VOLUME 6 NUMBER 4
WINTER 2019

HDIAC JOURNAL

A Quarterly Publication of the Homeland Defense & Security Information Analysis Center

Protecting CRITICAL INFRASTRUCTURE in the DIGITAL AGE

HOMELAND DEFENSE & SECURITY
CRITICAL INFRASTRUCTURE PROTECTION
WEAPONS OF MASS DESTRUCTION
CBRN DEFENSE
BIOMETRICS
MEDICAL
CULTURAL STUDIES
ALTERNATIVE ENERGY

HDIAC Homeland Defense & Security Information Analysis Center

ABOUT THE HDIAC

The Homeland Defense & Security Information Analysis Center is one of three Department of Defense Information Analysis Centers. HDIAC is responsible for acquiring, analyzing, and disseminating relevant scientific and technical information – in each of its eight technical focus areas – in support of the DoD and U.S. government Research & Development activities.

OUR MISSION

The mission of the HDIAC is to provide users with focused expert technical consulting and unbiased scientific and technical information through in-depth analysis and the creation of specialized information products in support of the HDIAC's eight vital technical focus areas:

- Homeland Defense and Security (HD)
- Critical Infrastructure Protection (CIP)
- Weapons of Mass Destruction (WMD)
- Chemical, Biological, Radiological, and Nuclear Defense (CBRN)
- Biometrics (BIO)
- Medical (MED)
- Cultural Studies (CS)
- Alternative Energy (AE)

HOW WE CAN HELP

CORE ANALYSIS TASK (CAT) PROGRAM

PRE-COMPETED CONTRACT VEHICLE FOR SPECIALIZED TECHNICAL SUPPORT WITH EASY CONTRACT TERMS

- Work can begin in as little as six weeks
- Especially valuable for efforts that cross multiple technical focus areas
- Leverages an extensive SME network
- Draws from the most recent studies across the DoD

TECHNICAL INQUIRY SERVICE

FOUR FREE HOURS OF ANALYTICAL, SCIENTIFIC, AND PROFESSIONAL RESEARCH ACROSS OUR EIGHT TECHNICAL FOCUS AREAS

ADDITIONAL PRODUCTS

- Quarterly Technical Journal
- Weekly Homeland Defense Digest
- Monthly Online Webinars & Podcasts
- Analytical Tools & Techniques
- Bi-Annual State of the Art Report

Homeland Defense & Security
Information Analysis Center
www.hdiac.org

901 North Stuart Street, Ste 401
Arlington, VA 22203

266 Genesee Street
Utica, NY 13502

GETTING STARTED

Contact HDIAC at
1-877-363-7422 or info@hdiac.org

HDIAC is sponsored by the Defense Technical Information Center, DoD IAC Program, Attn: DTIC-I, 8725 John J. Kingman Rd., Fort Belvoir, VA 22060-6218

An archive of past HDIAC Journals are available at **https://www.hdiac.org/journal/.**

To unsubscribe from HDIAC Journal Mailings please email us at ***info@hdiac.org*** *and request that your address be removed from our distribution mailing database.*

ABOUT THE JOURNAL OF THE HOMELAND DEFENSE AND SECURITY INFORMATION ANALYSIS CENTER

ABOUT THIS PUBLICATION

The Journal of the Homeland Defense and Security Information Analysis Center is published quarterly by the Homeland Defense and Security Information Analysis Center (HDIAC). The HDIAC is a Department of Defense (DoD) Information Analysis Center (IAC) sponsored by the Defense Technical Information Center (DTIC) and operated by Quanterion Solutions Incorporated in Utica, NY.

Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the HDIAC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the HDIAC, and shall not be used for advertising or product endorsement purposes.

ARTICLE REPRODUCTION

Images and information presented in these articles may be reproduced as long as the following message is noted:

"This article was originally published in the HDIAC Journal of Homeland Defense and Security Volume 6, Number 4"

In addition to this print message, we ask that you notify HDIAC regarding any document that references any article appearing in the HDIAC Journal.

Requests for copies of the referenced journal may be submitted to the following address:

Homeland Defense and Security Information Analysis Center
901 N. Stuart St.
Suite 401
Arlington, VA 22203

Phone: 877-363-7422 / Fax: 315-732-3261 / E-mail: info@hdiac.org

COVER PHOTO

Cover Graphic Composite: Shelley Stottlar, Quanterion Solutions Inc., **Featuring U.S. Military Photos:** 140716-A-YG824-003 by Arkansas National Guard, 180214-N-GC347-082, U.S. Navy photo by Mass Communication Specialist 2nd Class Scott Swofford, and 190324-N-PX867-1409, U.S. Navy photo by Mass Communication 3rd Class Justin Whitley. **Featuring Deposit Photos Stock Images:** by TTstudio, vska, Rost9, marclschauer, and artjazz.

JOURNAL OF THE HOMELAND DEFENSE AND SECURITY INFORMATION ANALYSIS CENTER

Protecting Critical Infrastructure in the Digital Age

Message from the Director

It is my distinct privilege to serve as the Director of the Homeland Defense and Security Information Analysis Center (HDIAC) and as a part of the broader HDIAC community of practice. The DoD IACs play a key role in the Defense Technical Information Center's mission to rapidly, accurately, and reliably deliver the knowledge necessary to develop the next generation of technologies in support of the warfighter and help assure national security. As a Marine Corps veteran with over 27 years of service to our country, I am deeply dedicated to this mission and focused on leveraging the vast scientific and technical resources at our disposal to support the DoD Acquisition Enterprise and our young men and women who are in harm's way.

The mission of the HDIAC is to provide users with focused expert technical consulting and unbiased scientific and technical information through in-depth analysis and the creation of specialized information products in support of the HDIAC's eight vital technical focus areas: Homeland Defense and Security, Critical Infrastructure Protection, Weapons of Mass Destruction, Chemical, Biological, Radiological, and Nuclear Defense, Biometrics, Medical, Cultural Studies, and Alternative Energy.

I am proud to be a member of an HDIAC team comprised of leaders in academia and industry including Syracuse University's Institute for National Security and Counterterrorism; State University of New York Upstate Medical University; George Mason University; the National Renewable Energy Laboratory; Assured Information Security; and, the Guardian Centers of Georgia.

Our vision is to build the HDIAC into a government and industry-recognized DoD center of excellence, serving as the "first stop" for data/information on Homeland Defense and Security issues and positioning the Center as the hub for collection, analysis, and dissemination of HD-related scientific and technical data. This will be accomplished by implementing an extensive outreach program, fostering awareness of the HDIAC BCO mission and capabilities, providing timely responses to the HD community, and leveraging the synergy gained from interaction across the DoD IAC community.

DoD IACs are recognized as an essential resource to affordably deliver technical data and analysis in support of current operations and maximize the utility of DoD research and development dollars by collecting, synthesizing, and disseminating scientific and technical information to provide solutions to government requirements. We create news summaries, quarterly journals, monthly webinars, and bi-monthly video podcasts, as well as assessments and reports. We can also quickly answer technical inquiries at no cost to the user as well as provide a means for more in-depth support in the form of extended technical inquiries or core analysis tasks – bottom line, we want to meet your needs. If you are part of the scientific and technical community or simply a warfighter with a question, we are interested in hearing from you and want to bring you into our community. We look forward to working with you as we advance the HDIAC community of practice.

Steve Redifer
HDIAC Director

Photo Composite (top of page): Shelley Stottlar, Quanterion Solutions Inc., **Featuring U.S. Military Photos:** 140716-A-YG824-003 by Arkansas National Guard, 180214-N-GC347-082, U.S. Navy photo by Mass Communication Specialist 2nd Class Scott Swofford, 190324-N-PX867-1409, U.S. Navy photo by Mass Communication 3rd Class Justin Whitley, 151104-M-SB674-578, U.S. Marine Corps photo by Lance Cpl. Harley Thomas, 330-CFD-DA-SD-05-06192, U.S. Army photo by Sgt. Vernell Hall. **Featuring Stock Images:** by Deposit Photos/SergeyNivens, Freeimages.com/Aaron Cushing, PhotoDisc/Volume 39

CRITICAL INFRASTRUCTURE CYBERSECURITY

Public - Private Partnerships, and Defense Support of Civil Authorities (DSCA)

By: **Paul B. Losiewicz**, PhD, CSIAC Senior Scientific Advisor, **Daryl Haegley**, Director, Mission Assurance & Deterrence, Principal Cyber Advisor to SECDEF, Office of the Assistant Secretary of Defense for Homeland Defense and Global Security (OASD HD&GS), **Stephen Redifer**, Director, HDIAC, and **Aleksandra Scalco**, Engineer, Naval Information Warfare Center (NIWC) Atlantic

THIS ARTICLE ADDRESSES RECENT ACTIONS TAKEN TO IMPROVE CYBER DEFENSE AND RESILIENCE OF UNITED STATES AND DOD CRITICAL INFRASTRUCTURE (CI), SPECIFICALLY CRITICAL INFRASTRUCTURE CYBERSECURITY AND DEFENSE SUPPORT OF CIVIL AUTHORITIES (DSCA).

RECENT EVENTS OF 2017-2018 CLEARLY DEMONSTRATE THE SEVERITY OF THE THREAT TO CI AND HENCE TO NATIONAL SECURITY BY A CYBER-PHYSICAL SYSTEMS (CPS) ATTACK.

Continued on Next Page »»

Photo Credit: Deposit Photos/TTstudio & Deposit Photos/vska

The most salient point about Cyber-Physical Systems as opposed to traditional Information technology (IT) is that they operate in two domains: the information systems domain that enables communications, monitoring, recording and reporting, and the Control Systems (CS) domain that executes physical operational effects. The understanding of a particular CPS' maintenance procedures, protections, Indications and Warnings (I&W), and response and recovery procedures, require detailed technical information about, and operational insight into, these two separate domains concurrently, the cyber and the physical. However, there is huge variation across the sixteen Federally defined CI sectors [1], and the challenges to maintenance of a uniform level of cyber resilience for these systems are significant. As Critical Infrastructure straddles both sides of a base perimeter fence, public-private collaboration is inescapable. Understanding of requirements and capabilities on both sides of the DCI fence is key. We will review here some of the most recent actions and recommendations by the U.S. Government to reduce the threat to national CI CPS, with a focus on DoD actions to carry out cyber DSCA tasking with respect to CI found in the 2017-19 National Defense Authorization Acts (NDAA).

"...there is huge variation across the sixteen Federally defined CI sectors [1], and the challenges to maintenance of a uniform level of cyber resilience for these systems are significant."

A CATALYST FOR CHANGE – GENERAL ACCOUNTABILITY OFFICE (GAO) REPORT 16-332

"DoD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents."

According to the General Accountability Office (GAO) 16-332, DoD's role in addressing Cyber DSCA goes back to at least the DoD's 2013 *Strategy for Homeland Defense and Defense Support of Civil Authorities* [2]. In addition, Cyber DSCA was addressed in subsequent DoD Directives, policy statements and NDAAs, prior to the issuance of GAO 16-332 [3]. However, when GAO 16-332 was released, fundamental flaws were revealed by GAO in the potential execution by DoD of its Cyber DSCA policies. The report described a "lack of clarity on key roles and responsibilities — specifically for DoD components, the supported command, and the dual-status commander — to support civil authorities in a cyber incident" [4]. The primary conflict rested on the roles and authorities assigned to Geographic Combatant Commands such as U.S. Northern Command (USNORTHCOM), and Functional Combatant Commands such as U.S. Cyber Command (USCYBERCOM). As of January 2016, according to GAO, "DoD had not begun efforts to develop or issue updated guidance on how DoD will support civil authorities during a cyber incident and did not have an estimate on when the guidance will be finalized" [5].

GAO recommended that the Office of the Under Secretary of Defense (OUSD) for Policy "issue or update guidance that clarifies roles and responsibilities for relevant entities and officials — including the DoD components, supported and supporting commands, and dual-status commander — to support civil authorities as needed in a cyber incident"[6]. DoD went on record concurring with the recommendation.

Subsequent to the issuance of GAO 16-322, additional Congressional directives and DoD policies were issued addressing the Cyber DSCA role of DoD. Some of these directives and policies are examined in this paper.

HOUSE ENERGY AND COMMERCE COMMITTEE REPORT

The Oversight and Investigations Subcommittee of the House Energy and Commerce Committee released their December 7, 2018 *Cybersecurity Strategy Report* [1] after spending several years analyzing cybersecurity issues impacting the 16 Critical Infrastructure Sectors defined in Presidential Policy Directive 21 (PPD-21) *Critical Infrastructure Security and Resilience* [1]. They also reviewed the requirement for Improving cross-sector information sharing by the 16 PPD-21 Section 9 entities required under the subsequent Executive Order (EO) 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* [1]. In their report, the Oversight and Investigations Subcommittee established six priorities, two of which are addressed here, *widespread adoption of coordinated disclosure programs* and *strengthening of the public-private partnership model.*

THE 2018 DOD CYBER STRATEGY

Following issuance of EO 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, the DoD Cyber Strategy [3] also addressed defense of CI. The DoD Strategy focused on "cybersecurity risks facing the defense industrial base, including its supply chain, and United States military platforms, systems, networks, and capabilities". However, DSCA via public-private partnership by DoD was also extended:

> "The Department must defend its own networks, systems, and information from malicious cyber activity and be prepared to defend, when directed, those networks and systems operated by non-DoD Defense Critical Infrastructure (DCI) and Defense Industrial Base (DIB) entities".

> "The Department seeks to preempt, defeat, or deter malicious cyber activity targeting U.S. critical infrastructure

> that could cause a significant cyber incident regardless of whether that incident would impact DoD's warfighting readiness or capability. Our primary role in this homeland defense mission is to defend forward by leveraging our focus outward to stop threats before they reach their targets. The Department also provides public and private sector partners with indications and warning (I&W) of malicious cyber activity, in coordination with other Federal departments and agencies" [4].

The obvious intersection with the House Report is the strengthening of coordinated disclosure and public-private partnerships, as implied by defending non-DoD operated Defense Critical Infrastructure (DCI) and DIB entities, and providing the private sector military I&W, as well as increased operational activity in Cyber DSCA. The strategy goes on to affirm that the DoD is the Critical Infrastructure "Sector Specific Agency (SSA) for the DIB and a business partner with the DIB and DCI". Additionally, as laid out in PPD-21, an SSA has clear responsibilities, which authorizes DoD increased interaction with, and oversight of, industry, including private utilities, local governments, and vendors providing DCI services.

NATIONAL DEFENSE AUTHORIZATION ACTS (NDAA)

Recent National Defense Authorization Acts (NDAA) have addressed the DoD role in cybersecurity of DCI as well as National CI and strengthening of corresponding public-private and multi-agency partnerships. [Note: During the intervening fiscal years the nomenclature used within DoD for cybersecurity of Control Systems (CS) had shifted, bifurcating into Facilities Related Control Systems (FRCS), formerly Operations Technology (OT), a key element of CI, and control systems found on military weapons platforms, which had been termed Platform Information Technology, or PIT]. Since the issuance of GAO 16-322, several NDAAs addressed Critical Infrastructure FRCS in detail. For example:

- DoD shall issue a joint training and certification standard for the protection of control systems for use by all cyber operations forces within the DoD [FY17 NDAA SEC. 1644]
- Initiate a pilot program under which the Secretary shall assess the feasibility and advisability of applying new, innovative methodologies or engineering approaches to improve the defense of control systems against cyber-attacks [FY17 NDAA SEC. 1650]
- Report the structural risks inherent in control systems and networks, assess the current vulnerabilities to cyber-attack initiated through Control Systems (CS)at DoD installations worldwide, proposes a common, Department-wide implementation plan to upgrade and improve the security of control systems, assess the extent to which existing DoD military construction regulations require the consideration of cybersecurity vulnerabilities and cyber risk. The effort is to employ the capabilities of the Army Corps of Engineers (USACE), the Naval Facilities Engineering Command (NAVFAC) and the Air Force Civil Engineer Center (AFCEC). F17 NDAA Report 114-255]
- The Secretary of Defense (SECDEF) shall make such changes to the cybersecurity scorecard as are necessary to ensure that the Secretary measures the progress of each element of the DoD in securing the Industrial Control Systems (ICS) of the Department against cyber threats, including such ICS as Supervisory Control and Data Acquisition (SCADA) systems, distributed control systems, programmable logic controllers, and platform information technology [FY18 NDAA SEC. 1639]
- SECDEF shall, in coordination with the Director of National Intelligence (DNI), the Secretary of Energy, and the Secretary of Homeland Security, submit to Congress a report identifying significant security risks to defense critical electric infrastructure posed by malicious cyber-enabled activities [FY18 NDAA SEC. 11604]

With respect to FRCS, the following was authorized in the 2019 NDAA:

- SECDEF shall designate one official to be responsible for matters relating to integrating cybersecurity and industrial control systems within the Department of Defense [FY19 NDAA SEC. 1643]

With respect to Critical Infrastructure Cyber DSCA, NDAA-19 required the following:

- A Tier 1 Exercise in Cyber DSCA by USCYBERCOM and USNORTHCOM

CRITICAL INFRASTRUCTURE SECTORS [1]

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater Systems

[NDAA-19 SEC. 1648]

- A pilot program in Modeling and Simulation for Cyber DSCA [NDAA-19 SEC. 1649]
- A pilot training program for Guard elements [NDAA-19 SEC. 1651]
- A study on use of Reserve elements for cyber civil support [NDAA-19 SEC. 1653]
- Immediate authorization for assignment of active duty military personnel to the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) [NDAA-19 SEC. 1650]

Section 1638, TIER 1 EXERCISE OF SUPPORT TO CIVIL AUTHORITIES FOR A CYBER INCIDENT, modifies the 2019 NDAA to extend the date of a cyber DSCA Tier 1 exercise to May 2020. [NDAA 2020 SEC.1638].

Section 5726, SECURING ENERGY INFRASTRUCTURE requires establishment of a 2-year control systems pilot program with the National Laboratories for implementation of critical infrastructure cybersecurity research of incidents that could reasonably result in catastrophic regional or national effects, for the purposes of—

(1) partnering with covered entities in the energy sector (including critical component manufacturers in the supply chain) that voluntarily participate in the Program to identify new classes of security vulnerabilities of the covered entities; and

(2) evaluating technology and standards, in partnership with covered entities, to isolate and defend industrial control systems of covered entities from security vulnerabilities and exploits in the most critical systems of the covered entities. [NDAA 2020 SEC. 5726]

PREVIOUS MODELING AND SIMULATION WITH DOD FOR CYBER DSCA: JACK VOLTAIC

Modeling and simulation actions pertaining to Cyber DSCA and CI had been done with DoD participation previously, notably *Jack Voltaic* [7], organized by the Army Cyber Institute (ACI) at West Point. Starting in 2016, *Jack Voltaic* (JV) employed the general exercise framework developed by DHS for tabletop exercises and has continued the exercise series to this day [8]. Of interest to potential DoD DSCA respondents is the extent of the public-private partnership model used in JV, which prominently features participation of the Critical Infrastructure Sector-based Information Sharing and Analysis Centers, or ISACs [9]. As we saw above, a stronger public-private partnership was a priority of the 2018 House Energy and Commerce Committee *Cybersecurity Strategy Report*. Takeaways from the JV series of exercises continue to include two items: the need for effective vertical and horizontal communications across all multi-agency responders, and the need for technical understanding of the operations of, and interactions between, multiple Critical Infrastructure sectors. This includes identifying the need for effective simulations down to the Programmable Logic Controllers (PLC) of a CS.

> *"Takeaways from the JV series of exercises continue to include two items: the need for effective vertical and horizontal communications across all multi-agency responders, and the need for technical understanding of the operations of, and interactions between, multiple Critical Infrastructure sectors."*

THE OUSD (P) NDAA 2019 SECTION 1649 TABLE TOP EXERCISE (TTX)

The Office of the Undersecretary of Defense for Policy (OUSD(P)) held a Table Top Exercise (TTX) on 7 August 2019 per direction provided under Section 1649 of the NDAA for Fiscal Year 2019, "Modeling and Simulation of Cyber Attacks on Critical Infrastructure to Improve Defense Support of Civil Authorities." The purpose of the TTX was to improve DoD's ability to respond to requests for DSCA in response to cyber incidents. The legacy of Jack Voltaic informed the OUSD (P) response to NDAA Sec 1649. The OUSD (P) TTX [10] was attended by nearly 50 participants representing the energy industry, state and local governments, the national laboratories (e.g. Sandia National Laboratories (SNL), Idaho National Laboratory (INL), and Pacific Northwest National Laboratory (PNNL)), and DoD laboratories (e.g. Johns Hopkins University Applied Physics Laboratory (JHU APL)), Federal departments and agencies (e.g., DHS, Federal Bureau of Investigation (FBI), Department of Energy (DOE), DoD), and DoD Components (e.g., OSD, the Joint Staff, USNORTHCOM, USINDOPACOM, and the National Guard Bureau [11]). The exercise was intended to:

- Examine coordination structures during a cyber incident;
- Identify thresholds for when Federal support might be required, and thresholds for when DoD capabilities might be required to augment other Federal Departments and Agencies;
- Identify potential gaps in processes or capabilities that might impede such activities.
- Explore the intersection of information sharing and the intersection of cyber and physical threats as they affect US critical infrastructure.
- Identify shortfalls in Federal, State, and local government and industry authorities to respond

to cyber incidents affecting Critical Infrastructure.

- Identify processes, procedures, roles, responsibilities and "red lines for coordination between government and industry in responding to a cascading event that affects multiple critical infrastructure sectors.
- Identify the means by which threat information is shared between critical infrastructure sectors when the effects of a cyber incident could have cascading impacts.

NDAA SEC 1649 TTX FINDINGS

Although the Federal Government itself was familiar with the mechanisms for sharing and integrating Federal interagency information and actions, State and local authorities were less clear on the Federal processes. DoD was also less attuned to the decision processes of non-Federal civilian agencies in order to understand when a member of a CI sector needed assistance. With respect to Cyber DSCA, there was also some concern about effectiveness of DHS and DoD coordination: "DHS' Cybersecurity and Infrastructure Security Agency (CISA) lacks the structure and the planners that exist in [the Federal Emergency Management Agency] (FEMA), which may hinder DHS' ability to plan, coordinate, and lead DHS cyber response. Several TTX participants felt that there may be an opportunity to mirror or connect with the existing Defense Coordinating Officers (DCO) who are currently located in the [FEMA] regions that are already established." [12]

It was identified that horizontally, i.e. across sectors and agencies, and vertically, i.e. within a sector's, private operators, local, state, and federal authorities, that there were only weakly defined "decision points" at which DSCA is to be invoked.

