and cyber-physical function (T). This potentially includes the acquisition process timeline for them and the integration time, if updates to the function imply component replacement. This may especially be the case if such algorithms are programmed in hardware. Additionally, an estimate should be made of the data sensitivity lifespan based both on data protected by such functions (D). The sensitivity of the data is calculated as $QVIT = T + D$. This represents the available PQ transition timeline. Based on Mosca's equation, the confidentiality of such data is at risk if $T + D > Q$, where Q is the estimated number of years before a CRQC is available. Some sources suggest that a realistic number for Q may be as little as $Q = 10$ years [38]. Thus, the larger the combined total $QVIT$ is from the above function lifespan calculations, the more at risk the data that depends on those function is.

3.3.2 Step 3.2: Develop Functional Model of Data Flow and Cyber Connections. Now, FSL must be developed for the cyber and cyber-physical functions. This requires that initiating events also be developed. In this case, the primary initiating event of interest is the development of a CRQC which then can compromise non-PQ-ready functions. This event has timeline Q as noted above.

3.3.3 Step 3.3: Connect Data Post-Quantum Transition Timelines to Functional Data Flow Model. The PQ transition timelines $QVIT$ developed for each cyber and cyber-physical function in Step 3.1 are now layered onto the FSL developed in Step 3.2. This information is embedded within each function.

3.4 Step 4: Failure Events

In this step, analysis is conducted where the CRQC initiating event is introduced to the cyber and cyber-physical functions and flows. The authors suggest that each function and flow be analyzed independently initially with the assumption that the CRQC initiating event can be injected anywhere with a cyber or cyber-physical function in the system regardless of nominal flows that cross the system boundary. This is in line with previous work on initiating events that can enter a system along non-nominal flow paths [2]. Then, failure flow propagation caused by the CRQC through the system should be analyzed.

It is useful to note that a failure flow does not necessarily have to exit the system boundary for a PQ system failure to have occurred. FFIP and FSL do not account for cyber security compromise particularly well from the perspective of what can be done with knowledge of encrypted data that has been compromised by a CRQC. Future work, discussed in a later section, may improve the situation. Until then, failure of a function due to the PQ transition timeline being insufficient to stop the CRQC initiating event is sufficient to indicate a function has failed, and potentially the system has failed from a confidentiality perspective.

Also of note is that a CRQC initiating event may pass through many functions via cyber flows until it encounters a function that does not have a sufficient PQ transition timeline (i.e., a CRQC can be used to attack any data link connection among the system communications). Thus, in modeling, an incipient failure may travel through the system at the functional level until it encounters a function that fails.

3.5 Step 5: Quantum Vulnerability Information Timeline Analysis

Cut sets of each failed function and component are next developed based on the failure flows produced in the prior step. This includes both purely cyber failure flows that lead to failure of a specific function within the system or that lead to a cyber failure flow exiting the system, as well as hardware or cyber-physical functional failures or failure flows that exit the system. The previously conducted FFIP can now be used to connect specific non-CRQC initiated failures that were already analyzed with failures caused by CRQC initiating events.

In a departure from FFIP and FLS, instead of developing failure probabilities, PQ practical transition timelines are used. PQ practical transition time can be considered as equivalent to the quantum vulnerable information timeline, i.e., $QVIT$. Therefore, the values $QVIT = T + D$ for each cut set are developed. The $QVIT$ must be less than Q (i.e., the estimated availability timeline of a CRQC) in order to protect against store-now-decrypt-later attacks. The authors advocate that the largest be identified and used as the $QVIT$ for the entire cut set. However, in the event that is possible to analyze how cyber failure flows can be transformed while moving between functions, more advanced analysis of cut set $QVIT$ may be possible. For instance, a CRQC-induced failure flow may be changed as it moves through functions to cause the $QVIT$ for specific functions to be shortened or increased. Such an extension of the method presented here may however be overly challenging to adequately implement and very specific to certain threat model cases. With the uncertainty in the timeline for CRQCs becoming available, this more advanced analysis is likely not warranted or useful. Instead, the authors advocate that the $QVIT$ with the most amount of time be used as a comparison point against possible values for Q (an estimate of the timeline until the CRQC is available). If $QVIT > Q$ then the system is considered vulnerable to store-now-decrypt-later attacks.

3.6 Step 6: Post Quantum Confidentiality Prioritization

Finally, the individual cut sets can be prioritized, with the cut sets that produce the longest duration ($QVIT$) that are most vulnerable to store-now-decrypt-later attacks being prioritized to be addressed first by engineers. Such expedited transition can reduce the value of T and therefore $QVIT$. Furthermore, prioritization can ensure that $QVIT$ is equal across functions, resulting in a common vulnerability timeline view of the system.[1]

[1]It should be noted that data with different levels of criticality may flow through different functions, and therefore in practice the model may be more complex in the mitigation step.

4. CASE STUDY

A case study is now presented to illustrate how the proposed method works. It should be noted that the case study is intentionally fictionalized to avoid any sensitive or proprietary data, or any sensitive geopolitical situations. However, the case study is based upon potential near-term and future international disputes or conflicts.

The system of interest is a remote polar facility that contains a power plant (both generating electricity and hot water for building heating), crew quarters, a communications facility (both secure and commercial communications located in adjoining buildings), scientific research labs, an air terminal (runway, hangar, control tower, radar, navigation beacons, and related support equipment), emergency services (fire, ambulance, hospital, police), a deep water port facility (pier, tugboat, cargo handling equipment, fuel handling equipment), a fuel farm, several nearby field camps and scientific instruments (radars, seismographs, etc.), and surveillance equipment for regional situational awareness. The polar facility is optionally crewed and can be left unattended and in an operational state over the winter months if funding is unavailable to keep the facility staffed with an overwinter crew. Additionally, due to the increasingly erratic regional climate induced by climate change, it is becoming less desirable to keep a crew at the facility through the winter months where storms are becoming potentially life-threatening if critical facility functions fail. However, the polar facility must remain habitable on a moment's notice in case the security situation in the region rapidly changes even during winter months [39–43].

The region where the polar facility is located is sovereign territory of a nation state that wishes to protect the area from development and pollution, prevent claims by other nations on the territory, and prevent non-nation-state actors from establishing clandestine resource extraction facilities (e.g., mines, whaling stations, fishing within territorial waters, etc.) [44–47]. Note that while some polar regions do have indigenous inhabitants that must be included in the discussion of matters of regional importance, and many nations are now making efforts towards ensuring that indigenous citizen rights are enforced, this is specifically excluded from this case study to simplify the analysis and avoid any potential politically sensitive issues such as the status of people living in Antarctica.

A physical component model of the polar facility is provided in Figure 1. Note that this has been greatly simplified compared to polar facilities such as McMurdo Station (Antarctica), Ny-Ålesund Research Station (Svalbard, Norway), Halley Research Station (Antarctica), or Eureka Research Station (Nunavut, Canada) for clarity in the case study. Any resemblance to polar defense facilities is unintentional, and has been intentionally avoided.

The polar facility was constructed without a functional model being developed and much of the facility pre-dates the last 30+ years of functional modeling development. While the original construction of the polar facility did not conceptualize the facility as a system, the modern understanding of a system includes such facilities. Some may argue that the polar facility is a system of systems, but for the purposes of this case study, it is treated as a single system.

