2023 Issue 2 // Volume 119

# THE BRIDGE

The Magazine of IEEE-Eta Kappa Nu

## Cybersecurity for *Critical* Infrastructure

**Cybersecurity for Critical Infrastructure**

A Barrier-based Approach to Cyber Security in Critical Infrastructures

Bridging the Gap between Cybersecurity and Reliability for Critical National Infrastructures

IEEE-HKN 2023 Student Leadership Conference Announcement

Cybersecurity – A Brief History

**IEEE-Eta Kappa Nu**

# IEEE-HKN AWARDS PROGRAM

As the Honor Society of IEEE, IEEE-Eta Kappa Nu provides opportunities to promote and encourage outstanding students, educators, and members.

Visit our new website to view the award programs, award committees, list of past winners, nomination criteria, and deadlines.

### ALTON B. ZERBY AND CARL T. KOERNER OUTSTANDING STUDENT AWARD (OSA)

Presented annually to a senior who has proven outstanding scholastic excellence and high moral character, and has demonstrated exemplary service to classmates, university, community, and country.
**(Deadline: 30 June)**

### C. HOLMES MACDONALD OUTSTANDING TEACHING AWARD (OTA)

Presented annually to electrical engineering professors who have demonstrated, early in their careers, special dedication and creativity in their teaching, as well as a balance between pressure for research and publications.
**(Deadline: Monday after 30 April)**

### DISTINGUISHED SERVICE AWARD (DSA)

Recognizes members who have devoted years of service and lifetime contributions to Eta Kappa Nu (or IEEE-HKN), resulting in significant benefits for all of the society's members.
**(Deadline: Monday after 30 April)**

### OUTSTANDING CHAPTER AWARD (OCA)

Recognizes chapters for excellence in activities and service at the department, university, and community levels. The award is based on the content contained in their Annual Chapter Report for the preceding academic year.
**(Deadline: 31 July)**

### OUTSTANDING YOUNG PROFESSIONAL AWARD (OYP)

Presented annually to an exceptional young engineer who has demonstrated significant contributions early in his or her professional career.
**(Deadline: Monday after 30 April)**

### IEEE-HKN ASAD M. MADNI OUTSTANDING TECHNICAL ACHIEVEMENT AND EXCELLENCE AWARD

Presented annually to a practitioner in the IEEE technical fields of interest who has distinguished himself or herself through an invention, development, or innovation that has had worldwide impact.
**(Deadline: Monday after 30 April)**

## IEEE-Eta Kappa Nu Board of Governors

IEEE-Eta Kappa Nu (IEEE-HKN) was founded by Maurice L. Carr at the University of Illinois at Urbana- Champaign on 28 October 1904, to encourage excellence in education for the benefit of the public. IEEE-HKN fosters excellence by recognizing those students and professionals who have conferred honor upon engineering education through distinguished scholarship, activities, leadership, and exemplary character as students in electrical or computer engineering or by their professional attainments. *THE BRIDGE* is the official publication of IEEE-HKN. The ideas and opinions expressed in *THE BRIDGE* are those of the individuals and do not necessarily represent the views of IEEE-HKN, the Board of Governors, or the magazine staff.

**Get in touch with Eta Kappa Nu Twitter: ieee_etakappanu Facebook: IEEE-HKN**

# THE BRIDGE

## The Magazine of IEEE-Eta Kappa Nu

**2023 ISSUE 2 | Cybersecurity for Critical Infrastructure**

## Features

## Departments

**Editor-in-Chief:**
Jason Hui

**Editorial Board Members**:
Sean Bentley, Burton Dicht, Emily Hernandez, Marcus Huggans, Hulya Kirkici, Kevin T. Kornegay, Zahra Manzoor, Emmanuel Oyekanlu, and Steve Watkins

**Managing Editor:** Nancy Ostin

**Assistant Managing Editor:**
Amy Michael

**Advertising Sales:** Nancy Ostin
n.ostin@ieee.org

**Design Company:** Tumbleweeds, LLC

**IEEE-HKN INTERNATIONAL HEADQUARTERS**

**Editorial inquiries:** IEEE-Eta Kappa Nu,
445 Hoes Lane, Piscataway, NJ 08854, USA
US Toll Free: +1 800 406 2590
Outside US: +1 732 465 5846
Email: info@hkn.org | www.hkn.ieee.org

Subscription address and email changes: IEEE Contact Center
US Toll Free: +1 800 678 4333 | Outside US: +1 732 981 0060 | Fax: +1 732 562 6380 | Email: contactcenter@ieee.org

Dr. Jason K. Hui

Epsilon Delta Chapter

## *THE BRIDGE*, May 2023

# Letter from the Editor-in-Chief

Dear IEEE-HKN Members and Friends,

This issue of THE BRIDGE magazine features current research efforts on cybersecurity for critical infrastructure - assets, systems, and networks that are so vital to society that their continued operation is required to ensure its security, economy, health and/or safety, or any combination thereof. This area is particularly noteworthy given the rising threats of cyberattacks. We express our appreciation to guest editor Dr. Cyril Onwubiko, a member of the IEEE Computer Society Board of Governors, and the authors of the feature articles for their expert insight on this important topic. This month's society spotlight is also on the IEEE Computer Society, the largest among IEEE's 39 technical societies while our history spotlight traces the origin of cybersecurity from the early days of the internet to the present day.

This issue includes highlights from the Pathways to Industry and HKN TechX virtual conferences that were held over the past few months as well as an announcement on this fall's Student Leadership Conference. We also encourage you to read about the recipients of the 2021-2022 IEEE-HKN Outstanding Chapter Awards and former IEEE-HKN Student Governor Ashley Kuhnley, Lambda Beta Chapter, winner of the 2022 Alton B. Zerby and Carl T. Koerner Outstanding Student Award, all of whom were recognized at this year's ECEDHA Annual Conference held in New Mexico, and the winner of the HKN Best Student Paper Award at IEEE SoutheastCon 2023.

We are excited to share that THE BRIDGE is working with the *IEEE Spectrum* along with *THE INSTITUTE* on ways to collaborate. This is fitting since both are the top two most downloaded publications on the IEEE App. Be on the lookout for content in future issues.

IEEE-HKN strives for effective communication through its various channels, including our website, YouTube, Facebook, LinkedIn, and this magazine. The Editorial Board welcomes your ideas and content and can be contacted by email at info@hkn.org. And as always, *THE BRIDGE* is available on the IEEE App (older archival issues can be accessed in the Engineering and Technology History Wiki).

## *THE BRIDGE*, May 2023

# Introduction from the Guest Editor

Dr. Cyril Onwubiko

IEEE Computer Society

Cybersecurity is a priority for everyone, e.g., consumers, enterprises, and nation-states. In fact, it should be considered an utmost priority for modern society. For example, cybersecurity is used to protect citizens' data and privacy and to identify and protect against false news and misinformation on social media networks and platforms. It is applied in addressing sustainability concerns (environmental, social, and governance (ESG)) and in promoting and guiding the responsible use of artificial intelligence (AI). It is the fabric for establishing national cybersecurity laws, data privacy directives and regulations, and protecting national security. Cybersecurity has become a fundamental building block for protecting citizens and modern society and influencing national interests.

These developments correlate with the increasing number of countries creating their own national cybersecurity strategies, as seen with the UK Cybersecurity 2021, US National Cyber 2018, Finland Cybersecurity 2019, and Australia Cybersecurity 2020. Regional national cybersecurity centres include the European National Information Security Agency (ENISA), the ASEAN Cyber Capacity Programme, and ASEAN-Japan Cybersecurity Capacity Building Centre. The growing national and regional data privacy regulatory derivatives, for instance, the European GDPR and national cybersecurity laws (e.g., Chinese Cyber Security Law) have been enacted to protect themselves, their intellectual property from cyber espionage, and foreign State interference in the rule of law and governance. An additional aim is to foster a secure and safe cyberspace to conduct businesses and to attract human capital and talent pipelines, bolstering innovation and economic potential and opportunities.

Cybersecurity covers a broad range of domains, such as legal and cyber laws, data privacy, risk management, digital forensics, architecture and engineering, systems development, human factors, psychology, linguistics, and STEAM (science, technology, engineering, arts, and mathematics). The articles featured in this issue are just a small demonstration of the multidimensional nature of cybersecurity.

**Cyril Onwubiko** is a Senior Director, Enterprise Security at Pearson, based in London, UK. He is a Board of Governors (BoG) and Distinguished Speaker (DVP) of the IEEE Computer Society and a member of the European Public Policy Committee (EPPC) Working Group on ICT. Cyril is a recipient of the IEEE Computer Society Distinguished Contributor Award. You can reach him at https://www.c-mric.com/cyril.

# A Barrier-based Approach to Cyber Security in Critical Infrastructures

*Knut Øien, Lars Halvdan Flå, Stein Hauge, and Martin Gilje Jaatun, Senior Member, IEEE*

## Abstract

Critical infrastructure environments that include process control systems have long been conversant with the concept of safety barriers that are intended to prevent major accidents and damage to personnel and property. Developments in the last decade where the domains of information technology (IT) and operational technology (OT) have become intertwined have made the need for cybersecurity management in the OT domain clear to all stakeholders, and this has led us to explore the possibilities of defining cybersecurity barriers as a complement to existing safety barriers. This article will describe a first step on the road to integrating cybersecurity barrier management into the already existing safety barrier management regime in the petroleum industry.

Index Terms—cybersecurity, barriers, safety, countermeasures

## I. INTRODUCTION

Actors utilizing industrial control systems have historically been most concerned with mitigating and protecting against unintended events. Consequently, a strong culture for ensuring the health and safety of humans and the environment has been built over the years.

However, with increased demands for the digitalization of industrial control systems, these systems have become increasingly vulnerable to cyberattacks that constitute intended events. Examples from the last decade illustrate how such attacks can interfere with normal operations and pose a threat to health and safety of humans and the environment. Thus, there is an urgent need to protect industrial control systems against cyber threats.

In this article, we discuss the potential for adapting some of the methods and procedures developed and used with success in the safety domain to the cyber security domain. Specifically, we investigate the applicability of *barriers* and *barrier* management to industrial cyber security. A barrier can be defined as a measure intended to identify conditions that may lead to failure, hazard and accident situations, prevent an actual sequence of events from occurring or developing, influence a sequence of events in a deliberate way, or limit damage and/or loss [1]. Barriers can be illustrated in the bow-tie model, see Figure 1 (adapted from Øie et al. [2]).

Many causes can lead to the same incident, following different event sequence paths, unless barriers prevent the development into an incident, and the same incident can lead to different consequences, following different paths, unless barriers mitigate the consequences. This gives the shape of a bow-tie, with the incident being the knot; thus, the name bow-tie diagram. See examples of the use of bow-ties for cybersecurity in Bernsmed et al. [3].

Integrated safety and cybersecurity barrier management is not something that has received a lot of attention [4], and in the following, we will describe an initial contribution toward rectifying this situation.

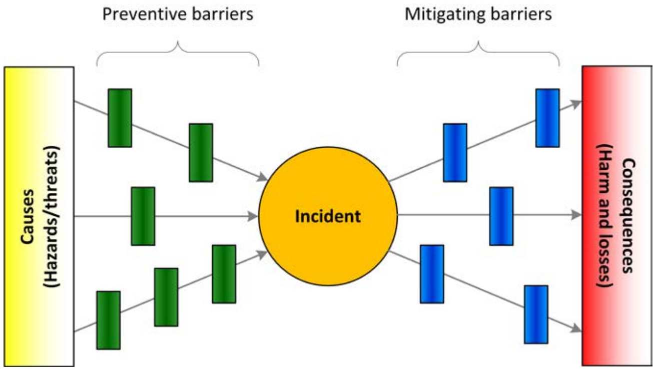


*Figure 1. Bow-tie model with barriers*

## II. BACKGROUND

### *A. Cyber Security Regulations and Guidelines for Critical Infrastructure*

The NIS Directive [5] – the first EU-wide cybersecurity law – and other EU cybersecurity documents, such as the *Cybersecurity Strategy* [6] and the EU cybersecurity package [7], do not refer to barriers explicitly but use terms like security measures and safeguards. We have found that it is primarily the oil and gas industry that explicitly uses the term barriers, as evident in the regulations from the Norwegian Petroleum Safety Authority (PSA), e.g., in the Management Regulations (§5 Barriers) [8]. However, the regulations have been criticized for not being specific about cybersecurity barriers [9], although it is implicitly understood that the regulations also apply to cybersecurity barriers. This is further elaborated in the next section.

The PSA regulations refer to national industry-developed guidelines for cybersecurity for industrial control systems (ICS) [10] and have also been criticized for not referring to international standards such as IEC 62443 [11], which at least some of the major industry actors have started using [12]. As discussed in the next section, the term barrier is rarely used in these standards and guidelines.

IEC 62443 is currently the most comprehensive international standard that covers cybersecurity of industrial control and automation systems (IACS). Its development engages a wide range of manufacturers, system integrators, and end users, and the standard seems to take the position as one of the preferred frameworks. The standard comprises several parts, with the first one published in 2009. Currently, extensive effort is made to revise and publish new parts covering requirements for organizations (processes), systems, and IACS components. These ongoing revisions and drafting of new parts (with resulting inconsistencies between different parts) make IEC 62443 challenging to use for regulators. IEC 62443 does not clearly separate requirements on control, monitoring, and safety functions implemented into IACS. It is therefore worth mentioning ISA-TR84.00.09 [13], which is directed to a specific part of IACS, the safety-instrumented systems (SIS). This technical report is often used in combination with the IEC 62443 documents.

### *B. Cybersecurity barrier management*

Safety barriers and barrier management have been well-known concepts for years, but barriers applied in the same sense for cybersecurity have received less attention [4], and the term barrier is thus rarely used in cybersecurity standards and guidelines.

In the past few years, PSA has funded several studies that consider various aspects of cybersecurity in the petroleum sector [14]. Cybersecurity barrier management is, however, not treated specifically in the reports; only the visualization of countermeasures as barriers. In addition, the current approaches do not clearly illustrate or model the possible relationship between the status of security barriers and safety barriers. A degraded security barrier may result in a degraded safety barrier that can go unnoticed, and such information may be critical in the event of an emerging cyberattack. Although not explicitly stated in current regulations, it is implicitly understood and generally accepted that barriers should also be established for ICT incidents, especially based on the clarifications in the Barrier Memorandum [1].