The need for decision support tools was also identified. Decision aids to correctly determine when and what DoD capabilities and resources should be mapped to the DSCA task were lacking. In addition, civil authorities needed more information on just what DoD resources are available. Such tools would help to apprise DoD of when use of its authorities are justified or, conversely, exceeded in their response, and thus adequately respond.

> *"The civil sector is often unaware of DoD capability, and thus does not know what to ask for."*

According to current Homeland Defense and Security Information Analysis Center (HDIAC) Director Steve Redifer, who attended the TTX for CSIAC, "as is frequently the case when the DoD develops concepts of support for the civil sector, a major hurdle is the establishment and understanding of civil sector capability gaps. The DoD asks the civil sector for its capability needs, and the civil sector responds by asking for a list of what capabilities DoD possesses; this has historically been a hurdle in all Humanitarian and Disaster Response (HADR) actions, and it was again at the TTX. The DoD provides support from its existing structure to respond to civilian capability needs — since there are few DoD organizations solely dedicated to civil support, DoD needs to understand civil requirements/shortfalls in order to repurpose what are essentially units optimized for OCONUS combat. The civil sector is often unaware of DoD capability, and thus does not know what to ask for. At the conclusion of the TTX, the civil sector agreed to survey its constituents for cyber response capability gaps, and the DoD agreed to look at producing summaries of its cyber capability" [13].

Effective knowledge of the impact to DoD of cyber physical events on national or local CI was also a weak point, due to the generally voluntary nature of the information shared by private industry within a sector or to an ISAC. There are both technical and administrative decision chains and information access constraints that need to be understood and made accessible to DoD components and industry in order to anticipate DSCA requests. This is not just to fulfill DSCA requirements, but to safeguard internal DoD operations as well, as DoD is also dependent on CI, and is implied by the 2018 Cyber Strategy tasking to protect DCI and the DIB.

With respect to DoD Component DSCA training, it was noted that "DoD has limited experience with Operational Technology (OT), and the civil representatives agreed that this would be important in order for DoD cyber operators to be of assistance during a crisis. The National Guard Bureau representative and the civil representatives highlighted past exercises (CYBER SHIELD) in which the industry had worked with Army cyber operators, instructing them on SCADA systems and providing insight into how OT is utilized; all agreed that this would be necessary knowledge for DoD cyber operators should they be asked to respond to attacks on civil infrastructure." [14] Given that DCI FRCS cybersecurity is required at DoD installations OCONUS, it is in the DoD's interest to train INCONUS active-duty personnel as well.

The purpose and result of the TTX was to carry out NDAA Sec 1649 requirements to improve DoD's ability to respond to requests for defense support of civil authorities (DSCA) in response to cyber incidents. The TTX was designed to address issues critical for DoD's long-term efforts to improve the means and mechanisms of providing DSCA in response to a cyber incident and will set the stage for future examinations of DSCA in connection with cyber incidents involving U.S. critical infrastructure. Subsequent exercises are in the planning phase, to include additional CI sectors.

COMPARISON OF THE FINDINGS OF AN ACTUAL CI SECTOR ATTACK TO THE EXERCISES

It will be instructive to compare the findings of the Colorado Department of Transportation (CDOT) Cyber Incident After Action Report (AAR) [15] to the findings of the above exercises. The CDOT ransomware attack of 2018 took down its internal network by use of a SamSam ransomware malware variant. Of concern, there was no "air-gap" between its IT and OT networks, just a firewall, which fortunately held. On Wednesday, 21 Feb, the Governor's Office of Information Technology (OIT) declared a security incident when the ransomware became active and infected approximately 150 servers and 2000 workstations.

The CDOT Cyber Incident did not culminate in a Cyber DSCA action, but a Colorado Army National Guard (COANG) cyber response team was activated by the governor, and a multi-agency Unified Command Group (UCG) was established within the State Emergency Operations Center. The UCG was later augmented with support from DHS, FBI, and FEMA. Only 80% of original service was restored by 23 March, a month later, due to subsequent reinfection.

FINDINGS OF THE COLORADO DEPARTMENT OF TRANSPORTATION (CDOT) AFTER ACTION REPORT (AAR)

The most significant deficiency was the lack of integration of a Cyber Incident Response procedure into the State Emergency Operations Plan. It is now being addressed, but the plan will need to be validated by modeling and simulation, and subsequent exercises with local and Federal agencies. The CDOT Continuity of Operations Plan (COOP) did not include a plan for continuing operations after a cyber incident had compromised state networks and servers. The previous assumption appears to have been that a COOP will simply require you to pick up your personnel and IT equipment and move them to a different location. This was identified for correction across all state departments. It was affirmed in the report that future cyber-attack responses *will* require external support from vendors, the National Guard and Federal assets. Pre-incident planning and coordination will help ensure the right support is provided and integrated as rapidly as possible to facilitate a cohesive response effort that leverages the capabilities of each asset. The need for exercises and improving coordinated disclosure: "The State must remain vigilant against future attacks by continuing to harden its networks, improving and rehearsing its cyber incident response plans and sharing information about this attack with stakeholders and partner agencies."

> *"The requirements by Congress in NDAA 19 for improvements in the Cyber Defense of Critical Infrastructure and the role of DoD in that protection via improvements in public-private partnerships, multi-agency communication and DSCA exercises is being carried out."*

CONCLUSION

The requirements by Congress in NDAA 19 for improvements in the Cyber Defense of Critical Infrastructure and the role of DoD in that protection via improvements in public-private partnerships, multi-agency communication and DSCA exercises is being carried out. The Office of the Undersecretary of Defense (OUSD) for Plans, in conjunction with multiple Federal, State, local and private entities have carried out exercises to validate existing procedures. The recent table top exercise in August 2019 has shown needs for improvements that will be addressed in future exercises. It remains to be seen whether all the conflicts in authorities identified by GAO have been addressed formally by DoD. The need for collection and dissemination of lessons learned to State, local and private actors also needs to be addressed. With respect to Cyber DSCA, collection and dissemination of technical information and lessons learned for the purpose of informing DoD agencies of DSCA-relevant incidents and operations needs to be specifically ensured by either DHS or DoD [16]. It bears repeating that the lessons learned from the CDOT attack included the observation that "future cyber response will require external support from vendors, the National Guard and federal assets. Pre-incident planning and coordination will help ensure the right support is provided and integrated as rapidly as possible to facilitate a cohesive response effort that leverages the capabilities of each asset". This means that multi-agency exercises need to continue and expand their scope to include multiple CI sectors. The exercises and subsequent information sharing will be essential to mitigate the effects of multisector, cascading effects on the national scale.

REFERENCES

[1] https://www.dhs.gov/cisa/critical-infrastructure-sectors

[2] https://www.gao.gov/products/GAO-16-332; p.1

[3] See DOD Directive 3025.18, ***Defense Support of Civil Authorities (DSCA)***; Joint Publication 3-28, ***Defense Support of Civil Authorities*** and the ***2015 DOD Cyber Strategy***.

[4] https://www.gao.gov/products/GAO-16-332; p.13

[5] ibid p.19

[6] Ibid p. 22

[7] https://cyber.army.mil/Research/Jack-Voltaic/

[8] https://cyber.army.mil/Portals/3/Documents/Jack-Voltaic/JV3_Concept.pdf?ver=2019-08-20-153840-527

[9] https://www.nationalisacs.org/

[10] NDAA Section 1649 After Action Report (AAR) is in publication. Contact CSIAC for publication status.

[11] Army Cyber Institute, ***Jack Voltaic*** organizer attended. Significant to GAO 16-332, two geographic COCOMs attended but USCYBERCOM did not.

[12] CSIAC Trip Report 7 Aug 2019, p3. Available from CSIAC on request.

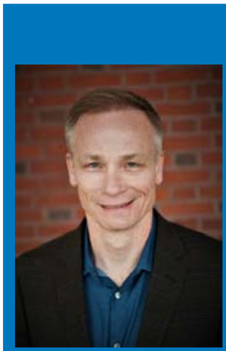
[13] Ibid p2.

[14] Ibid p3.

[15] CDOT Cyber Incident After-Action Report July 17, 2018, Colorado Division of Homeland Security and Emergency Management, Releasable to the Public; Report is available from CSIAC on request.

[16] The use of the DOD Information Analysis Centers to collect sector-specific DSCA relevant STI for archiving by DTIC is recommended.

ABOUT THE AUTHORS



MR. DARYL HAEGLEY is the Director, Cyberspace Mission Assurance and Deterrence in the Office of the Secretary of Defense, advising on cyberspace activities, cyber mission forces, and offensive and defensive cyber operations and missions. His distinguished career includes military, federal, civilian and commercial consulting experience. He oversees the strategic cybersecurity effort to protect the control systems and operational technology (OT) enabling the Department of Defense's (DoD) critical infrastructure. For the past six years, Mr. Haegley has brought awareness to the ever-increasing cyber threat to unprotected connected OT devices and has led the government to make change. Specifically, he has successfully advocated to change laws, DoD policy and standards, and academic curricula while initiating the first comprehensive facilities related control systems cybersecurity program of its kind within the federal government. He maintains four certifications, three Masters' degrees, two college tuitions & one patent.

DR. PAUL B. LOSIEWICZ is Senior Scientific Advisor for the Cybersecurity and Information Systems Information Analysis Center (CSIAC), a DoD information analysis center operated by Quanterion Solutions Incorporated for the Defense Technical Information Center (DTIC), Ft Belvoir, VA. He has over 30 years of DoD RDT&E experience, including R&D for Navy Special Warfare, Air Force Research Laboratory, Air Force Office of Scientific Research, and Office of Naval Research Global. Dr. Losiewicz has two patents. He recently presented "Data Sets for Autonomous Intelligent Cyber-defense Agent Research" at the 1st NATO-Industry workshop on Autonomous Cyber Defence, Cranfield University, as well as served on the NATO Research Task Group (RTG) IST-152 "Intelligent Autonomous Agents for Cyber Defense and Resilience."

MR. STEPHEN REDIFER is the Director of the Homeland Defense and Security Information Analysis Center. His experience includes emergency management, national security affairs, survivability/vulnerability, directed energy weapons, and space systems operations. Mr. Redifer served over 27 years in the U.S. Marine Corps, retiring at the rank of Colonel. During that time, he commanded the Marine Corps' Chemical-Biological Incident Response Force and Region 8 (Central Europe/Balkans), Marine Corps Embassy Security Group. His staff experience includes tours at Headquarters Marine Corps as well as serving in the office of the Director, Operational Test and Evaluation. Mr. Redifer's combat tours include Operation Restore Hope, Mogadishu, Somalia and Operation Iraqi Freedom, Fallujah, Iraq. Mr. Redifer holds an M.S. in Applied Physics and an M.S. in Space Systems Operations from the Naval Postgraduate School, a Master of Strategic Studies from the Air War College, and a Bachelor of Aerospace Engineering from Auburn University.

ALEKSANDRA SCALCO is an engineer with the Naval Information Warfare Center (NIWC) Atlantic. She is working towards a Systems Engineering Ph.D. at Colorado State University (CSU). Her research field is cyber resilience for Operational Technology (OT). She earned a Master's Degree in Engineering from Iowa State University in 2012, and a Master's Degree in Business Administration (MBA) in 2009. She is a member of the Defense Acquisition Corps in engineering. Ms. Scalco is Defense Acquisition Workforce Improvement Act (DAWIA) career certified Level 3 Engineering, Level 1 Science & Technology, and Level 1 Program Management. She holds ITIL Intermediate Certifications. Before joining NIWC Atlantic Ms. Scalco was a member of the National Security Agency (NSA) workforce as an Information System Security Designer (ISSD). As an ISSD, she provided technical expertise to clients on cyber assurance to advance the state of cybersecurity solutions to harden the National Security Enterprise against adversarial threats.

Bringing the Hospital to You: IMPLANTABLE NANO SENSORS

By: **Thomas J. Webster Ph.D.**, Art Zafiropoulo Chair and Professor, Department of Chemical Engineering, Northeastern University

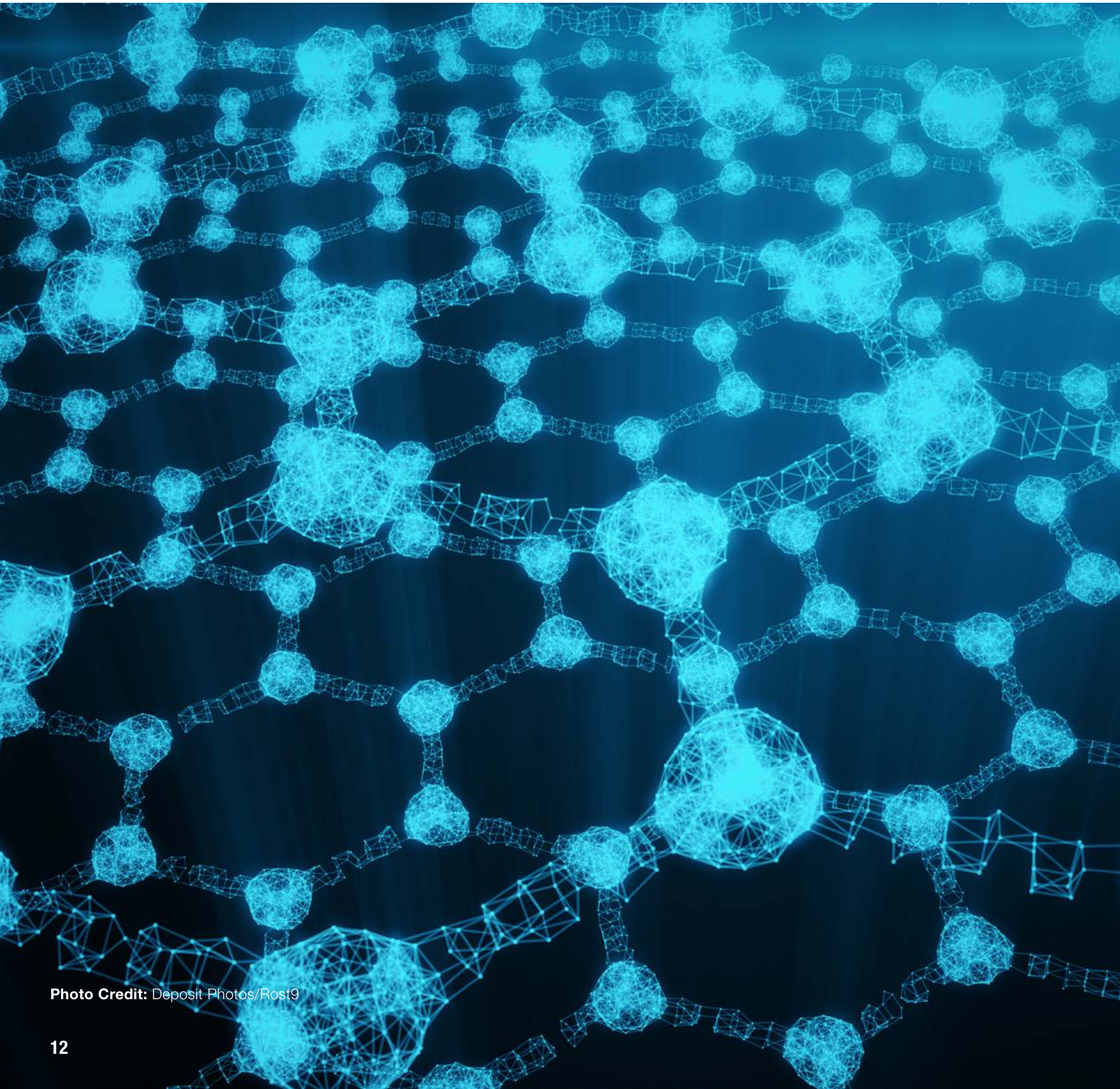


Photo Credit: Deposit Photos/Rost9

THE NEED

The average life expectancy in the U.S. barely increased this year, which alarmingly represents the first time it has even increased at all in four years. This is unlike some other highly industrialized countries in which life expectancy has been increasing steadily over the past four (and more) years. While there are numerous reasons for this, one is the extremely high barrier that exists for patients to even know they have a healthcare problem and, upon such a realization, make an appointment to see a doctor [1]. It is clear that we need to make healthcare more accessible, and bring the hospital to the patient, in order to reverse these disheartening trends in life expectancy.

The poor increase in life expectancy in the U.S. compared to the rest of the world is also indicative of a healthcare system that generalizes treatments instead of making them personal for that specific patient, relies too heavily on pharmaceutical agents to "fix" everything, is "reactive" rather than "proactive", and does not empower the patient to return to an active lifestyle after an injury. This is true for members of the military also, where a lack of empowerment after an injury often leads to a loss of motor activity, lack of feeling of contributing to the unit's mission after a significant injury, depression, and sometimes even a loss of life. As just one of many examples, consider a soldier with an orthopedic injury suffered on the battlefield which leads to insertion of an implant, recovery, and physical therapy. Alarmingly, soldiers suffering from a bone fracture will receive the same implant an elderly woman receives when falling down the stairs, yet, their needs and reason for an orthopedic implant are much different. If civilians and soldiers had more control over their health, for example, to both monitor possible disease or bone fractures, earlier intervention of healthcare problems would be possible which would clearly lead to people more engaged in their health and better healthcare outcomes. Think, for example, of a soldier on the battlefield who is able to detect a small hairline bone fracture (before pain), fix that fracture, and quickly return to their duties. This not only obviously aids in their physical abilities, but mentally, returns confidence, a feeling of contribution, and lifetime of service to our country. It would be a revolution in military medicine.

Nanomedicine, or the use of materials with nanometer dimensions, may provide the answer to all that ails our current impersonal healthcare system. Specifically, implantable nanosensors can essentially bring the hospital to inside a patient's body to better prevent, diagnose, and even treat a disease – all in one. The Defense Advanced Research Projects Agency has an extensive program to design and evaluate the use of implantable nanosensors that can detect healthcare problems before they even become healthcare problems [2]. While the idea is exciting and is destined to improve the quality and quantity of life for all who receive such an implantable nanosensor, developing implantable nanosensors is quite complex. One needs body-friendly materials, a sensor component, a method of communication, and, one that most people forget, a response mechanism to change adverse healthcare events after they are detected. It is also clear that implantable sensors involve many fields requiring not only strong technical expertise but also considerations for data security, data storage, and other factors involved when real time healthcare data can be collected every second of every day.   Imagine your neighbor logging into your nanosensor to monitor (and control) your health! Despite these challenges, if we want to improve our life expectancy and quality of life as we age, we need to move forward and create such implantable nanosensors, for which are already so close.

THE IDEA

So, let me describe my study team's idea to fabricate and use an implantable nano-

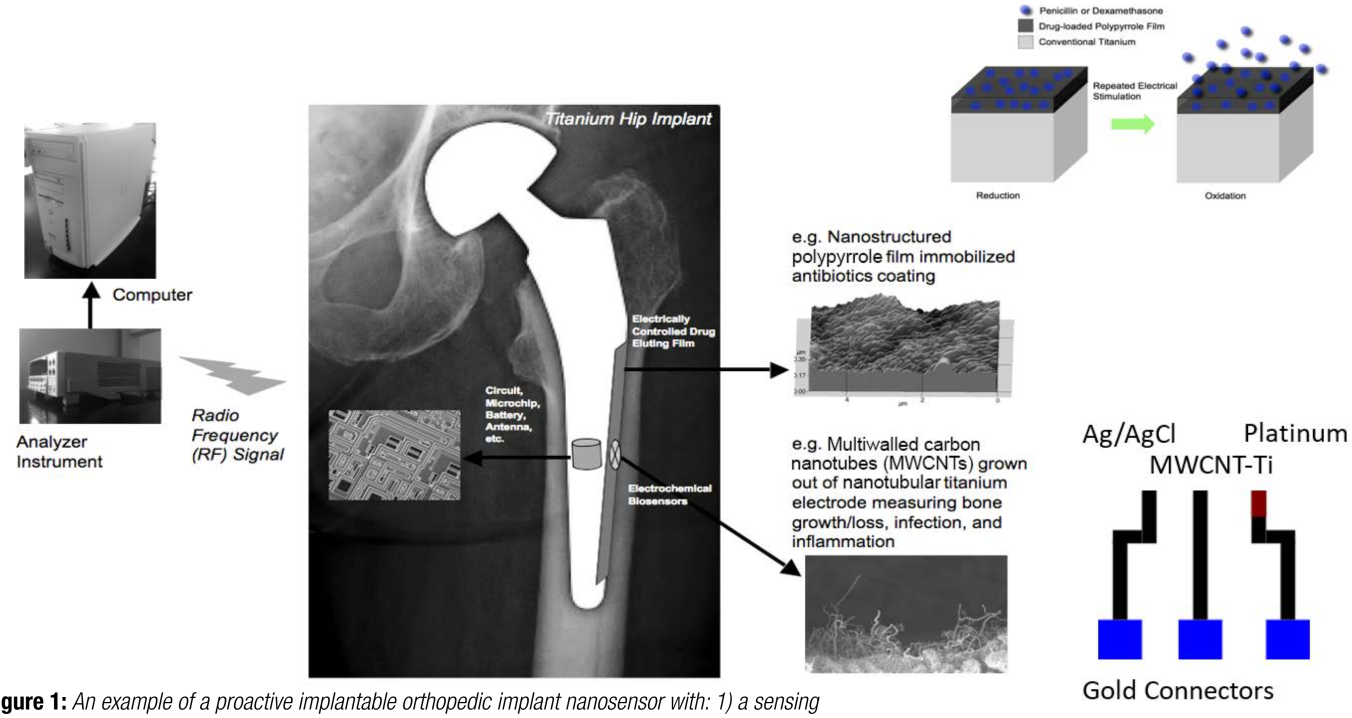

Penicillin or Dexamethasone
Drug-loaded Polypyrrole Film
Conventional Titanium
Repeated Electrical Stimulation
Reduction
Oxidation
Titanium Hip Implant
Computer
Analyzer Instrument
Radio Frequency (RF) Signal
Electrically Controlled Drug Eluting Film
Circuit, Microchip, Battery, Antenna, etc.
Electrochemical Biosensors
e.g. Nanostructured polypyrrole film immobilized antibiotics coating
e.g. Multiwalled carbon nanotubes (MWCNTs) grown out of nanotubular titanium electrode measuring bone growth/loss, infection, and inflammation
Ag/AgCl
Platinum
MWCNT-Ti
Gold Connectors

Figure 1: *An example of a proactive implantable orthopedic implant nanosensor with: 1) a sensing component based on carbon nanotubes grown out of an anodized nanoporous titanium implant, 2) a communication device dependent on radio frequency, and 3) a response component based on an on-demand degradable polymer which releases antibiotics, anti-inflammatory agents, and/or bone growth factors.*

sensor to improve medicine. While this example was tailored for orthopedics (specifically, hip implants), the idea is translatable to all of medicine. Back when developed, hip implants revolutionized medicine, but few advances have been made in their design and use since then and they represent a part of our healthcare system that "reacts" rather than "predicts" healthcare problems. For this project, in order to increase our chances for implementation into medicine, we started by buying off-the-shelf titanium-based implants. (By using current medical devices, we could provide for an easier transition into implantable nanosensors). We then followed an anodization process to create nanopores into the titanium implant. Then, using chemical vapor deposition (without toxic catalysts), we grew carbon nanotubes out of the now nanoporous titanium implant. First, nanopores in titanium were necessary in order to securely fix the carbon nanotubes into the titanium implant. Orthopedic implant surgeries are not gentle. Mechanical tests have shown that when using typical orthopedic surgical equipment, the carbon nanotubes only stayed in place, fixed in the titanium, when they were grown out of the nanopores. Secondly, carbon nanotubes are the sensing component of our sensor. As has been well established, carbon nanotubes are electrically active and can be used to measure electrical properties of the cells that attach and the tissue that has grown on the implant. Since osteoblasts, bacteria, and scar tissue forming cells have different electrical properties, it is the carbon nanotubes that enable our sensor to work. Specifically, we use cyclic voltammetry to determine cellular and tissue forming events around the implant once in the body.