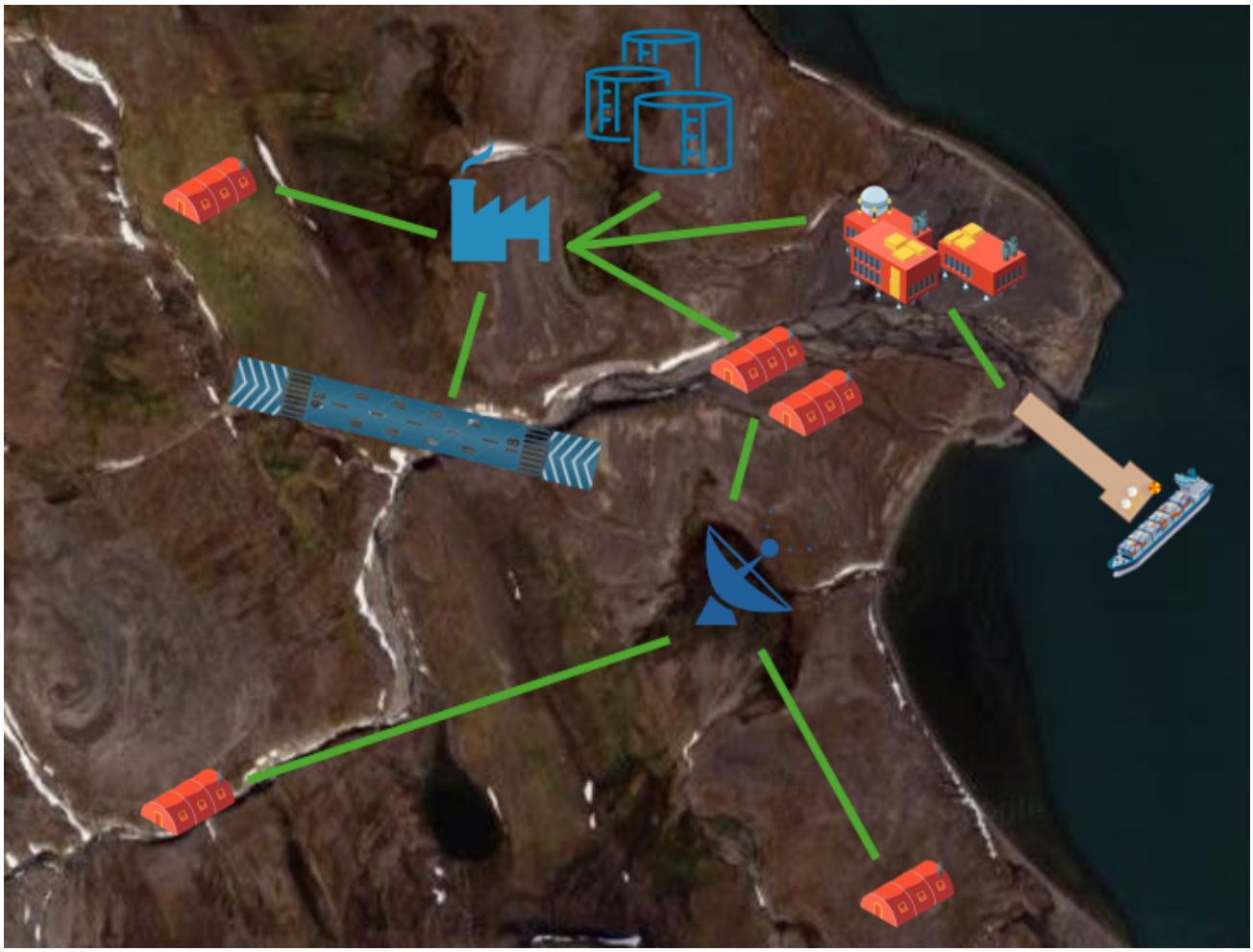

FIGURE 1: A physical component model in the form of a map of the polar facility system of interest. Port facilities (on the right side of the image in the center), crew quarters (the cluster of buildings by the port), a communications facility (indicated by a satellite dish icon), scientific labs (represented by the two Quonset hut structure icons near the crew quarters), a fuel farm (the icons of fuel tanks in the upper center of the image), an airport (represented by the runway in the center of the image), a power plant (represented by the power plant icon next to the fuel tanks), and several remote facilities (represented by individual Quonset hut icons away from the main facilities) are included. The green lines indicate facilities connections including power and communications.

4.1 Step 1: Develop Functional Models of System

Figure 2 shows a simplified top level functional model of the polar facility. The flows between the major functions include energy flows (electricity), material flows (hot water, humans, equipment, food, etc.), and information flows (data). Figure 3 shows the functional decomposition of the "convert chemical energy to electrical energy" function (the power plant). This shows how cyber and cyber-physical functions can be embedded in all of the top level functions. Of particular importance is the control function which represents the supervisory control and data acquisition (SCADA) system that digitally controls the plant and connects with other digital communications systems throughout the polar facility [48, 49]. The control function representing the SCADA system is a cyber-physical function. Not shown are the many functions that support the control function (SCADA system) connected to each of the other major functions within the power plant. In a typical polar research station power plant, many hundreds of instrumentation and control sensors and actuators are digitally connected to the SCADA system, and most are cyber-physical in nature.

Detailed functional models for each of the top level polar research facility functional model functions are created but not shown here for brevity. Each top level function has a similar mix of cyber, cyber-physical, and physical functions as shown in the power plant (Figure 3). It should be noted that the authors take no stance on the level of decomposition that the functional models should achieve. The literature has a long-running debate over the appropriate level of decomposition [13], and this research does not attempt to answer this question.

4.2 Step 2: Develop Function Failure Identification and Propagation Models

An FFIP model is now developed. The FFIP model for the power plant subsystem (the convert chemical energy to electrical energy top level function) is shown in Figure 4 with one external initiating event shown and the failure flow paths indicated by

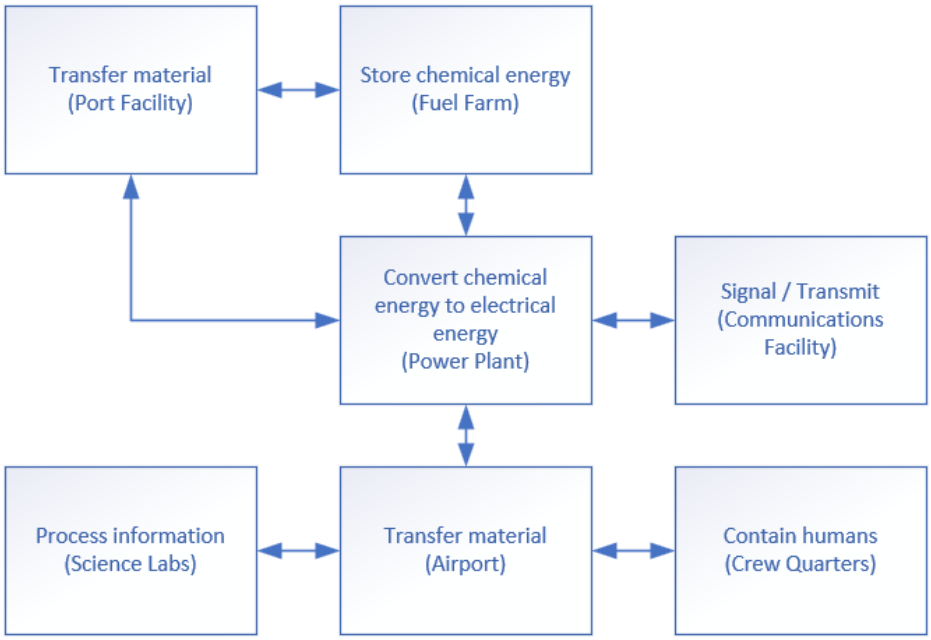

FIGURE 2: Simplified top level functional model of a polar facility.