### *C. Safety barrier management*

A typical safety barrier management process [14] is illustrated in Figure 2. The main input to the barrier management process is an overview of the risk picture along with a plan for the barrier management. The risk picture can be established through, e.g., Hazard Identification (HAZID), Quantitative Risk Analysis (QRA), Emergency Preparedness Analysis (EPA), and the Emergency Preparedness Plan (EPP). The result is used as input when dividing the installation into different areas (step 1) and to identify accidental events with major accident potential. These events are documented as Defined Situations of Hazard and Accident (DSHAs) or as Major Accident Hazards (MAH) (step 2a). The division into areas should ensure that the systems inside an area experience the same level of risk, somewhat similar to how a facility should be partitioned into zones according to IEC 62443.

Step 2b identifies the barrier functions needed to mitigate the events with major accident potential identified in

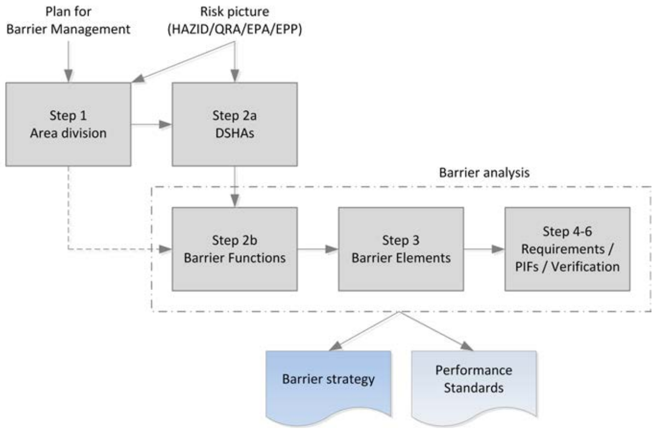


*Figure 2. Typical safety barrier management process*

step 2a. As an example, the event *hydrocarbon leakage* is prevented by several barrier functions, among them *prevent leakage from process equipment.*

In step 3, each of the barrier functions are broken down into a set of sub-functions, which in turn are realized through one or more barrier elements. Barrier elements can either be technical, operational, or organizational. Continuing our example, the *prevent leakage from process equipment-function* can partly be realized, e.g., through the sub-function *prevent leaks due to technical degradation.* This sub-function is in turn realized through the technical barrier elements *sand detectors and corrosion/erosion probes,* and the organizational element *corrosion monitoring by inspection team.*

Step 4 defines the performance requirements for barrier elements. Step 5 identifies performance influencing factors for barrier elements and functions. These are the factors which may significantly affect the element or barriers function to perform its task. Step 6 is concerned with the verification of performance requirements.

The safety barrier management process results in a barrier strategy and performance standards. The barrier strategy can be defined as *"a result of a process that on the basis of the risk picture, describes and clarifies the barrier functions and elements to be implemented in order to reduce risk."* It will typically include methodology (including a description of the barrier management process), including a description of the facility, the area division, the DSHAs (or MAHs), and barrier functions per area (or globally). It continues with barrier elements, in each area (or globally), performance requirements for the barrier elements, performance influencing factors affecting the barrier elements and verification activities for monitoring of barrier performance. Detailed information about performance requirements, PIFs, and verification activities is usually documented separately in the corresponding performance standards [14].

The focus on barriers and the use of the term barrier (strategy) have increased. (Technical) safety strategy was the term used in the past, but this has changed, a change that is also advocated by Norwegian authorities.

### *D. Performance standards for cyber security*

Some companies have started developing dedicated performance standards for cybersecurity (and physical security) based on NOROG 104 [10] or requirements from the NIST Cybersecurity Framework (CSF) [15]. NOROG 104 refers to and maps their requirements to the NIST CSF, which further refers to IEC 62443. A brief overview of such mappings is shown in Table I.

### *E. Secure Safety in oil and gas – way forward*

The process of developing performance standards (requirements) for cyber security varies between companies. We know of instances where NOROG 104 and NIST CSF have been used as a foundation and complemented with requirements from IEC 62443. However, some companies report that the development of cybersecurity requirements is not the main challenge, but rather verifying compliance with the requirements and assessing the status of cybersecurity solutions.

**TABLE I**
**Mappings Between Standards/Frameworks**

| | NIST CSF [16] | IEC 62443 [11] | ISO 27001/2 [17] | NIST SP 800-53 [18] | CIS CSC [19] | COBIT 5 [20] |
|---|---|---|---|---|---|---|
| NOROG 104 | X | | | | | |
| NIST CSF | ▨ | X | X | X | X | X |
| IEC 62443 | X | ▨ | X | X | | |

It is not clear whether the assessment of cyber security should be tied to the assessment of safety, whether the assessment should be qualitative or quantitative, what failure modes are relevant for network components, or how different types of failure states in cyber security solutions and equipment can be classified.

It is an open question whether these cyber security measures and corresponding requirements should be included in a dedicated cybersecurity performance standard or whether they should be included in existing performance standards for the systems that should be protected. Reasons for choosing a dedicated cybersecurity performance standard include obtaining the necessary ownership and visibility, and potentially greater confidentiality since all requirements will be compiled in one document. A related consideration is how to treat requirements for operational and organizational barrier elements, both for cybersecurity barriers and safety barriers, i.e., either as a separate performance standard or added to the technical requirements in the different performance standards.

Apart from assessing compliance with requirements and the status of cybersecurity, several aspects of a barrier approach to cybersecurity must be investigated. These include how to integrate security and safety, how to align IT and OT cultures, and what the alternatives are to a barrier-oriented approach to cyber security.

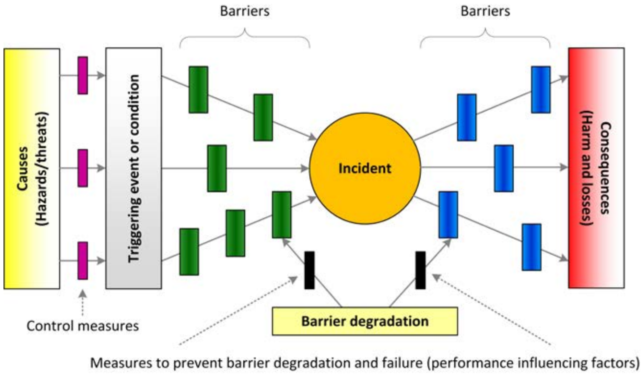

Barriers
Barriers
Causes (Hazards/threats)
Triggering event or condition
Incident
Consequences (Harm and losses)
Control measures
Barrier degradation
Measures to prevent barrier degradation and failure (performance influencing factors)

*Figure 3. Bow-tie model with barriers, control measures and PIFs [2]*

## III. WHAT IS A CYBERSECURITY BARRIER?

In the vernacular, there seems to be little difference between the terms "barrier" and "countermeasure" when used in the context of cybersecurity. However, if we adopt the same reasoning as PSA does in the case of safety barriers, a barrier is something that comes into play for exceptional events, not something that is just part of normal operations or good security management practice. This can be illustrated and explained using a bow-tie diagram, as shown in Figure 3 (adapted from Øie et al. [2]).

PSA makes a distinction between barriers and: 1) measures to prevent triggering events or conditions (control measures) being part of normal operation; and 2) measures to prevent barrier degradation and failure (performance influencing factors - PIFs). In a cybersecurity context, countermeasures often seems to be the term used for all of these measures, i.e., barriers, control measures, and PIFs.

**TABLE II**
**Differentiation Between Countermeasures and Barriers**

| Countermeasure | Cybersecurity Barrier Consideration |
|---|---|
| Vigilant user | Can be a cybersecurity barrier |
| Patch management (ad hoc/formal/centrally managed) | Performance influencing factor |
| Anti-virus (AV) software (updated/centrally managed) | Can be a cybersecurity barrier |
| Audit log | Control measure – part of normal operation |
| Portable media prevented via administrative controls/software/hardware/ physical removal of ports | Intrinsic security – part of normal operation |
| Personnel security | Control measure – part of normal operation |
| Physical access control/locks | Control measure – part of normal operation |
| Intrusion detection | Can be a cybersecurity barrier (function) |

Looking at the example countermeasures in ISA-TR84.00.09-2017 [13], it is clear that many do not satisfy the "exceptional" criterion to count as a barrier. Note that the countermeasures do not distinguish between functions and systems or elements, e.g., intrusion detection, included in Table II, is a function, whereas an intrusion detection system (IDS) can be considered a barrier.

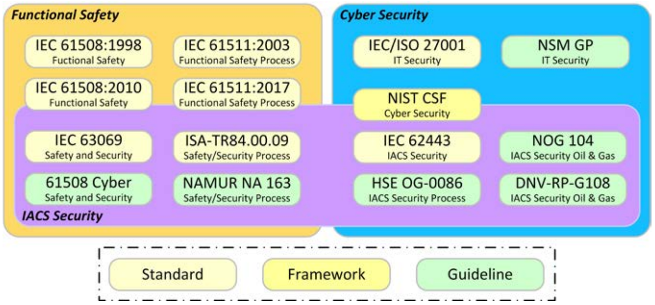


*Figure 4. Selected standards and guidelines for functional safety and cybersecurity*

As an example, physical (or logical) access control is used as part of normal operation, also to avoid unauthorized access from employees who may unintentionally make a mistake. Access control is not only used to prevent intentional cyberattacks. If unauthorized access is discovered, e.g., by an IDS, then it is the IDS that represents a barrier.

Another example is patch management. Patching in itself is comparable to maintenance; something that affects the performance of what is being patched (or maintained). If this is e.g., a server, then it is the server that may be a barrier, depending on the function of the server.

Following the reasoning of PSA, the main motivation for limiting what is included as barriers is to focus on the cyber security countermeasures that can detect and mitigate an ongoing cyber intrusion; the cyber security analogy is to a system being outside normal operating conditions. Establishing requirements for the barriers (and verification/follow-up during operation) is mandatory according to the Norwegian petroleum regulations; however, this does not mean that you cannot or should not define requirements for performance influencing factors or control measures; it is just not mandatory.

## IV. METHOD

The approach used is multi-faceted, including an overall action research approach with close and iterative interaction with the main stakeholders, engaging experts in specific domains (e.g., international standards and cybersecurity project execution), and engaging the relevant cybersecurity community in professional forums (including authorities, petroleum companies, system integrators, product suppliers, consultants, research institutes, and academia). Detailed methods include traditional approaches such as document reviews, literature review, workshops, and interviews.

## V. RESULTS

### A. Current status in the industry

The practices for cybersecurity barrier management were briefly described in Sections II-D and E. It is mainly based on close dialogue with two companies (A and B). For both companies, cybersecurity barrier management has been included as an “add-on” to safety barrier management; thus, it depends on how safety barrier management is practiced, which differs between the two companies (and most other companies). One difference is that company A attempts to use a barrier panel to automatically visualize the status of technical cybersecurity barrier elements on a daily basis, whereas company B provides a status based on more manual considerations every three months.

Company A follows a typical safety barrier management approach as described in Section II-C. They map the cybersecurity barrier elements against requirements in the NOROG 104 guideline [10] (and some requirements from IEC 62443 [11]). These requirements are included in a cybersecurity performance standard (PS). All the requirements are regularly followed up during operation, whereas the status of some safety critical equipment, such as servers, firewalls, gateways, and domain controllers, is provided daily in the barrier panel based on, e.g., failures reported in the maintenance management system.

Company B has developed a somewhat similar performance standard for cybersecurity as company A, where the status is presented every three months together with all the (20 or so) safety performance standards (which is the same as what company A is doing using the barrier panel). The requirements in the cybersecurity performance standard are based on NIST CSF [15] and IEC 62443. Company B applies a more comprehensive approach for assessing the status of the important systems, including manual assessments.

Whereas company A follows a typical barrier management approach, starting with an installation-specific (security) risk analysis and ending with an area specific cybersecurity barrier strategy and a PS on cybersecurity, company B follows a different track, also ending with a PS on cybersecurity but without an installation– and area-specific cybersecurity barrier strategy document.

However, the approaches for indentifying performance requirements are, de facto, rather similar. Both companies map requirements from a cybersecurity framework to “barrier” functions. It is the cybersecurity PS that is actively used in operation. The prior steps are meant to develop the PS.

### B. Most relevant standards

Standards and guidelines for functional safety and cybersecurity, and the bridging of these domains, are illustrated in Figure 4 (inspired by Kanamaru [20]). The most relevant standards are those dealing with operational technology (OT) – here labeled IACS security – or the integration between IT and OT, such as the NIST Cyber Security Framework (NIST CSF) [15].

The most relevant standards in our context are IEC 62443 [11], IEC 63069 [21] and IEC 61511 [22], as well as IEC 61508 [23]. However, there are currently no standards addressing barrier management, either for safety or cybersecurity, or combined or integrated. The most relevant standards for integration are IEC 63069 [21], and ISA-TR84.00.09 [13]. Whereas ISA-TR84.00.09 focuses extensively on integrating cybersecurity into the functional safety lifecycle with reference to IEC 61511, IEC 63069 explains and provides guidance on the common application of IEC 61508 and IEC 62443 more broadly, including life-cycle recommendations.

DNV-RP-G108 [24] is a guideline for use of IEC 62443 in the petroleum industry, especially in the Norwegian petroleum industry. HSE OG-0086 [25] has certain parallels with DNV-RP-G108 for the process industry in the UK. The

61508 Association [26] provides lifecycle maps for the process industry based on either IEC 62443 or HSE OG-0086.

Finally, NAMUR NA 163 [27], a German guideline, refers to the IEC 61511 requirement of performing a security risk assessment for SIS, but IEC 61511 does so without providing specific guidance. NAMUR NA 163 provides a practical risk assessment method for SIS engineers based on ISO/IEC 27005 [28] and IEC 62443-3-2 [29]. It also provides a checklist of security measures as an additional document.

As stated in Section II-A, regulations and standards, including IEC 62443, rarely use the term barrier. More commonly used terms are "countermeasures" (currently used in IEC 62443) and "security measures", as used in the NIS Directive (and also to be adopted in the future by IEC 62443). However, the main question is how the countermeasures or security measures used in relevant cybersecurity standards and guidelines relate to the barrier term used within safety barrier management. This was discussed in Section III.

## VI. DISCUSSION

Based on the definition of a cybersecurity barrier as discussed in Section III, only a subset of cybersecurity activities will be included in the barrier management process. Care must be taken to ensure that cybersecurity activities inside and outside of the barrier management process are harmonized. As an example, patching of a system after a vulnerability has been disclosed may be delayed due to operational concerns (e.g., excessive costs associated with testing and shutdown of the process), a decision that will be made outside the barrier management process. To reduce some of the risk caused by this decision, it may be desirable to configure intrusion detection and anti-virus solutions to better detect and prevent attempts at exploiting the vulnerability. As opposed to patch management, this is an activity that will be performed as part of the barrier management process.