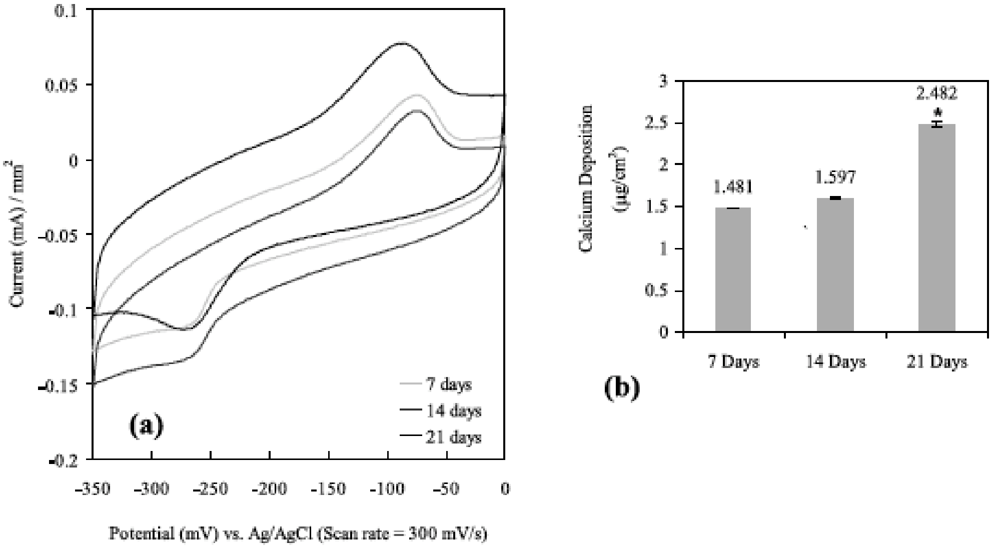


Figure 2: *a) A typical cyclic voltammagram demonstrating unique reduction and oxidation peaks indicating bone formation after 7, 14, and 21 days and b) the amount of calcium deposited next to an implant as assessed by calcium staining at each respective time confirming the trends measured by the sensor. Note: different reduction-oxidation peaks are observed for bacteria and inflammatory cells present next to an implant.*

Further, we have incorporated radio frequency technology (such as that currently used in pace-makers) for sensor communication to a hand held device. Lastly, we have created a new polymer, a combined form of poly-lactic acid and polypyrrole, which can be electrically activated to degrade to then release a drug (for example, and antibiotic, anti-inflammatory, or bone growth factor) necessary to ensure implant success. The polymer is incorporated onto the sensor surface yet still allows for the carbon nanotubes to protrude in order to assess cellular events. The sensor is picture in figure 1.

THE PERFORMANCE

Of course, one critical question for any implantable sensor used in medicine is whether the sensor is biocompatible (of which many are not) and can it still sense biological events once in the body. We have published numerous in vitro studies providing evidence that not only is this sensor biocompatible, but it actually promotes bone growth more than current titanium-based implants (even without sensing or responding to biological events) [3-7]. However, the proof always comes through in vivo studies.

Thus, we implanted the sensor (as mentioned above, with the polymer coating embedded with gentamicin, an antibiotic, in some portions and bone-morphogenic protein-7, a known bone forming agent, in other portions) into the calvaria of rats for up to 7 days and used our sensor as well as typical histological and push out test to assess device performance. We also pre-seeded the implant with 10^5 CFU of *Staph epidermidis*, a bacterium which commonly infects implants. First, we used cyclic voltammetry to determine what biological events were occurring. Initially, we saw reduction-oxidation peaks indicative of bacteria and released gentamicin from the polymer coating after 1 day which proved to kill the bacteria. We then released bone-morphogenic protein-7 to promote bone growth and quickly saw characteristic reduction-oxidation peaks indicative of bone which grew with time (Figure 2). This is in contract to the control titanium implant without a sensor which showed increase bacteria presence with time.

Traditional histology and push out tests matched the information we received from our sensor of greater bone growth and less bacteria on our implant with an embedded sensor compared to the control titanium without a sensor (Figure 3).

Now, imagine the real-world consequence of this implantable nanosensor for service members. Of course, bone fractures are a common healthcare problem for service members which may lead to implant surgery. Unfortunately, orthopedic implants fail too often due to infection and poor bone growth from a variety of reasons. But most importantly, few patients return to the active lifestyle they had before their catastrophic bone fracture. This type of implantable nanosensor can enable a service member to monitor, in real time, the success or failure of their implant. They can monitor the health of their bone next to an implant. They can observe whether bacteria have infiltrated the implant at pre-infection levels, and control the sensor to kill such bacteria and promote bone growth. This can be done anywhere and at any time to ensure a quick active return to the battlefield. And, this is just an example for orthopedics, think of the promise for any part of the body or healthcare problem that might exist.

THE FUTURE

Of course, such results imply an ability to detect implant failure well before what can be accomplished today with traditional X-rays, bone scans, or blood cultures for bacteria. By detecting implant failure earlier, success is likely especially in an approach like this in which biological events can be reversed without removing the implant. It is also hoped that over time, the sensor could determine if the implant separates from bone leading to failure. This is especially important for soldiers who are active on the battlefield and under high use. Such an implant is prone to additional fracture in the bone surrounding the implant. Further, while issues such as long-term power, data security, data storage, and others are still being explored, the present results of being able to detect cellular events around an orthopedic and change them on demand are quite promising to the future of healthcare.

Such sensors have also been incorporated into catheters, endotracheal tubes, vascular stents, neural probes, and others further expanding the role that implantable nanosensors will have in the future of medicine. In some of the most exciting future applications, such sensors are being incorporated into nanoparticles which can roam the body and send information concerning cell mutations, individual bacteria presence, the initial formation of blood clots and so much more at times and quantities much less than what is currently available with conventional methods. Think of the day when a soldier can monitor his or her own health, especially while deployed, rather than rely on a hospital. The possibilities are endless to improving healthcare. It is our hope that implantable nanosensors have a very bright future for military medicine, and also to hopefully one day reverse current poor increases in U.S. life expectancy.

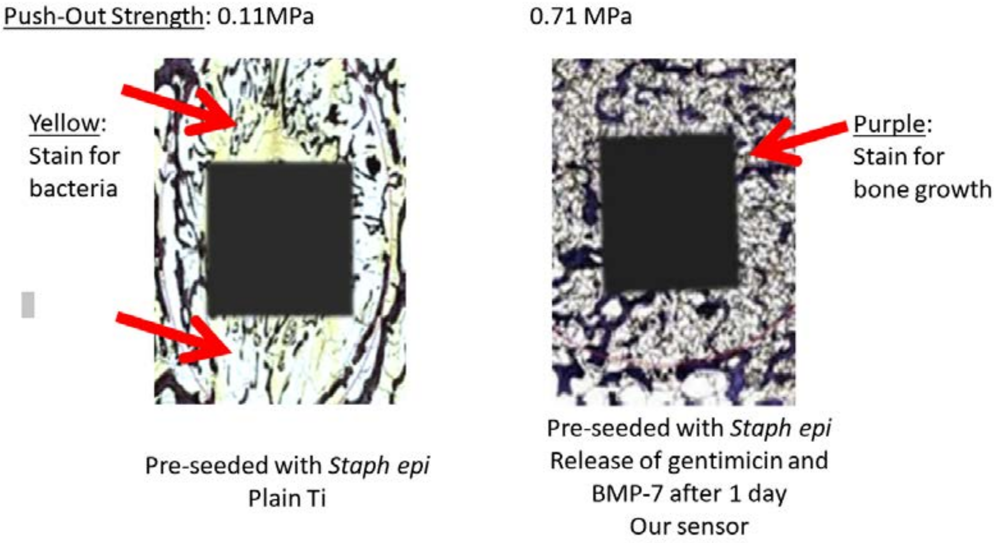

Push-Out Strength: 0.11MPa
0.71 MPa
Yellow: Stain for bacteria
Purple: Stain for bone growth
Pre-seeded with Staph epi
Plain Ti
Pre-seeded with Staph epi
Release of gentimicin and BMP-7 after 1 day
Our sensor

Figure 3: *Histology sections of the in vivo confirmation of our sensor function and promoted bone growth when a titanium implant with sensor was preseeded with 10^5 CFU of* ***Staph epi*** *(right) compared to titanium controls without a sensor (left). Bacteria = yellow and bone = purple. Implants were inserted into rat calvaria for 7 days and gentimicin (an antiobitic) and bone morphogenic protein-7 (a bone growth factor) were control released after 1 day from a polymer coating on the sensor. Also listed above the histological images are standard push out strengths which show greater push out strengths for the titanium with the embedded sensor compared to the control titanium without a sensor.*

REFERENCES

[1] Sara Heath, “Top Challenges Impacting Patient Access to Healthcare,” accessed at https://patientengagementhit.com/news/top-challenges-impacting-patient-access-to-healthcare, September 13 (2019).\

[2] The Defense Advanced Research Projects Agency, “In Vivo Nanoplatforms (IVN),” accessed at https://www.darpa.mil/program/in-vivo-nanoplatforms, February 5 (2020).

[3] S. Sirivisoot and T.J. Webster, “Multiwalled carbon nanotubes ce electrochemical properties of titanium to determine in situ bone formation,” ***Nanotechnology*** 19(29): 295101-295113 (2008).

[4] S. Sirivisoot and T.J. Webster, “Is my implant working: Nanotechnology sensors for determining bone growth,” ***BoneZone®Online Magazine, Strategic Sourcing for the Orthopaedic Industry*** (2007).

[5] S. Sirivisoot, R. A. Pareta, and T. J. Webster, “Electrically-controlled penicillin/streptomycin release from nanostructured polypyrrole coated on titanium for orthopedic implants,” ***Solid State Phenomena*** 151: 197-202 (2009).

[6] S. Sirivisoot, T.J. Webster, “Nanotechnology enabled in situ orthopaedic sensors for personalized medicine,” ***Biomedical Applications of Smart Technologies***, 86: 40-50 (2013).

[7] S. Sirivisoot, T.J. Webster, “Nanotechnology-derived orthopedic implant sensors integrated microsystems,” ***International Journal of Nanomedicine*** 650-667 (2016).

ABOUT THE AUTHOR

THOMAS J. WEBSTER’S (H index: 90) degrees are in chemical engineering from the University of Pittsburgh (B.S., 1995) and in biomedical engineering from Rensselaer Polytechnic Institute (M.S., 1997; Ph.D., 2000). Prof. Webster has graduated/supervised over 189 graduate students and his lab group has generated over 700 peer reviewed articles, 13 textbooks, 68 book chapters, 276 invited presentations, 867 conference presentations, and 42 provisional or full patents. He has formed 12 companies who collectively have over 21 FDA approved medical products currently helping the lives of thousands. He is the founding editor-in-chief of the International Journal of Nanomedicine (pioneering the open-access format) and an associated editor of Nanomedicine: NBM. Prof. Webster is a fellow of over 8 societies. He has appeared on BBC, NBC, ABC, Fox News, the Weather Channel, the Discovery Channel, and the recent special ‘Year Million’ TV series on National Geographic talking about the future of medicine and science.

BIOINSPIRED STRUCTURAL ENERGY STORAGE FOR ROBOTICS

By: **Volkan Cecen, Ph.D.**, **Ahmet Emre**, and **Nicholas A. Kotov, Ph.D.**, University of Michigan

Photo Credit: Deposit Photos/Gorodenkoff

STRUCTURAL BATTERIES, I.E. THOSE THAT CAN PERFORM TWO FUNCTIONS AT THE SAME TIME – TO STORE CHARGE AND TO CARRY STRUCTURAL LOAD, ARE KNOWN TO EFFECTIVELY REDUCE TOTAL SYSTEM WEIGHT [1,2]. THIS IS A UNIVERSAL DESIGN IMPROVEMENT FOR ALL THE DEVICES THAT HAVE POTTERIES REGARDLESS OF THEIR SIZE- FROM ELECTRIC VEHICLES [3-8] TO AIRPLANES AND SATELLITES [4,5,8].

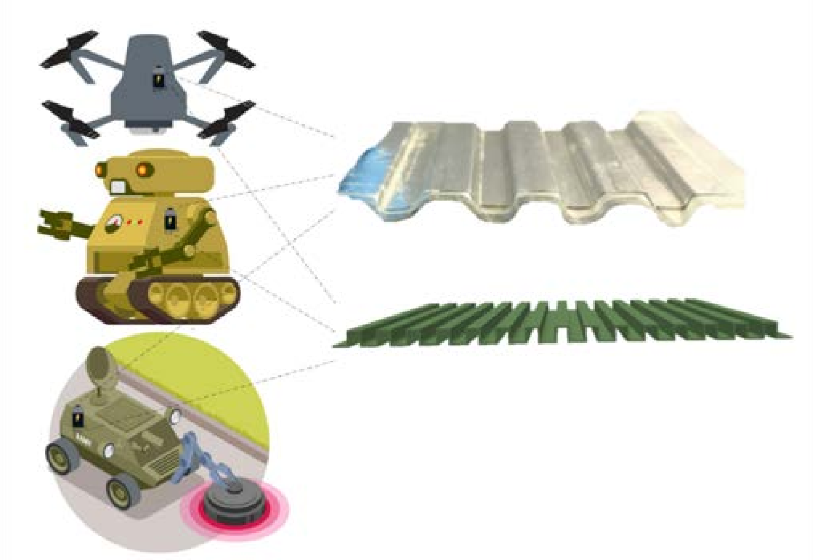


Figure 1: *Schematics of structural batteries in robotic devices.*

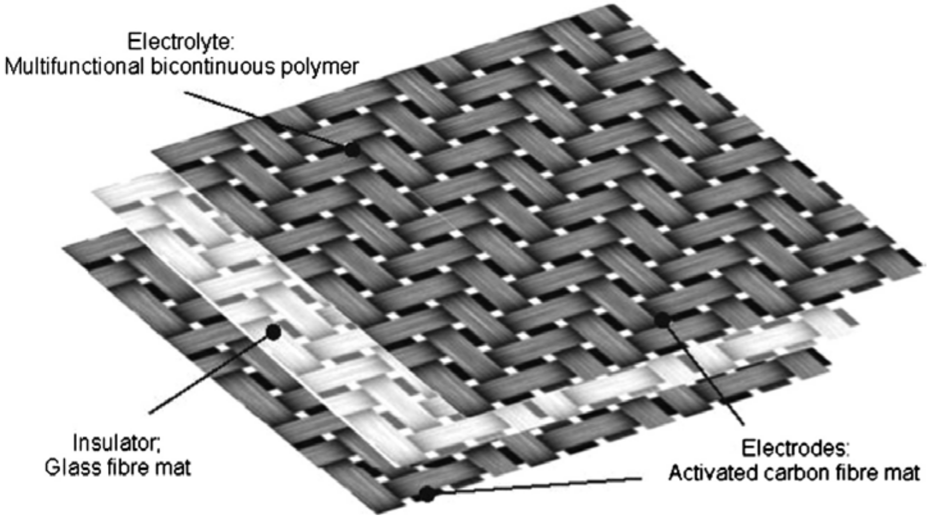

Electrolyte:
Multifunctional bicontinuous polymer
Insulator:
Glass fibre mat
Electrodes:
Activated carbon fibre mat

Figure 2: *Assembly of a structural supercapacitor. [18]*

For instance, combining the energy storage and load bearing functions makes possible weight reduction of an exemplary electrical vehicle by about 350 kg [3-8]. The U.S. Department of Defense (DoD) employs an increasingly sophisticated force of unmanned systems. On December 2007 Unmanned Systems Roadmap spanning 25 years was published that anticipated and projected a major shift toward greater reliance on unmanned vehicles in U.S. military operations [9,10]. The performance of all of them can benefit from the broad implementations of structural batteries and other structural power options that could be integrated in different load-bearing elements of the robotic devices from protective covers to radiator grids (Figure 1) and aerodynamic components. The need for structural batteries becomes obvious when one considers the technical challenges that robotic devices encounter in the military. For example, short flight duration is one of the main challenges of unmanned aerial vehicles (UAV) and utilization of the structural batteries can substantially improve this critical performance characteristic. Although the small lithium/polymer batteries are the best choice of power due to their capabilities to provide required high discharge current rate, most UAVs still have limited storage capacity, leading their limited flight time up to 30 minutes [11]. Initial assessments and flight tests indicate that structural batteries have the possibility to markedly extend the flight duration of UAVs and other aerial vehicles [12]. Further development of this technology can also be guided by the use of structural energy storage in biology and biomimetic design of some of the battery components.

For some time, efforts have been devoted worldwide to developing flexible, textile and stretchable energy storage devices such as supercapacitors and lithium ion batteries [13-18]. The team of researchers from Kungliga Tekniska Högskolan (KTH), Sweden successfully inserted Li ions in the carbon fiber. Their results suggested that the inserted ions created elastic strains in the fiber, which hence becomes pre-stressed in tension rather than causing irreversible damage to the carbon fiber [19]. The team of researchers from Imperial College London, United Kingdom, reported that a carbon fiber reinforced polymer composite can act as a supercapacitor whilst sustaining mechanical loads (Figure 2) with compressive moduli of up to 39 GPa and capacitances of up to 52 mF g^{-1} [18]. Here, we must underline the difference between energy and power density. Energy density indicates total energy stored in a given mass or volume

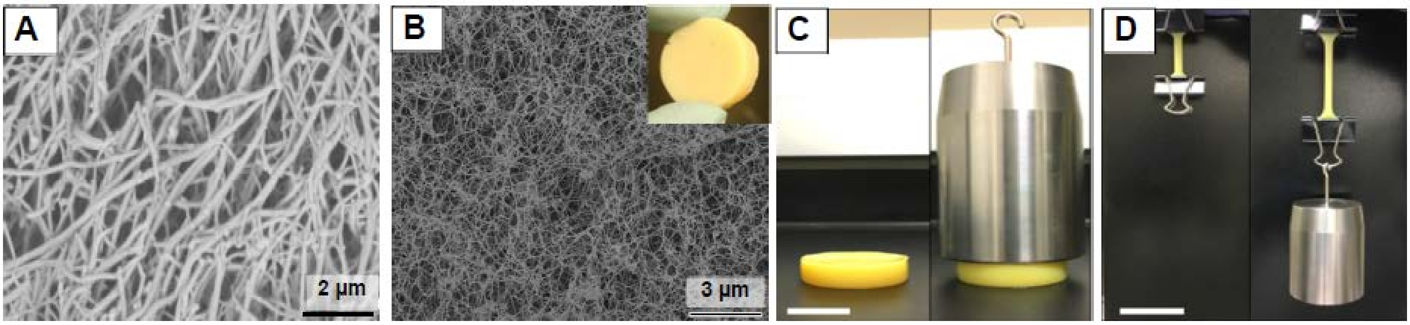


Figure 3: *Scanning electron microscopy (SEM) images of (**A**) cartilage (Dr. Nipun Chadha, Department of Biomedical Engineering, U. Rochester) and (**B**) 3D fibrous network from aramid nanofibers used in the inset. (**C**, **D**) Ion-conductive ANF nanocomposites under unusually large (**C**) compressive and (**D**) tensile stresses. [27]*

whereas power density shows how fast stored energy is released in a given mass or volume [20]. The latter is directly related to maximum current we can apply from a given mass. Though supercapacitors have high power density (W/kg), the insufficient energy density (Wh/kg) limits their applications; batteries possess significantly higher energy density [21].

However, structural batteries and other types of structural energy storage are not a part of current technological landscape devices because of the fundamental conflict between the ability of all material to carry load and transport charge [1]. The simultaneous attainment of high ionic conductivity and high stiffness [22,23] requires opposite structural requirements in materials. High density of permanent covalent bonds is required for load carrying, while dynamic labile ionic and coordination bonds typical for fluids are needed for fast charge transport.

The same is true for high mechanical strength and high ion intercalation capacity [24] – an equally important pair of properties for structural batteries. This clash of properties can be cumulatively described as the load bearing functionality requiring strong chemical bonds and dense robust materials, whereas charge transport and storage functionalities require weak chemical bonds and porous, deformable materials.