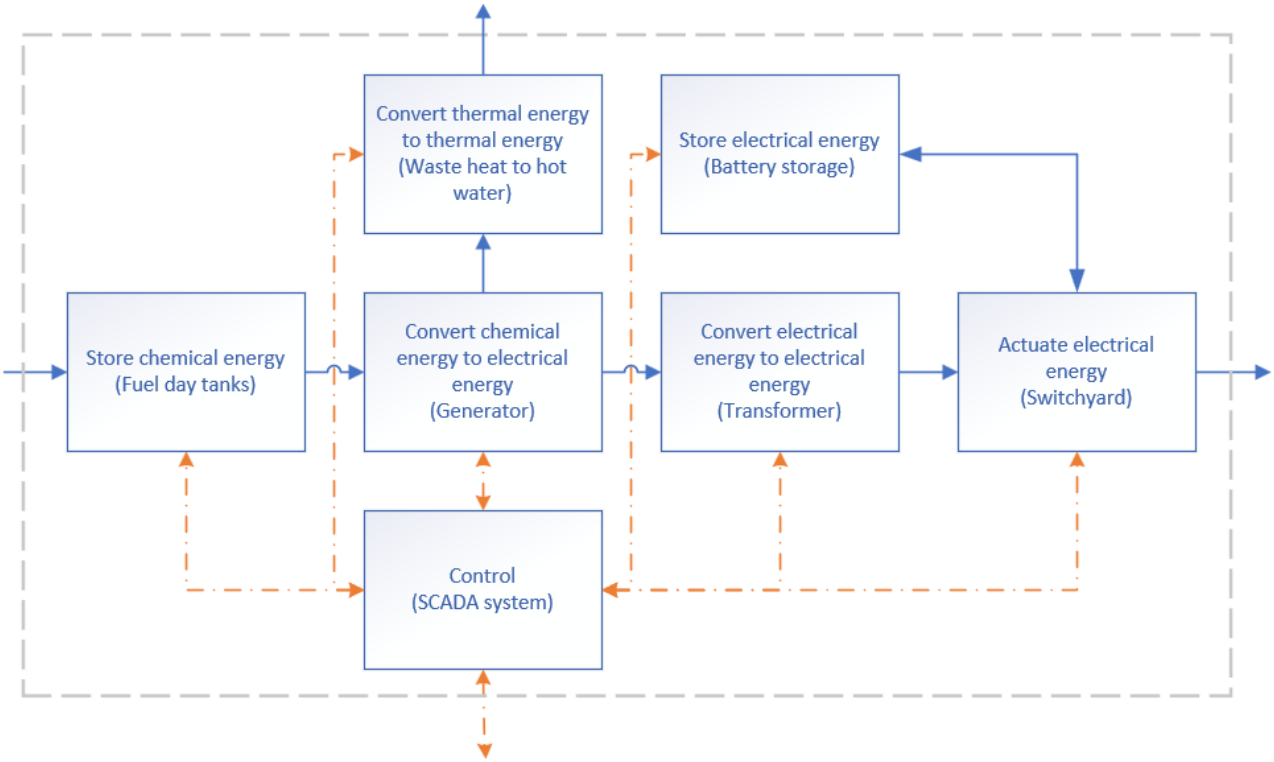

FIGURE 3: Simplified power plant functional model. The gray dashed line indicates the system boundary for the power plant subsystem in the larger polar facility system. The blue solid arrows represent flows such as chemical (oil), liquid (hot water), electrical current (electricity), and related flows move through the power plant. The dashed orange lines indicate signal flow (digital information) through the system. The control function represents the SCADA system that digitally controls the power plant.

red dashed lines. The graphical representation in Figure 4 is replicated for each initiating event (both external and internal) for each top level function in the top level functional model of the polar facility (Figure 2) but is omitted here for brevity. As an example of various initiating events and their failure flow paths, the following cut set represents the failure flow shown in Figure 4: Initiating event: loss of chemical energy flow Cut set: store chemical energy – convert chemical energy to electrical energy – convert thermal energy to thermal energy. In this case, the initiating event is a loss of chemical energy flow coming into the subsystem boundary which physically is the loss of petroleum fuel flowing from the fuel farm. The failure flow propagates through the subsystem and causes a failure flow export of the lost of thermal heat which represents the loss of the hot water loop that keeps the buildings at the polar research facility heated. However, the flow export of electrical energy remains intact because the function of store electrical energy, representing a large battery bank, continues to supply electrical energy for a period of time. In reality, this would give the personnel at the plant time (probably several hours) to fix the fuel flow from the tank farm before pipes in buildings freeze and the stored electrical energy in the battery bank is depleted. Generally, polar research facilities have "lifeboats" or "refugea" where personnel congregate in buildings that have backup electrical power and heating equipment while the facilities services and infrastructure personnel work to restore critical facility services. In the event that these services cannot be restored with equipment and personnel on hand, the facility must be evacuated if what is missing cannot be brought in from elsewhere quickly enough.

4.3 Step 3: Identify Cyber Functions

The identification of cyber and cyber-physical functions is now performed. In the case study, it is relatively straight forward to identify these functions at the top level functional model and on the power plant functional model. All functions at these levels have some cyber element. However, the underlying cyber and cyber-physical functions are currently obscured without deeper functional analysis. But the signal flows are indicative of cyber and cyber-physical functions at the next layer of functional decomposition.

Figure 5 decomposes the convert chemical energy to electrical energy function (the generator) in the power plant functional model to show the underlying cyber and cyber-physical functions. Note that this is a greatly simplified functional decomposition of the function that represents a generator and is only meant to illustrate that there are many cyber and cyber-physical functions contained in almost every top and second-level function in the polar research facility functional model.

From a practical adversarial point of view, proximity for data gathering to conduct a CRQC-based attack can be achieved through temporary physical access or dropping a relevant device (such as through unmanned system delivery) in close proximity to the flow points. Such a device can gather data at the polar facility and transmit via satellite link back to the attacker for application of a CRQC. The exact ex-filtration method does not need to be known *a priori* in the model; it is worth noting, however, that there are various methods applicable within the case study that make it feasible.

4.3.1 Step 3.1: Determine Post-Quantum Transition Timeline of Each Function. The PQ practical transition timeline for each cyber-physical and cyber function is now calculated. Table 1 shows some of the estimated calculations and results for several of the cyber-physical functions shown in Figure 5.

4.3.2 Step 3.2: Develop Functional Model of Data Flow and Cyber Connections. FSL is now developed for the cyber and cyber-physical functions within the functional models. Figure 6 shows this performed on the convert chemical energy to electrical energy functional decomposition (the generator). The initiating event is the development of CRQC which then can compromise non-PQ-ready functions. Several initiating events are shown on the same graphic and represent confidentiality breaks where data in these cyber-physical functions is compromised and read by an adversary. This information can be used to plan and initiate a variety of other initiating events (attacks) both physically and in the cyber domain. In this case, electrical generation information likely corresponds to electrical demand information which can reveal what activities the polar research station is conducting.

4.3.3 Step 3.3: Connect Data Post-Quantum Transition Timelines to Functional Data Flow Model. The PQ practical transition timelines developed for each cyber and cyber-physical function in Step 3.1 now is integrated into the FSL developed in Step 3.2. This is done by connecting the data collected in Table 1 with the FSL shown in Figure 6.