Even if the breakdown of barrier functions to barrier elements follows a traditional safety barrier management process (cf. Figure 2), the barrier elements are mapped against standards and guidelines, thus capturing "everything," i.e., all countermeasures or security measures, not only requirements for barriers, as defined in Section III.

However, whether a traditional safety barrier management approach, with its restricted definition of barriers, is appropriate for cybersecurity "barriers," still needs further consideration.

## VII. CONCLUSION

In this article, we outline an initial effort to adapt the barrier management process in the safety domain to the cybersecurity domain. In the safety domain, a barrier is something that comes into effect to regain control or mitigate the consequences when a system is outside its normal mode of operation. To remain coherent with this approach, following the reasoning of PSA, cybersecurity barriers are a subset of cybersecurity countermeasures, excluding those that can be regarded as part of good practice security operations (e.g., audit logs) and those that affect the performance of a barrier (e.g., patching).

The two companies mentioned in the article both determine performance requirements for cybersecurity by mapping requirements from standards and frameworks (e.g., IEC 62443 and NIST CSF) to barrier functions. However, some companies report that the development of cybersecurity requirements is not the main challenge, but rather to verify compliance with the requirements and assess the status of the cybersecurity solutions.

The most relevant standards for bridging functional safety and cybersecurity are IEC 62443 [11], IEC 63069 [21], and IEC 61511 [22], as well as IEC 61508 [23]. However, there are currently no standards addressing barrier management, either for safety or cybersecurity, or combined or integrated. The most relevant standards for integration are IEC 63069 [21] and ISA-TR84.00.09 [13].

We will continue to explore how to integrate cybersecurity barrier management into the existing safety barrier management regime, including the definition of cybersecurity barriers.

## ACKNOWLEDGMENT

The authors are grateful for the participation of the CDS Forum members.

### REFERENCES

[1] A. Eltervåg, *et al.*, 'Principles for barrier management in the petroleum industry', Jan. 2019. Accessed: Dec. 01, 2022. [Online]. Available: https://www.ptil.no/en/technical-competence/explore-technical-subjects/news/2017/barrier-memorandum/

[2] S. Øie, A. Wahlstrøm, H. Flataker, and S. Rørkjær, 'Barrier Management in Operation for the Rig Industry - Good Practices', DNV-GL, 2013–1622, Mar. 2014.

[3] K. Bernsmed, C. Frøystad, P. H. Meland, D. A. Nesheim, and Ø. J. Rødseth, 'Visualizing Cyber Security Risks with Bow-Tie Diagrams', in *Graphical Models for Security*, Cham, 2018, pp. 38–56. doi: 10.1007/978-3-319-74860-3_3.

[4] K. Øien, S. Hauge, M. G. Jaatun, L. Flå, and L. Bodsberg, 'A Survey on Cybersecurity Barrier Management in Process Control Environments', in *Proceedings of 2022 IEEE International Conference on Cloud Computing Technology and Science*, Bangkok.

[5] *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance*), vol. 333. 2022. Accessed: Feb. 02, 2023. [Online]. Available: http://data.europa.eu/eli/dir/2022/2555/oj/eng

[6] *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS* Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. 2013. Accessed: Feb. 02, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013JC0001

[7] *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL* Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. 2017. Accessed: Feb. 02, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505294563214&uri=JOIN:2017:450:FIN

[8] *REGULATIONS RELATING TO MANAGEMENT AND THE DUTY TO PROVIDE INFORMATION IN THE PETROLEUM ACTIVITIES AND AT CERTAIN ONSHORE FACILITIES*. 2021. Accessed: Feb. 02, 2023. [Online]. Available: https://www.ptil.no/en/regulations/all-acts/?forskrift=611

[9] O. Lysne, 'NOU 2015: 13 - Digital sårbarhet - sikkert samfunn - Beskytte enkeltmennesker og samfunn i en digitalisert verden'. Regjeringen, Nov. 30, 2015. Accessed: Dec. 01, 2022. [Online]. Available: https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/

[10] 'Norwegian Oil and Gas recommended guidelines on information security baseline requirements for process control, safety and support ICT systems', Norwegian Oil and Gas Association, Guideline NOROG 104, 2016. Accessed: Aug. 01, 2022. [Online]. Available: https://www.norskoljeoggass.no/arbeidsliv/retningslinjer/integrerte-operasjoner/104-anbefalte-retningslinjer-krav-til-informasjonssikkerhetsniva-i-ikt-baserte-prosesskontroll--sikkerhets--og-stottesystemer-ny-revisjon-pr-05.12.2016/

[11] 'IEC 62443: Industrial communication networks - Network and system security'. IEC. [Online]. Available: https://www.iec.ch/blog/understanding-iec-62443

[12] T. Onshus et al., 'Security and Independence of Process Safety and Control Systems in the Petroleum Industry', *J. Cybersecurity Priv.*, vol. 2, no. 1, pp. 20–41, 2022.

[13] H. W. Thomas, 'Cybersecurity Related to the Functional Safety Lifecycle', ISA, ISA-TR84.00.09-2017, 2017. Accessed: Dec. 01, 2022. [Online]. Available: https://www.isa.org/products/isa-tr84-00-09-2017-cybersecurity-related-to-the-f

[14] 'Industrial ICT systems'. https://www.ptil.no/en/technical-competence/explore-technical-subjects/news/2021/ict-security---robustness-in-the-industry/ (accessed Feb. 15, 2023).

[15] K. Øien and S. Hauge, 'Guidance for Barrier Management in the Petroleum Industry', SINTEF Report SINTEF A27623, Sep. 2016. [Online]. Available: https://www.sintef.no/globalassets/project/pds/reports/pds-report-guidance-for-barrier-management-in-the-petroleum-industry.pdf

[16] 'Framework for Improving Critical Infrastructure Cybersecurity', Feb. 2018. Accessed: Feb. 02, 2023. [Online]. Available: https://www.nist.gov/cyberframework/framework

[17] ISO, 'ISO/IEC 27001:2013', Standard. Accessed: Mar. 22, 2022. [Online]. Available: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/45/54534.html

[18] 'Security and Privacy Controls for Information Systems and Organizations', National Institute of Standards and Technology, NIST Special Publication (SP) 800-53 Rev. 5, Dec. 2020. doi: 10.6028/NIST.SP.800-53r5.

[19] 'CIS Controls', *CIS*. https://www.cisecurity.org/controls/ (accessed Feb. 02, 2023).

[20] 'COBIT 5 Framework Publications', ISACA. https://www.isaca.org/resources/cobit/cobit-5 (accessed Feb. 02, 2023).

[21] H. Kanamaru, 'Bridging functional safety and cyber security of SIS/SCS', in *2017 56th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE)*, 2017, pp. 279–284.

[22] 'Industrial-process measurement, control and automation - Framework for functional safety and security', IEC TR 63069:2019, 2019. Accessed: Feb. 02, 2023. [Online]. Available: https://webstore.iec.ch/publication/31421

[23] 'Functional safety - Safety instrumented systems for the process industry sector', IEC, IEC 61511:2023 SER, 2023. Accessed: Feb. 02, 2023. [Online]. Available: https://webstore.iec.ch/publication/5527

[24] 'IEC 61508-1:2010'. Accessed: Jul. 11, 2022. [Online]. Available: https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=429346

[25] 'DNV-RP-G108 Guideline for the use of IEC 62443 in the oil and gas industry', *DNV*. https://www.dnv.com/Default (accessed Feb. 02, 2023).

[26] 'Cyber Security for Industrial Automation and Control Systems (IACS)', HSE OG-0086, 2018. Accessed: Feb. 02, 2023. [Online]. Available: https://www.hse.gov.uk/foi/internalops/og/og-0086.pdf

[27] 'Considerations for cybersecurity during the safety lifecycle', The 61508 Association, T6A032, Nov. 2020. [Online]. Available: https://www.61508.org/images/downloads/T6A032_Technical_Guide_-_Considerations_for_Cybersecurity_during_the_Safety_Lifecycle_V1_e112020.pdf

[28] 'Security Risk Assessment of SIS', NAMUR, Worksheet NA 163, Dec. 2017. Accessed: Feb. 02, 2023. [Online]. Available: https://www.namur.net/en/recommendations-and-worksheets/current-nena.html

[29] 'ISO/IEC 27005:2018'. ISO/IEC. Accessed: Nov. 04, 2022. [Online]. Available: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/52/75281.html

[30] IEC, 'IEC62443-3-2 :2020 Security for industrial automation and control systems - Part 3-2: Security Risk assessment for system design', International Electrotechnical Commission, 2020.

**Knut Øien** is a senior scientist at SINTEF Digital in Trondheim, Norway. He has been adjunct professor at NTNU, in the Department of Production and Quality Engineering within Risk Analysis for 10 years (2005-2015). He holds a Ph.D. from 2001 in Risk Control of Offshore Installations and a M.Sc. from 1986 in Mechanical Engineering from the Norwegian Institute of Technology (NTH). His main fields of competence include, e.g., risk assessment, indicators (risk, safety, and resilience), barrier management, maintenance management, accident investigation, and emergency preparedness analysis, in which he has more than 30 years of experience with national and international research projects.

**Lars Halvdan Flå** is a Master of Science at SINTEF Digital, Trondheim, Norway. He holds a master's degree in cybernetics and robotics from the Norwegian University of Science and Technology (NTNU). His main research interest is in the cyber security of industrial control systems, and he has worked on research projects within the domains of smart grid and oil and gas. Additional projects include 5G security and security in public spaces.

**Stein Hauge** is a senior safety advisor at SINTEF Digital. He holds a master's degree in industrial mathematics from the Norwegian University of Science and Technology (NTNU) and a master's degree in operational research from Strathclyde Business School. His main fields of competence include reliability of Safety Instrumented Systems (SIS), barrier and risk management, operational safety follow-up, and technical safety.

**Martin Gilje Jaatun** Senior Member, IEEE, is a senior scientist at SINTEF Digital in Trondheim, Norway, and an Adjunct Professor at the University of Stavanger. He graduated from the Norwegian Institute of Technology (NTH) in 1992 and holds a Ph.D. from the University of Stavanger. Previous positions include scientist at the Norwegian Defense Research Establishment (FFI) and senior lecturer in information security at the Bodø Graduate School of Business. His research interests include software security, security in cloud computing, and the security of critical information infrastructures.

Dr. Jaatun is vice chairman of the Cloud Computing Association (cloudcom.org), vice chair of IEEE CS TCCLD, vice chair of IEEE CS STC Blockchain, and a senior member of the IEEE. He is also an IEEE Cybersecurity Ambassador and an IEEE CS Distinguished Visitor.

# Bridging the Gap between Cybersecurity and Reliability for Critical National Infrastructures

*Leandros Maglaras, Senior Member IEEE, Mohamed Amine Ferrag, Senior Member IEEE, Helge Janicke, William J Buchanan, Leandros Tassiulas, Fellow IEEE*

## Abstract

In this article, we attempt to bridge the gap between cybersecurity and the reliability of Critical National Infrastructures (CNIs). We discuss new methodologies to map system requirements by incorporating security (and privacy) with reliability (and safety), thus introducing a new research area under the broad term of securability.

Keywords: Critical Infrastructures, Cybersecurity, Reliability

### I. INTRODUCTION

Cybersecurity for CNIs involves securing critical networks and systems that are essential to the operation of a nation. These critical infrastructures include the fields of health care, finance, energy, transportation, and telecommunications, among others, as presented in Figure 1. Providing reliability and cybersecurity for these types of systems is essential since they perform critical services that are fundamental to the safety and security of a nation's citizens.

Cybercrime inflicted harm that amounted to $6 trillion USD worldwide in 2021; this number is expected to rise to $10 trillion annually by 2025 [11]. Cybersecurity threats against CNIs can be generated from multiple potential sources, including government-sponsored hackers, cybercriminals, and insiders with unauthorized access to the networks [1]. The threats can involve phishing, Advanced Persistent Threats (APTs), Denial of Service (DoS), ransomware, malware, etc. that can cause serious damage or disruption to critical systems. APTs are a highly targeted and sophisticated type of cyber threats, which are carried out by nation states or other well-financed and highly organized criminal entities. APTs typically employ long-term stealthy penetrations of individual target networks to gather critical data or obtain a base for future cyberattacks. A DoS attack aims to overwhelm a system or network with massive amounts of traffic in order to disrupt the system. These attacks can interrupt the accessibility of CNI networks, resulting in severe disruptions and sometimes serious physical damage. Phishing attacks are a popular strategy for hackers to trick susceptible users into sharing their sensitive data or installing malware. Specifically, phishing attacks are frequently conducted by spamming individuals with fraudulent emails or fake websites that look legitimate in order to trick them into signing in or launching malicious software. Malware is any program or software application that is intended to corrupt or destroy a system. The malware application can be distributed via a combination of different techniques, such as malware downloads, infected websites, or email attachments. Malware can expose the safety of CNI information systems and enable the hacker to obtain access or control without authorization [2].

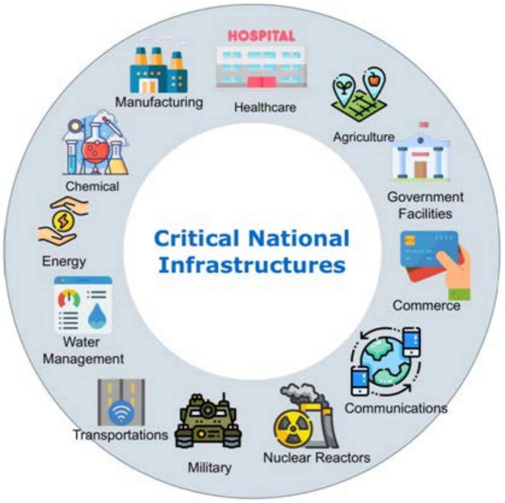


*Figure 1. Critical Infrastructure Sectors*

To provide cybersecurity and reliability for CNIs, there are various efforts that both governments and agencies can employ, including:

- Having systems and policies to address and overcome incidents that may occur.
- Performing periodic assessments of security status and testing for penetration.
- Employing robust security mitigation measures, such as intrusion detection systems, cryptography methods, firewalls, anti-virus software, and emerging security technologies (i.e., Blockchain technology, Artificial Intelligence).
- Maintaining and updating software and hardware on a periodic schedule.
- Providing appropriate cybersecurity training to staff.
- Enforcing robust new cybersecurity technology policies and operating procedures.

By implementing these actions, agencies can assist in securing and protecting their organizations' critical assets as well as ensuring the availability of continuous and necessary services to their customers. We focus on the gap between cybersecurity and reliability for CNIs and present future solutions.