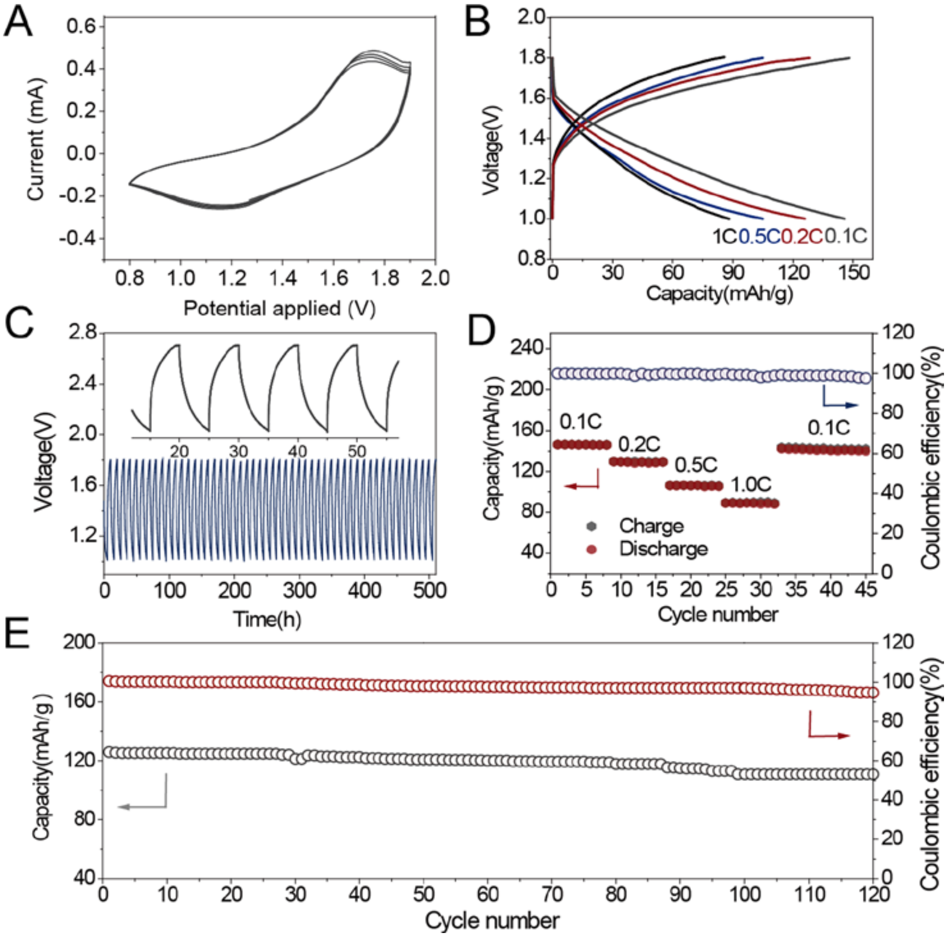


Figure 4: *(**A**) CVs of Zn/PZB-931/γ-MnO_2 battery scanned at 0.1 mVs–1. In cathodic scans, a peak at 1.2 V is attributed to the electrochemical intercalation of Zn^{2+} ions into γ-MnO_2. In anodic scans, a peak at 1.65 V is attributed to extraction of Zn^{2+} ions. CV curves remain unchanged after five cycles, demonstrating nearly ideal reversibility of the cathode material between Zn-rich and Zn-depleted states. (**B** and **D**) Galvanistatically charge and discharge curves and rate capability of the Zn/PZB-931/γ-MnO_2 battery cycling within the voltage range of 1–1.8 V at current density from 0.1 to 1.0 C (1 C = 150 mAg^{-1}). (**C**) Voltage–time curve for the Zn/PZB-931/γ-MnO_2 battery discharge and charge at 0.2 C. (**E**) Cycling performance of the Zn/PZB-931/γ-MnO_2 battery at 0.2 C. [12]*

Out-of-the-box approaches to engineering materials and devices as a whole are needed to resolve the fundamental bottleneck. It is a difficult but worthy task because the development of high capacity structural batteries without sacrificing their safety has far-reaching implications for global energy, the environment, and sustainability. For example, in UAVs the structural support around the batteries takes as much as twice the weight of a battery [25]. This additional weight imposes a high penalty on vehicle range and energy consumption [25]. Combining the load bearing and charge storage functions will, therefore, be the key factor determining flight duration for drones and other systems.

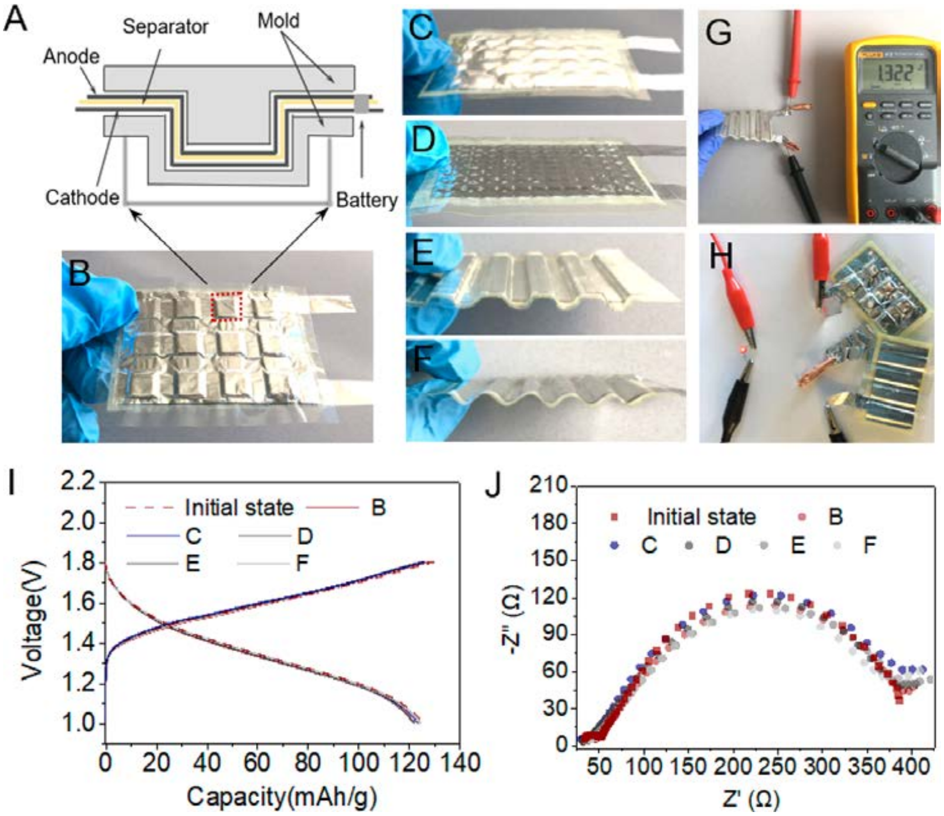


Figure 5: *(**A**) Schematic of the mold used for plastic deformation studies. (**B–F**) Different plastically deformed shapes of Zn battery with solid-state biomimetic electrolyte PZB-931. (**G**) Open-circuit voltage of Zn/PZB-931/γ-MnO_2 battery with square wave shape plastic deformation. (**H**) LED light powered by the two serial structural batteries. (**I**) Galvanostatic charge and discharge curves of Zn/PZB-931/γ-MnO_2 at 0.2 C for the corrugation batteries in B–F. (**J**) Comparison of EIS curves for original and plastically deformed corrugation batteries in B–F. No change in EIS can be observed even for high degree of plastic deformation as in (B), indicating high damage tolerance.[12]*

Looking ahead of the technological curve, structural batteries will determine energy-based, economic viability of future mobility technologies. Using UAVs as another example, reducing the weight of piloted commercial aircraft by 1 kg results in a savings of 30 tons of fuel per year [26], illustrating the necessity and impact of structural batteries in terms of environmental problems, climate change, energy sustainability, and national security. The fundamental materials bottleneck of structural batteries can be overcome by utilizing biomimetic engineering of naturally occurring nanocomposites. The once-believed "impossible" combination of high mechanical properties and fast ionic transport necessary for the electrolyte and cathode in, for instance, Zn and Mg batteries was realized by following materials engineering blueprints made by nature when designing living tissues that combine efficient transport of nutrients and high load bearing properties [12]. These tissues were optimized over millions of years of evolution and are exemplified by articular cartilage, canalicular bones, and the dentin of teeth. All these tissues have a common basic structural motif represented by porous three-dimensional (3D) network of stiff nanoscale fibers with 20–100 nm pores (Figure 3A) [27]. Abiotic replicas of such networks (Figure 3B) have been made from aramid nanofibers that retain the exceptional mechanical properties of their precursor - the iconic ultrastrong material Kevlar® (Figure 3 C,D). Similar to their biological prototypes they can be self-assembled from individual fibers and their production is scalable.

Taking advantage of aramid nanofibers, structural batteries with Zn metal anodes, solid state Zn^{2+}electrolytes, and mechanically robust cathodes intercalating Zn^{2+} ions. Rechargeable zinc ion batteries are expected to be more promising as textile power sources, owing to their combined advantages of high energy density, safety, and low cost [28-32]. Having theoretical energy densities similar to those of lithium-ion batteries [33,34], they are attractive as potential energy storage solutions for many applications.

We demonstrated that it is possible to engineer a solid Zn^{2+} electrolyte as a composite of aramid nanofibers. The high stiffness of the branched aramid nanofibers, BANF network combined with the high ionic conductivity of soft poly (ethylene oxide), PEO enable effective suppression of dendrites and fast Zn^{2+} transport. The cartilage inspired composite displays the ionic conductance 10× higher than the original polymer. The batteries constructed using the nanocomposite electrolyte are rechargeable and have Coulombic efficiency of 96–100% after 50–100 charge–discharge cycles (Figure 4).

Importantly, the metallic nature of the anodes simplifies acquisition of load-bearing capabilities [12]. High capacity rechargeable batteries with Zn metal anodes can be stamped into stiff corrugated shapes that can be fit to a specific load bearing profile (Figure 5). Zn batteries with PZB-931 were corrugated by molds (Figure 5A) with different "teeth" shaped as square (Figure 5B), half-sphere (Figure 5C), dot (Figure 5D), square wave (Figure 5E), or round wave (Figure 5F). These capabilities will open the door for numerous lightweight structural power applications. The battery voltage and capacity remained virtually unchanged, and its power showed no significant decay under a variety of deformation conditions and corrugated states. While plastic deformability has obvious limits, the constancy of the ionic conductivity spectra obtained by Electrochemical Impedance Spectroscopy (EIS) (Figure 5J) and galvanostatic charge and discharge (Figure 5I) for the studied range of deformations is remarkable.

Furthermore, the biomimetic solid-state electrolyte enables the batteries to

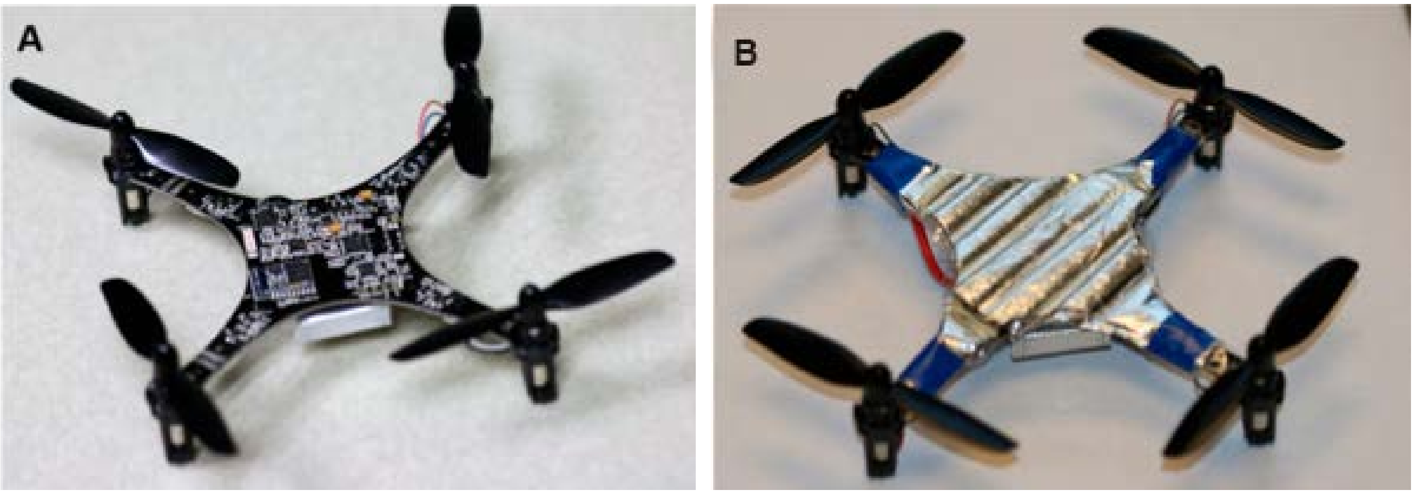


Figure 6: *(**A**) Tested UAV without cover. (**B**) Corrugated Zn/γ-MnO_2 battery pack as a replacement for the original device cover to supplement main power source of UAVs.[12]*

withstand not only elastic deformation during bending but also plastic deformation. This capability makes them resilient to different type of damage and enables shape modification of the assembled battery to improve the ability of the battery stack to carry a structural load. This property also suppresses formation of sharp zinc dendrites on the anode side and prevent any possible short circuit as a result of zinc metal penetration through separator during cycles. The corrugated structural batteries can be integrated into body elements of unmanned aerial vehicles as auxiliary charge storage devices (Figure 6). Taking advantage of the plastic deformability of these devices, we shaped them to replace covers of UAVs and enabled them to serve as auxiliary charge storage devices supplementing the main power source with lithium ion chemistry. The lightness of the auxiliary battery back afforded by the replacement of the liquid electrolyte with thin layers of dendrite suppressing BANF and PEO composite is essential for structural batteries in aerial vehicles. The practicality of structural batteries and significance of their shape versatility was demonstrated for several small drones of different types and power requirements. In all cases, we observed successful take off of the UAVs after their factory-installed covers were replaced with our corrugated batteries. Depending on capacity of UAVs own batteries and other parameters such as ambient temperature and size of UAVs, we calculated 5-27% of flight duration extension. The corrugated batteries were connected to the power circuits of the drones as secondary energy sources serving as structural components combining load-bearing and charge storage functions.

REFERENCES

[1] González, C., Vilatela, J. J., Molina-Aldareguía, J. M., Lopes, C. S. & LLorca, J. Structural composites for multifunctional applications: Current challenges and future trends. ***Prog. Mater.*** Sci. 89, 194–251 (2017).

[2] Ferreira, A. D. B. L., Nóvoa, P. R. O. & Marques, A. T. Multifunctional Material Systems: A state-of-the-art review. ***Compos. Struct.*** 151, 3–35 (2016).

[3] Asp, L. E., Leijonmarck, S. & Carlson, T. Realisation of Structural Battery Composite. ***20th Int. Conf. Compos. Mater.*** 19–24 (2015). doi:10.13140/RG.2.1.2029.1922

[4] Sairajan, K. K., Aglietti, G. S. & Mani, K. M. A review of multifunctional structure technology for aerospace applications. ***Acta Astronautica*** (2016). doi:10.1016/j.actaastro.2015.11.024

[5] Belvin, W. K., Watson, J. J. & Singhal, S. N. Structural Concepts and Materials for Lunar Exploration Habitats. ***Struct. Mater.*** 1–15 (2006). doi:10.2514/6.2006-7338

[6] Thomas, J. P. et al. Proceedings of IMECE ASME International Mechanical Engineering Congress. in 41512 1–4 (2003).

[7] Willgert, M. ***Solid Polymer Lithium-Ion Conducting Electrolytes for Structural Batteries.*** (2014). doi:978-91-7595-035-8

[8] Aglietti, G. S., Schwingshackl, C. W. & Roberts, S. C. Multifunctional structure technologies for satellite applications. ***Shock Vib. Dig.*** 39, 381–391 (2007).

[9] Office of the Secretary of Defence. Office of the Secretary of Defence Umanned Systems Roadmap 2007-2032. 19–20 (2007).

[10] Valavanis, K. P. & Vachtsevanos, G. J. ***Handbook of unmanned aerial vehicles. Handbook of Unmanned Aerial Vehicles*** (2015). doi:10.1007/978-90-481-9707-1

[11] Hassanalian, M. & Abdelkefi, A. Classifications, applications, and design challenges of drones: A review. ***Progress in Aerospace Sciences*** (2017). doi:10.1016/j.paerosci.2017.04.003

[12] Wang, M. et al. Biomimetic Solid-State Zn2+ Electrolyte for Corrugated Structural Batteries. ***ACS Nano*** (2019). doi:10.1021/acsnano.8b05068

[13] Liu, M. et al. Resist-Dyed Textile Alkaline Zn Microbatteries with Significantly Suppressed Zn Dendrite Growth. ***ACS Appl. Mater. Interfaces*** (2019). doi:10.1021/acsami.8b19825

[14] Asp, L. E. & Greenhalgh, E. S. Structural power composites. ***Composites Science and Technology*** (2014). doi:10.1016/j.compscitech.2014.06.020

[15] Ekstedt, S., Wysocki, M. & Asp, L. E. Structural batteries made from fibre reinforced composites. in ***Plastics, Rubber and Composites*** (2010). doi:10.1179/174328910X12647080902259

[16] Liu, P., Sherman, E. & Jacobsen, A. Design and fabrication of multifunctional structural batteries. J. ***Power Sources*** 189, 646–650 (2009).

[17] Yu, Y. et al. Co-continuous structural electrolytes based on ionic liquid, epoxy resin and organoclay: Effects of organoclay content. ***Mater. Des.*** 104, 126–133 (2016).

[18] Shirshova, N. et al. Structural composite supercapacitors. ***Compos. Part A Appl. Sci. Manuf.*** (2013). doi:10.1016/j.compositesa.2012.10.007

[19] Jacques, E., Hellqvist Kjell, M., Zenkert, D., Lindbergh, G. & Behm, M. Expansion of carbon fibres induced by lithium intercalation for structural electrode applications. ***Carbon N. Y.*** (2013). doi:10.1016/j.carbon.2013.03.015

[20] Aifantis, K. E., Hackney, S. A. & Kumar, R. V. ***High Energy Density Lithium Batteries: Materials, Engineering, Applications. High Energy Density Lithium Batteries: Materials, Engineering, Applications*** (2010). doi:10.1002/9783527630011

[21] Zeng, Y. et al. An Ultrastable and High-Performance Flexible Fiber-Shaped Ni–Zn Battery based on a Ni–NiO Heterostructured Nanosheet Cathode. ***Adv. Mater.*** (2017). doi:10.1002/adma.201702698

[22] Armand, M. Polymers with Ionic Conductivity. ***Advanced Materials*** 2, 278–286 (1990).

[23] Wang, Y. et al. Design principles for solid-state lithium superionic conductors. ***Nat. Mater.*** 14, 1026–1031 (2015).

[24] Jacques, E., H. Kjell, M., Zenkert, D. & Lindbergh, G. The effect of lithium-intercalation on the mechanical properties of carbon fibres. ***Carbon N.Y.*** 68, 725–733 (2014).

[25] Shiau, C. S. N., Samaras, C., Hauffe, R. & Michalek, J. J. Impact of battery weight and charging patterns on the economic and environmental benefits of plug-in hybrid vehicles. ***Energy Policy*** (2009). doi:10.1016/j.enpol.2009.02.040

[26] Steinegger, R. Fuel Economy as Function of Weight and Distance. ***Zürcher Fachhochschule*** 1–11 (2017).

[27] Xu, L., Zhao, X., Xu, C. & Kotov, N. A. Water-Rich Biomimetic Composites with Abiotic Self-Organizing Nanofiber Network. ***Adv. Mater.*** (2018). doi:10.1109/CEC.2008.4630985

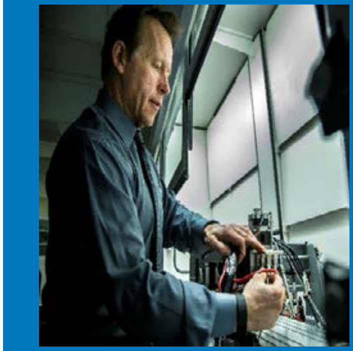
[28] Parker, J. F. et al. Rechargeable nickel-3D zinc batteries: An energy-dense, safer alternative to lithium-ion. ***Science (80-.).*** 356, 415–418 (2017).

[29] Xiao, X. et al. Fiber-based all-solid-state flexible supercapacitors for self-powered systems. ***ACS Nano*** (2012). doi:10.1021/nn303530k

ABOUT THE AUTHORS

Prof. **VOLKAN CECEN** received his Ph.D. degree in mechanical engineering from Dokuz Eylul University, Turkey, in 2006. After that he received a Humboldt Research Fellowship from the Alexander von Humboldt Foundation and worked at the Institute for Macromolecular Chemistry and Freiburg Material Research Center in Freiburg, Germany. Dr. Cecen joined as a visiting scholar in Professor Kotov's group in August 2018. His current research interests mainly include design of aramid nanofiber biomimetic composites and their application in electrochemical storage.

AHMET EMRE, MS is a PhD candidate in Biomedical Engineering under the guidance of Professor Nicholas Kotov at the University of Michigan. Prior to starting his graduate studies, he worked at Harvard-MIT Division of Health Science Technology as a research associate specialized in biomaterials and cell printing for tissue engineering. His current research focuses on fabrication, characterization and optimization of bioinspired polymer nanocomposites for energy storage applications. His work has been recently recognized by American Chemical Society and has been selected for Excellence in Graduate Polymer Research in 2019.



Prof. **NICHOLAS A. KOTOV** is working on conceptual foundations and technical realizations of biomimetic nanostructures. Examples of biomimetic nanostructures associated with his works include graphite oxide,- graphene- and clay-based layered biomimetic nanocomposites, chiral nanomaterials, and omnidispersible colloids. His contribution to technology include ultrastrong nacre-mimetic nanocomposites, soft neuro-prosthetic implants, 3D tissue replicas for drug-testing, chiral biosensors, and cartilage-like electrolytes for batteries. Prof. Kotov is a founder of several start-up companies that commercialized bioinspired nanomaterials for biomedical, energy, and automotive technologies.