4.4 Step 4: Failure Events

Figure 7 shows how a CRQC initiating event (red X) can compound with a physical initiating event (yellow lightning bolt) and associated failure flows (cyber failure flow represented by dashed red line, physical failure flow represented by bold yellow line) can cause a failure in a critical function. In this case, a CRQC initiating event in the convert chemical energy to electrical energy (power plant) provides a confidentiality break which allows an attacker to know what functions are operational at the polar research facility based on power usage. This allows the attacker to target the signal/transmit function (communications facility) with an initiating event of a physical attack against functions inside the signal/transmit function when it is powered down for a maintenance event that then propagates through a physical failure flow to the process information function (science labs) to cause a failure there (blue star). This failure could be on e.g., a radar system used to detect intrusion by an illegal fishing fleet into a marine sanctuary. Failure results to the system's inability to get information out to maritime patrol forces nearby to intercept the fishing fleet before it does significant environmental damage. This is a hybrid attack where a cyber initiating event from the CRQC and a physical attack from an adversary combine to cause the failure.

4.5 Step 5: Quantum Vulnerability Information Timeline Analysis

The QVIT values from Table 1 are now connected to the failure analysis from Figure 7 to develop cut sets with QVIT data.

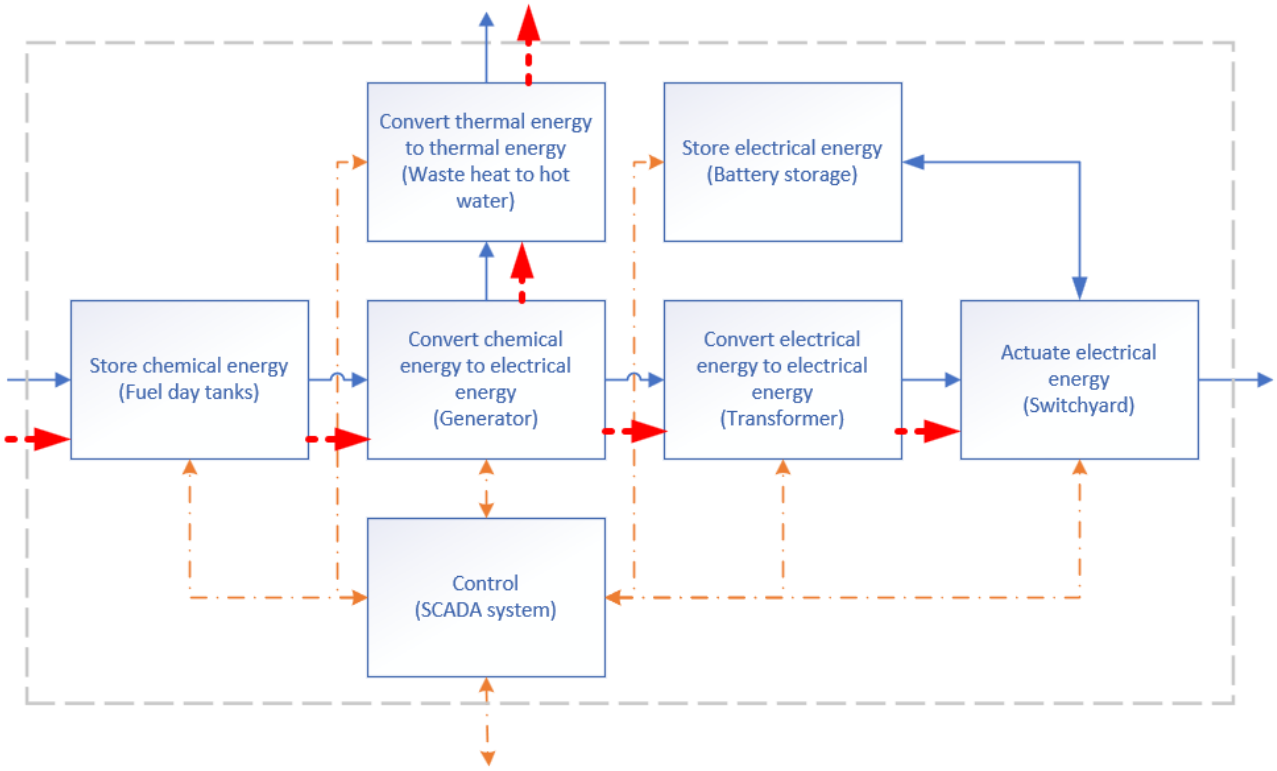

FIGURE 4: Example FFIP of the power plant (convert chemical energy to electrical energy top level function). The external initiating event is a loss of chemical energy flow which represents losing petroleum fuel input to the power plant from the fuel farm tanks. This failure propagates through the subsystem and causes the thermal heat (hot water to heat the buildings) flow export to fail. The polar research facility maintains electrical supply (the electrical energy flow export) because the store electrical energy function (representing a battery bank) continues to supply electrical energy for a period of time after the initiating event.

The cut set and the related $QVIT$ is shown below.

Note that the shortest $QVIT$ is chosen from all of the cyber and cyber-physical functions in cases where one CRQC initiating event causes a cyber failure flow that passes through multiple cyber or cyber-physical functions that causes them to fail *and* the entire chain of functions must fail to cause a system failure. This is because the shortest $QVIT$ can "break" the chain of events in the cut set and stop the system failure. Under confidentiality, this corresponds to when an attacker must be able to gather data from all components before having actionable intelligence to finish their attack.

When multiple different CRQC initiating events can cause multiple different cyber or cyber-physical functions to fail and cause the same failure outcome, the longest $QVIT$ is used because the initiating event is still possible until all functions have PQ transitioned. If any given single function failure could result in the failure outcome, the longer of its $QVIT$ and any other combination case can be used. The longest $QVIT$ may also be used as a conservative estimate for the system.

The cut set of interest is as follows and represents a hybrid attack with both a cyber initiating event and a physical initiating event: CRQC initiating event - convert chemical energy to electrical energy - signal/transmit - physical attack initiating event on signal / transmit - convert chemical energy to electrical energy - transfer material - process information. Note that the failure flow from the signal/transmit function passes through the convert chemical energy to electrical energy and transfer material functions without causing failures in those functions before reaching the process information function where the failure is realized. In this case, there are four identified CRQC initiating events possible in the convert chemical energy to electrical energy function. The longest QVIT is 29 years, and thus is used.

4.6 Step 6: Post Quantum Confidentiality Prioritization

Now, prioritization of the confidentiality cut sets created above can be conducted. The cut sets with the longest QVIT have the highest priority. While the case study here has not shown the development of additional cut sets, if additional cut sets were developed, they would be prioritized as such.

5. DISCUSSION

The above modeling provides a basis for overall system status and transition time sensitivity. It does not provide in-depth cryptographic analysis or contain the detail for relative algorithm and protocol strength comparisons and considerations throughout a system that a cryptographic analysis offers [50–55]. However, the system model is intended for a less detailed and specific view that gives more general insight into the overall system and helps system managers estimate their system lifetime against a quantum threat.