## II. RELIABILITY IN CNIS

Safety and security are essential for the dependable operation of cyber-physical systems (CPS) because of the close connection between the cyber and physical components. Security implies protection from both intentional and unintentional threats, whereas safety aims to protect systems from unintentional actions. Moreover, reliability is a metric that measures a system's ability to operate in accordance with its requirements under specific operational and temporal conditions. Reliability is the possibility that the system will work properly for a certain amount of time. Those requirements determine how well the system can accommodate the application's requirements. In order to determine the system's reliability, we need to have a thorough understanding of the system's components and how they work. To determine a system's reliability, it is necessary to calculate the dependability of each subsystem or entity, as well as their connections and interdependencies.

One of the primary functions of a CNI is to ensure the consistent offering of its service to customers. When referring to reliability, the existence of protection systems that can automatically respond to service interruptions caused by faults or attacks is included. Depending on the service provided, several automated incident response mechanisms must be in place. For example, for power systems, protective devices must detect hardware faults like short circuits or aging equipment, as well as a variety of other incidents like severe weather, human error, or cyber attacks, and initiate automated response actions like opening network breakers. The grid outage time and the effect of fault currents on the system and customers are minimized by these protective devices' prompt and effective intervention. Having in mind that all digital services are dependent on continuous energy supply, we understand that these countermeasures could potentially apply to all CNIs.

The reliability (in terms of integrity) of the data received by the data concentrators and hardware and software failures for the communication and industrial control networks must also be taken into account when conducting CNIs reliability calculations. Methods for evaluating reliability fall into two main categories: techniques based on analysis and those based on simulation. Analytical methods are hard to use on complicated systems and hard to keep up with changes in

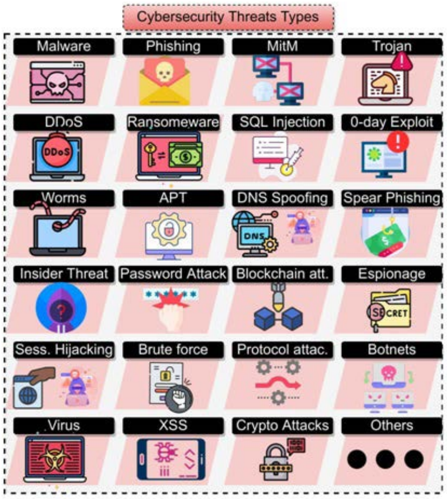


*Figure 2. Types of Cybersecurity Threats*

architecture. In contrast, the most widely used simulation technique, Monte Carlo, is a time-consuming and efficient way to evaluate the dependability of large, complex systems like CNIs. For CNI reliability calculations, there is a need for novel approximate methods that can be both efficient and less time-consuming [3].

The system's reliability is measured, among other things, by the Mean Time to Failure (MTTF) and the Mean Time to Repair (MTTR). Reliability theory can be used to support a system's robustness by analyzing the behavior of complex systems and developing new stable ones.

## III. CYBERSECURITY IN CNIS

As the various types of cyber threats continue to multiply, the following are some common and highly prevalent cyber threats (presented in Figure 2) that CNIs should be aware of:

- **Malware attacks:** Malware is software intended to interrupt, disrupt, or obtain access to a network or system without permission. When malicious software is used to attack a CNI, it can interrupt the function of sensitive public services such as transportation, water, or electricity.
- **Phishing attacks:** Phishing involves the distribution of fake messages or emails that seem to be from legitimate sources in order to encourage users to provide sensitive information or to click on links that may be malicious. CNIs, such as water treatment facilities, transportation systems, and electrical grids, are especially susceptible to these kinds of attacks since they can have extensive effects on society.
- **Man in the Middle attacks:** These attacks require the unauthorized interception and manipulation of communications between two different entities, which allows hackers to obtain critical information or interrupt critical system operations.
- **Trojan attacks:** These attacks can be used to obtain unauthorized access to a system and then remain undiscovered for significant time periods, which enables the attacker to disrupt operations or collect critical information.
- **Distributed Denial-of-Service attacks:** These attacks usually consist of overwhelming a targeted system or network with massive quantities of traffic in order to cause it to become unavailable or malfunction.
- **Ransomware attacks:** The purpose of these attacks is to access and then encrypt the data in the CNI systems, which will make them unavailable to the operators until the hackers are paid a ransom.
- **SQL injection attacks:** These attacks consist of the injection of malicious code into the SQL database of a critical infrastructure system, allowing an attacker to disrupt the infrastructure as well as manipulate data.
- **Zero-day attacks:** This indicates that the vulnerability has not been detected or resolved by the security services provider, and therefore, the application is susceptible to future attacks.
- **Worm attacks:** Computer worms are usually developed with malicious intentions and can significantly disrupt the infrastructure they are attacking, causing potentially massive damage and disruption. The worm spreads by self-replicating and propagating to multiple systems, usually via email or by exploiting software or operating system vulnerabilities.
- **Brute force attack:** This is a form of cyberattack where an attacker employs the use of various automated techniques to generate a different password or key combinations in order to obtain unauthorized access to systems, accounts, or websites. The attacker will usually employ a list of popular passwords or a word dictionary to guess the correct password.

## IV. PRIVACY REQUIREMENTS IN CNIS

CNIs are generally viewed as critical systems or assets for the operation of a nation or region, and, as such, they are often required to meet rigorous privacy requirements. These requirements are intended to preserve the integrity, confidentiality, and availability of information and systems associated with CNIs. However, depending on the region or country in which the CNI is located and the characteristics of the CNI in question, various standards, laws, and regulations may apply to the privacy of the CNI. The following are some examples of these standards, laws, and regulations:

- The General Data Protection Regulation (GDPR) in the European Union.
- The Health Insurance Portability and Accountability Act (HIPAA) in the United States.
- The California Consumer Privacy Act (CCPA) for residents of California in the United States.
- The Personal Data Protection Act (PDPA) in Singapore.
- The Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada.
- The Federal Data Protection Act (FDPA) in Switzerland.

The CNI privacy requirements are generally intended to provide assurance that the CNI information and systems are secured from any disclosure, unauthorized use, tampering, or other unauthorized access. The following are the privacy requirements in CNIs that should be taken into consideration:

- **Confidentiality and data protection:** Sensitive and private data should be protected from disclosure and unauthorized access.
- **Periodic monitoring and audits:** Regular monitoring and audits are required to ensure that appropriate privacy and security systems are in operation and working to secure CNIs.

- **Access control:** The use of CNI systems is restricted to only authorized employees.
- **Privacy compliance:** The national critical infrastructure systems are required to be compliant with the appropriate laws and regulations related to privacy, such as GDPR, HIPAA, CCPA, etc.
- **Network security:** There are network security measures such as blockchain, cryptography methods (e.g., symmetric key algorithms, asymmetric key algorithms, digital signatures, and hash functions), intrusion prevention systems based on deep learning models, and firewalls. The symmetric key algorithms include the Advanced Encryption Standard (AES) and ChaCha20. The asymmetric key algorithms include the Rivest-Shamir-Adleman (RSA) algorithm and the Elliptic Curve Cryptography (ECC) algorithm. Solutions like the one proposed in [8] could offer an advanced level of protection for data privacy. These security measures should be in place to ensure security against cyber threats.
- **Physical security:** Access to national critical infrastructure systems should be controlled and protected with the help of video surveillance cameras and alarms to detect and deter potential threats.
- **Recovery and data backup:** CNI systems should have the most robust data backup and recovery processes to ensure the availability and integrity of data in the event of system failure. Two techniques, namely, data replication and cloud backup, could be used as recovery and data backup for CNIs. Data replication refers to the creation of duplicate copies of data in various places, that are accessible during critical situations.

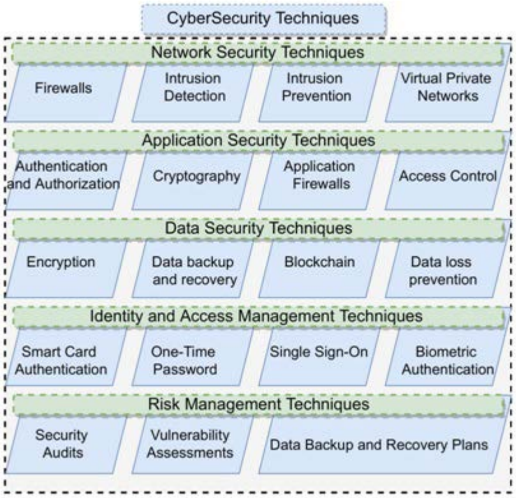


*Figure 3. Types of Cybersecurity Techniques*

As presented in Figure 3, the cybersecurity techniques for CNIs can be categorized into five types: network security techniques, application security techniques, data security techniques, identity and access management techniques, and risk management techniques.

## V. SECURABILITY

Most existing works address security or safety as separate fields of study, although recently a number of scholars have tried to fill this gap. The existing co-analysis of safety and security is approached in two ways: 1) an integrated strategy and 2) a unified strategy [7]. Unfortunately, methodologies that incorporate security (and privacy) with reliability (and safety) are still lacking and are expected to be introduced in the upcoming years. These methodologies would also introduce a new research area under the umbrella term, securability.

Faults and failures can and should be taken into account in the evaluation of securability because they are components that have an impact on the system's proper operation. The idea of security can be found in the triplet of analysis, prediction, and optimization of system's operation. Using terms like Mean Time to Attack (MTTA), Mean Time to Compromise (MTCR), and Mean Time to Recovery (MTTR), which are based on plans for responding to and mitigating incidents, we could model the operation of the system under investigation [5]. Some of the initial steps in this strategy have already been taken, using patterns that combine dependability and security as well as attack prediction with Markov models [6]. The idea of including a probabilistic model of the behavior of a part (or the whole system) in terms of tentative failures or errors could provide a better picture of the system in analysis and a prediction of tentative future states.

Securability can be used as a metric to show how well a system can function in accordance with the demands of the services it is providing by embracing the fundamental ideas of reliability as described in [4]. This definition is different from the one proposed several years ago (by Professor Miroslaw Malek), where the term was used as a property of a system or service that expresses reliance that can be placed on a system or service even in the presence of hostile attacks and other attempts to breach security. In that approach, Malek was trying to integrate dependability and security, especially for cloud computing. Securability, as defined in [4] and also as proposed here, is a holistic metric to measure or predict the correct operation of a system incorporating both faults and attacks. When cybersecurity is incorporated into this reliability analysis, the probability of failure, misuse for each component must include both failures and potential attacks.

## VI. FUTURE DIRECTIONS

There are various subject areas in which future work is required to deal with cybersecurity and reliability challenges for CNIs:

- Cyber resilience: Since cyber attacks are increasingly a serious threat to CNIs, there are ongoing challenges to enhance their level of cybersecurity, and efforts should be made to strengthen the cybersecurity of these systems.

Specifically, this includes the implementation of effective measures for robust cybersecurity, such as emergency response programs, intrusion detection systems, and security firewalls.

- Improving the process of maintenance and recovery: Ensuring the reliability of CNIs requires regular maintenance and recovery. The focus of upcoming efforts could be on enhancing repair and service processes, including employing technologies for predictive maintenance and developing resilient emergency plans. For example, wearable sensors and ultrasonic testing can be used as predictive maintenance technologies. The secured wearable sensors are connected to the machine or mounted by service technicians to track the status of the machine in real time. Secured ultrasonic testing uses high-frequency sound waves to identify defects such as cracks or other faults in the machine.
- Cooperation and communication for reliability: Cooperation and communication among the various organizations and authorities that are responsible for the CNIs is fundamental to their reliability. Future work should focus on enhancing collaboration and coordination among these entities to provide timely emergency incident response and effective decision-making.
- Enhancing the regulation of cybersecurity: At present, there are no complete cybersecurity regulations in place to secure CNIs. Countries and governments require the development and enforcement of enhanced regulations to guarantee that adequate cybersecurity measures are in place for organizations that utilize critical infrastructure.
- Cybersecurity technology investment: To efficiently deploy defenses against cyber threats, organizations require investment in cutting-edge cybersecurity technologies such as Data Loss Prevention (DLP), Internet of Things (IoT) security, network security analytics, biometric authentication, blockchain technology [9], artificial intelligence , and machine learning . The focus of future work in this area should be on the development and implementation of these technologies to enhance the global security posture of CNIs.
- Internet of intelligence security: As more and more smart things are connected to the internet, the potential for cyberattacks against these smart things will continue to increase. Securing these connected smart devices and supporting networks will be a major challenge in the future.
- Increased awareness and training in cybersecurity: In order for criminals to gain access to a target, they only need to find one human, preferably one with high privileges, who is using insecure passwords or who can be tricked into giving information away [10]. Upcoming work efforts are expected to focus on cybersecurity awareness and training for employees working in critical areas of CNIs. The following five awareness and training strategies can be used to enhance cybersecurity: 1) recognizing and reporting cyber threats and incidents; 2) understanding data privacy and laws such as GDPR and HIPAA; 3) recognizing and avoiding phishing attacks; 4) strong password creation and management; and 5) use of secure networks and encryption.

## Concluding remarks

A large-scale failure in CNIs could lead to disruptions in critical services like heating, water supply, internet access, mobile communications, online banking, transportation, and almost every aspect of our modern digital lives. In this article, we presented a holistic approach to addressing attacks and failures at CNIs by merging cybersecurity and reliability. We believe that the work presented in this article, can serve as a basis for further research in this area.

## REFERENCES

1. Osei-Kyei, R., Tam, V., Ma, M., & Mashiri, F. (2021). Critical review of the threats affecting the building of critical infrastructure resilience. International Journal of Disaster Risk Reduction, 60, 102316.
2. Abdalzaher, M. S., Fouda, M. M., & Ibrahem, M. I. (2022). Data privacy preservation and security in smart metering systems. Energies, 15(19), 7419.
3. Memari, M., Karimi, A., & Hashemi Dezaki, H. (2021). Reliability evaluation of smart grid using various classic and metaheuristic clustering algorithms considering system uncertainties. International Transactions on Electrical Energy Systems, 31(6), e12902.
4. Maglaras, L., Janicke, H., & Ferrag, M. A. (2022). Combining Security and Reliability of Critical Infrastructures: The Concept of Securability. Applied Sciences, 12(20), 10387.
5. Maglaras, L. (2022). From Mean Time to Failure to Mean Time to Attack/Compromise: Incorporating Reliability into Cybersecurity. Computers, 11(11), 159.
6. Maglaras, L. A., Ferrag, M. A., Janicke, H., Ayres, N., & Tassiulas, L. (2022). Reliability, Security, and Privacy in Power Grids. Computer, 55(9), 85-88.
7. Kavallieratos, G., Katsikas, S., & Gkioulos, V. (2020). SafeSec Tropos: Joint security and safety requirements elicitation. Computer Standards & Interfaces, 70, 103429.
8. Gupta, S., Sacchetti, T., & Crispo, B. End-to-End Encryption for Securing Communications in Industry 4.0, DOI: DOI: 10.13140/RG.2.2.11247.92325
9. Tibrewal, I., Srivastava, M., & Tyagi, A. K. (2022). Blockchain technology for securing cyber-infrastructure and internet of things networks. Intelligent Interactive Multimedia Systems for e-Healthcare Applications, 337-350.
10. 2022 Data Threat Report, Critical Inftrastructure Edition, https://cpl.thalesgroup.com/critical-infrastructure-data-threat-report#download-popup
11. Morgan, S. (2020). Cybercrime to cost the world $10.5 trillion annually by 2025. Cybercrime Magazine, 13(11).