[30] Ma, L. et al. Flexible waterproof rechargeable hybrid zinc batteries initiated by multifunctional oxygen vacancies-rich cobalt oxide. ***ACS Nano*** (2018). doi:10.1021/acsnano.8b04317

[31] Wang, R. et al. Nickel@Nickel Oxide Core–Shell Electrode with Significantly Boosted Reactivity for Ultrahigh-Energy and Stable Aqueous Ni–Zn Battery. ***Adv. Funct. Mater.*** (2018). doi:10.1002/adfm.201802157

[32] Zeng, Y. et al. Oxygen-Vacancy and Surface Modulation of Ultrathin Nickel Cobaltite Nanosheets as a High-Energy Cathode for Advanced Zn-Ion Batteries. ***Adv. Mater.*** (2018). doi:10.1002/adma.201802396

[33] Li, Y. & Dai, H. Recent advances in Zinc-air batteries. ***Chemical Society Reviews*** (2014). doi:10.1039/c4cs00015c

[34] Chen, X. et al. Ultrathin Co3O4 layers with large contact area on carbon fibers as high-performance electrode for flexible zinc–air battery integrated with flexible display. ***Adv. Energy Mater.*** 7, 1–11 (2017).

MORE SITUATIONAL AWARENESS FOR INDUSTRIAL CONTROL SYSTEMS (MOSAICS) JOINT CAPABILITY TECHNOLOGY DEMONSTRATION (JCTD):

A Concept Development for the Defense of Mission Critical Infrastructure

By: **Aleksandra. Scalco**, Naval Information Warfare Center – Atlantic, Data Science & Analytics Competency, Enterprise Data Science/Cyber Readiness, **Manan Jayswal**, JPM Prototype & Manufacturing, Inc., and **Dr. Steven Simske,** Colorado State University, Department of Systems Engineering

Aspects of this work are being used in fulfillment of the requirements for a Systems Engineering Ph.D. at Colorado State University

CYBER-PHYSICAL SYSTEMS OF MISSION-CRITICAL INFRASTRUCTURE ARE SUSCEPTIBLE TO CYBER-ATTACKS, SUCH AS RANSOMWARE ATTACKS DEPENDENCY ON VULNERABLE INFORMATION TECHNOLOGY (IT) AND INDUSTRIAL CONTROL SYSTEMS (ICS) OF CYBER-PHYSICAL SYSTEMS EQUATES TO AN INCREASED RISK OF THREAT EXPOSURE TO A CYBER-ATTACK.

Cyber-physical systems relate to mission-critical infrastructure systems affecting the physical environment, such as power, water, wastewater, safety controls. These systems have traditionally relied on physical security and necessary firewalls as access control. Cyber-physical systems have long technology refresh cycles of 20 years or more, which undermines the ability to address vulnerabilities with engineering upgrades. Extended refresh cycles present a complex system engineering challenge. There is an operational need for cyber defense capabilities to defend cyber-physical systems from cyber-attacks. Systems engineering principles were applied in the concept development of the Department of Defense (DoD) More Situational Awareness for Industrial Control Systems (MOSAICS) Joint Capability Technology Demonstration (JCTD) to convert operational needs into an engineering-oriented view for the development of a prototype.

THE 8-STAR LETTER

In February 2016, two four-star Admirals signed a letter identifying an operational need to defend the Department of Defense (DoD) mission-critical infrastructure. The letter subsequently was referred to as the "8-star letter" by a growing team of stakeholders. Sandia National Laboratories (Sandia) Critical Infrastructure Systems Department and the Naval Facilities Engineering Command (NAVFAC) Cybersecurity Technical Warrant Holder (TWH) responded in late 2016, with a concept to address the operational need by bringing the best of breed Department of Energy (DOE) Laboratory tools to the DoD, and named it "MOSAICS," or More Situational Awareness for Industrial Control Systems (MOSAICS) (Scalco, R., Waugaman, B, Lacoste, J., Andrews J., Beary B., Roley R, 2018) [1].

The MOSAICS capability concept was to automate the exiting procedures to detect, mitigate and recover from a cyberattack, combined with the best of breed technologies related to analytics, visualization, decision support, and information sharing.

Further system studies were performed that identified three initial MOSAICS capabilities: 1) an integration/operational capability to enable defense of control systems; 2) an ICS (Industrial Control Systems) baselining tool and Programmable Logic Controller (PLC) sensors; and 3) tailored visualizations, analytics, and automated cybersecurity orchestration. The latter was an emerging technology in the IT domain known as Integrated Adaptive Cyber Defense (IACD) developed by Johns Hopkins University Applied Physics Laboratory (JHU APL). IACD addresses the application of cybersecurity orchestration to the automation of cyber defense actions. A senior analyst supporting the U.S. Indo-Pacific Command (USINDOPACOM) Joint Innovation and Experimentation Division within the Requirements and Resources Directorate (J8) attending an IACD community of interest meeting proposed applying IACD principles to the MOSAICS initiative.

It took less than a few months for the concept of a cyber defense system for mission-critical infrastructure to be articulated into a proposal. As the needs analysis gained energy from stakeholders, the proposed approach was further developed in the form of a white paper that made its rounds through the DoD community. Early stakeholders in support of MOSIACS included Office of Secretary of Defense (OSD), NAVFAC, the National Security Agency (NSA), the Department of Energy (DOE), U.S. Cyber Command (USCYBERCOM), USINDOPACOM, U.S. Northern Command (USNORTHCOM), U.S. Air Force, and U.S. Marine Corps.

Finally, in the spring of 2017, forces were joined with DOE and DoD labs forming what is now the MOSAICS team. The 8-star letter and this concept became the basis for the MOSAICS Joint Capability Technology Demonstration (JCTD), which commenced in 2018.

The purpose of an engineering Needs Analysis is to identify the needs – and the gaps between – where an organization is and where the organizational goals and priorities for resource allocation and business decisions lie. In this case, the Combatant Command wanted to be "left of the boom," or in front of potential cyber threats to mission-critical infrastructure to avert threats. The challenge, or problem statement, was how to achieve cyber resiliency of mission-critical infrastructure through a cyber-attack.

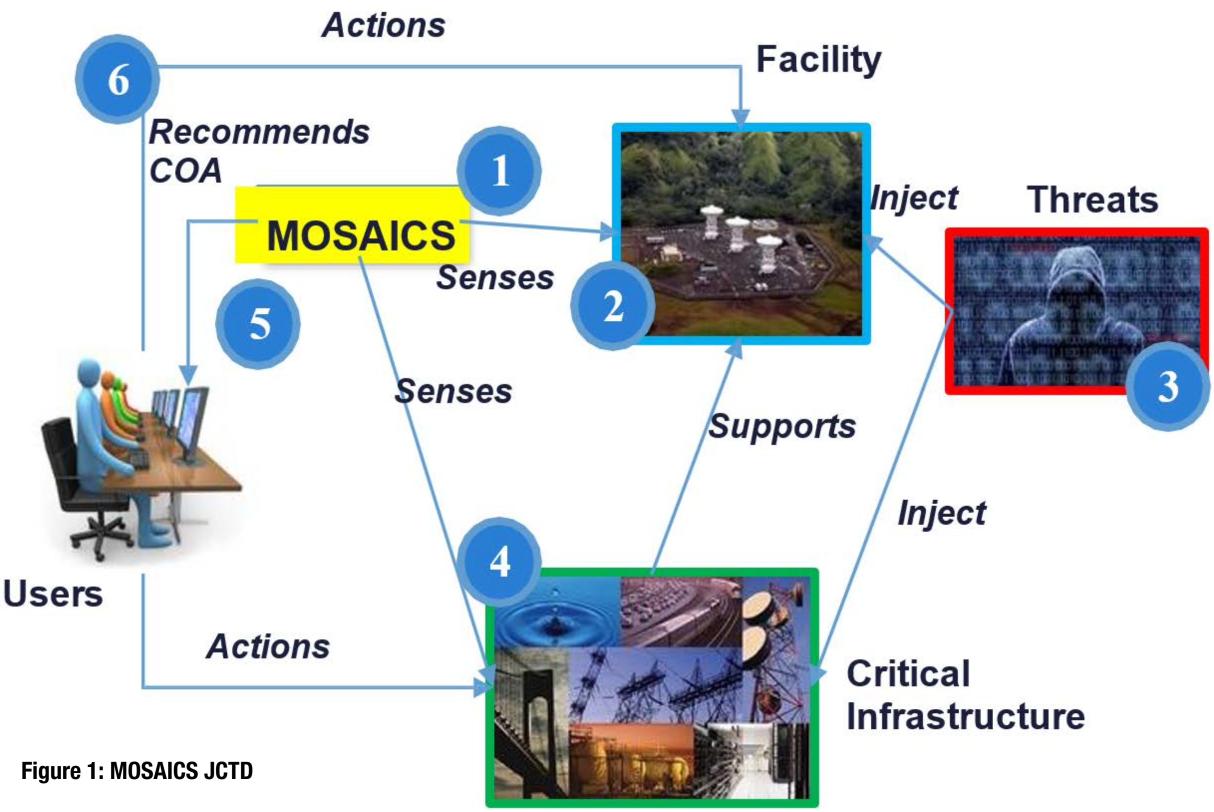


Figure 1: MOSAICS JCTD

1. **Establish baseline**
2. **Monitor for changes in equipment, network, or status**
3. **Threats inject malicious activity**
4. **Senses disruption, provide alerts**
5. **Provides available mitigation COA's**
6. **Users take action based on recommendations**

Source: ***MOSAICS JCTD, Overview Brief, October 2019 [2]***

Lifeline critical infrastructure sectors (e.g., water, power, and fuel), are commercial, privately owned entities, or known as existing "outside the fence." This "inside/outside the fence" relationship inhibits the DoD's ability to exert influence over the entire system network. The DoD, in most cases, does not produce power; however, it is highly dependent on power resources. Asset owners providing critical infrastructural support to the DoD are "outside the fence." DoD assets reside "inside the fence," which poses a complex challenge for the DoD's ability to defend these critical assets since U.S. legislation and Title Authorities strictly define boundaries of how the DoD behaves with commercial industry and state, tribal and municipal entities.

Until recently, these OT systems were generally considered as being separated from cyber vulnerability by a complete disconnection, referred to as being "air-gapped" from other networks and the internet. For such a system, access control restrictions are behind firewalls. Digital technology innovations expose mission-critical infrastructure to an increasing level of connectivity, resulting in greater potential cyber vulnerability to the adversarial hacker kill chain. The need for systematic studies to address the wide attack surface required bringing together the expertise, including test engineers, as early in the process as possible—that is, before the JCTD kick-off meeting, and then throughout the different stages of the MOSAICS development. This process required close coordination with senior leaders to address policy constraints.

Early system studies revealed additional challenges for the MOSAICS team, particularly regarding the system boundaries. The Department of Homeland Security (DHS), designated as the lead federal agency to protect critical infrastructure for the United States against cyber-physical threats, identifies 16 critical infrastructure sectors as vital to the United States. This means those sectors "whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof," (Department of Homeland Security, 2019) [3].

SMART POWER INFRASTRUCTURE DEMONSTRATION FOR ENERGY RELIABILITY AND SECURITY (SPIDERS) JCTD

The MOSAICS team referenced other Science and Technology (S&T) efforts such as the Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS) JCTD and the IACD framework, which is a design approach focused on speed and scale for cyber defense operations using secure orchestration. The team examined, for comparison and contrasting, predecessor systems such as IT systems, ICS, and Supervisory Control and Data Acquisition (SCADA) systems. Various methodologies were used to test and stretch the potential technologies under consideration to evaluate if the technology would meet or fail the requirements, and if the technology would make a significant cost difference in the solution, or potentially introduce new risk factors.

Sandia's Computational Engine for Particle Transport for Radiation Effects (SCEPTRE) was identified as the test environment for the MOSAICS system. Lab Test 1 performed at Sandia informed the Measures of Effectiveness (MOEs), and subsequent design validation was performed to simulate and test the development of MOSAICS. A future lab test will be performed at the Expeditionary Warfare Center (EXWC), which is one of the target sites for the JCTD, and the final Military Utility Assessment (MUA) will be conducted during the Department of Navy (DON) Trident Warrior.

MOSAICS is a complex hierarchy of systems. It is the initial operational defense of mission-critical infrastructure.

Since MOSAICS is a JCTD, the "best" options were optimized for cost, schedule, and performance. Predecessor systems and essential building blocks were identified as system elements for a proof-of-concept, which would be verified and validated against the requirements. Elements of IACD, SCEPTRE, and Map-to-Model were integrated with key technologies at JHU APL (e.g., simulation, advanced sensors, Automation & Autonomy, analytics, Machine Learning (ML), security orchestration, customized human-machine interfaces, and visualizations). Ultimately, the tools and methodologies MOSAICS will deliver are an integrated MOSAICS tool suite, a control system cyber baselining tool, a design guide, and updated Unified Facilities Criteria (UFC) and a framework-based concept of employment. Subsequent systems engineering phases address other critical infrastructure sectors such as water, wastewater, fuel, and HVAC.

"Ultimately, the tools and methodologies MOSAICS will deliver are an integrated MOSAICS tool suite, a control system cyber baselining tool, a design guide, and updated Unified Facilities Criteria (UFC) and a framework-based concept of employment."

MOSAICS OPERATIONAL ANALYSIS

MOSAICS has turned out to be a complex hierarchy of systems. Initially, MOSAICS is intended to address the combatant command (CCMD) operational view "inside the fence," which the DoD can eventually share with industry partners "outside the fence," and commercial industry to further enhance and advance the technical capability. High-level goals were given to explain the system study objectives. The anticipated MOSAICS benefits are to meet an operational need and to enhance understanding of risk to critical infrastructure and supported operational capabilities. MOSAICS is intended to detect control system threats faster — from months to minutes; to improve situational awareness driving near-real-time decisions to enable faster cyber defender response, and to disrupt adversary kill-chain in mission-relevant time to limit adversary re-use of attacks through enhanced sharing of indicators and mitigations. It is the initial operational defense of mission-critical infrastructure.

CONCEPT EXPLORATION

From the start, MOSAICS leadership briefed senior leaders at the Pentagon, at Combatant Commands, and at the locations of critical industry partners during conferences to gain valuable community feedback. The JCTD process designates the Technical Manager (TM) as the leader among peers to bring the appointed Integrated Management Team (IMT) to an essential consensus. In the case of MOSAICS, a hybrid approach was designed by a Government TM at the Naval Information Warfare Center – Atlantic (NIWC – Atlantic) and a National Lab TM Sandia National Laboratories (SNL) to jointly guide the interactions. To realize the benefit of senior industry leaders, high group interaction involved all IMT members for problem-solving.

To realize the benefit of bringing advanced technology and commercial-off-the-shelf (COTS) knowledge to bear in the MOSAICS efforts, resident expertise in the technical areas of consideration was leveraged at the national laboratories for the operational domain knowledge to understand how advanced technology and COTS may be applied to the problem set.

REQUIREMENTS ANALYSIS

In the entire DoD, there is no other predecessor system like MOSAICS. Sandia performed a threat analysis of the requirements during the requirements analysis stage of the CCMD's operational view. Pacific Northwest National

Laboratory (PNNL) collaborated with JHU APL to perform site visits to clarify, correct, and quantify the requirements. The MOSAICS IMT and discuss technical problems and component material solutions to meet the functional and physical specifications of the system design. They also assessed ensured the consistency of documented requirements. Site visits resulted in the selection of the initial predecessor system. During the functional definition phase, the functional building blocks included threat capabilities, decomposed functions, and operational context. As potential threats were identified, and the functional capabilities of MOSAICS were further defined, a Security of Operations (SECOPS) was developed to describe how the system responds to the identified threat, and Use Cases drafted by the IMT Operational Manager (OM). The OM was also a hybrid approach with both USINDOPACOM and USNORTHCOM sharing the duty. The various technical teams were connected through the Joint Information Operations Range (JIOR) to allow for collaboration between the participating DOE and DoD labs.

"Cyber-physical systems are susceptible to cyberattacks, and dependency on vulnerable IT and ICS equates to an increased risk of threat exposure, and certainly an increased threat surface area, to a cyber-attack."

The early planning focused on the system to be developed. Performing system-level studies helped the engineering team better understand the component capabilities. Pushing the limits to assess the operating range of every component helped further trace any failure that may be faced during the testing. Three critical activities for a system engineer that require technical knowledge to the component level are specifications requirements development, cost estimates, and the Analysis of Alternative (AoA)/ trade-off studies. For the MOSAICS team, this component level expertise was critical. The MOSAICS systems engineers needed to probe into sub-component levels to effectively identify and discuss technical problems and component material solutions to meet the functional and physical specifications of the system design. They also assessed the technology readiness levels (TRL) to meet the best performance versus cost. Idaho National Laboratory (INL) and JHU APL performed a detailed survey of commercial tools. An evaluation of the technologies was performed to inform the physical definition phase.

ANALYSIS OF ALTERNATIVES (AOA)

It was important to the MOSAICS IMT to consider alternatives for feasible and attractive concepts for satisfying the requirements for this new system. Several alternative system concepts were examined before defining a set of system performance requirements. This AOA informed the potential for innovative technical approaches that featured advanced technology. It also avoided "the natural temptation" that "can easily preclude the identification of other potentially advantageous approaches based on fundamentally different concepts" (Kossiakoff, 2011) [4].

In the case of MOSAICS, Government-off-the-Shelf (GOTS) solutions were only considered to fill gaps recognized for cyber-physical integration with the intention of a research transition of MOSAICS to the commercial industry. The team performed substantial trade-off analysis to consider other alternatives before deciding which approaches to select for development because GOTS was deemed an unsustainable model. The research and development expense to create a GOTS solution was deemed too cost-prohibitive, and the time its application would have put the schedule at risk.

The MOSAICS team selected Sandia's Map-to-model baselining tool because there was none other like it available for use on critical infrastructure. The down-select for other technologies was based on the cost against the requirements for "best" technology fit. The trade-off analysis was also essential before deciding which to select for development so that the commercial industry can participate in the future critical transition phase of the new system into the field.

FUNCTIONAL AND PHYSICAL ARCHITECTURES

Sandia's SCEPTRE environment was used to better understand the functional aspects of the system, and to ensure that system components fit together and interact effectively to make up the total system (Kossiakoff, 2011) [4]. Mechanical components of MOSAICS were modeled in SCEPTRE at the PLC level along with the electrical interfaces and the IACD software components. To realize the MOSAICS physical architecture, a broad knowledge of disciplines in the development of complex critical infrastructure systems was leveraged. Domain expertise was again needed that extended through the system component level and across several categories in contract to the design specialist whose expertise and experience is usually within a single discipline.

The MOSAICS engineering team had to take multiple types of mission-critical infrastructure cyber-physical systems into consideration with different system design hierarchies. For example, a system design hierarchy for an electric power plant consists of a power plant generating station, and subsystems such as a transmission substation, made up of components such as transformers, and subcomponents such as turbines, further decomposed into parts such as the circuit breakers and switches.

The electrical power plant system covers a considerable distance from the generating station to the end-user. This complex network makes cyber-physical systems susceptible to the cyber-attack kill chain.

CONCLUSION

In conclusion, there is an operational need for cyber defense capabilities such as MOSAICS to defend mission-critical infrastructure from cyber-attacks, which presents a complex system engineering challenge. Cyber-physical systems are susceptible to cyberattacks, and dependency on vulnerable IT and ICS equates to an increased risk of threat exposure, and certainly an increased threat surface area, to a cyber-attack. MOSAICS addresses an operational need for cyber defense capabilities to defend mission-critical infrastructure from cyber-attacks. The principal objective of the first phase of MOSAICS was the concept development phase of the systems engineering process to convert the operationally oriented view of the need into an engineering-oriented view required in the development of cyber defense capabilities of critical infrastructure. MOSAICS is anticipated to enter Military Utility Assessment (MUA) in the third quarter of FY21.

REFERENCES

[1] Scalco, R., Waugaman, B, Lacoste, J., Andrews J., Beary B., Roley R, (2018). ***"More Situational Awareness for Industrial Control Systems (MOSAICS) Joint Capability Technology Demonstration (JCTD)."*** Retrieved October, 2019, from https://www.iacdautomate.org/may-2018-integrated-cyber.

[2] Scalco, R., Waugaman, B, Lacoste, J., Andrews J., Beary B., Roley R, (2018). ***"More Situational Awareness for Industrial Control Systems (MOSAICS) Joint Capability Technology Demonstration (JCTD)."*** Retrieved October 2019, from https://www.iacdautomate.org/may-2018-integrated-cyber.

[3] https://www.dhs.gov/cisa/critical-infrastructure-sectors

[4] "Critical Infrastructure Sectors." Retrieved October 2019, 2019, from https://www.dhs.gov/cisa/critical-infrastructure-sectors.

ABOUT THE AUTHORS

ALEKSANDRA SCALCO is an engineer with the Naval Information Warfare Center (NIWC) Atlantic. She is working towards a Systems Engineering Ph.D. at Colorado State University (CSU). Her research field is cyber resilience for Operational Technology (OT). She earned a Master's Degree in Engineering from Iowa State University in 2012, and a Master's Degree in Business Administration (MBA) in 2009. She is a member of the Defense Acquisition Corps in engineering. Ms. Scalco is Defense Acquisition Workforce Improvement Act (DAWIA) career certified Level 3 Engineering, Level 1 Science & Technology, and Level 1 Program Management. She holds ITIL Intermediate Certifications. Before joining NIWC Atlantic Ms. Scalco was a member of the National Security Agency (NSA) workforce as an Information System Security Designer (ISSD). As an ISSD, she provided technical expertise to clients on cyber assurance to advance the state of cybersecurity solutions to harden the National Security Enterprise against adversarial threats.

DR. STEVEN SIMSKE joined Colorado State University in 2018 as a Professor in Systems, Mechanical, and Biomedical Engineering. Before then, he was an HP Fellow and a Research Director in HP Labs. He led HP in research and development in algorithms, multi-media, labels, brand protection, security and secure printing, imaging, 3D printing, analytics and life sciences. He is a long-time member of the World Economic Forum Global Agenda Councils (2010-2016), leads the Steering Committee for the ACM DocEng Symposium, and is former President of the Imaging Science and Technology professional organization. Dr. Simske has nearly 200 granted US patents and more than 400 professional publications, including the recent books, Meta-Algorithmics and Meta-Analytics. He is an Honorary Professor in Computer Science at the University of Nottingham, UK. Dr. Simske was a payload specialist on a dozen Space Shuttle missions, and has designed devices ranging from exercise-responsive pacemakers to impedance tomography systems.