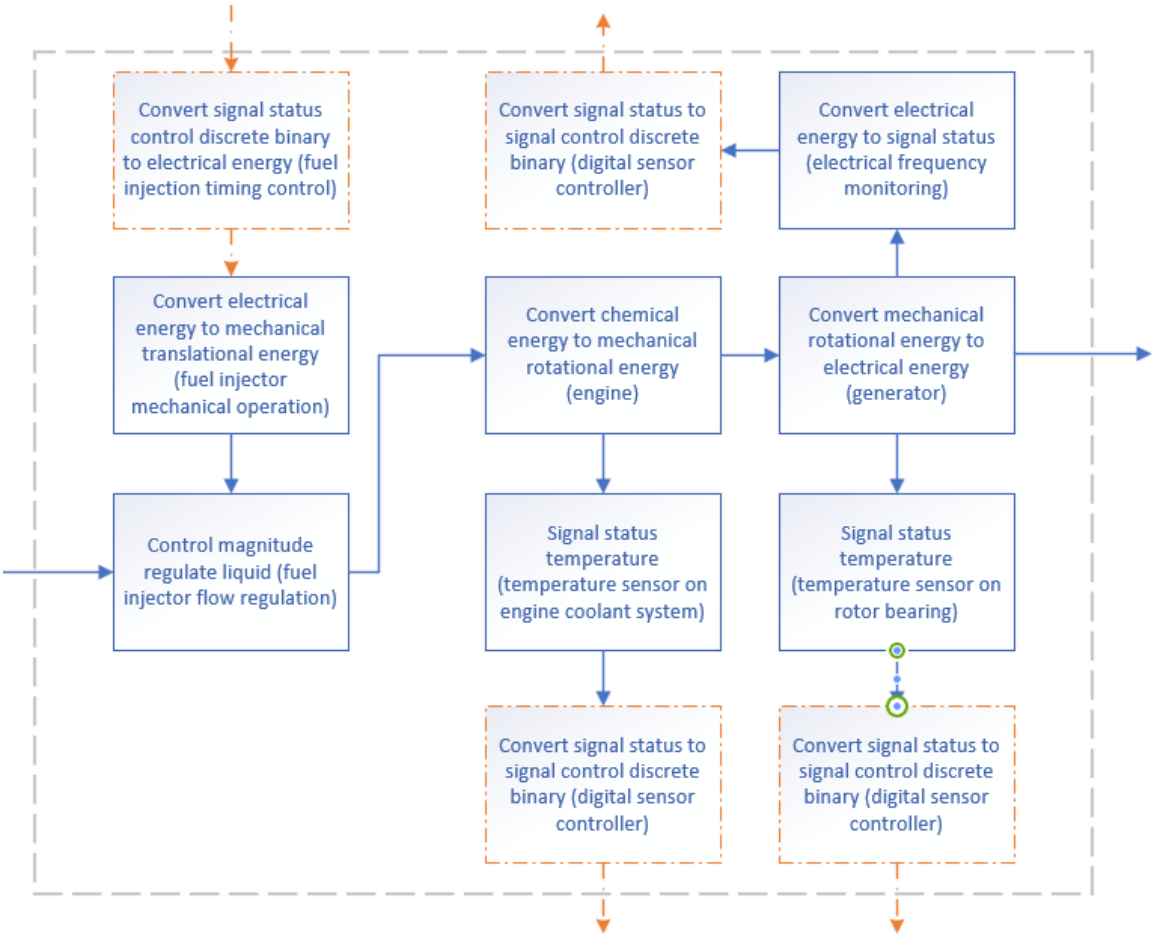

FIGURE 5: Functional decomposition of convert chemical energy to electrical energy function function representing a generator. The solid blue lines indicate nominal flow paths of liquid chemical energy (fuel), mechanical rotational energy, and electrical energy. The dashed orange lines indicate signal (data) flow. The orange dashed boxes indicate cyber-physical functions. Further decomposition of cyber-physical functions would uncover cyber sub-functions and additional cyber-physical functions.

Estimating input values can be difficult in some cases. For instance, if a software update with relevant cryptographic components can be rolled out in a matter of months, it is possible that $T = 0.25$ years. This estimate can be deceptive, however, as that software update roll out time does not account for testing time and algorithm/protocol standardization and approval time. Furthermore, if algorithms are programmed in hardware, an "update" can require replacement of the hardware component, and physical access time, as well as purchasing and acquisition time, should be added to the estimate for T.

Costs of maintenance can be a practical factor for system managers. Consequently, even if it is physically possible to update a system on a shorter timeline, T may have to also account for budget delays for such updates. The final value of T is the sum of all delays and time considerations.

The value of D may also vary notably across system components and is of particular interest in cyber-physical systems. Namely, some types of sensor data may appear innocuous at first evaluation, with a data sensitivity lifetime of only minutes. However, as in the case study above, such data can be aggregated to give an attacker an internal view of system behavior and settings that can later be exploited for either cyber or physical attacks. Thus, careful consideration of all possible ways system data could be abused is necessary in estimating D. It is advised that such estimations are done in collaboration between system managers and engineers, where questions can be asked about how data could potentially be abused by an attacker and estimates for D adjusted accordingly.

In practical terms, estimating the CRQC development timeline Q can be difficult and estimates vary considerably. A conservative estimate is recommended from a risk management perspective. Even for a rough approximations of Q, any $QVIT$ that is larger than Q should immediately flag a closer review, as this indicates quantum vulnerable confidential information.

While the functional modeling approach for analyzing confidentiality quantum resilience of cyber-physical systems was presented here using FFIP and FSL, the broad brushstrokes of this method may also be applied to physical component architectures. The authors advocate for functional analysis instead of component analysis because abstracting to the functional level can allow for earlier identification of CCPS vulnerabilities in CRQCs during system design. For existing systems, it may be more advantageous

Function	T	D	$QVIT = T + D$
Convert Signal Status Control Discrete Binary to Electrical Energy	4 yr	25 yr	29 yr
Convert Signal Status to Signal Control Discrete Binary #1	5 yr	8 yr	13 yr
Convert Signal Status to Signal Control Discrete Binary #2	5 yr	10 yr	15 yr
Convert Signal Status to Signal Control Discrete Binary #3	4 yr	10 yr	14 yr

TABLE 1: The Quantum Vulnerability Information Timeline $QVIT$ (also equal to the PQ Transition Timeline) Calculations for the Convert Chemical Energy to Electrical Energy function (generator). In the heading, T: Device update timeline, D: Data sensitivity lifespan, $QVIT$: PQ Transition Practical Transition Timeline. Note that there are three separate Convert Signal Status to Signal Control Discrete Binary functions that represent the three digital sensor controllers because each function is physically realized by a different brand of digital sensor controller with its own different PQ transition timeline.

to instead do this analysis at the component level.

This method requires knowledge of both PQ security and cryptography, and systems engineering methods such as FFIP. It is likely that at least initially an expert in PQ security and cryptography and an expert in systems engineering will need to perform this method together. Indeed, the authors of this paper fit this profile and have found the collaboration to be useful in identifying potential risks posed by CRQCs in CCPSs.

Due to the nature of functional modeling, the QVIT results may not be replicable between different people executing the method proposed in this paper. In the authors' professional experience and observations, functional modeling, like much of conceptual system design, is more of an art form than a science. The authors have observed many different functional models be developed to satisfy the same requirements by different engineers or even the same engineer. This diversity is often desired during initial functional model development because it allows for design space exploration. Similarly, this diversity has been used to develop plans for system upgrades when faced with new threats to existing deployed systems [35]. Thus, QVIT may be used as another figure of merit when conducting design space exploration on cyber-physical systems when analyzing CRQC vulnerabilities.

In the event that emergent, unexpected, cascading failures, or other highly complex failures that may never have been documented before occur, the basic QVIT analysis method discussed in this paper may not fully capture such failures. However, a significant body of work exists that extends FFIP to analyze many different such failure behaviors. A summary of many of the methods that extend FFIP address emergent and other behaviors is currently in press [56].

It can be challenging to estimate D because different industries and different types of data can have vastly different D. For instance, some types of defense industry data may remain sensitive for many decades while some types of data used in the agricultural sector may not be relevant after one growing season. Because of the highly industry-specific and data type-specific nature of D, no recommendation is provided by the authors on how to estimate D.

5.1 Future Work

This work initiates system engineering modeling for transition to quantum resistance. Future work can expand both on detail of the modeling for specific components as well as scope for more complex systems. For instance, data generated at or flowing through particular functions may fall under different criticality measures, and finer-grained modeling that accounts for such criticality can highlight further prioritization considerations for transition of various system components. Similarly, future work should look into more complex systems, such as systems of systems, and how CRQC-initiated failure propagate and effect the system of systems.