**Leandros A. Maglaras** is a professor of cybersecurity in the School of Computing at Edinburgh Napier University. From September 2017 to November 2019, he was the Director of the National Cyber Security Authority of Greece. Contact him at l.maglaras@napier.ac.uk

**Mohamed Amine Ferrag** is a lead researcher with the AI and Digital Science Research Center, Technology Innovation Institute, Masdar City, Abu Dhabi, United Arab Emirates. Contact him at mohamed.ferrag@tii.ae

**Helge Janicke** is currently the Research Director of the Cyber Security Cooperative Research Centre, Australia. He is affiliated with Edith Cowan University and holds a visiting professorship in cyber security at De Montfort University, U.K. Contact him at helge.janicke@cybersecuritycrc.org.au

**William (Bill) J Buchanan** OBE is a professor in the School of Computing at Edinburgh Napier University and a Fellow of the BCS and Principal Fellow of the HEA. He was appointed an Officer of the Order of the British Empire (OBE) in the 2017 Birthday Honours for services to cybersecurity. He has won student-voted awards for teaching excellence in 2011, 2014, 2015, 2019, and 2020.

**Leandros Tassiulas** is the John C. Malone Professor of Electrical Engineering at Yale University, New Haven, Connecticut, 06511, USA. Contact him at leandros.tassiulas@yale.edu

IGARSS
Pasadena, California 2023
Register Now
Save the Date
International Geoscience and Remote Sensing Symposium
JULY | 16-21 | 2023
www.igarss2023.com
IEEE
GRSS

# Celebrating the Research Contributions of Our Graduate Student Members

Graduate students, an important and growing part of the IEEE-HKN global community, are performing groundbreaking research. We have developed this award-winning section in *THE BRIDGE* to celebrate and elevate their research contributions. The HKN Graduate Student Research Spotlight is a standing feature in *THE BRIDGE*. The profiles of the students and their work will also be shared on our social media networks.

Each profile will showcase the intellectual merit and broader impact of HKN graduate student members' research and provide information about the students' backgrounds and where people can learn more about them and their work.

We will spotlight these achievements while also showing potential graduate students what is possible!

### Would you like to be featured?

Fill out our submission form. Submissions will be reviewed, assembled into a profile template, and posted on HKN's social media pages. A select number of profiles will also be featured in *THE BRIDGE*.

### New Advertising Opportunity

IEEE-HKN is the professional home to the world's top graduate students in electrical and computer engineering, computer science, and allied fields of interest. Get your company or university in front of these students and HKN's undergraduate students who are considering their next steps by advertising in a special section of *THE BRIDGE*. Click here for more information and rates.

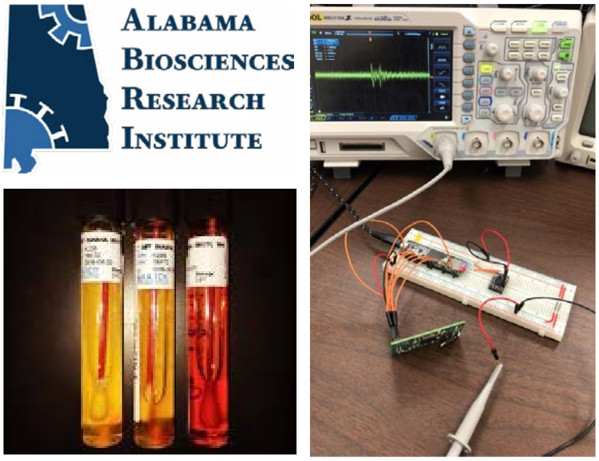
## Jonathan Swindell

Theta Eta
University of Alabama in Huntsville, Jump M.S. Student in Computer Engineering

### RESEARCH TOPIC

AI/ML quantitative assessment of cardiovascular disease using bioimpedance

The combination of my engineering and science research experiences, coupled with my industry experience, has prepared me for advanced graduate study that centers on interdisciplinary applications of machine learning in the biomedical engineering fields. As a co-founder of the Alabama Biosciences Research Institute, my contribution to previous research work in emergency medical services has led to important sanitization policy changes. I co-authored a follow-up Emergency Medical Services studying the Assessment of Prehospital Monitor/Defibrillators for Clostridioides difficile Contamination which was published in Cambridge University Press. In recognition of my peer-reviewed research, I was offered a research internship with DAAD RISE. Additionally, I am currently working to develop a wearable, continuous, real-time bioimpedance and activity monitoring embedded system for use in cardiovascular diagnosis. This project, in collaboration between ABRI and the University of Alabama in Huntsville, is a wonderful example of interdisciplinary work where I am applying computer engineering and biological concepts to develop an application that has the potential to provide real-time ambient intelligence to medical professionals and save patients' lives.



*Left to Right:. ABRI Logo, Positive MSRA Vials that Cased Sanitization Policy Changes, Real Time Wearable Bioimpedance Monitoring Embedded System*

**LEARN MORE**
https://www.researchgate.net/profile/Jonathan-Swindell

**CONTACT**
www.linkedin.com/in/000jonathan-swindell

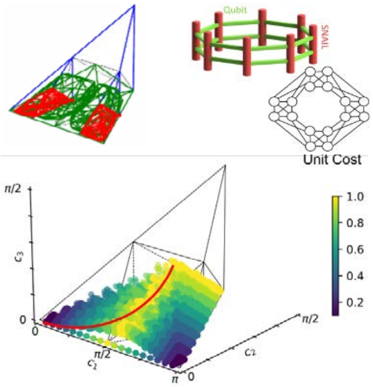
## Evan McKinney

Nu
University of Pittsburgh, Ph.D. Student in Computer Engineering

### RESEARCH TOPIC

Quantum Computing Hardware-Software Co-Design

We research the design of quantum computers for efficient and reliable operation. Our previous work has focused on the design of qubit coupling topologies for a reduction in data movement and an optimized selection of quantum instruction sets based on hardware speed limitations. Our designs utilize Superconducting Nonlinear Asymmetric Inductive eLement (SNAIL) modulators to enable high-degree couplings between qubits which support parallelized quantum circuit execution. First, we proposed a quantum hypercube-inspired "Corral" built from interconnected SNAILmodules.. The SNAIL natively implements a powerful family of gates realized through photon exchange operations; however, there is a practical speed limit that arises from the couplers' tolerance for strong driving when one or more pumps are applied. Second, we proposed a method for selecting the best ratio of parametric drives, considering both the theoretical computing power and practical speed limits for each gate naturally realized by the system. Our proposed parallel drive technique drives the modulator and qubits simultaneously, enabling a richer capability of two-qubit basis gates and potentially eliminating single-qubit drive duration costs. This research has the potential to improve the performance and reliability of quantum computers, especially for scaling devices past the NISQ era.



*Left to Right:. [smush_primative] Candidate Basis Gates from Parallel Drive visualized in the Weyl Chamber, [corral1] Corral SNAIL configuration and Qubit Coupling Topology, [coverage_set] Parallel Driven \sqrt{iSwap} Decomposition Coverage Spanning Regions*

**LEARN MORE**
https://scholar.google.com/citations?user=Qx3TAbkAAAAJ&hl=en&oi=ao

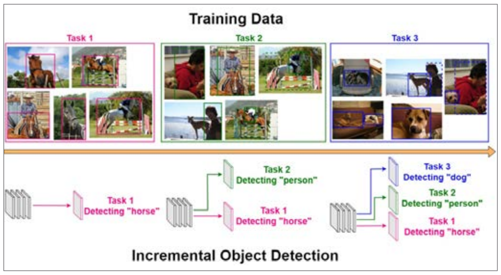
**CONTACT**
https://www.linkedin.com/in/evm9/

## Can Peng

Mu Kappa
The University of Queensland, Ph.D. Student in Computer Science

**RESEARCH TOPIC**
Computer Vision, Incremental Learning, Object Detection

Can pursued her Ph.D. at the University of Queensland (UQ). Prior to her Ph.D., she received her Bachelor in Electrical and Biomedical Engineering at UQ. Can's Ph.D. thesis explores incremental learning on image classification and object detection tasks. Image classification and object detection are significant tasks in the computer vision area and have been adopted in many real-life applications, such as autopilot, augmented reality, and mobile shopping. In the dynamic real world, new objects of interest might continually appear over time. Learning to detect and classify new objects incrementally in an accurate and timely manner is crucial in many application scenarios. Unfortunately, current deep learning networks are ill-equipped for handling incrementally appearing non-stationary data distributions. The purpose of Can's Ph.D. study is to tackle dynamic real-world scenarios and design effective incremental models that can continually learn new tasks without forgetting the previously learned knowledge. After graduating from UQ recently, she is interested in continuing to explore in the AI areas, especially in the lifelong learning and embodied AI area. Can joined the Queensland Chapter of the IEEE-HKN Society in 2021. During her Ph.D. life, besides the accumulation of academic aspects, by participating in various interesting activities hosted by the HKN chapter, she also strives to grow into an all-rounded person.



*An example of an incremental object detection task. Incremental learning tasks require the model to continually learn new tasks without forgetting the previously learned knowledge.*

**LEARN MORE**
https://scholar.google.com.au/citations?user=HmzYOu4AAAAJ&hl=en

## Foram Sanghavi

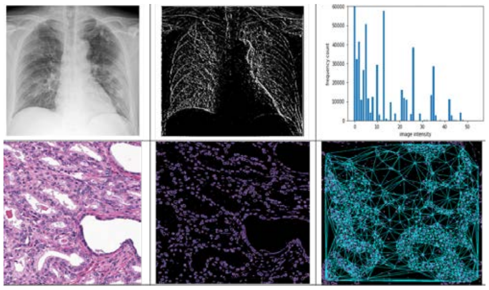
Epsilon Delta
Tufts University, Ph.D. Student in Electrical Engineering

### RESEARCH TOPIC

Artificial Intelligence based Disease Recognition Systems

Leveraging Artificial Intelligence concepts for effective disease prediction has always been the focal area of my research. The main aim of developing and deploying the AI model is to help radiologists/pathologists make quicker and more accurate disease predictions by overcoming human challenges that can affect diagnostic decisions. These challenges include fatigue, prediction and tissue staining variability, and visual or feature similarity between diseases. During my Ph.D., with my advisor, Dr. Karen Panetta, 2019 IEEE-HKN President, we are striving to develop tools for diagnosing diseases such as COVID-19, cervical, prostate, and breast cancer. My work centers on understanding the critical disease attributes such as textures, cell distribution, and morphologies essential for disease detection to develop different disease-diagnostic systems. This was achieved by developing different texture and morphology feature descriptors to extract complex critical information for better disease prediction. Our developed AI tools have demonstrated 98.44% sensitivity for distinguishing COVID-19 x-rays from viral pneumonia X-rays [1]. This was challenging for the radiologists to perform with the naked eye, as the symptoms and visual textures look very similar for both diseases in the images. Similarly, our system has been shown to deliver > 95% accuracy in predicting cervical and breast cancer tissue images.

[1] Panetta, Karen, et al. "Automated detection of COVID-19 cases on radiographs using shape-dependent Fibonacci-p patterns." IEEE Journal of Biomedical and Health Informatics 25.6 (2021): 1852-1863.



*The figure illustrates the different feature descriptors developed for different disease types. (Top-left) A Covid-19 chest x-ray (Top-middle) is a Shape-Dependent Fibonacci image, a texture feature descriptor image that extracts necessary disease information from lungs, and (Top-right) is a histogram of this image used for diagnosis. (Bottom left) is a Prostate Cancer biopsy image, (Bottom -middle) is cell segmented image from which texture, morphological and spatial information is extracted, and (Bottom-right) is a spatial graph constructed on the cell-segmented image from which spatial distribution features as obtained and used for classification.*

**LEARN MORE**
https://www.karenpanetta.com/lab-members

**CONTACT**
https://www.linkedin.com/in/foram-sanghavi-375507b0/

# IEEE-HKN Celebrates Outstanding Chapter Award Recipients!

The IEEE-HKN Outstanding Chapter Award (OCA) is a prestigious recognition of excellence in chapter administration and programs. The award, created by the IEEE-HKN Board of Governors, is based on the activities and descriptions of chapter programs documented in the Annual Chapter Report.

*The Sandia Mountains provided a beautiful background for the OCA Award Ceremony in New Mexico.*

The OCA committee considers various factors when determining recipients, with an emphasis on service activities towards the department, school, community, and chapter. Additionally, it is essential that the chapter promote IEEE-HKN's objectives by inducting eligible undergraduate and graduate students and faculty in the technical fields of interest designated by IEEE and participating in student chapter projects. The winning chapter reports are evaluated based on criteria that include enhancing professional development, improving instructional and institutional standards, fostering scholarship and creativity, providing public service, and advancing IEEE-HKN's established goals. With its members' high standards of scholarship and leadership qualities, each chapter has significant potential. The OCA is traditionally regarded as a prestigious honor due to the excellence of past winning chapters.

The 2021-2022 OCA was awarded to 21 IEEE-HKN chapters. Plaques were presented to the department chairs of the winning HKN chapters on Sunday, 19 March 2023 at the IEEE-HKN Awards Reception during the Electrical & Computer Engineering Department Heads Association (ECEDHA) Annual Conference, held in Albuquerque, New Mexico. Dr. Karen Panetta, 2019 IEEE-HKN President, represented HKN at the ceremony and was joined by students from Purdue University - Beta Chapter, University of North Texas - Lambda Zeta, and Arizona State University - Epsilon Beta Chapter.

