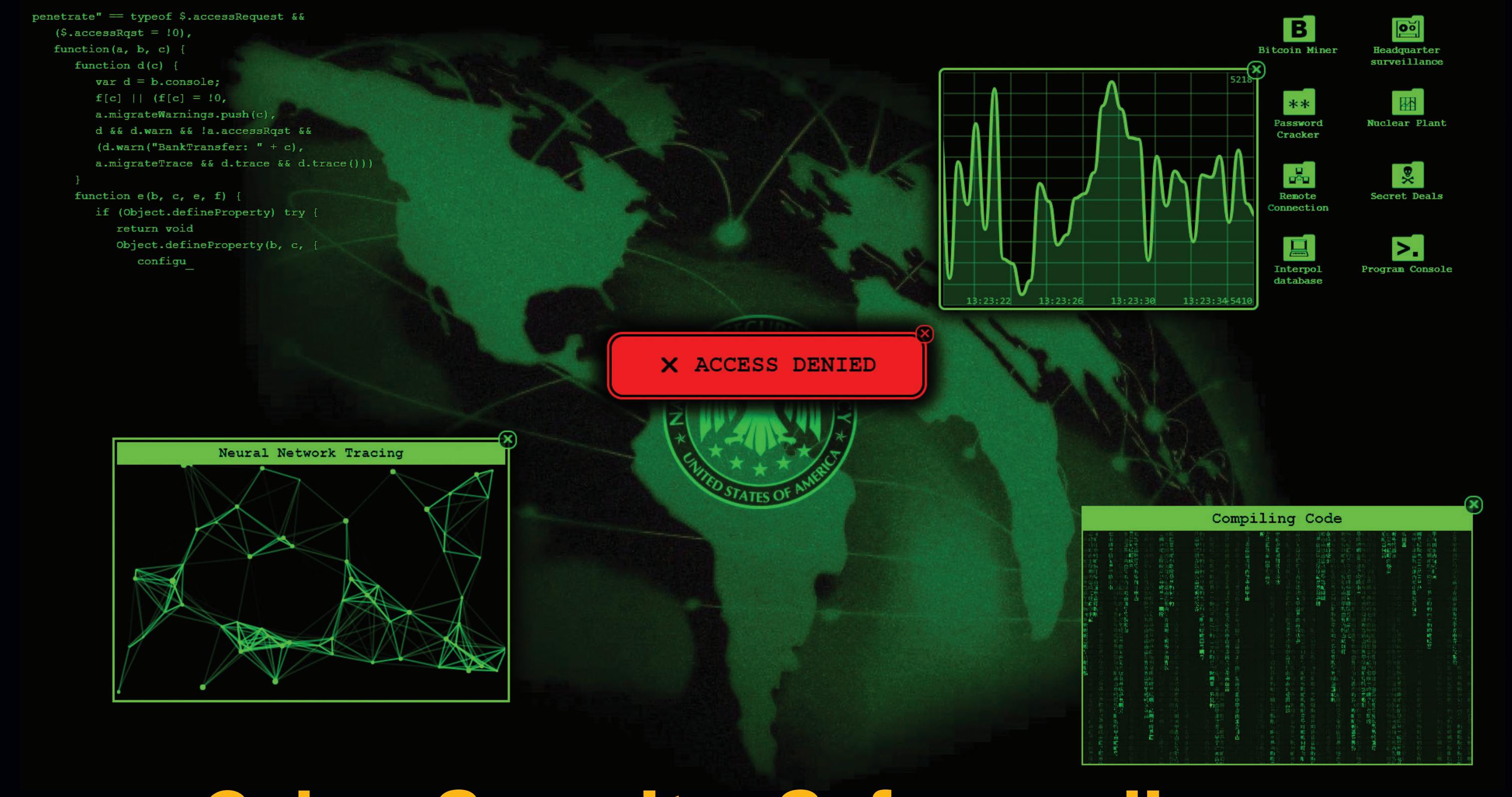
Defence Global

Land, Sea, Air and Security

November 2018 Edition

Foreword by
General Mark Carleton-Smith CBE ADC Gen,
Chief of the General Staff



```
penetrate" == typeof $.accessRequest &&
    ($.accessRqst = !0),
    function(a, b, c) {
        function d(c) {
            var d = b.console;
            f[c] || (f[c] = !0,
            a.migrateWarnings.push(c),
            d && d.warn && !a.accessRqst &&
            (d.warn("BankTransfer: " + c),
            a.migrateTrace && d.trace && d.trace()))
        }
        function e(b, c, e, f) {
            if (Object.defineProperty) try {
                return void
                Object.defineProperty(b, c, {
                    configu_
```

Cyber Security: Safeguarding Critical Operational Technology

Introducing Nebraska Applied Research Institute (NARI) at the University of Nebraska

University of Nebraska Medical Center's iEXCEL is working closely with NARI to develop a virtual test bed which will anticipate cyber risks for training facilities and engineering staff.