Additionally, future work should expand on the range of quantum effected cybersecurity aspects. This work focused on confidentiality, but a CRQC does not only put public-key based cryptographic confidentiality at risk but also public-key based authenticity. Effects on authenticity and propagation of failures through systems using digital certificates and digital signatures can be explored through similar modeling techniques.

In this paper, the level of criticality of specific failure flows was ignored. However, in practice the level of criticality may vary between different flows and as flows move through different functions. The method presented above should be expanded in the future to account for the level of criticality.

While the method calculated QVIT for a system, the method could be modified to calculate a vulnerability timeline for any number of cyber-security issues. Similarly, the method could be modified to more broadly support analysis of any timeline-related failures such as corrosion or metal fatigue. Future work should investigate how the method can be modified to serve many different timeline-related analysis needs within the FFIP analysis framework.

6. CONCLUSION

As practitioners plan and prepare for quantum threats to cybersecurity, the entire system, including dependencies, must be accounted for. Functional modeling and analysis offers techniques for tracing vulnerability effects throughout a complex system or system of systems. Cryptographic design and analysis has paved the way, providing replacements for traditional algorithms and protocols, but integration and understanding system effects from utilizing those options – or delaying such integration – is up to the system designers, engineers, and managers. This work provides a first look into system modeling for understanding such integration.

REFERENCES

[1] Bernstein, Daniel J., Buchmann, Johannes and Dahmen, Erik. *Post Quantum Cryptography*, 1st ed. Springer Publishing Company, Incorporated (2008).

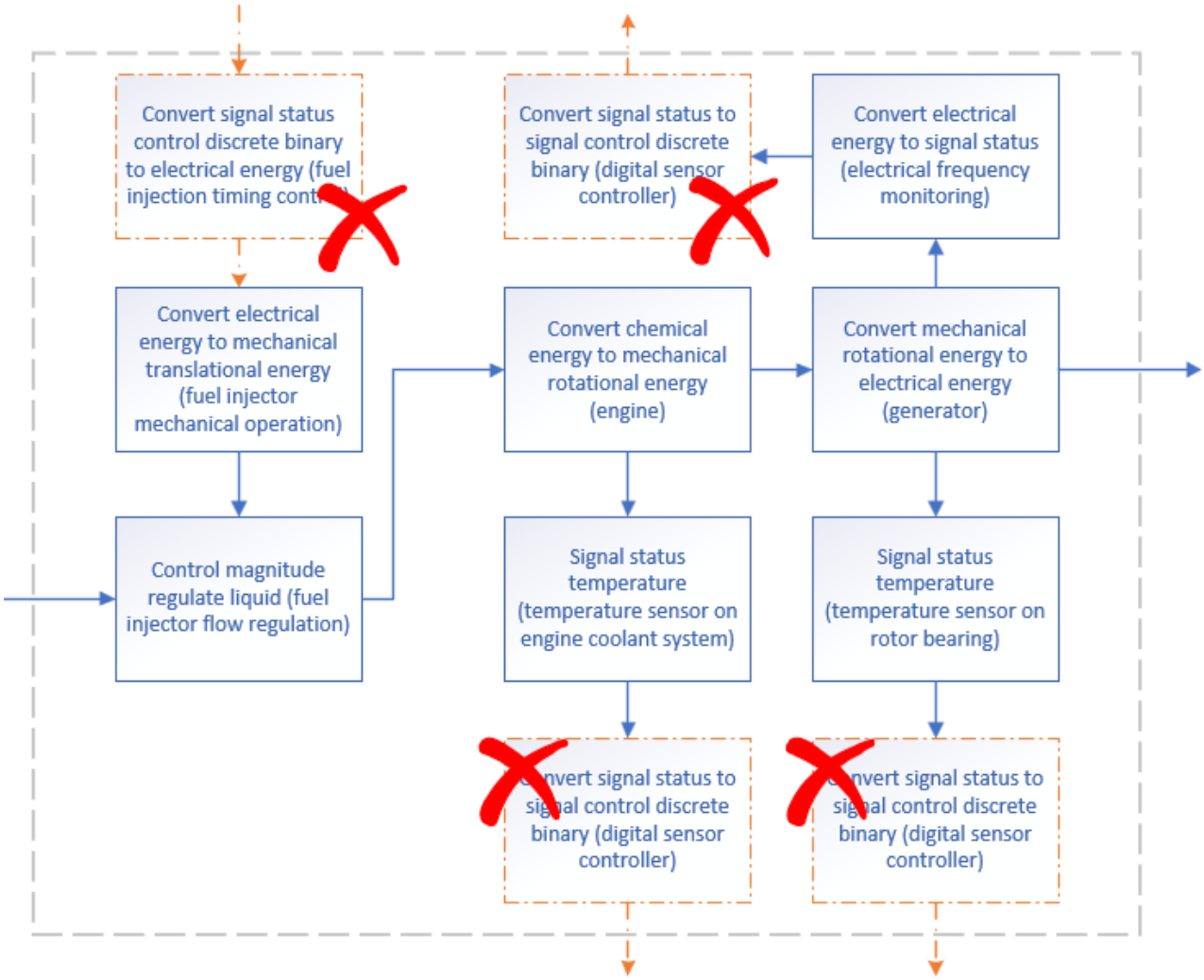

FIGURE 6: FSL for for cyber connections of the convert chemical energy to electrical energy functional decomposition (the generator). Initiating events are indicated with a red X. Compromised data (a confidentiality break) in this function can give an adversary knowledge of electrical output and demand, which can indicate activities that the polar research facility is carrying out. This can then allow and adversary to plan further physical actions.

[2] Hale, Britta and Bindel, Nina and Van Bossuyt, Douglas. *Quantum Computers: The Need for a New Cryptographic Strategy* (2023): pp. 125–158. DOI 10.1007/978-3-031-39542-0_7.

[3] Shor, Peter W. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer." *SIAM Journal on Computing* Vol. 26 No. 5 (1997): p. 1484–1509. DOI 10.1137/s0097539795293172. URL http://dx.doi.org/10.1137/S0097539795293172.

[4] "Post-Quantum Cryptography (PQC): Overview." National Institute of Standards and Technology (NIST) (2024). URL https://csrc.nist.gov/projects/post-quantum-cryptography.

[5] Bindel, Nina and Hale, Britta and Deirdre Connelly, Florence D. "Hybrid signature spectrums: draft-hale-pquip-hybrid-signature-spectrums-03." International Engineering Task Force (IETF) (2023). URL https://datatracker.ietf.org/doc/draft-hale-pquip-hybrid-signature-spectrums/.

[6] Nina Bindel and Britta Hale. "A Note on Hybrid Signature Schemes." Cryptology ePrint Archive, Paper 2023/423 (2023). URL https://eprint.iacr.org/2023/423. https://eprint.iacr.org/2023/423.

[7] "Post-Quantum Use In Protocols (pquip)." International Engineering Task Force (IETF). URL https://datatracker.ietf.org/wg/pquip/about/.

[8] Stebila, D. and Fluhrer, S. and Gueron, S. and Haifa, U. "Hybrid key exchange in TLS 1.3: draft-ietf-tls-hybrid-design-09." International Engineering Task Force (IETF) (2023). URL https://datatracker.ietf.org/doc/html/draft-ietf-tls-hybrid-design.

[9] Roy, Ranjit K. *A primer on the Taguchi method*. Society of manufacturing engineers (2010).

[10] Ullman, David G. *The mechanical design process*. Vol. 6. BVT Publishing New York (2017).