### The 2021-2022 Outstanding Chapter Award Recipients are (listed Chapter, School):

- Beta, Purdue University
- Beta Epsilon, University of Michigan
- Beta Eta, North Carolina State University
- Beta Mu, Georgia Institute of Technology
- Delta, Illinois Institute of Technology
- Delta Omega, University of Hawaii, Manoa
- Epsilon, Pennsylvania State University
- Epsilon Beta, Arizona State University
- Epsilon Eta, Rose-Hulman Institute of Technology
- Epsilon Mu, University of Texas at Arlington
- Gamma Theta, Missouri University of Science and Technology
- Kappa Psi, University of California, San Diego
- Lambda Lambda, American University-Sharjah
- Lambda Zeta, University of North Texas
- Mu, University of California, Berkeley
- Mu Beta, Arab Academy For Science & Tech – Alexandria
- Mu Nu, Politecnico Di Torino
- Nu, Iowa State University
- Nu Alpha, Universidad Nacional De Educación A Distancia
- Sigma, Carnegie-Mellon University
- Zeta Iota, Clemson University

According to Nancy Ostin, HKN Director, *"the Outstanding Chapter Award recognizes the commitment HKN and our chapters have to community service. Last year, HKN Chapters performed over 100,000 hours of service and impacted many thousands of fellow students and members of their communities; this is what we recognize and celebrate."*

Thank you to ECEDHA for your support of HKN!

# Ashley Kuhnley – 2022 IEEE-HKN Outstanding Student Award Winner

*Dr. Karen Panetta, 2019 IEEE-HKN President presents the Outstanding Stude Award to Ashley Kuhnley of the Lambda Beta Chapter*

Being selected for the Outstanding Student Award is a great honor and emphasizes the advocacy I did in my department, college, and university on behalf of bettering students. There is a lot of power that students don't realize they have, and I was able to find areas within our academic environments that were affecting students in profound ways that I felt I had the motivation and capacity to help with. I did not do any of this alone, but with the support of faculty and fellow students. There will always be something to ameliorate, and it may feel like there aren't any changes being made because we're not at the university for long, but everything you do does make a difference. IEEE-HKN and my department helped me hold our college administration accountable when we, as students, felt our voices were diminishing.

Lambda Beta has been thrilled to be a part of the process and to continue working on the goals we set. The Lambda Beta advisors, Dr. Ramesh and Dr. Ashley Geng (our ECE department chair), have been instrumental in how both myself and our chapter have grown from reactivation in February of 2021 to now; our chapter is focused on helping students in high failure rate classes, guiding first generation students through the hidden curriculum, and aiding ECE and CS transfers in their transition to a four-year university, to name a few areas of need.

Everyone's university environment is different, which creates opportunities for students to support their communities in unique ways, and the Outstanding Student Award is a great way for chapters to recognize their members for that work.

### Honorable Mentions:

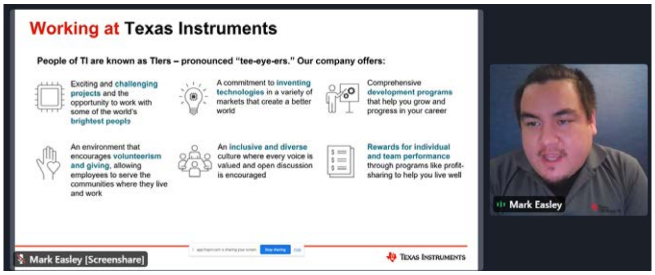
- **Ideal Ademaj** – Lambda Zeta Chapter, University of North Texas
- **Abdullah Hyder** – Iota Delta Chapter, Stevens Institute of Technology
- **Elanor Jackson** – Gamma Theta Chapter, Missouri University of Science and Technology
- **Sara Zayan** – Mu Beta Chapter, Arab Academy for Science, Technology, and Maritime Transport

*Ashley was presented with the award at the Electrical & Computer Engineering Department Heads Association meeting on March 19, 2023 in Albuquerque, NM.*

Senior Member
2023
Sampathkumar Veeraraghavan
Member #484B4E21
Boston Section
IEEE-HKN Member
Saifur Rahman
2023 IEEE President
VALUED MEMBER FOR 17 YEARS
VALUED THROUGH 31 DECEMBER 2023
IEEE
Advancing Technology for Humanity
www.ieee.org

# IEEE-HKN Pathways to Industry

IEEE-HKN Pathways to Industry brings together students and industry, young professionals and graduate schools, experts, and thought leaders to have critical discussions and present helpful information needed to prepare our future workforce. This two-day event, is filled with career coaching, professional development, technical discussions, and panels to addresses the questions and needs of students and young engineers as they make the decisions that will shape their future.



Working at Texas Instruments

People of TI are known as TIers – pronounced "tee-eye-ers." Our company offers:

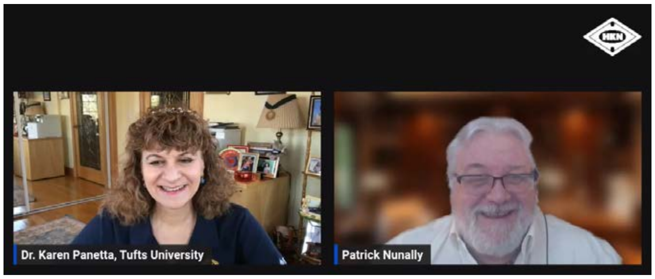
- Exciting and challenging projects and the opportunity to work with some of the world's brightest peopl॰
- A commitment to inventing technologies in a variety of markets that create a better world
- Comprehensive development programs that help you grow and progress in your career
- An environment that encourages volunteerism and giving, allowing employees to serve the communities where they live and work
- An inclusive and diverse culture where every voice is valued and open discussion is encouraged
- Rewards for individual and team performance through programs like profit-sharing to help you live well

*Mark Easley, Texas Instruments University Programs presents "How to Find and Rock Your Internship or Early Career"*

The 2023 Pathways to Industry featured keynote addresses by IEEE President-Elect and HKN member Tom Coughlin on IEEE–Your Professional Home, and by the father of the Arbitron Rating System and HKN member Dr. Patrick Nunally, inspiring students and young professionals about the opportunities to make their mark in tackling the technology challenges of their generation.

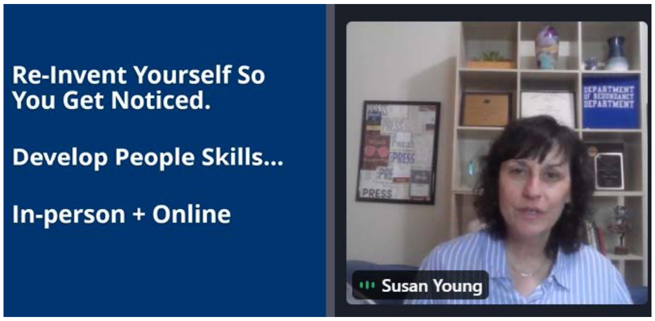
Over 350 people attended the 10 sessions, with topics ranging from "How to Find and Rock Your Internship and Early Career" to "Electrification of Transportation" and "Amplify Your Online Presence". Two days, 24 speakers, two keynotes and a recruitment fair with over 350 attendees. The HKN Board of Governors extended special invitations to development nations, making this a truly international event. Our recruitment fair produced a resume book of over 400 resumes, real-time interviews, and interactive booths that offered attendees a chance to interact directly with recruiters for internships and full-time positions for new graduates and experienced engineers as they look to advance their careers.

IEEE-HKN hosts two virtual conferences (Pathways to Industry and HKN TechX) during the year that are open to HKN and IEEE members. The annual HKN Student Leadership Conference, which is exclusive to HKN students and members, is held in person. Industry, graduate schools, and technical societies are welcome to sponsor and interact at our events. For more information, contact Nancy Ostin, n.ostin@ieee.org.



*Karen Panetta 2019 HKN President with Patrick Nunally "Father of the Arbitron Rating System"*

> "
>
> I want to take this opportunity also to thank you very much for Pathways to Industry. It was a fantastic event, and I was very happy to participate. Thank you, Nancy, Michael, Amy, Sylvie, and all who contributed; it was spectacular!"
>
> MATTEO, MU NU CHAPTER



Re-Invent Yourself So You Get Noticed.

Develop People Skills...

In-person + Online

*Amplify Your Online Presence to Build Your Confidence, Credibility, and Career by Susan Young, Sue Young Media*

# IEEE-HKN Welcomes New Professional Members to the Eta Chapter

## Region 9 Regional Meeting, Panama City, Panama

*R9 Professional Member Inductees with HKN President Sampath V.—and R9 Chair and HKN Professional & Graduate Committee Chair Enrique Tejera*

March 10, 2023

Sampath Veeraraghavan, 2023 IEEE-HKN President presides along with Region 9 Director and Chair IEEE-HKN Professional & Graduate Committee Chair, Enrique Tejera

Carlos Andres Lozano Garzon<br>
Carlos Medina<br>
Celia Shahnaz<br>
Diana Valadez<br>
Hector Poveda<br>
Ivan Armuelles<br>
Natalia Lopez<br>
Susana Lau<br>
Tania Quiel<br>
Yessica Saez

*HKN Region 9 inductees*

## SoutheastCon 2023, Region 3 Meeting

*Alessio Medda signs the signature book*

April 16, 2023

Jim Conrad, 2022 IEEE-HKN President presides, along with Enrique Tejera, IEEE-HKN Professional & Graduate Committee Chair and Bala Prasanna, member of the Professional Member Committee

Carrie Root

Alessio Medda

If you are interested in professional membership in IEEE-HKN, visit the website for information or email info@hkn.org.

*Enrique Tejera and Bala Prasanna present certificates to Carrie Root and Alession Medda*

*HKN members welcome the new professional members to the Eta Chapter*

# Congratulations to the Following HKN Chapters Celebrating Milestone Anniversaries in 2023!

If you were inducted into one of these chapters and would like to connect, please let us know! Once HKN...Always HKN! We are sure your chapter would love to hear from you.

| | | | Month | Day | Year | Anniversary # |
|---|---|---|---|---|---|---|
| Lambda Phi | Khalifa University | Abu Dhabi, UAE<br>(United Arab Emirates) | 3 | 13 | 2018 | 5 |
| Lambda Lamda | American University Sharjah | United Arab Emirates | 3 | 14 | 2018 | 5 |
| Beta Upsilon | University of Kentucky | Lexington, KY (Lexington) | 4 | 24 | 1948 | 75 |
| Zeta Lambda | Prairie View A&M<br>(University of Texas) | Prairie View, TX (Houston) | 4 | 3 | 1973 | 50 |
| Sigma | Carnegie-Mellon University | Pittsburgh, PA (Pittsburgh) | 5 | 19 | 1923 | 100 |
| Tau | University of Cincinnati | Cincinnati, OH (Cincinnati) | 5 | 26 | 1923 | 100 |
| Zeta Nu | University of Tulsa | Tulsa, OK (Tulsa) | 5 | 18 | 1973 | 50 |
| Lambda Rho | Tecnologico de Monterrey | Monterrey, NL (Mexico) | 5 | 21 | 2013 | 10 |
| Mu Sigma | National Chiao Tung University | | 5 | 17 | 2018 | 5 |
| Mu Tau | Waseda Univeristy | Tokyo | 7 | 25 | 2018 | 5 |
| Mu Phi | California Univ Of-Santa Cruz | Santa Cruz, CA (California) | 8 | 24 | 2018 | 5 |
| Beta Phi | University of Tennessee | Knoxville, TN (East Tennessee) | 12 | 11 | 1948 | 75 |

Please consider a gift to IEEE-HKN to help us sustain our honor society and traditions. If you would like to discuss ways you can support IEEE-HKN, please email Nancy Ostin n.ostin@ieee.org.

# 2023 IEEE-HKN Best Paper Award

The IEEE-HKN Best Student Paper Award is presented annually at the IEEE Region 3 Technical, Professional, and Student Conference, "SoutheastCon". The 2023 conference was held in Orlando, Florida, with the theme "Engineering the Magic!".

The primary and presenting author must be a student. Of the eight papers submitted, four finalists were selected. Each author presented their paper to a panel of four judges.

Ruchik Mishra: Toward Forecasting Engagement in Children with Autism Spectrum Disorders Using Social Robots and Deep Learning

Bishwas Praveen: An Effective Transfer Learning Based Landmark Detection Framework for UAV-Bases Arterial Imagery of Urban Landscapes

Mohammed Yousef Mousa Naser: Prediction of Model Breast Cancer Survival Months: a Machine Learning Approach

Marc Jean: A 30 GHz Steerable Patch Array Antenna for Software-Defined Radio Platforms

Marc Jean of the University of Central Florida was the winner. He received a $500 check from IEEE-HKN.

The IEEE-Eta Kappa Nu Best Student Paper Award was established by a generous donation by Dr. Hulya Kirkici and the IEEE Power Modulator Conference.

### A 30 GHz Steerable Patch Array Antenna for Software-Defined Radio Platforms

*Abstract*—We present the design and simulation of a beamsteering patch antenna array that operates at 30 GHz. The antenna design includes feeding lines needed for connection to a software-defined radio (SDR) platform. Phase differences on the feeding lines are minimal, and the impact of the feeding network on the gain is negligible at the operational frequency. Each patch element of the antenna has an associated 5-bit phase shifter, allowing fine granularity beam-forming capability out of the array. The simulation results show that the antenna attains very similar gain patterns to ideal ones.

# IEEE-HKN 2023 Student Leadership Conference Announcement

A big HOWDY to y'all! The IEEE-HKN Board of Governors is pleased to announce that the 2023 Student Leadership Conference (SLC) will be held in Houston, Texas, from Friday, November 3 to Sunday, November 5. Special thanks to the University of Houston Electrical and Computer Engineering Department for serving as our local hosts for this event.

The SLC is always a great experience for current AND future officers of IEEE-HKN Chapters. We will have plenty of opportunities for you to meet with fellow members from around the world and discuss success stories on planning and running activities. We will also have leadership development training, professional development sessions, and technology panels. Again, this year we are planning for a large exhibit hall with plenty of employers, universities, and IEEE societies present. Bring your resumes!

We will cap off Saturday night with our annual Awards Banquet. We are working on a special venue, so stay tuned for the details.

Below is our planned schedule of activities. Chapter participants should plan to check into the hotel by 3pm in order to participate in the hands-on technology activities. Participants should also schedule their departures later Sunday afternoon in order to participate in the region meetings; this is always a popular activity to share ideas and interact with your fellow officers.

So Chapters, start planning now! Through a generous donation from the Samueli Foundation, we will provide one hotel room for each chapter for the two nights of the conference, and we have greatly reduced the cost to attend. You will need to secure funding for transportation to Houston and for ground transportation in Houston (if needed).