MANAN JAYSWAL is an engineer with JPM Prototype & Manufacturing, Inc. Mr. Jayswal holds a Bachelor of Science degree in Aerospace Engineering from the University of Michigan. He is currently pursing a Master of Science degree sin Systems Engineering from Colorado State University (CSU). While at the University of Michigan, he worked with Dr. James Driscoll on a research project that focused on performing Computational Fluid Dynamics at the component level for Gas Turbine Engines. The primary focus of the project was to help develop more efficient engines and to understand the dynamics of different fluids in various atmospheric environments.

CURRENT ISSUES IN FACE RECOGNITION AND PHOTO-ID

By: **Robin S. S. Kramer, Ph.D.**, **Tessa R. Flack, Ph.D.**, and, **Kay L. Ritchie Ph.D.**, University of Lincoln

FROM PASSPORT ISSUING AUTHORITIES AND BORDER PROTECTION TO LAW ENFORCEMENT, SECURITY OFFICIALS AROUND THE WORLD MAKE IDENTITY JUDGEMENTS ABOUT MEMBERS OF THE PUBLIC BASED ON PHOTO-ID EVERY DAY. CRUCIALLY, RESEARCH TELLS US THAT THIS IS A DIFFICULT AND ERROR-PRONE TASK [1-3]. IN THIS ARTICLE, WE WILL DETAIL SOME OF THE MOST UP-TO-DATE RESEARCH ON ISSUES THAT ARE KEY TO THE USE OF PHOTOS AS IDENTIFICATION.

Illustration Credit: Deposit Photos/ Skydesigne

IMPROVING PHOTO-ID

When we use photo-ID, an image is compared to a live person or to a second image, and the observer decides whether or not these represent the same person. In the research literature, this is referred to as a face matching task. We know that it is difficult, if not impossible, to train people to improve on this task. In fact, UK police officers [4], Australian passport officers [5], and Australian grocery store cashiers [6] have been shown to be as error-prone as untrained students at face matching tasks. In the latter two studies mentioned, the researchers also recorded each passport officer and cashier's years of experience in the job. Both studies found that there was no relationship between face matching accuracy and years of experience, meaning that people who had been in the job performing the task for a long time were no better than new recruits.

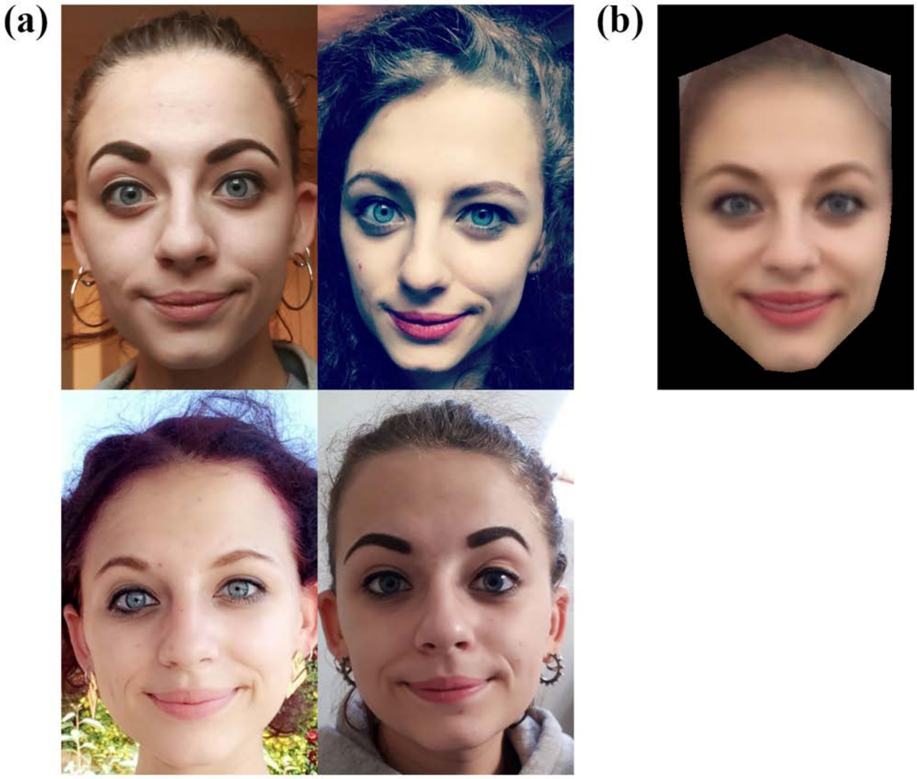


Figure 1: *(a) Multiple images and (b) a face average of the same person.* Photo Source: Authors

Rather than attempting to improve accuracy through training, recent research has turned to the notion of improving the photo-ID itself. One influential study suggested that using multiple images on a photo-ID document might improve accuracy on a face matching task [7], and this idea has also been reported in a previous edition of this journal [8]. The idea here is that multiple images show a selection of the different ways the person can look (in comparison with the current use of a single, passport-style image), and so can go some way to providing a comprehensive representation of that person to which a new image or a live person can be compared (see Figure 1). Importantly, the original work used only a computerised face matching task. More recent work, using a live person-to-photo task, has found no benefit of multiple images over a single image [9]. Another suggestion for improving photo-ID is to use a face average, combining multiple images of the same person using computer software [7-8], which should also theoretically produce a more representative image of the person (free from the idiosyncrasies of any single photograph; see Figure 1). It has been suggested that the brain might store familiar people as a face average [10-11] but this has been challenged by more recent research which shows that averages of familiar people are neither recognised more quickly nor rated as a better likeness than real images [12]. It is well established that face averages improve algorithm (i.e. machine-based) face recognition performance [13-15], however, two previous reports have shown that human observers do not benefit from the use of face averages [9, 15]. Therefore, despite promising preliminary data, the idea of updating photo-ID documents to include either multiple images or face averages is no longer supported by the most recent research.

IMPROVING MORPH ATTACK DETECTION

A relatively new area for security concern with photo-ID use is the issue of 'morph attacks'. This refers to a situation in which two people create a morph image, combining a photo of each of them to create a new image (see Figure 2). If this new morphed image looks sufficiently like the first person in the pair, they can apply for a new passport with this morphed image, obtaining a fraudulently obtained genuine (FOG) document. If the morphed image also looks sufficiently like the second person, then that person can subsequently pass through border control using the FOG passport. Two research articles [16-17], along with reports in this journal [18-19], have provided evidence that, although naïve observers frequently accept morphed images as genuine images, either alerting observers to this type of fraud or training them through a simple feedback task can dramatically improve morph detection rates. More recent research, however, suggests that these reports may lead Department of Defense officials to dramatically underestimate the threat posed by face morphing attacks [20]. In the original artifacts, the face morphs contained artefacts of the morphing process such as the ghost outline of

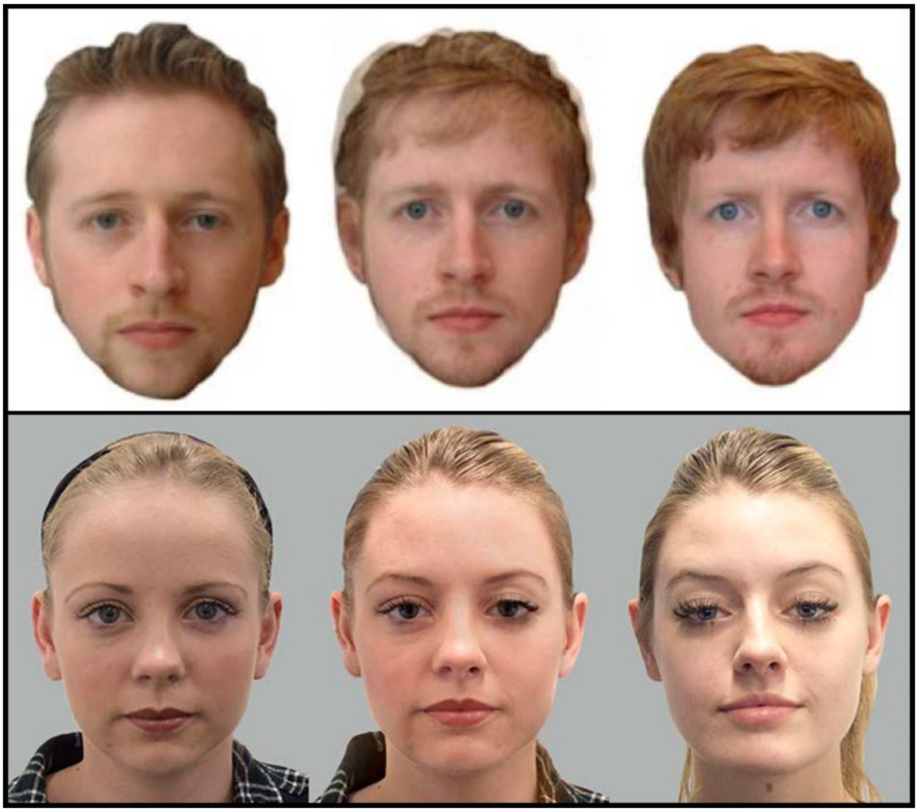


Figure 2: *Top row: An example of the images used in previous work. Bottom row: An example of the more sophisticated images used in recent work. The three faces depict two individuals (left, right) and a morph created using these images (centre).* (Photo Source: Adapted from Kramer et at., 2019, under CC BY 4.0)

hair or jawlines (see Figure 2, top row). We can be fairly certain, therefore, that training can improve detection rates for these 'low quality' (unedited) morphs.

With the advent of freely available image editing software, it is likely that fraudsters would utilise such tools to improve the quality of their morphs by removing artifacts created by the morphing process (see Figure 2, bottom row). Research using more sophisticated morphs, edited to remove obvious flaws in the images [20], has painted a more alarming picture than the original studies. Not only did training fail to improve morph detection rates, performance during the training session was at chance level (i.e., equivalent to guessing). In another experiment in the same study, judges compared morphed and genuine images to a live person standing in front of them. In this task, morphs were accepted as a genuine photo of the person on 49% of trials. Judges were also asked, "Do you have any reason why you wouldn't accept this as an ID photo?" Of the 1,410 judges tested, only 18 gave reasons that specifically included mention of computer manipulation or similar, e.g., "doesn't look real", "looks filtered", "looks photoshopped". This presents a worrying picture for security services as there is no evidence to suggest that people can be trained to detect higher quality face morphs. There is, however, hope for the detection of face morphs, and this comes from computer algorithms. In a final study, a basic computer algorithm was able to detect the high quality morphed images significantly better than humans [20]. In an ideal scenario, the best way to tackle these types of morph attacks would be for government officials to directly acquire ID photos at the place of issue, preventing fraudsters from submitting pre-made morph images for consideration. However, this would require a wide-spread systematic change in the procedure for obtaining a passport. Therefore, our recommendation is that security officials do not focus on human morph detection since it is inevitable that morphs will continue to improve in quality and will soon be indistinguishable from genuine photographs. Instead, we champion the use and development of computer algorithms to help in the detection of this kind of fraud.

MAKING LIVE IDENTITY JUDGEMENTS

The vast majority of work on face recognition has focused on testing people at computer screens, comparing one image to another. Although this reflects some aspects of the processing of photo-ID in the real world (e.g., a passport issuing officer comparing a new passport photo to previous images of the applicant), many judgements are made by comparing photo-ID to a live person (see Figure 3). As mentioned above, when a face morph is compared to a live person, the morph is accepted 49% of the time. This presents a dangerously high rate of morph acceptance in live settings.

People may believe that they would be more accurate in judging whether a photo shows the same person as the real person standing in front of them than they would be at judging whether two photos show the same person. In

Figure 3: *Providing a passport as photo-ID during a live interaction.* (Photo Source: Pixabay Images)

the eyewitness literature, this is referred to as the 'live superiority hypothesis' [21]. Research which has tested live face matching – comparing a person to a photo – has shown relatively low accuracy levels of 67% [6], 80% [9] and 83% [22]. As an illustration, Hartsfield-Jackson Atlanta International Airport sees more than 260,000 passengers daily, and so 20% errors would mean 52,000 people being erroneously questioned or being let through using someone else's passport. These values are not any higher than those observed with computerized versions of face matching tasks, where the standard Glasgow Face Matching Test shows around 80% accuracy [23]. Therefore, evidence suggests there is no live superiority effect in face matching – people are just as error-prone when matching live faces to images as they are at matching two images. Photo-ID is typically used in a live setting, and so we recommend that future research should continue to reflect this by utilizing live tasks.

HUMANS VS ALGORITHMS

It can be tempting to think of the human brain as a highly complex computer, particularly with the advent of computational neural networks which purport to mimic the brain. It is important, however, to acknowledge differences between human and computer face processing. Familiarity is not a topic covered in this article, but it is worth noting that humans are experts in recognizing familiar faces, and personal familiarity is very difficult to fully computationally model. While cutting edge algorithms (e.g., deep convolutional neural networks) are now performing at levels comparable with forensic facial examiners [24], we know that familiar human viewers remain superior in terms of accuracy.

As mentioned earlier in this article, where the latest research suggests that humans do not benefit from face averages (a computer-generated blend of multiple images of the same person) for recognition [9,15], computers do seem to show accuracy gains [13-15]. In fact, algorithms have been found on multiple occasions to produce 100% accuracy using face averages. In one study, algorithm recognition from single images was 54% but improved to 100% with face averages [13]. Another study showed a cell phone app's face recognition increased from 86% with single images to 100% with face averages [15]. The same study showed in another experiment that a commercially available face recognition system (FaceVACS-DBScan 5.1.2.0. running Cognitec's B10 algorithm [25]) was 100% accurate at searching for a target identity in a large database when the target image was an average of the identity [15].

As well as benefiting from averages where humans do not, algorithms can detect high quality face morphs where humans cannot [20]. Indeed, computers are well suited to picking up on imperceptible (at least, to humans) inconsistencies in images between, for example, reflections visible in the eyes and skin [26].

Facial recognition technology is increasingly used in the criminal justice system. Despite the growing appeal of facial recognition systems worldwide, there have been several high profile reports of their failure. A prominent civil liberties group, Big Brother Watch, conducted a series of freedom of information requests, finding that the Metropolitan Police's use of facial recognition technology has misidentified people in 98% of cases of its use [27] (i.e., the system found "match" images which, in fact, showed a different person). This statistic is particularly important when considering the use of such technologies at events with high Black and minority ethnic populations, such as the well-publicised failure of the Metropolitan Police's use of facial recognition technology at the Notting Hill Carnival, an event with a high proportion of British African Caribbean attendees. Of concern is the anecdotally-reported failure of facial recognition technologies with non-White faces [28]. This is arguably a more fundamental problem than the issue of civil liberties, which of itself led to San Francisco's Board of Supervisors recently voting to ban facial recognition technology [29]. Biased algorithms are the product of biased humans – we are more accurate at recognizing people of our own race than other races, and an algorithm trained on White faces will not perform as accurately with non-White faces. It is, therefore, important that we strive to train algorithms on ethnically diverse image sets.

CONCLUSION

Looking to the future, it is important that we utilize the most up-to-date research and technology in our defense and security systems. It is also vitally important that the use of algorithms is not seen as a fool-proof tool for the task in hand, but that we bear in mind that the algorithm may be as biased as the humans who built it.

REFERENCES

[1] Bruce, V., Henderson, Z., Newman, C., & Burton, A. M. (2001). Matching identities of familiar and unfamiliar faces caught on CCTV images. ***Journal of Experimental Psychology: Applied, 7***(3), 207–218.

[2] Bruce, V., Henderson, Z., Greenwood, K., Hancock, P. J. B., Burton, A. M., & Miller, P. (1999). Verification of face identities from images captured on video. ***Journal of Experimental Psychology: Applied, 5***(4), 339–360.

[3] Ritchie, K. L., Smith, F. G., Jenkins, R., Bindemann, M., White, D., & Burton, A. M. (2015). Viewers base estimates of face matching accuracy on their own familiarity: Explaining the photo-ID paradox. ***Cognition, 141,*** 161-169.

[4] Burton, A. M., Wilson, S., Cowan, M., & Bruce, V. Face recognition in poor-quality video: Evidence from security surveillance. ***Psychological Science, 10***(3), 243-248.

[5] White, D., Kemp, R. I., Jenkins, R., Matheson, M., & Burton, A. M. (2014). Passport officers' errors in face matching. ***PLoS ONE, 9,*** e103510.

[6] Kemp, R., Towell, N., & Pike, G. (1997). When seeing should not be believing: Photographs, credit cards and fraud. ***Applied Cognitive Psychology, 11,*** 211–222.

[7] White, D., Burton, A. M., Jenkins, R., & Kemp, R. (2014). Redesigning photo-ID to improve unfamiliar face matching performance. ***Journal of Experimental Psychology: Applied, 20,*** 166–173.

[8] Robertson, D. J., & Burton, A. M. (2016). Unfamiliar face recognition: Security, surveillance and smartphones. ***HDIAC Journal, 3***(1), 15-21.

[9] Ritchie, K. L., Mireku, M. O., & Kramer, R. S. S. (2019). Face averages and multiple images in a live matching task. ***British Journal of Psychology.*** Advance online publication.

[10] Burton, A. M., Jenkins, R., Hancock, P. J. B., & White, D. (2005). Robust representations for face recognition: The power of averages. ***Cognitive Psychology, 51***(3), 256–284.

[11] Robertson, D. J. (2015). Spotlight: Face recognition improves security. ***HDIAC***

[12] Ritchie, K. L., Kramer, R. S. S., & Burton, A. M. (2018). What makes a face photo a ‘good likeness’? ***Cognition, 170,*** 1-8.

[13] Jenkins, R., & Burton, A. M. (2008). 100% accuracy in automatic face recognition. ***Science, 319,*** 435.

[14] Robertson, D. J., Kramer, R. S. S., & Burton, A. M. (2015). Face averages enhance user recognition for smartphone security. ***PLoS ONE, 10***(3), e0119460.

[15] Ritchie, K. L., White, D., Kramer, R. S. S., Noyes, E., Jenkins, R., & Burton, A. M. (2018). Enhancing CCTV: Averages improve face identification from poor-quality images. ***Applied Cognitive Psychology, 32,*** 671-680.

[16] Robertson, D. J., Kramer, R. S. S., & Burton, A. M. (2017). Fraudulent ID using face morphs: Experiments on human and automatic recognition. ***PLoS ONE, 12***(3), e0173319.

[17] Robertson, D. J., Mungall, A., Watson, D. G., Wade, K. A., Nightingale, S. J., & Butler, S. (2018). Detecting morphed passport photos: A training and individual differences approach. ***Cognitive Research: Principles and Implications, 3***(27), 1-11.

[18] Robertson, D. J. (2018). Face recognition: Security contexts, super-recognizers, and sophisticated fraud. ***HDIAC Journal, 5***(1), 7-10.

[19] Robertson, D. J. (2017). Spotlight: Face morphs – a new pathway to identity fraud. ***HDIAC***

[20] Kramer, R. S. S., Mireku, M. O., Flack, T. R., & Ritchie, K. L. (2019). Face morphing attacks: Investigating detection with humans and computers. ***Cognitive Research: Principles and Implications, 4***, 28.

[21] Fitzgerald, R. J., Price, H. L., & Valentine, T. (2018). Eyewitness identification: Live, photo, and video lineups. ***Psychology, Public Policy and Law, 24***(3), 307–325.

[22] Megreya, A. M., & Burton, A. M. (2008). Matching faces to photographs: Poor performance in eyewitness memory (without the memory). ***Journal of Experimental Psychology: Applied, 14,*** 364–372.

[23] Burton, A. M., White, D., & McNeill, A. (2010). The Glasgow face matching test. ***Behavior Research Methods, 42***(1), 286-291.

[24] Phillips, P. J., Yates, A. N., Hu, Y., Hahn, C. A., Noyes, E., Jackson, K., ... O’Toole, A. J. (2018). Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms. ***Proceedings of the National Academy of Sciences, 115***(24), 6171-6176.

[25] Cognitec FaceVACS DBScan. 2017. Available from: http://www.cognitec.com/facevacs-dbscan.html Accessed 1/8/2016

[26] Seibold, C., Hilsmann, A., & Eisert, P. (2018, July 5). Reflection analysis for face morphing attack detection. Retrieved from http://arxiv.org/pdf/1807.02030.pdf

[27] Face off: The lawless growth of facial recognition in UK policing. Big Brother Watch, May 2018. Available from https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf

[28] Facial recognition is accurate, if you’re a white guy. New York Times. Available from https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html

[29] San Francisco bans facial recognition technology. New York Times. Available from https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

ABOUT THE AUTHORS

ROBIN S. S. KRAMER, PH.D., is a lecturer in psychology at the University of Lincoln. After completing his PhD at Bangor University in Wales, he carried out postdoctoral research at universities in both Canada (Brock, Trent) and the UK (Kent, Aberdeen, York). His research integrates human and computer aspects of face processing, specifically focussing on face perception and recognition.

TESSA R. FLACK, PH.D., is a Lecturer in Psychology at the University of Lincoln. She completed her PhD at University of York, UK. From there she worked at Durham University before moving to Lincoln in 2018. Her work focuses on face learning, and where and how faces are processed in the brain. Tessa uses a range of behavioural and neuroimaging methods, to investigate the link between how our brain represents faces, and how this relates to our behaviour.

KAY L. RITCHIE PH.D., is a senior lecturer at the University of Lincoln. Her research focuses on understanding and improving face identification. Kay holds a Phd in psychology from the University of Aberdeen, UK, and has worked at the University of York, UK and the University of Western Australia prior to joining the School of Psychology in Lincoln. Kay currently leads a team funded by the British Academy investigating public attitudes towards the use of facial recognition technology in the criminal justice system.

Transform your Knowledge of the Research Development Test and Evaluation (RDT&E) Budget Process

Quickly search, connect and analyze multiple RDT&E budget datasets, such as:

- President's Budget (PB)
- R2s and P40s
- Research Projects (URED)
- Congressional Budget Marks

R&E Gateway Powered by DTIC

START TODAY! Visit DTIC' New Research Budget and Project Information (RBPI) tool at https://www.dtic.mil/bt/ui

Defense Technical Information Center (DTIC) | Fort Belvoir, VA | https://discover.dtic.mil

IMPROVING POWER SYSTEM RESILIENCE WITH INTEROPERABLE COMMUNICATIONS

By: **Scott Manson**, Schweitzer Engineering Laboratories, Inc.