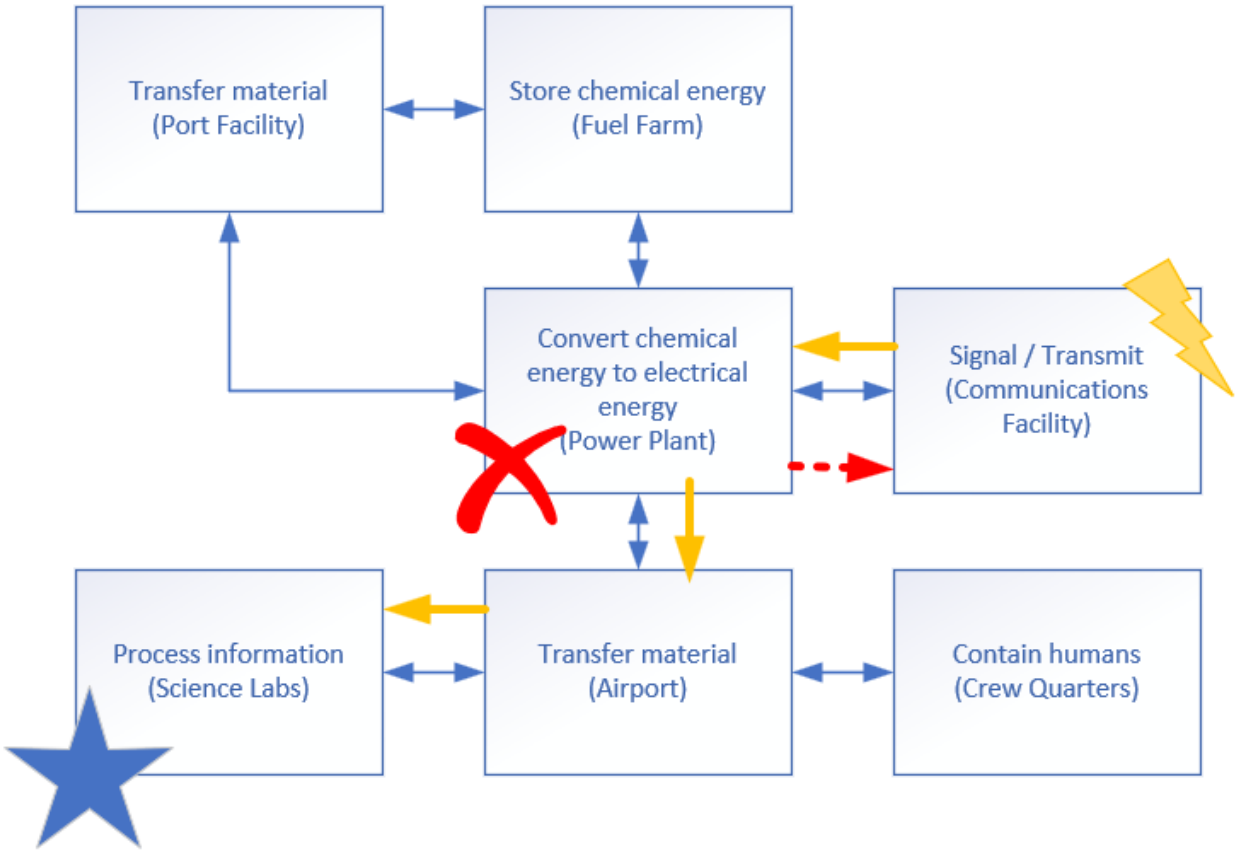

FIGURE 7: Functional model of data and physical failure flows from a hybrid cyber and physical attack where the cyber initiating event is from the CRQC.

[11] Otto, Kevin N. *Product design: techniques in reverse engineering and new product development*. Pearson (2003).

[12] Blanchard, Benjamin S, Fabrycky, Wolter J and Fabrycky, Walter J. *Systems engineering and analysis*. Vol. 4. Prentice hall Englewood Cliffs, NJ (1990).

[13] Crawley, Edward, Cameron, Bruce and Selva, Daniel. *System architecture: strategy and product development for complex systems*. Prentice Hall Press (2015).

[14] Sage, Andrew P and Rouse, William B. *Handbook of systems engineering and management*. John Wiley & Sons (2014).

[15] Haberfellner, Reinhard, Nagel, Peter, Becker, Mario, Büchel, Alfred and von Massow, Heinrich. *Systems engineering*. Springer (2019).

[16] Giachetti, Ronald. *Design of enterprise systems: Theory, architecture, and methods*. CRC Press (2016).

[17] Mannion, Mike and Keepence, Barry. "SMART requirements." *ACM SIGSOFT Software Engineering Notes* Vol. 20 No. 2 (1995): pp. 42–47.

[18] Eisenbart, Boris, Gericke, Kilian and Blessing, Luciënne. "An analysis of functional modeling approaches across disciplines." *Ai Edam* Vol. 27 No. 3 (2013): pp. 281–289.

[19] Arlitt, Ryan, Van Bossuyt, Douglas L, Stone, Rob B and Tumer, Irem Y. "The function-based design for sustainability method." *Journal of Mechanical Design* Vol. 139 No. 4 (2017): p. 041102.

[20] Kurtoglu, Tolga, Tumer, Irem Y and Jensen, David C. "A functional failure reasoning methodology for evaluation of conceptual system architectures." *Research in Engineering Design* Vol. 21 (2010): pp. 209–234.

[21] Tolga, Kurtoglu and Tumer, Irem. "Ffip: A framework for early assessment of functional failures in complex systems." *INTERNATIONAL CONFERENCE ON ENGINEERING DESIGN, ICED*. 2007.

[22] O'Halloran, Bryan M and Papakonstantinou, Nikolaos and Van Bossuyt, Douglas L. "Modeling of function failure propagation across uncoupled systems." *2015 Annual Reliability and Maintainability Symposium (RAMS)*: pp. 1–6. 2015. IEEE.

[23] L'her, Guillaume, Van Bossuyt, Douglas L and O'Halloran, Bryan M. "Prognostic systems representation in a function-based Bayesian model during engineering design." *International Journal of Prognostics and Health Management* Vol. 8 No. 2 (2017).

[24] O'Halloran, Bryan M and Papakonstantinou, Nikolaos and Giammarco, Kristin and Van Bossuyt, Douglas L. "A graph

theory approach to predicting functional failure propagation during conceptual systems design." *Systems Engineering* Vol. 24 No. 2 (2021): pp. 100–121.

[25] Hirtz, Julie, Stone, Robert B, McAdams, Daniel A, Szykman, Simon and Wood, Kristin L. "A functional basis for engineering design: reconciling and evolving previous efforts." *Research in engineering Design* Vol. 13 (2002): pp. 65–82.

[26] Spreafico, Christian, Russo, Davide and Rizzi, Caterina. "A state-of-the-art review of FMEA/FMECA including patents." *computer science review* Vol. 25 (2017): pp. 19–28.

[27] Stamatelatos, Michael, Dezfuli, Homayoon, Apostolakis, George, Everline, Chester, Guarro, Sergio, Mathias, Donovan, Mosleh, Ali, Paulos, Todd, Riha, David, Smith, Curtis et al. "Probabilistic risk assessment procedures guide for NASA managers and practitioners." Technical report no. 2011.

[28] Modarres, Mohammad, Kaminskiy, Mark P and Krivtsov, Vasiliy. *Reliability engineering and risk analysis: a practical guide*. CRC press (2016).

[29] "The NIST Cybersecurity Framework (CSF) 2.0." National Institute of Standards and Technology (NIST) (2024). URL https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

[30] "CVE Program Mission." The MITRE Corporation (2024). URL https://www.cve.org/.