## Student Leadership Conference Schedule

### Friday, November 3, 2023

- 1-4 pm - Arrival from all over the world!
- 4-6 pm – Hands-on workshops (Texas Instruments, RF signal "Fox Hunt", others)
- 7-8:30 pm – Welcome dinner and keynote address

### Saturday, November 4, 2023

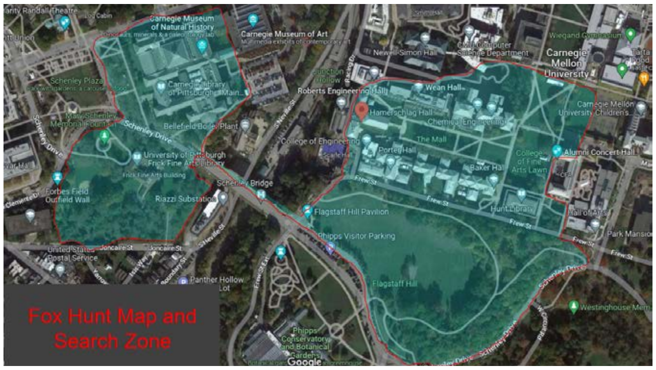
- 8-9 am – Breakfast and keynote address
- 9 am – 5:30 pm – Sessions on Leadership, Technology, and Professional Development. Lunch. Exhibit Hall open – HKN Recruitment Fair.
- 7-9 pm – Awards Banquet

### Sunday, November 5, 2023

- 8-9 am – Breakfast
- 9-11 pm – IEEE-HKN Region meetings
- 12 pm – Departure!

# HKN Spends a Day in Pittsburgh

IEEE-HKN is a community of communities that interact and learn from one another. Within the society, friendships are forged and collaborations are created. In February, three university chapters in Pennsylvania got together to do just that. Beta Delta Chapter of the University of Pittsburgh (Pitt), Epsilon Chapter of Pennsylvania State University (Penn State), and Sigma Chapter of Carnegie-Mellon (CMU) gathered in Pittsburgh for a day of social and technical activities. The HKN chapters also welcomed peers from their schools' IEEE Student Branches, IEEE Power & Energy Society and Power Electronics Society chapters, and Radio Clubs for this in-person event.



The day started with a gathering and a catered meal at Carnegie-Mellon. This was followed by a Keysight Technologies-sponsored interference Fox Hunt, where participants searched for signals originating from commercially available IoT devices. These devices were placed around the CMU and Pitt campuses, and teams competed to be the first to find the hidden transmitter. The day closed at Dave and Buster's for some fun arcade games.

This event not only brought members from different HKN chapters together, but also fostered connections between students from the same school who might not have otherwise met. Each chapter has seen increased member engagement in the time since their day in Pittsburgh. Sabrina Helbig, Beta Delta Chapter president, reflects, "Even within a month of the event, we're seeing some increased excitement… we're able to get our chapter's visibility out there a little bit more… it's exciting as a smaller chapter to gain some traction and momentum as a result of an event like this."

The effort it took to plan and execute the full day of activities is paying off in other ways, too. Epsilon Chapter president, Aaryan Patel said that the event "helped the Penn State chapter in increasing engagement and getting corporate contacts… and we were struggling with both these things before." Helbig touches on another positive outcome. She says that doing this enabled her chapter "to learn how to plan events of this scope, magnitude, and type and to collaborate… with other chapters."

It is the hope that HKN chapters seek and create opportunities like this, to meet fellow HKN members, and connect wherever possible. This inter-chapter and inter-club event was supported in part by the IEEE-HKN Student Chapter Support Initiative, which awards small grants to university chapters in good standing. All three chapters involved in the event applied for and received grant funds through this program to offset the costs of participation. The goal of the initiative is to fuel the innovation and ingenuity of IEEE-HKN, its chapters, and its members.

Royal Caribbean International
INDEPENDENCE of the SEAS

# The IEEE Computer Society – World's Largest Global Community of Computer Scientists and Engineers

### We Are the Largest Global Community of Computer Scientists and Engineers

The IEEE Computer Society (CS) is the trusted organization dedicated to engaging the engineers, scientists, academia, and industry professionals from across the globe driving continued advancements in computer science and technology.

### We Are the Preeminent Society for Knowledge-Sharing and Education in Computer Science and Engineering

- 189 International Conferences
- 29 Technical Communities
- Distinguished lectures monthly
- 654 Chapters and Student Chapters
- 3 Software Engineering Certifications
- Digital Library with 900k+ Resources
- Video Library featuring Supplemental and Conference Content

### We Are Leading the Developments and Advancements in the Fields of Computer Science and Engineering

- 49 Periodicals and Magazines
- Technical, Education, Service, and Student Awards
- Tech Trends and Predictions
- Free Topical Reports
- Career Guides
- Funding for Emerging Technologies Activities
- Technical and Career Building Webinars

### We Set the Standard for the Future

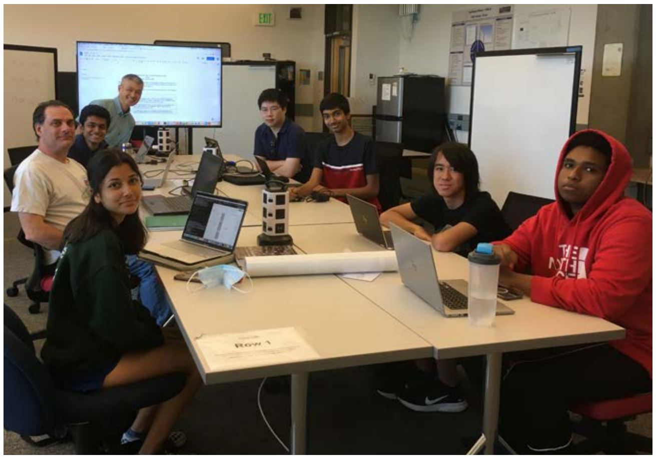
- Home to 217+ active technical standards
- Dedicated to diversity, equity, and inclusion throughout all programs and activities

### Get involved!

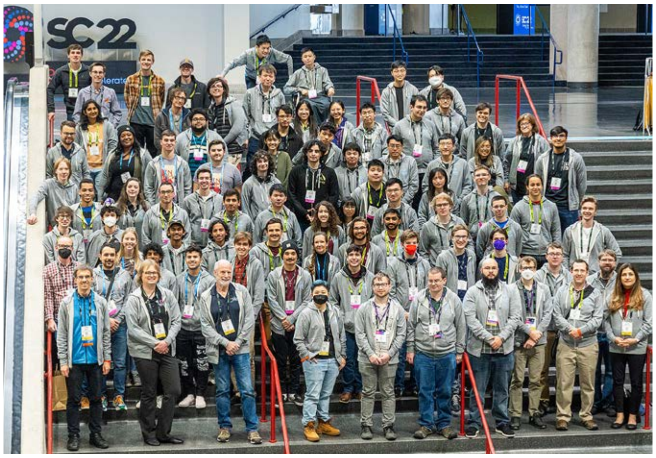
- Become a Member
- Publish a Paper
- Get Involved with your Local Chapter
- Join a Technical Community
- Nominate a Worthy Individual for an Award
- Volunteer

### Connect with CS

- Facebook
- Twitter
- LinkedIn
- YouTube
- Career Building Newsletters



*IEEE CS D&I Fund Activity - Summer High School Internship for BIPOC Students*



*SC22 Student Cluster Competition Participants*

# Cody Fan

Iota-Gamma Chapter, Grad Student/ Alumni Advisor

Cody Fan grew up in Cincinnati, Ohio, and is a proud fan of the Cincinnati Bengals. He received a Bachelor of Science in electrical engineering and a Bachelor of Science in physics at the University of California, Los Angeles, in 2022. He is a recipient of the NSF-Graduate Research Fellowship and is pursuing a Ph.D. in electrical engineering under the guidance of Professor Chee Wei Wong. Currently, his main research focus is to build quantum transducers between microwave and optical photons. He also has research interests in variational quantum algorithms, quantum communications, RF/microwave electronics, superconducting qubits, and silicon qubits. Previously, he worked on consensus algorithms for networks with of non-Gaussian distributions.

### Why did you choose to study the engineering field (or the particular field you are studying)?

I decided to choose quantum information due to its broad applications in other scientific fields. Quantum computers promise to speed up discoveries in carbon sequestration, protein folding, and material science. Quantum communications will improve the security of our communication infrastructure. These types of discoveries will help fight climate change, cure cancer, and create a better future for humanity. I chose to work on the hardware side of quantum information because I believe the main bottleneck in quantum technology lies with the limitations of hardware.

### What do you love about engineering?

I love that I get to solve complex problems on a daily basis, and the challenges that I face every day are different. Additionally, I also love the fact that the discoveries and inventions that I am working towards can change the world for the better.

### What don't you like about engineering?

There is a fair bit of administrative work that one must do while being an engineer, such as keeping track of equipment orders and filling out paperwork. However, I think this also exists in every job.

### What is your dream job?

My dream job is to work on math and science projects every single day.

### Whom do you admire (professionally and/or personally) and why?

I admire Michael Faraday, Sir Humphry Davy, and Marie Curie. Faraday was a self-taught scientist and came up with discoveries that made electrical engineering possible as a field (Faraday's Law, among other discoveries). He came from a less fortunate background and was taken under the wing of Sir Humphry Davy. I hope to be a mentor like Davey, and become a scientist like Faraday or Curie. Marie Curie won the Nobel Prize twice, and used the money to fund her own research institute. If I had a lot of money, I would also establish my own research institute to fund the projects of other scientists and engineers.

### In what direction do you think the engineering and other IEEE fields of interest are headed in the next 10 years?

A lot of money is being poured into the fields of artificial intelligence and quantum information. I think this trend will continue due to national security interests. There appears to be interesting work on both the hardware and software sides of things for both fields, with a resurgence in the field of analog IC design and analog computing towards improving AI.

### What is the most important thing you've learned in school?

Learning how to treat people with care and respect is more important than any technical skill that you can learn. Things like convex optimization and quantum mechanics can be learned by reading textbooks and are important (aside: I recommend Vandenberghe's textbooks for optimization and Griffiths' quantum mechanics), but soft skills like patience, clear communication, resilience, and hard work are more important to gain in comparison.

### What advice would you give to other students entering college and considering studying your major?

If you know you want to do STEM, don't give up. It is okay to fail, and sometimes that is even a good thing. There is an old Japanese proverb that says, "Fall seven times, get up eight". I think this is important as an engineer since many times, your first designs and ideas will fail (all of mine have), so it is important to not give up after the first few attempts (and often even beyond that!).

### Finish this sentence. "If I had more time, I would …"

Spend more time with family, friends, and loved ones.

# Sampathkumar Veeraraghavan

President, Brahmam Innovations Lab, USA
Global President, 2023 IEEE Eta Kappa Nu
Epsilon Delta Chapter

Sampathkumar Veeraraghavan is a globally renowned technologist best known for his technological innovations in addressing global humanitarian and sustainable development challenges. He is a seasoned technology leader in the computing and software industries and has spearheaded major technology and R/D programs at the top Fortune 500 companies. He is the founder and president of "The Brahmam," a humanitarian program that aims to deliver next-generation social innovations to achieve sustainable development goals and benefit marginalized communities globally. For close to two decades, Sampath spearheaded more than 20 global technology forums dedicated to advancing technology for the benefit of humanity. He has made significant leadership contributions to the social innovation field and the computing industry, which have had a broader impact on the marginalized communities.

Sampathkumar is the 2023 global president of the IEEE Eta Kappa Nu (IEEE-HKN). He served as the 2021-2022 HAC global chair and 2019-2020 IEEE SIGHT chair, leading the program to record-breaking growth globally through high-impact, technology-driven, sustainable programs benefiting members in more than 160 countries. He is credited with launching several novel global programs in the IEEE humanitarian engineering space, like SIGHT week, SIGHT day, SIGHT fund, and the Global HAC Summit. Sampath served as an expert in the 2020 Broadband Commission working group on school connectivity, co-chaired by UNESCO, UNICEF, and ITU. Sampath currently leads the global partnership efforts for the newly formed 2023 IEEE Humanitarian Technologies Board.

Sampath has been honored with numerous global awards for his leadership and technical excellence in delivering innovative technologies and global programs to address universal challenges. He has delivered over 500 invited talks at global technology forums, industry panels, and conferences around the globe. He currently works as a senior technology and program management leader in the conversational artificial intelligence industry.

*HKN President Sampath Veeraraghavan—with Michael Benson, Chair of the Chapter & Ritual Committee at SLC 2022*

### As the HKN president, what is your vision for HKN in 2023?

My vision and top priorities for IEEE-HKN members are to deliver an exceptional membership experience and address the key challenges faced by chapter leaders. To achieve this goal, the 2023 HKN BoG plans to launch a portfolio of highly impactful global programs that will promote career development, increase transnational networking opportunities, strengthen partnerships with industry and global organizations, and make IEEE-HKN one of the world's top trusted sources in technology and innovations. This year, the HKN BoG will focus on the following five top priorities:

1) Strengthen Chapters
2) Strengthen Committees
3) Building the Brand
4) Strengthen Collaboration and Partnerships
5) Scale up Development efforts

> “
> Today as a leading technologist, HKN’s core values and volunteer experience strongly shaped my vision and passion towards serving underserved communities globally.”

### Why did you choose to study the engineering field (or the field you studied)?

As a kid, science and math were my favorite subjects. As a student, I was fascinated with problem solving and applying my learned skills to solving real-world problems. During my high school years, I was exposed to computer programming and was thrilled to develop software applications. This motivated me to pursue a bachelor’s degree program in computer science and engineering from Anna University, India. After working in the computer industry in India for a few years, I pursued my Master of Science in electrical engineering from Tufts University, Massachusetts, in the USA, with a research focus on advanced computer vision technologies.

### What do you love about the industry?

As part of my journey in the industry, I enjoy solving complex technological problems and delivering innovative solutions that have broader positive impacts on end-users. Throughout my career, I have led business-critical strategic R & D programs and successfully delivered cutting-edge technologies in the areas of conversational artificial intelligence (AI), natural language understanding, cloud computing, data privacy, enterprise systems, infrastructure technologies, and assistive and sustainable technologies. Currently, I work in the area of conversational artificial intelligence, where I lead a portfolio of key strategic programs. It’s fascinating to work on complex technology programs and deliver solutions that touch the lives of millions of people.

### Have IEEE and HKN played a role in your career? How? What does IEEE mean to you?

IEEE-HKN has been an integral part of my professional and leadership journey. Throughout my career, IEEE and HKN provided a strong pathway to follow my passion in serving differently-abled children, impoverished students, and women in developing nations. Today, as a leading technologist, HKN’s core values and volunteer experience have strongly shaped my vision and passion for serving underserved communities globally. My journey with IEEE started as a student member involved in developing technological solutions to assist children with autism. As a student, IEEE helped me find mentors and like-minded people to guide my passion to serve underserved communities through technical solutions. As I grew in my career, IEEE-HKN provided me with opportunities to spearhead several major IEEE humanitarian programs and global committees in engineering and science, which enabled me to strengthen my leadership skills and expand on my professional network. It is amazing to work with key leaders from diverse cultures and technical backgrounds. Most recently, I served as the global chair of the IEEE Special Interest Group on Humanitarian (SIGHT) program (2019-2020) and IEEE Humanitarian Activities Committee (2021-2022), and led the programs to record-breaking growth and impact.