U.S. ARMY RESEARCH LABORATORIES AND THE MASSACHUSETTS INSTITUTE OF TECHNOLOGY (MIT) LINCOLN LABORATORY HAVE DEVELOPED A NEW DRAFT STANDARD CALLED TACTICAL MICROGRID STANDARD (TMS). SCHWEITZER ENGINEERING LABORATORIES, INC. (SEL) WAS HIRED TO VALIDATE THE SPECIFICATION BY BUILDING A PROTOTYPE TMS MICROGRID SYSTEM.

SEL TEAMS BLENDED PROVEN POWERMAX® CONTROL AND PROTECTION METHODS WITH THE TMS STANDARD, THE RESULT OF WHICH IS A NEW LEVEL OF SAFE, RELIABLE, AND ECONOMIC POWER SYSTEMS. THIS ARTICLE DESCRIBES HOW TMS SYSTEMS AUTOMATICALLY CONFIGURE A MICROGRID PROTECTION AND CONTROL SYSTEM WITHOUT HUMAN INVOLVEMENT. TWO VARIANTS OF THIS SOLUTION ARE SHARED: ONE FOR A RAPIDLY DEPLOYED, MOBILE POWER SYSTEM, AND ONE FOR A FIXED GARRISON FACILITY. THE ARTICLE CONCLUDES WITH A SUMMARY OF PROVEN SUPPLY CHAIN SECURITY METHODS.

Photo Credit: U.S. Navy Photograph by Mass Communication Specialist 2nd Class Daniel Barker (120719-N-RI884-240)

INTRODUCTION

Electric power is essential to our modern society and in U.S. Department of Defense (DoD) facilities. The short-term effects of no power are no heat, lights, defense systems, or communications. Longer-term effects are no fresh water, no sewage treatment, and spoiled food.

This article reviews a significant improvement in technology to provide safer and more reliable, resilient, and economic delivery of electric power to DoD facilities worldwide. This technology has been praised by the U.S. Department of Energy [1] [2] and independent researchers [3], and it has received an international award [4].

The technology outlined in this article is a large step forward in reliable power delivery for the DoD and offers the following benefits:

- There is no single point of failure.
- The systems reduce fuel consumption up to 73 percent.
- They have a plug-and-play configuration, which requires limited training to configure or operate.
- They are Tactical Microgrid Standard (TMS)-compliant.
- They are designed to meet risk management framework (RMF) cybersecurity control policies.
- They allow interoperability with all makes, models, and sizes of military and commercial off-the-shelf (COTS) generators.
- They mitigate the accumulation of unburned hydrocarbon residue in the exhaust system, known as wet stacking, and the need for corresponding maintenance.
- All controllers are identical, making parts easily interchangeable.
- They allow load sharing and interoperation with any proprietary generator or inverter.
- The electronics meet NERC CIP, RMF, NIST, and ISA 99 security requirements.
- The control method allows generator sets (gensets) to be geographically dispersed to improve power resiliency.

THE CHALLENGE

The problems of the latest-generation power systems deployed by the U.S. armed forces today make for a fragile power system. These challenges are addressed with the technology described in this article.

Military acquisition is locked into a specific genset brand and model for an entire fleet, creating cost overruns and single-manufacturer vulnerabilities. This lock is caused by genset manufacturers because their technology does not interoperate with the technology of other genset manufacturers. Dissimilar or mismatched gensets and inverters must be capable of working in parallel for a resilient acquisition program. Inverters are required for batteries and photovoltaic (PV) sources to connect to a microgrid.

Gensets are oversized to guarantee full rated power in harsh environments. Oversized gensets are not optimized for low-load conditions, creating many problems. These problems, including fuel waste, increased emissions, and engine damage, shorten mission effectiveness due to excessive fuel consumption and endanger lives in the transportation of excessive fuel. Oversized gensets require the transportation of additional fuel to the battlefield and prematurely destroy the engines with wet stacking.

Interoperability is not possible with present equipment being procured by the DoD. All genset manufacturers use a proprietary isochronous (ISO) engine load-sharing system, thereby preventing interoperability. ISO load-sharing techniques require high-speed communications between gensets to stabilize the inherently unstable ISO control mode. Without this high-speed link, gensets have frequency and voltage instabilities and will trip offline. North American utilities do not allow these control techniques on the bulk electric power system because they are inherently destabilizing, impractical to maintain, unreliable, and do not allow interoperation between diverse manufacturer gensets.

Conventional gensets use outdated proportional integral derivative (PID) control loop techniques. When paralleled with inverters or electronic loads, PID controls commonly cause frequency and voltage instabilities [5], high fuel usage, and high emissions.

Co-located generators, especially the load-sharing lines between gensets, are a primary target for adversaries. Conventional load-sharing communications lines cannot transmit farther than a few meters, requiring that all paralleled gensets be co-located. Note that load-sharing lines are not required on the bulk electric power system because of its superior design.

The systems deployed by the U.S. armed forces today are too complicated. Many genset operators are not electric power system experts, nor can they be. Their expertise lies with other military tasks. This discrepancy, combined with a great number of technology overcomplexities, makes it time-consuming and expensive to configure a reliable forward operating base. Only the most simplistic and inefficient designs are typically achievable without assistance from outside a unit. Equipment specifications, site designs, field installation, repairs, and field commissioning require that specialists spend significant time traveling and in the field, often putting the DoD's limited talent pool in harm's way. This reduces the practicality of a rapidly mobile forward operating base.

Cybersecurity challenges for legacy DoD communications systems include open protocols, managed switches, nonsecure ports, and the logistical difficulties that come with operating system maintenance and malware and software updates.

COOPERATIVE RESEARCH AND DEVELOPMENT

The U.S. Army Corps of Engineers Construction Engineering Research Laboratory (CERL), the U.S. Army Combat Capabilities Development Command (C5ISR), and MIT Lincoln Laboratory developed the TMS interoperable communications system standard. Schweitzer Engineering Laboratories, Inc. (SEL) was hired by the DoD to validate the TMS specification by building a prototype TMS microgrid system. During this project, SEL simultaneously self-funded (cost-shared) the research and development (R&D) to solve a great number of additional DoD mobile power problems not directly addressed by TMS. SEL's project demonstrated successful technology transfer from the DoD, improved the maturing TMS documentation, and proved interoperability to be practical.

SEL power system experts determined the root cause of each of the aforementioned challenges and designed a safe, reliable, low-cost solution. This was accomplished by blending gigawatt-scale utility and industrial controls and protection methods [6] with the TMS standard [7]. The system SEL developed has no single point of failure, does not lock the acquisition into a single manufacturer, does not depend on antiquated PID control methods, allows for geographic dispersal of the gensets, allows for minimally sized and highly efficient gensets from multiple manufacturers to interoperate, and provides superior grid power system resiliency, reliability, and power quality.

The SEL system is simple to operate; high school interns have successfully set up, operated, and performed failure recovery of a 440 kW power system comprised of eight gensets from four different manufacturers (TQG, CAT, Taylor, and Gillette). The cybersecurity posture of the systems is also improved and simplified, and all electronics are sourced from U.S. manufacturers.

This work is a testament to the power of linking industrial power and cybersecurity experts with DoD research facilities. These efforts have recently been recognized with a significant award [4]. The R&D100 awards committee selected TMS for this award over several other industry standards after analysis of the benefits. The award summary identified the technology as unlocking many opportunities for the DoD, accelerating the acquisition and fielding of advanced technology, and providing faster and more resilient field operations.

The result of these cooperative efforts is a power delivery system with superior resilience. This resiliency improves power system quality and reliability. Reliability is objectively measured in the electric utility industry by outage time with parameters such as the System Average Interruption Duration Index (SAIDI) and System Average Interruption Frequency Index (SAIFI).

COMMUNICATIONS INTEROPERABILITY

TMS specifications call for an interoperable communications structure layered upon the proven Data Distribution Service (DDS) protocol. DDS is a publish/subscribe protocol that uses User Datagram Protocol (UDP) messaging between controllers. DDS has been used by the DoD for over a decade for mission-critical applications.

The TMS roles are as follows:

1. Microgrid controller (MC)—sends configuration settings and commands to other TMS-compliant devices.
2. Source power device (SRC)—gensets or other power-providing distributed energy resources (DERs).
3. Storage power device (STOR)—battery systems that store power.
4. Distribution power device (DIST)—power distribution hardware that contains cabling and circuit breakers.

The TMS standard calls for a fixed message set (data structure) for each of these roles. This facilitates interoperable communication between all manufacturers.

Every device on the TMS network is assigned one of these TMS roles. Communication between each device is automated based on device roles and requires no human configuration. For example, as an authorized SRC (genset) is connected to the TMS local-area network (LAN), the SRC role provides a device announcement to the network. In this example, the MC automatically subscribes to the SRC and starts communication of metering and control signaling information. The MC sends configuration parameters to the SRC, thus facilitating acceptance on the microgrid with a known parameterization and control method.

MOBILE MICROGRIDS

Rapidly deployed, mobile power systems without connections to a bulk electric power system are commonly powered by diesel reciprocating engine gensets. These mobile power systems are designed for forward operating bases and disaster relief.

In the SEL design, all controllers are identical and only require that their role be specified prior to operation with a control (DIP) switch. Identical controllers are employed to minimize the spare parts inventory requirements and are not required for interoperability. Once the role is specified, the electronics automatically configure all communications, controls, and protection for an entire power system. There is no software required to configure these systems.

Dispatch is accomplished via a microgrid controller, which dispatches all generator sources (SRCs). In the SEL design, there are five modes for the operator to select:

1. Rapid stop (shutdown mode). This stops all power sources (gensets) for a rapid demobilization of the facility.
2. Normal resiliency (equal percentage load sharing). These controls ensure nominal frequency and voltage are maintained and that watts and volt-amperes reactive (VAR) are shared between gensets of any size or from any manufacturer.
3. Optimal fuel usage (start/stop control). These controls temporarily suspend operation of unnecessary gensets, allowing the remainder of gensets to operate at a higher efficiency. Testing has proven that fuel usage is reduced between 10 and 73 percent by employing these methods.

4. Optimal resilience mode (emergency mode). This brings all gensets online for the maximum durability of the power system, ensuring that destruction of one or more gensets does not compromise the flow of reliable, high-quality power to the loads. Basic physics identifies that optimal resiliency and optimal fuel usage modes are mutually exclusive. They cannot happen simultaneously, so the user must select which mode they desire depending on site conditions.
5. Maintenance mode (wet-stacking mitigation mode). This mode is used to de-foul the engines one at a time. This is achieved through modifications to the power dispatch plan and does not require the addition of load banks or isolation of the generator undergoing wet-stack mitigation activities.

These simplified controls are sufficient to control power systems from several megawatts down to a few kilowatts in scale, making them ideal for expeditionary warfare and emergency response teams.

Fig. 1 shows a Mobile Electric Power (MEP) 806B TQG upgraded with energy packet controls and TMS communications. TQGs with the controls upgrade shown in Fig. 1 parallel and seamlessly share load with any genset, battery, photovoltaic (PV) installation, or wind turbine, old or new. Reference [8] provides more details. This older TQG technology procured by the DoD can be modified in less than 30 minutes with TMS technology to interoperate with gensets, inverters, or host nation interconnects of all sizes and from all manufacturers.

Real-time automation controllers (RTACs) were used as universal translators (protocol gateways) between SRC, MC, and DIST per the predefined TMS data structures. They also provide firewalled security and a physical network isolation barrier between the TMS LAN and the communication within an SRC, MC, or DIST. The architecture is shown in Fig. 2.

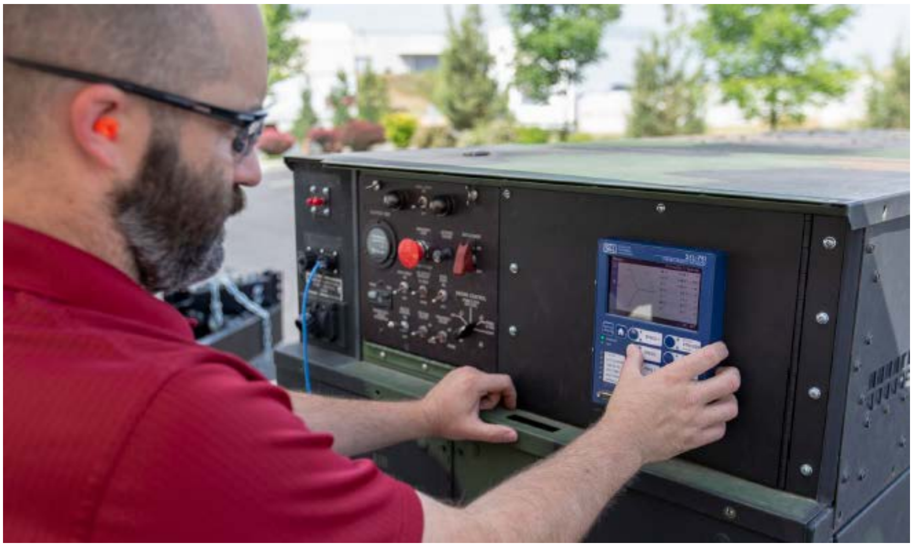


Figure 1: *TQG After a Controls Upgrade* (Photo Source: Author)

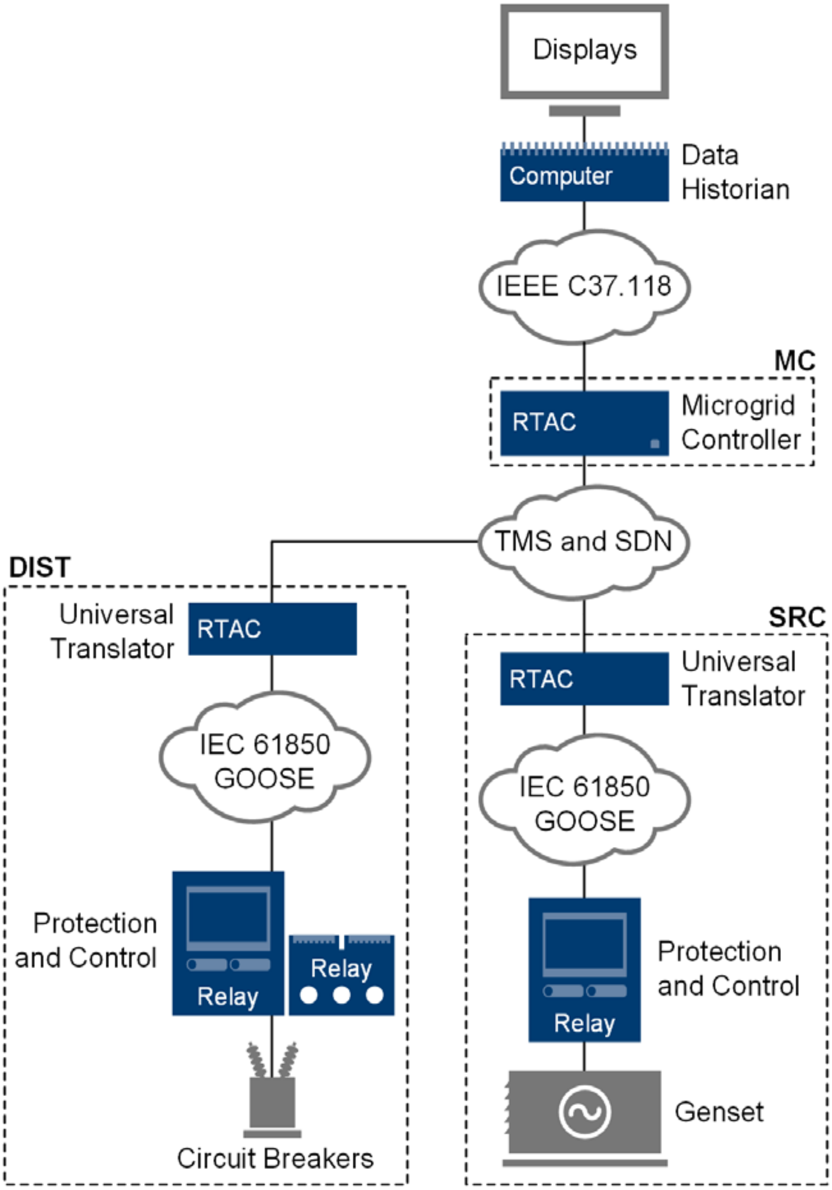


Figure 2: *Communications Architecture*

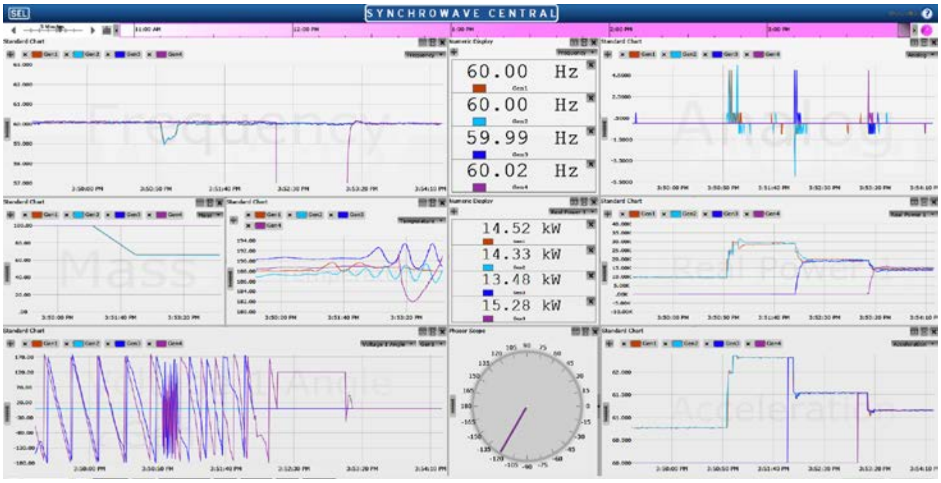


Figure 3: *Time-Synchronized Condition Monitoring*

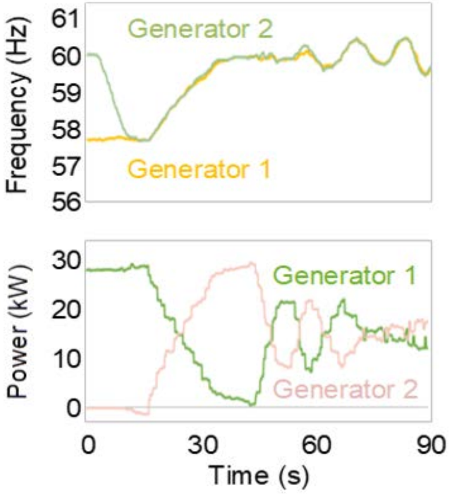


Figure 4: *Conventional Load Sharing*

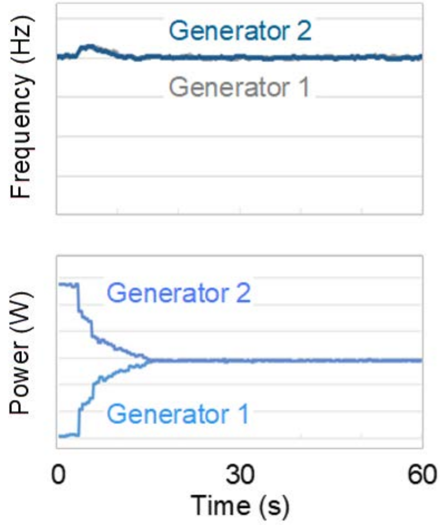


Figure 5: *Energy Packet Load Sharing*

SITUATIONAL AWARENESS

Time-synchronized, condition-monitoring systems are provided on a single heads-up display; this system records historical data for over 20 years of continuous runtime of the microgrid. Network traffic, cooling water temperatures, oil pressures, power values, frequencies, voltages, reactive power, phase angles, and machine wet-stack fouling are displayed on the single display shown in Fig. 3.

This single display provides predictive, condition-based maintenance indicators, which alert operators to potentially hazardous situations before they become a danger.

ENERGY PACKET CONTROL

One of the more challenging problems to solve has been PID and ISO load-sharing control methods. All reciprocating gensets manufactured today use PID and ISO methods.

The oil and gas industry and utilities have discovered that ISO techniques are inadequate. In fact, these larger, more reliable power systems have standards that specifically forbid ISO control in the interconnect contracts that power producers must follow.

ISO parallel controls require high-speed controls, signaling between gensets, and geographically close generators. These methods are known to fail to interoperate between manufacturers, to have serious frequency and voltage instability modes for modern electronic loads, and to not play well with renewable energy sources, batteries with inverters, and power electronic loads (e.g., data centers).

PID controls are inherently dependent on inertia, i.e., the rotating mass of the gensets and loads. As the loads become primarily power electronic, these PID control methods are proven to destabilize the power system [5].

Fig. 4 shows two 30 kW synchronized (paralleled) gensets sharing load using conventional small-network techniques. These units use the conventional PID control method for ISO parallel controls. Note the oscillation (hunting) in power (kW) and frequency. This hunting wastes fuel, reduces engine life, and is precariously close to tripping off the gensets (this is not resilient power system behavior).

Energy packet controls are the preferred alternative to inertia dependence, PID control, ISO paralleling methods, and power electronic loads (synonymous with –R loads or P/Q loads). Those same two gensets under energy packet controls are shown in Fig. 5 in the same parallel load-sharing scenario. This is resilient power system behavior.

Energy packet control methods do not require a human to tune the controllers. They are faster to configure, and all gensets can be factory set with a guarantee of interoperability with any other manufacturer's gensets, inverter, or host nation country.

Energy packet controls have a reduced dependence on inertia and, thus, no retuning requirement as power systems are assembled and reassembled. Inertia, load compositions, and impedances can change dramatically without impact on the power system. Engines with energy packet controls can be geographically distributed. These methods have been proven and are on display in live demonstrations [9].

CYBERSECURITY UNDERLAYMENT

SEL applied a cybersecurity underlayment to secure the TMS-based solutions. After examining conventional network security approaches, SEL chose a design that uses three components: RTACs, protective relays, and operational technology software-defined networking (OT SDN) Ethernet switches (shown in Fig. 6). This is a proven, practical solution [10].