[31] Jensen, David, Tumer, Irem Y and Kurtoglu, Tolga. "Flow State Logic (FSL) for analysis of failure propagation in early design." *International Design Engineering Technical Conferences and Computers and Information in Engineering Conference*, Vol. 49057: pp. 1033–1043. 2009.

[32] Short, Ada-Rhodes, Lai, Ann D and Van Bossuyt, Douglas L. "Conceptual design of sacrificial sub-systems: failure flow decision functions." *Research in Engineering Design* Vol. 29 (2018): pp. 23–38.

[33] Van Bossuyt, Douglas L and O'Halloran, Bryan M and Arlitt, Ryan M. "A method of identifying and analyzing irrational system behavior in a system of systems." *Systems Engineering* Vol. 22 No. 6 (2019): pp. 519–537.

[34] Hale, Britta and Van Bossuyt, Douglas L and Papakonstantinou, Nikolaos and O'Halloran, Bryan. "A zero-trust methodology for security of complex systems with machine learning components." *International design engineering technical conferences and computers and information in engineering conference*, Vol. 85376: p. V002T02A067. 2021. American Society of Mechanical Engineers.

[35] Van Bossuyt, Douglas L and Hale, Britta and Arlitt, Ryan M and Papakonstantinou, Nikolaos. "Multi-mission engineering with zero trust: A modeling methodology and application to contested offshore wind farms." *International Design Engineering Technical Conferences and Computers and Information in Engineering Conference*, Vol. 86212: p. V002T02A058. 2022. American Society of Mechanical Engineers.

[36] Papakonstantinou, Nikolaos, Van Bossuyt, Douglas L, Linnosmaa, Joonas, Hale, Britta and O'Halloran, Bryan. "A zero trust hybrid security and safety risk analysis method." *Journal of Computing and Information Science in Engineering* Vol. 21 No. 5 (2021): p. 050907.

[37] Short, Adam R, Van Bossuyt, Douglas Lee et al. "Rerouting failure flows using logic blocks in functional models for improved system robustness: failure flow decision functions." *DS 80-6 Proceedings of the 20th International Conference on Engineering Design (ICED 15) Vol 6: Design Methods and Tools-Part 2 Milan, Italy, 27-30.07. 15*: pp. 031–040. 2015.

[38] "Science & Tech Spotlight: Securing Data for a Post-Quantum World." U.S. Government Accountability Office (GAO) (2023). URL https://www.gao.gov/products/gao-23-106559.

[39] Klein, Andrew G, Kennicutt, Mahlon C, Wolff, Gary A, Sweet, Steve T, Bloxom, Tiffany, Gielstra, Dianna A and Cleckley, Marietta. "The historical development of McMurdo station, Antarctica, an environmental perspective." *Polar Geography* Vol. 31 No. 3-4 (2008): pp. 119–144.

[40] Yan, Xiaoying Winston and England, Marijane E. "Design evaluation of an Arctic research station: From a user perspective." *Environment and Behavior* Vol. 33 No. 3 (2001): pp. 449–470.

[41] Pollard, Wayne, Haltigin, Tim, Whyte, Lyle, Niederberger, Thomas, Andersen, Dale, Omelon, Christopher, Nadeau, Jay, Ecclestone, Miles and Lebeuf, Martin. "Overview of analogue science activities at the McGill Arctic research station, axel heiberg island, canadian high arctic." *Planetary and Space Science* Vol. 57 No. 5-6 (2009): pp. 646–659.

[42] Keil, Kathrin. "The Arctic: A new region of conflict? The case of oil and gas." *Cooperation and conflict* Vol. 49 No. 2 (2014): pp. 162–190.

[43] Mitchell, Barbara and Kimball, Lee. "Conflict over the cold continent." *Foreign Policy* No. 35 (1979): pp. 124–141.

[44] Quillérou, Emmanuelle, Jacquot, Mathilde, Cudennec, Annie, Bailly, Denis, Choquet, Anne and Zakrewski, Laure. "The Arctic: Opportunities, Concerns and Challenges." *Scientific Fact sheets of the Ocean & Climate Platform* (2020): pp. 73–87.

[45] Dahl, Jens. "Mining and Local Communities: A short comparison of mining in the Eastern Canadian Arctic (Nanisivik/Arctic Bay) and Greenland (Marmorilik/Uummannaq)." *Études/Inuit/Studies* Vol. 8 No. 2 (1984): pp. 145–157.

[46] Muir, Magdalena AK. "Illegal, unreported and unregulated fishing in the circumpolar arctic." *Arctic* Vol. 63 No. 3 (2010): pp. 373–378.

[47] Shephard, Grace Elizabeth, Dalen, Kari, Peldszus, Regina, Aparício, Sara, Beumer, Larissa, Birkeland, Roger, Gkikas, Nikolaos, Kourantidou, Melina, Ktenas, Panagiotis, Linde, Peter Wilhelm et al. "Assessing the added value of the recent declaration on unregulated fishing for sustainable governance of the central Arctic Ocean." *Marine Policy* Vol. 66 (2016): pp. 50–57.

[48] Daneels, Axel and Salter, Wayne. "What is SCADA?" (1999).

[49] Bailey, David and Wright, Edwin. *Practical SCADA for industry*. Elsevier (2003).

[50] Avanzi, Roberto, Hoerder, Simon, Page, Dan and Tunstall, Michael. "Erratum to: Side-channel attacks on the McEliece and Niederreiter public-key cryptosystems." *Journal of Cryptographic Engineering* Vol. 1 (2011): pp. 271–281. DOI 10.1007/s13389-011-0024-9.

[51] Zhandry, Mark. "Tracing Quantum State Distinguishers via Backtracking." *Advances in Cryptology – CRYPTO 2023: 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20–24, 2023, Proceedings, Part V*: p. 3–36. 2023. Springer-Verlag, Berlin, Heidelberg. DOI 10.1007/978-3-031-38554-4_1. URL https://doi.org/10.1007/978-3-031-38554-4_1.

[52] Jackson, Kelsey A., Miller, Carl A. and Wang, Daochen. "Evaluating the security of CRYSTALS-Dilithium in the quantum random oracle model." (2024).

[53] Hhan, Minki, Morimae, Tomoyuki and Yamakawa, Takashi. "From the Hardness of Detecting Superpositions to Cryptography: Quantum Public Key Encryption and Commitments." Hazay, Carmit and Stam, Martijn (eds.). *Advances in Cryptology – EUROCRYPT 2023*: pp. 639–667. 2023. Springer Nature Switzerland, Cham.

[54] Guo, Qian, Nabokov, Denis, Nilsson, Alexander and Johansson, Thomas. *SCA-LDPC: A Code-Based Framework for Key-Recovery Side-Channel Attacks on Post-quantum Encryption Schemes* (2023): pp. 203–236. DOI 10.1007/978-981-99-8730-6_7.

[55] Haodong, Jiang and Zhang, Zhenfeng. *Post-quantum Security of Key Encapsulation Mechanism Against CCA Attacks with a Single Decapsulation Query* (2023): pp. 434–468. DOI 10.1007/978-981-99-8730-6_14.

[56] Jensen, David, Van Bossuyt, Douglas L., Bello, Oladapo, O'Halloran, Bryan M. and Papakonstantinou, Nikolaos. "A Survey of Function Failure Identification and Propagation Analysis Methods for System Design." *Journal of Computing and Information Science in Engineering* (2024) In Press.

[57] Force, Joint Task. "NIST SP 800-37 Rev. 2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy." National Institute of Standards and Technology (NIST) (2018). URL https://csrc.nist.gov/pubs/sp/800/37/r2/final.