Offering cutting-edge cyber security solutions, NARI focuses on cyber physical systems in the healthcare, utilities and defense domains. Risks to operational control systems sustaining vital infrastructures have grown exponentially. Training opportunities, applied research and the availability of cybersecurity testbeds make NARI the right solution to your cyber security concerns.

The Davis Global Center, future home to the UNMC iEXCEL program, incorporates a wide range of innovative, best-in-class technologies – from visualization to high fidelity clinical simulators – to address competency development through the use of safe simulated yet realistic environments.

Expertise & Capabilities:

iEXCEL:

- Augmented and Virtual Reality (AR/VR) content development
- Clinical and surgical training using simulation and visualization
- Dedicated simulation environments for research, development & testing

NARI:

- Cybersecurity testbeds for replication of operational environments
- Applied research in complex cyber problems
- Training a cyber savvy IT and operational technology workforce

Explore training and research opportunities with UNMC by contacting: Pamela Boyers, Ph.D., at 00-1-402-559-2442 or pamela.boyers@unmc.edu / Omaha, Nebraska, USA

unmc.edu/iexcel
nari-cyber.com

UNIVERSITY OF NEBRASKA
MEDICAL CENTER
iEXCEL℠

NEBRASKA APPLIED
RESEARCH INSTITUTE
at the University of Nebraska

Nebraska Applied Research Institute (NARI): University of Nebraska

Cybersecurity of Operational Technology Control Systems

The Nebraska Applied Research Institute (NARI) specializes in solving complex cybersecurity problems for operational technology (OT) systems in the healthcare, utilities and defense domains. With cyber attacks a persistent threat, the risks to operational control systems that sustain vital infrastructures have grown exponentially. In 2017, hospitals and healthcare facilities became the number one target of cyber criminals utilizing ransomware, due to the life-critical nature of the environments. Cyber criminals, nation states and terrorist organizations are increasingly probing and attacking power grid, utility and defense operational technology networks to cause or threaten critical impacts.

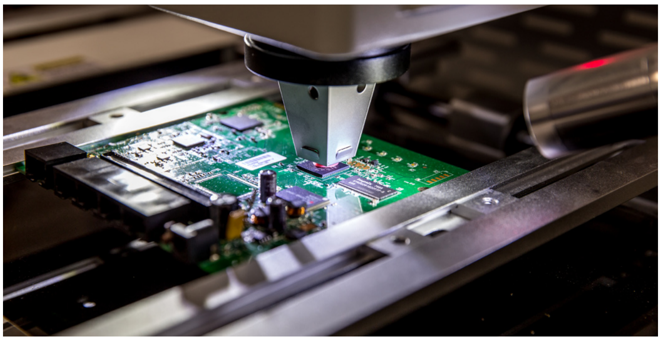
The NARI Team

NARI's multi-disciplinary, industry-certified team employs engineering and cybersecurity best practices to tailor solutions for OT networks. NARI's collective expertise stems from skilled professionals with 30+ years in the power and utilities markets, 20+ years in the Intelligence Community (IC) and Department of Defense (DoD), and over a decade of experience in managing healthcare facilities. Staff include cyber testbed and software engineers who possess industry-recognized certifications (relevant to their roles), including but not limited to, the GICSP, CSSLP, and CISSP, which are DODi 8570 compliant, and US government security clearances. This experienced team truly understands the full range of IT and OT problems spanning technology, risk-management, compliance and business aspects of cybersecurity. NARI also has access to university faculty researchers and facility experts, as well as the full resources of the University of Nebraska.

Through contracting with utilities, health systems, architectural/engineering firms, the United States DoD, regulatory agencies and many private industries, to respond to their needs, NARI helps to solve pressing and vital problems that potentially lead to security breaches.