*HKN President Sampath Veeraraghavan with IEEE President (and HKN member) Saifur Rahman*

### What advice can you offer recent graduates entering the field?

Never give up on your dreams. Be persistent. IEEE-HKN offers a portfolio of global resources to equip yourself with the right skills and networking to become a global citizen. Find a mentor who can guide you toward your career aspirations. IEEE-HKN alumni are a strong network of great leaders from different domains and a great place to find your mentor. It’s always day one; keep learning new technologies in your field of expertise and having fun with what you do.

You can choose to directly support IEEE-HKN via the IEEE Foundation to one of the IEEE-HKN Funds: Chapter Support Initiative, including Chapter Support Grants and the "Passing the Gavel" officer training, and Student Leadership Conference. Invest in the next generation of HKN leaders!

# Susan K. (Kathy) Land

Program Manager, U.S. Missile Defense Agency, Eta Chapter

Susan K. (Kathy) Land is a program manager for the U.S. Department of Defense's Missile Defense Agency. She has more than 30 years of industry experience in the application of software engineering methodologies, the management of information systems, and the leadership of software development teams.

Kathy served as the 2021 IEEE president and CEO. In 2018, she served as vice president, IEEE Technical Activities. She was president of the IEEE Computer Society in 2009.

Kathy has been an active member of the IEEE Standards Association for more than 20 years and served as the Computer Society's vice president for standards in 2004. She was the recipient of the 2007 IEEE Standards Medallion.

An IEEE Fellow, and professional member of HKN, Kathy is the author and co-author of a number of texts and publications supporting software engineering principles and the practical application of software process methodologies. She is an IEEE Computer Society Richard E. Merwin Award recipient.

## Why did you choose to study the engineering field (or the field you studied)?

My professional background is a bit different from most of HKN inducted as students. My induction into HKN was as a professional member later in my career. It is important for people to understand that IEEE brings together and welcomes to membership not only engineers but also technologists from the fields of computer sciences and information technology, physical science, biological and medical science, mathematics, technical communications, education, management, and law and policy.

When I started college in the 1980's, presenting an obvious aptitude in math and science, I was not encouraged to pursue engineering or science. In fact, the University of Georgia Department of Computer Science was established the year I graduated, in 1984. When I entered the work force, it was the 'wild, wild west' of computing. It was the advent of personal computing, team programming and the challenge was to keep up with an evolving and constantly changing technical landscape. It was an exciting and wonderful time to be a woman in technology, as opportunity was abundant.

The computer science landscape for women in the 1960s and 1970s was vastly different from that of 1980s. The pioneers of women in computing, the true groundbreakers, were relegated as second-class citizens, not receiving full credit for their contributions. Given the legacy of women in computer science, the biggest question for me personally was 'Why?' 'Why the field of computer science?' This was a new field, and I knew no one, male or female, in it. In addition, the examples of women in early computing were not very attractive. My answer is that in the 1980s and 1990s employers were willing and able to hire anyone, regardless of gender, who understood computing technology. Employers understood that this new and growing field was critical to their future success, and they were willing to hire based on performance rather than academic pedigree. I went into computer science, because of the equitable opportunities available and what looked like a promising career.

## Who do you admire, and why?

I admire individuals who say what they mean and who back up what they say. This is to say that I admire individuals who are ethical, possess integrity, are direct, and stick by their word. I cannot single out a specific individual; there are many, particularly within IEEE and HKN, who I admire.

## How has the engineering field changed since you entered it?

I am from the 'in-between' generation of technologists. Not there as an early pioneer, but along for the technical ride as things progressed dramatically through the 80s and 90s. In my field, programming languages and software engineering were progressing, and it was super important to keep up and stay current. This is why I am such a fan of the IEEE and the IEEE Computer Society. The IEEE has been crucial to my career success. I started my career when personal computing was just beginning. Look at the power of computing now – just think of all the computing power in the cell phones that we carry around. The changes have been dramatic.

### In what direction do you think the engineering and other IEEE fields of interest are headed in the next 10 years?

I am not sure, but to think about possible advances in the areas of green energy, if I were starting out right now, I would probably enter that field.

### What is the most important lesson you have learned during your time in the field?

The most important lesson for me has been to keep current. Technology is always advancing, and working in these fields, it is critical to keep up. Understanding the latest advances, so that you can apply them for yourself or your employer is critical to individual success.

### What advice can you offer recent graduates entering the field?

Pay attention to your soft skills. There is a joke, ‘How can you tell if an engineer is an extrovert?’… ‘They look at your shoes when they are speaking to you’. Most programmers and engineers are introverts, preferring to focus on their ‘inner worlds’. Interpersonal soft skills are important because they help us develop and foster strong working relationships; they contribute to increasing team and organizational productivity; and they are particularly important when working in fast-paced or constantly changing technical work environments.

Recent data I found backs this up: 72% of CEOs believe that soft skills are more important to the success of their business than hard skills; 94% of recruiters believe that soft skills outweigh experience; and 94% of recruiting professionals believe that an employee with stronger soft skills has a better chance of promotion to a leadership position (than an employee with more years of experience but with weaker soft skills).

This is where graduates should leverage IEEE and HKN. I can tell you without question that the technical information, leadership experience, and mentorship I gained through my volunteer activities with IEEE placed me in front of my work colleagues. I was promoted earlier, got better assignments, and got better raises. It is that simple. Employers recognize when you bring the excellence of IEEE and HKN into their organization. I would encourage recent graduates to stay engaged with IEEE. Sometimes it is hard to find opportunities for engagement. The IEEE Young Professionals launched a web portal last year to help with these connections. Visit the site at volunteer.ieee.org to explore and find an opportunity where you might connect.

*Kathy Land with Jim Conrad (2022 HKN President) at SLC 2019*

### What is your favorite Eta Kappa Nu memory?

I have had the privilege to attend the HKN Leadership Conference a couple of times. These are my favorite memories. The promise of the next generation is incredibly inspiring.

### Why do you support IEEE-HKN?

I support HKN because of its mission and purpose. This is somewhat more broad than what was originally conceived. HKN’s mission has grown from the original mission of helping engineering graduates find employment and gain footholds in their careers to the addition of assisting its members throughout their lives in becoming better professionals as well as better citizens. I am proud to be a member of IEEE and HKN. As a member of HKN, I am inspired when I see this purpose put into action by the peer advising, exam prep, mentoring and tutoring programs, and programming activities at each one of the over 250 HKN chapters across the globe.

### What are the greatest opportunities for IEEE-HKN over the next three years?

I think the greatest opportunities for IEEE-HKN remain in the areas of scholarship and leadership development.

# Cybersecurity – A Brief History

*Burt Dicht, Eta Chapter*

Growing up in a big city, it was second nature to lock the doors to our homes and our cars. So, I was surprised at times when visiting friends or family who lived in more rural areas that, when leaving home, they left their doors unlocked. Even though it was perceived to be safe, why not, in an abundance of caution, just lock your doors? There are bad players everywhere and protecting yourself, your family and property is a priority. That has made me think about the history of cybersecurity and how far we have come both in terms of threats and in our ability to protect our networks.

*Len Kleinrock (HKN Eminent Member) with the server used to send the first messages over the APRANET Oct 30, 1969*

I am dating myself, but I remember the days of AOL dialup. On a personal level, I don't think many people thought of internet security at that time. But it was becoming apparent that those with malicious and criminal intent saw opportunities to target both personal, business, and government networks. And today, cybersecurity is an essential part of doing business, protecting our data and assets and ensuring that everyday life functions, from hospitals, to airlines, to utilities–basically, everything we do.

The cybersecurity industry has grown tremendously since those AOL days, with estimated global spending to exceed $1.75 trillion through 2025 [1]. In 2004, spending was just $3.5 billion. This is also reflected in the number of information security analysts–the people whose job is to protect computer networks and systems. According to the Bureau of Labor Statistics, in the U.S. alone, growth through 2031 will be 35% faster than the average for all occupations [2].

With such a heavy investment and the critical need for these protections, it would be beneficial to look back and trace the history and development of cybersecurity. The origins go back to 1971, when computer researcher Bob Thomas developed packet switching networks for ARPANET, which was the internet's forerunner. His program, named Creeper, moved across the ARPANET's network and left a breadcrumb trail wherever it went. This was not a malicious program; you might refer to it as tagging. Ray Tomlinson, also a computer researcher, who is credited as the inventor of email (and for choosing the "@" sign for separating the user from the destination), developed a program to counter the Creeper. His "Reaper" program chased Creeper and deleted it. It was the first example of antivirus software.

The 1980s saw several high-profile attacks that included AT&T, the Los Alamos National Laboratory, and the National CSS. The terms "computer virus" and "trojan horse," were coined at that time. This was new territory for most companies, and protecting networks became a priority, with security becoming a major focus. As the use of computers for personal and business purposes expanded, several programmers are credited with creating the first commercial antivirus programs. In 1987, John McAfee founded his company, McAfee Associates and released its first program, VirusScan. In that same year, Andreas Lüning and Kai Figge of Germany released their first antivirus product for the Atari ST, which also saw the release of Ultimate Virus Killer in 1987 [3].

The 1990s saw a major shift as computer use expanded and people and companies went online. The threats from criminals and bad players had expanded exponentially. Infecting networks and stealing data presented a profit motive. With these threats, the cybersecurity industry grew. It was a constant give-and-take between hackers and security experts. Cybercriminals even invented the first anti anti-virus program to combat security programs. As protections increased, the use of a Secure Socket Layer (SSL) was put in place in 1995. Developed by Netscape, it was designed to protect activities like online purchases. This would later evolve into the Hypertext Transfer

Protocol Secure (HTTPS), which we always looked for as we surfed the net.

The 2000s saw massive growth in computer usage and online activities. Computers were commonplace both in homes and offices. That offered tremendous opportunities for cybercriminals. Like viruses in nature, computer viruses and other threats adapted and evolved. Viruses no longer needed to be downloaded; you could catch them just by going to a website. New threats emerged along with new terms like malware and ransomware. And the threat also increased as state-sponsored cyberattacks became commonplace.

To combat these threats, such as computer forensics, multi-factor authentication, network behavioral analysis (NBA), real-time protection, threat intelligence, updated automation, sandboxing, backup and mirroring, multi-vector attacks, social engineering, and web application firewalls. New technologies are one of the tools needed to address cyberattack threats. Also needed were talented individuals trained to address this new computer environment.

IEEE members trained in electrical engineering, computer engineering, and other associated fields have been involved from the start. But it was also apparent that university engineering education needed to be adapted and specialty programs to turn students into cybersecurity professionals needed to be developed. As these programs began to emerge in the 2010s, IEEE, through its work with ABET, began exploring the need to assess and accredit these emerging "cyber" protection programs. In 2014 a group of ABET volunteers participated in the Cyber Education Project and determined an accrediting program in what they termed the "Cyber Sciences" was warranted and necessary to ensure that students graduating were prepared to practice. In January 2016, IEEE established a committee to create ABET program criteria for "cybersecurity" engineering programs. And in March 2016, the CSAB (Computing Sciences Accreditation Board) established a committee to create ABET program criteria for "cybersecurity" computing programs [5]. These new criteria were approved by ABET in 2018.

Today, there are approximately 20 programs at the bachelor and associate's degree levels accredited by ABET and many more programs at colleges and universities around the world, reflecting the global nature of this need. Volunteer leaders in the IEEE Computer Society and IEEE Future Directions Committee, also recognizing the importance of focusing attention and resources on the needs of cybersecurity students and professionals, launched the IEEE Cybersecurity Initiative in 2014. And on the IEEE Learning Network today, professionals can find more than 30 courses related to cybersecurity.

Since the creation of the Creeper in 1971, both cybersecurity threats and protections have evolved. The danger remains high, so it is important that the cybersecurity industry continues to grow and stay ahead of potential threats. Highly trained information security analysts and new tools such as AI, machine learning, and other new technologies need to be developed. We need to make sure we lock our doors.

## References:

[1] D. Braue, (2021, Sept 10), "Global Cybersecurity Spending To Exceed $1.75 Trillion From 2021-2025," *Cybercrime Magazine*, https://cybersecurityventures.com/cybersecurity-spending-2021-2025/

[2] Bureau of Labor Statistics, (2022, Sept 8), Occupational Outlook Handbook, Information Security Analysts, https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

[3] V. Davies, (2021, Oct 4), "The History of Cybersecurity," *Cybermagazine.com*, https://cybermagazine.com/cyber-security/history-cybersecurity

[4] "History of Cyber Security," *Cyber-Security.degree*, https://cyber-security.degree/resources/history-of-cyber-security/

[5] S. Lingafelt, (2017, Nov 11), "The History and Development of a Cyber Security Program Criteria," ABET, https://www.abet.org/the-history-and-development-of-a-cyber-security-program-criteria/

## To Learn more:

IEEE Cybersecurity Initiative – https://cybersecurity.ieee.org/

IEEE Learning Network – https://iln.ieee.org/

ABET – https://www.abet.org/

**Burt Dicht** is a member of IEEE-HKN's *THE BRIDGE* Editorial Board and the former Director of Student and Academic Education Programs for the IEEE's Educational Activities Department. He is also a member of HKN's Eta Chapter.

# IEEE-Eta Kappa Nu Launches IEEE-HKN Career Center

IEEE-Eta Kappa Nu

LOG ON TODAY!

IEEE-Eta Kappa Nu is proud to announce its new IEEE-HKN Career Center–the premier resource to connect career opportunities with highly qualified engineering talent.

IEEE-HKN Career Center will allow you to:

**MANAGE YOUR CAREER:**

- Search and apply to more engineering jobs than in any other job bank.
- Upload your anonymous resume and allow employers to contact you through IEEE-HKN Career Center's messaging system.
- Set up job alerts specifying your skills, interests, and preferred location(s) to receive email notifications when a job is posted that matches your criteria.
- Access career resources and job searching tips and tools.
- Have your resume critiqued by a resume-writing expert.

**RECRUIT FOR OPEN POSITIONS:**

- Post your job in front of the most qualified group of Engineering talent in the industry.
- Promote your jobs directly to candidates via the exclusive Job Flash email.
- Search the anonymous resume database to find qualified candidates.
- Manage your posted jobs and applicant activity easily on this user-friendly site.

IEEE

ieee-hkn.careerwebsite.com