Multifunction relays and RTACs are architecturally different. Relays operate with an embedded environment that includes safeguards to detect alteration of programming and prevent malware infection or other corruption. RTACs use an embedded operating system that whitelists applications at the kernel level to prevent alteration. This equipment is used in power system utility substations around the world and is commonly part of NERC CIP-certified substation designs at mission-critical facilities [12].

OT SDN underlayment technology is used to lock down the network and to identify intrusions. OT SDN is essential for securing the TMS publish-subscribe network. For a fraction of the cost and complexity of conventional solutions, this system provides a simple and effective networking solution. In the 2017 worldwide microgrid shootout sponsored by the Department of Energy (DOE) National Renewable Energy Laboratory (NREL) [1] [2], the NREL cyber red team was not able to gain entrance to an SDN network. This has been verified multiple times by DoD red teams. SEL OT SDN underlayment technology is designed to obsolete Ethernet network military attack toolkits [12].

OT SDN complements TMS with preconfigured routing circuits that are programmed instead of the self-configured rerouting used in conventional IT networking methods such as Rapid Spanning Tree Protocol (RSTP). OT SDN limits the spread of threats, improves situational awareness, has native intrusion detection, identifies and quarantines threats, and seamlessly reroutes traffic after failures.

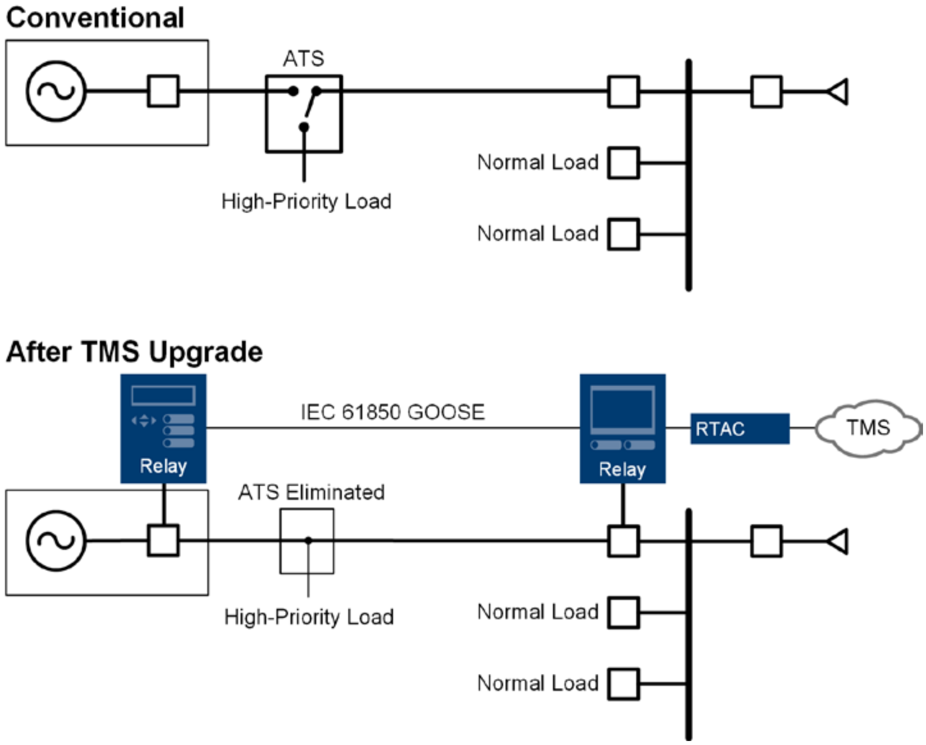


Figure 6: *Converting Emergency Diesel Genset With ATS to Microgrid*

OT SDN is different than the IT SDN used by IT departments or data centers. OT SDN is designed to be a low-cost, small form-factor, rugged solution and is locked down after a one-time configuration. OT SDN has much lower latency and jitter than traditional networking, as required by protection and control equipment. OT SDN is tailored to the industrial control system (ICS) environment.

Cybersecurity teams provide operators supporting authorization to operate (ATO) documentation such as the RMF Plan of Action and Milestones (POA&M). The POA&M is a key document in the security authorization package and for continuous monitoring activities of a microgrid. Teams provide a security assessment or vulnerability scan for the delivered solutions; results of that scan are checked against NIST SP800-53A and DISA STIGs. Findings are placed in a POA&M and delivered to the customer. Teams continuously work to remediate any vulnerabilities found and to ensure the delivered solution follows required standards.

GARRISON MICROGRIDS

Garrison (campus) microgrids benefit from the TMS communication, SDN security, and microgrid control solutions developed in the oil and gas industry. These designs provide the improved resilience, reduced fuel usage, cybersecurity, simplicity, power quality improvements, and easy scaling of mobile microgrids.

TMS-based garrison systems are slightly different from the mobile solution in that they are designed to retrofit existing onsite backup power gensets and switchgear to quickly convert an existing garrison facility into a microgrid.

Fig. 6 shows how to retrofit an automatic transfer switch (ATS) to a TMS genset to power a garrison microgrid. In this retrofit, the ATS is eliminated and existing circuit breakers at the genset and the switchgear are controlled by two intelligent multifunction relays. This allows an emergency genset to power a microgrid.

In this solution, the microgrid is isolated from a bulk electric power system (host nation country) by a multifunction relay and circuit breaker at the point of common coupling (PCC) with the bulk electric power system (not shown in figure). The PCC relay provides seamless islanding and compliance to IEEE 2030.7, IEEE 2030.8, and IEEE 1547 [13] [14] [15].

SEL TMS garrison systems are designed for incremental procurement. Gensets and ATS equipment can be retrofitted one device at a time; usually, systems can be retrofitted with a single one-day outage. This allows a crew to economically scale up a facility one generator at a time, minimizes technology adoption risks, and allows purchase of the upgrades in small, affordable increments.

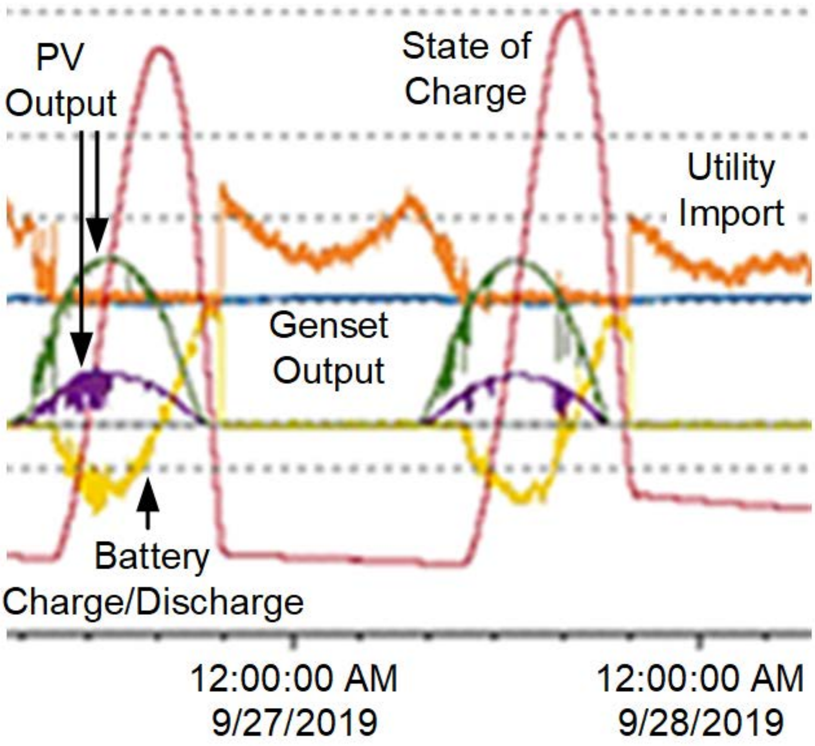


Figure 7: *Parris Island Integrated DER Results*

PARRIS ISLAND MICROGRID

The U.S. Marine Corps (USMC) Recruit Depot Parris Island microgrid project in South Carolina was a collaboration between the USMC, Ameresco, and SEL. In addition to substantial site upgrades, the facility proved interoperability between PV, batteries, turbines, and reciprocating diesel gensets.

Because TMS does not yet fully define the inverter, PV, or battery interfaces, this project used the TMS controller constructs but not the protocol implementation. The results are still remarkable.

The plot in Fig. 9 shows a day in the life of the Parris Island microgrid. Green and purple are the megawatt output of two PV fields, yellow is the megawatt charge/discharge of a battery-backed inverter (energy storage), red is the state of charge of the battery, blue is the output from a site turbine, and orange is the utility import megawatts. The battery system stores excessive energy from the PV output, lessening the evening load. The turbine stays on baseload unless a major upset occurs. The PV, turbine, and battery system work together to reduce utility charges.

Notwithstanding the success at Parris Island, as with any new technology, the TMS standard has room for improvement. The TMS specification needs enhancement, and further projects must be completed before TMS is formally adopted as a military standard (MIL-STD).

The Parris Island project is the first of many that will be incrementally adopting TMS technology. Only through commercial adoption and more projects can the standard be thoroughly vetted.

RESILIENT PROCUREMENT

The Parris Island microgrid project used resilient procurement methods similar to those practiced for decades by the oil and gas industry and utility power systems.

The USMC specified that best-in-class electronics (the brains of the power system) be embedded into third-party, low-cost switchgear, transformers, reclosers, distribution gear, etc. This means that mission-critical electronics, software, networking equipment, inverters, controllers, and protection relays are sourced from trusted U.S. manufacturers. Switchgear, transformers, cables, engines, and generators (also known as commoditized assets comprised of copper and steel) are safely and economically procured.

PROVEN TECHNOLOGY

SEL powerMAX garrison and mobile solutions are the merger of the TMS standard and SEL's long-standing powerMAX Power Management and Control Systems. Each of the points in Fig. 9 represents a completed powerMAX project. The x-axis is the amount of onsite generation on each microgrid.

The y-axis is the percent of control functionality performed in protective relays. One hundred percent means all functionality is completed in the relays; 0 percent means all functionality is performed in a centralized RTAC.

This scatter plot shows that smaller power systems are predominately controlled by protective relays. Larger

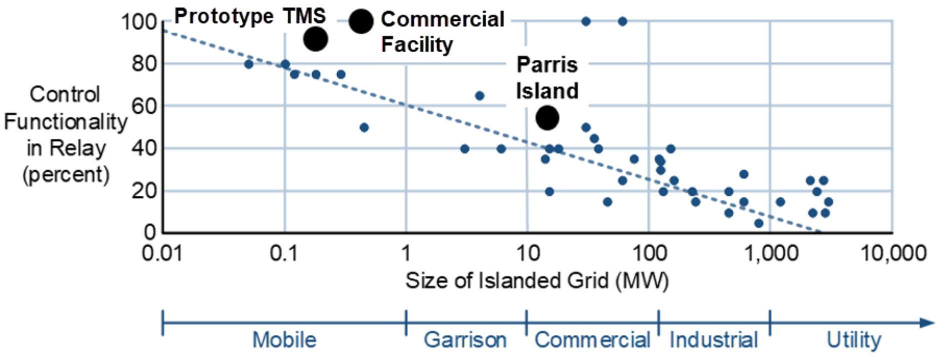


Figure 8: *Completed POWERMAX Projects*

power systems involving more relays require a comprehensive central microgrid controller [16] [17] [18].

SECURITY FROM THE GROUND UP

Multifunction protective relays are the primary control, protection, and automation devices used in the U.S. transmission, generation, and distribution stations of America's bulk electric grid. U.S. utilities strongly prefer relays invented, researched, developed, manufactured, assembled, tested, and supported in the USA [19]. Manufacturers must have a culture of cybersecurity rooted in the concepts of least privilege, need-to-know, and defense-in-depth. Access to manufacturing facilities must be tightly controlled, and 24/7 security must monitor all buildings and access.

The design of multifunction relay hardware, firmware, and supporting software must be subjected to a rigorous peer-review process to ensure the products correctly satisfy customer needs, do not include unnecessary features, and are as simple as possible to use.

A thorough product testing regimen is exhaustive. Threat model analysis is used to review full system architecture. All source code must be reviewed for correctness of function and implementation, then subjected to automated and manual testing designed to detect errors that could result in malfunction or vulnerability. Automated code inspection is used to augment peer code reviews. Version control ensures that all source code, specification documents, and drawings are maintained in a secure, access-controlled repository.

Unit testing ensures that all code modules are exercised and satisfy the design specification. Functional tests are performed on the product or system by automated tools and human testers to verify that it performs as expected on a function-by-function basis. Negative testing, one of which is fuzz testing, is used to prove that the system does not misoperate. For example, deliberately distorted data is sent to external interfaces, trying to induce an error condition. Commercial vulnerability scanning tools are also used to test mission-critical products. Validation testing ensures that the product functions as intended in realistic use cases.

Software is digitally signed using an extended validation code-signing certificate with a key securely held in a hardware security module. Firmware can be authenticated by comparison with a reference hash value available from the manufacturer.

When a manufacturer identifies a defect in a product that could cause a misoperation, failure, or vulnerability, customers should be quickly notified with a service bulletin, which describes the problem, risk to the customer, and mitigation steps.

SUPPLY CHAIN SECURITY

Manufacturers of mission-critical electronics must embed supply chain security in their principles of operation. Suppliers must be viewed as part of the manufacturing process and educated in the mission, values, and processes of a manufacturer.

An essential step in ensuring supply chain security (cyber and otherwise) and quality is to form lasting, collaborative relationships with each supplier [20]. Manufacturers should clearly communicate their expectations, while at the same time cultivating a commitment to the success of the supplier. Forming strategic relationships results in wins for all parties. A successful supplier selection process requires input from R&D, quality, purchasing, and security teams, ensuring that every supplier and component is vetted from different perspectives.

Manufacturers should use a trust-but-verify approach to conduct onsite audits of suppliers to verify that security safeguards and quality processes conform to their own understanding and expectations, and to better understand risks to supplier business models. Supplier assessment and monitoring is continuous and extends to cybersecurity and financial health.

It is essential to maintain a detailed record of every product manufactured. Recording where each product is installed allows a manufacturer to rapidly notify customers about potential quality or security concerns. Product serial number, firmware, and subassemblies must be tracked. Manufacturers must know who built a product, when it was built, which plant built it, what assembly lines it was built on, and what test station was used. Manufacturers must track who bought it, the identity of the end user, how it was shipped, and who is supporting the product.

A warranty program can be used to improve supplier quality. A long warranty period guaranteeing repair or replacement for the life of a product provides an incentive for customers to return products when they fail. Returned products are analyzed by product experts until root cause is identified, allowing R&D and manufacturing teams to constantly improve designs.

Manufacturers must ensure every critical subcomponent can be sourced from at least two vetted suppliers. Components must be obtained from U.S. suppliers whenever feasible. Suppliers subject to control by potential geopolitical adversaries must be avoided. All software must be created internally, providing a quality control advantage along with the ability to make rapid fixes and enhancements. Vertical integration enhances oversight and custody of products, from R&D design through the complete manufacturing process. This control mitigates the chances of malicious code or components making their way into mission-critical products.

Suppliers must autonomously and continuously scan the threat landscape outside their own company. A devoted 24/7 security operations center, in concert with a business intelligence unit, works to enhance security. These teams must scour an array of public and private threat and other intelligence streams to detect cybersecurity or physical threats to supply chains and internal infrastructure.

CONCLUSION

The result of these cooperative R&D efforts is a power delivery system with superior resilience, lower fuel usage, less emissions, interoperability with renewables and batteries that is simple to set up, operate, and maintain.

TMS-compliant mobile and garrison microgrid systems can be acquired from SEL today. These SEL systems are designed to update older gensets and switchgear with the latest TMS technology. Users can upgrade their existing onsite gensets in small, affordable increments.

ACKNOWLEDGMENT

SEL acknowledges the U.S. Army Corps of Engineers Construction Engineering Research Laboratory (CERL), the U.S. Army Combat Capabilities Development Command (C5ISR), and MIT Lincoln Laboratory for their close cooperation.

REFERENCES

[6] NREL, “Unique Procurement Process Expands Microgrid Research Capabilities at the ESIF,” February 2019. Available: https://www.nrel.gov/news/program/2018/procurement-expands-microgrid-research-capabilities-at-esif.html

[7] SEL, “NREL Selects SEL Microgrid Controller for the Energy Systems Integration Facility,” August 2018. Available: selinc.com.

[8] “Navigant Research Leaderboard: Microgrid Controls – Assessment of Strategy and Execution for 15 Microgrid Controller Vendors,” 2018. Available: https://www.navigantresearch.com/reports/navigant-research-leaderboard-microgrid-controls.

[9] MIT Lincoln Laboratory, “Ten Lincoln Laboratory Technologies Earn 2019 R&D 100 Awards,” November 2019. Available: https://www.ll.mit.edu/news/ten-lincoln-laboratory-technologies-earn-2019-rd-100-awards.

[10] S. Manson, B. Kennedy, and M. Checksfield, “Solving Turbine Governor Instability at Low-Load Conditions,” proceedings of the 2015 IEEE Petroleum and Chemical Industry Technical Conference, Houston, TX, October 2015.

[11] “Microgrid System Design, Control, and Modeling Challenges and Solutions Webinar,” June 2019. Available: https://selinc.com/events/on-demand-webinar/126002/.

[12] Department of Defense Interface Standard TMS, Tactical Microgrid Standard, February 2017.

[13] Tactical Microgrid Explainer Video. Available: https://selinc.com/solutions/microgrids/.

[14] SEL POWERMAX for Mobile Microgrids trailer demonstration. Available: https://selinc.com/solutions/microgrids/.

[15] S. Manson and D. Anderson, “Practical Cybersecurity for Protection and Control System Communications Networks,” proceedings of the 2017 Petroleum and Chemical Industry Technical Conference (PCIC), Calgary, AB, Canada, September 2017.

[16] North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards. Available: nerc.com.

[17] Pacific Northwest National Laboratory and U.S. Department of Energy, “Expanding the Impact of DOE Technology for Energy Cybersecurity.” Available: https://selinc.com/api/download/124796/.

[18] IEEE 2030.7, IEEE Standard for the Specification of Microgrid Controllers.

[19] IEEE 2030.8, IEEE Standard for the Testing of Microgrid Controllers.

[20] IEEE 1547, IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources With Associated Electric Power System Interfaces.

[21] K. G. Ravikumar, S. K. Raghupathula, and S. Manson, “Complete Power Management System for an Industrial Refinery,” proceedings of the 2015 IEEE Petroleum and Chemical Industry Technical Conference, Houston, TX, October 2015.

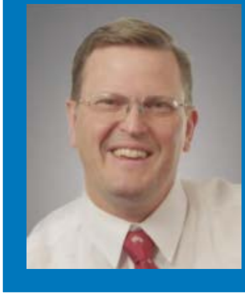
[22] E. Roy Hamilton, J. Undrill, P. S. Hamer, and S. Manson, “Considerations for Generation in an Islanded Operation,” *IEEE Transactions on Industry Applications*, Vol. 46, Issue 6, Nov.-Dec. 2010.

[23] S. Manson, K. G. Ravikumar, and S. K. Raghupathula, “Microgrid Systems: Design, Control Functions, Modeling, and Field Experience,” proceedings of the 2018 Grid of the Future Symposium, Reston, VA, October 2018.

[24] Newton-Evans, “Worldwide Study of the Protective Relay Marketplace in Electric Utilities: 2019-2022.” Available: newton-evans.com.

[25] SEL, “Securing Your Supply Chain: Best Practices From SEL,” Available: selinc.com.

ABOUT THE AUTHOR



SCOTT MANSON received his M.S.E.E. from the University of Wisconsin–Madison and his B.S.E.E. from Washington State University. Scott is presently the engineering services technology director at Schweitzer Engineering Laboratories (SEL), Inc. In this role, he provides consulting services on control and protection systems worldwide. Scott is a registered professional engineer in five states and holds 11 patents.

FUTURE EVENTS

HDIAC *Homeland Defense & Security Information Analysis Center*

JANUARY

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

FEBRUARY

S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29

MARCH

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

APRIL

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

JANUARY 2020

DoD CBRN Survivability Conference
San Diego, CA
January 14, 2020 thru January 15, 2020

Surface Navy Association's 32nd Annual National Symposium
Arlington, VA
January 14, 2020 thru January 16, 2020

UFC-DoD Minimum Antiterrorism Standards for DoD Buildings
San Diego, CA
January 28, 2020 thru January 30, 2020

Operational Energy Summit 2020
Washington, DC
January 29, 2020 thru January 31, 2020

FEBRUARY 2020

Military Additive Manufacturing Summit and Technology Showcase
Tampa, FL
February 5, 2020 thru February 6, 2020

Marine West
Marine Corps Base, Camp Pendleton, CA
February 6, 2020 thru February 7, 2020

National Fire Control Symposium
Lake Buena Vista, FL
February 10, 2020 thru February 13, 2020

MARCH 2020

Human Systems Conference
Arlington, VA
March 3, 2020 thru March 4, 2020

Border Security Expo
San Antonio, TX
March 11, 2020 thru March 12, 2020

Biometrics Institute US Conference
Alexandria, VA
March 26, 2020

Cyber Security for Critical Assets Conference
Houston, TX
March 24, 2020 thru March 25, 2020

WearRAcon20 – Wearable Robotics Association
Scottsdale, AZ
March 30, 2020 thru March 31, 2020

2020 Preparedness Summit
Dallas, TX
March 31, 2020 thru April 3, 2020

Homeland Defense and Security Systems
Information Analysis Center
901 N. Stuart St
Suite 401
Alrington, VA 22203

THE CENTER OF EXCELLENCE IN HOMELAND DEFENSE AND SECURITY INFORMATION SYSTEMS

Leveraging the best practices and expertise from government, industry, and academa in order to solve your scientific and technical needs.

https://www.hdiac.org/journal

To subscribe to the HDIAC Journal please email us at ***info@hdiac.org****, and to learn more about the HDIAC please visit us at* ***https://www.hdiac.org*** *and register to become a member of the HDIAC community of practice.*

HDIAC Mission Statement

The mission of the HDIAC is to provide users with focused expert technical consulting and unbiased scientific and technical information through in-depth analysis and the creation of specialized information products in support of the HDIAC's eight vital technical focus areas.