Scope of Capabilities

Capabilities and services focus on developing solutions in the TRL 3-7+ space and ensure clients discover, assess, manage and mitigate OT cybersecurity problems in safety, mission and life-critical environments. NARI's services provide both offensive and defensive solutions to customers' OT needs, including risk assessments, penetration testing, testbed design, training and awareness, applied research, and vulnerability and mitigation research.



1. **Testbeds - Test and Development Environments**

Test and Development Environments (TDEs) allow for high-fidelity replication of operational environments. They enable deep introspection of each device in the environment - without risk to its corresponding operational environment. TDEs are increasing due to being required by federal and other regulatory bodies as a significant component of validating the cybersecurity of operational controls in buildings. These testbeds serve to assess the interaction of diverse control systems, IP networks, and ongoing software and hardware updates. With competent testbeds, building systems can be designed without risk to protect occupants, revenue streams and valuable assets. The NARI TDE facilitates the organization's ability to test how patches will affect the environment prior to deployment and how to properly mitigate vulnerabilities without affecting the production network.

2. **Training and Research Needs**

It is essential for leaders, executives and facility managers to fully comprehend the business risks and protection requirements of operational control systems. Therefore, NARI offers cutting-edge training for a wide range of participants in order to provide the necessary experience and skills required to excel in decision making for companies and associated stakeholders.

For the majority of organizations, the cybersecurity skill and knowledge gap between IT and OT staff creates organizational, regulatory and compliance risks, and vulnerabilities that can be addressed with the right training.

NARI's training philosophy is similar to the DOD's "train as you fight", such that hands-on training brings together IT and OT audiences to build skills, communications and collaboration to address gaps in real-world scenarios and live networks using testbeds. NARI offers training opportunities tailored not only to operators and technicians, but also for the executive level leadership. All NARI courses are taught on site at the Omaha, Nebraska facility with access to industrial testbeds which are incorporated into the classes. All laptops, training materials and other training aids are fully provided, leaving attendees free to concentrate on the material presented. All courses are instructor led and include a mix of hands-on and lecture/discussion-style training. Specialized training workshops include: Executive Cybersecurity, Network Analysis and Building Control Systems Incident Response.

3. **Vulnerability Assessment**

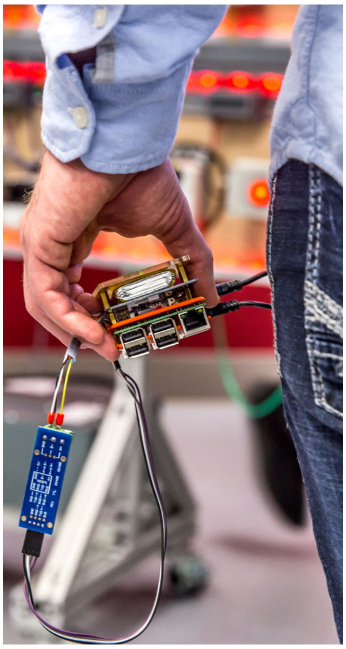
NARI's certified staff performs penetration testing and assessments of vulnerabilities in operational control systems, medical and other devices; and evaluations of OT networks for vulnerabilities, network designs for weaknesses, and individual control systems for specific vulnerabilities.

4. **Creation of Software and Firmware Tools**

NARI developers create custom tools to address analysis, security and virtualization of control systems. Modern software architecture and best practice secure coding standards are combined to create resilient and flexible tools to develop revolutionary capabilities to bridge the IT and OT cybersecurity gaps.

5. **Applied Research**

NARI's applied research group focuses on solving complex cyber problems for customers. Research areas include: medical device security, industrial control systems, utility control systems, fire and life-safety systems, building control systems, and machine learning to discover cyber defense mechanisms, as well as incident response technology. All research is conducted in strict confidence and complies with applicable guidelines and regulations.



Author:
W. Owen Redwood, Ph.D. GICSP, Chief Research Officer for NARI

Contributing Editor:
Pamela J. Boyers, Ph.D., Associate Vice Chancellor for iEXCEL, University of Nebraska Medical Center

NEBRASKA APPLIED
RESEARCH INSTITUTE
at the University of Nebraska

UNIVERSITY OF NEBRASKA
MEDICAL CENTER
iEXCEL℠

For more information please visit:
www.unmc.edu/iexcel