Lawrence Livermore National Laboratory

Science & Technology REVIEW

March 2022

CYBERDEFENSE OF CRITICAL INFRASTRUCTURE

Also in this issue:

Carbon Dioxide Storage Simulations

Early Career Research Program Update

Advancing 3D Nuclear Batteries

About the Cover

Livermore researchers have developed an immune infrastructure framework that brings together advanced cyber–physical modeling and simulation, network analysis, software assurance, artificial intelligence, and collaborative autonomy algorithms to defend the industrial control systems that manage the nation's critical infrastructure. On the cover, an artist's rendering depicts a protective framework blocking red malicious code.

Cover design: Alii Diaz; illustration: Ryan Goldsberry

About *S&TR*

At Lawrence Livermore National Laboratory, we focus on science and technology research to ensure our nation's security. We also apply that expertise to solve other important national problems in energy, bioscience, and the environment. *Science & Technology Review* is published eight times a year to communicate, to a broad audience, the Laboratory's scientific and technological accomplishments in fulfilling its primary missions. The publication's goal is to help readers understand these accomplishments and appreciate their value to the individual citizen, the nation, and the world.

The Laboratory is managed by Lawrence Livermore National Security, LLC (LLNS), for the National Nuclear Security Administration (NNSA), a semi-autonomous agency within the U.S. Department of Energy (DOE). LLNS is a limited liability company managed by Bechtel National, Inc.; the University of California; BWXT Government Group, Inc.; and Amentum. Battelle Memorial Institute also participates in LLNS as a teaming subcontractor. Cutting-edge science is enhanced through the expertise of the University of California and its 10 campuses and LLNS' affiliation with the Texas A&M University system. More information about LLNS is available online at www.llnsllc.com.

Please address any correspondence (including name and address changes) to *S&TR*, Mail Stop L-664, Lawrence Livermore National Laboratory, P.O. Box 808, Livermore, California 94551, or telephone (925) 422-1651. Our e-mail address is str-mail@llnl.gov. *S&TR* is available online at str.llnl.gov.

Prepared by LLNL under contract
DE-AC52-07NA27344

Science & Technology REVIEW

March 2022

Lawrence Livermore National Laboratory

Contents

S&TR Staff

Scientific Editor
Amanda Askin

Managing Editor
Mitch Vander Vorst

Publication Editor
Genevieve Sexton

Writers
Allan Chen, Shelby Conn, Caryn Meissner, and Genevieve Sexton

Art Director
Alii Diaz

Proofreaders
Caryn Meissner and Deanna Willis

***S&TR* Online**
Jason Barrett, Pam Davis Williams, and Cyndy Willis-Chun

Print Coordinator
Chris Brown

S&TR, a Director's Office publication, is produced by the Technical Information Department under the direction of the Office of Planning and Special Studies.

S&TR is available online at str.llnl.gov

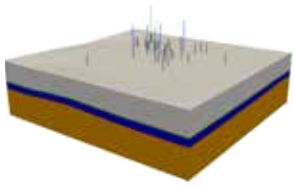
Printed in the United States of America

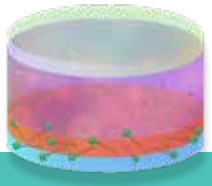
Available from
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Road
Springfield, Virginia 22161

UCRL-TR-52000-22-3
Distribution Category UC-99
March 2022

Feature

Research Highlights





Departments

Researchers Pin Down Elusive Tantalum Properties

Work by Lawrence Livermore researchers has quelled debate surrounding the melting point for the transition metal tantalum. The June 24, 2021, *Physical Review Letters* paper notes that scientists had previously disagreed on whether tantalum experiences structural phase changes before melting. This work refines existing experimental techniques and shows that investigating thoroughly studied materials bolsters the scientific community's confidence in obtained results.

Utilizing the Omega Laser Facility at the University of Rochester's Laboratory for Laser Energetics (LLE), the team subjected tantalum samples to a series of increasingly powerful shockwaves, bringing the metal closer to a fully liquid state. Nanosecond x-ray diffraction, which avoids heating-induced chemical reactions, probed the sample's interior and revealed the internal phase structure. The team found that tantalum, in fact, keeps its body-centered cubic formation until melting and that the melt curve at multimegabar pressures is steeper than previously thought.

"Our work provides improved physical information for how materials melt and respond at extreme conditions," says Rick Kraus, the paper's lead author. "Our findings increase understanding of how the iron cores of rocky planets solidify and improve predictions of materials experiments at the National Ignition Facility." Livermore contributors included Dayne Fratanduono, Ray Smith, Amy Lazicki, Christopher Wehrenberg, and Jon Eggert, as well as LLE researchers J. Ryan Rygg and G. W. Collins.

Contact: Rick Kraus (925) 422-1454 (kraus4@llnl.gov).

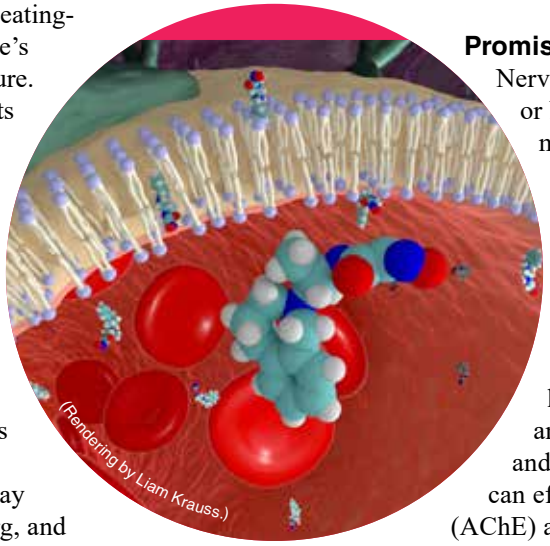
New Technology Powers X-Ray Movies

The ongoing active reset research for linear induction accelerators is quickly progressing toward a functional x-ray movie technology—a new diagnostic capability to Lawrence Livermore. In a Laboratory first, the project's Bipolar Research Experiment, a bipolar solid-state, pulsed-power system, accelerated (provided energy gain to) kiloamps of electron beam at Livermore's Flash X-Ray (FXR) deep-penetration radiographic facility.

Accelerator physicist Nathaniel Pogue explains, "The objective is to produce 20 to 100 beam pulses, separated by tens to hundreds of nanoseconds. Each beam pulse creates a frame in a radiographic movie." Such rapid timing is made possible by the newly added bipolar cells and solid-state pulsers along the FXR beamline. Between pulses, the cells quickly reenergize to accelerate the next beam pulse. Measurements confirmed that the cells transferred energy from the pulser to the beam, confirming the viability of both the hardware and methodology.

Pogue leads a multidisciplinary team working to finish the design, construction, and demonstration of a test injector, the Imperator. Once completed, the integrated system, which includes the bipolar solid-state, pulsed-power system, led by Katherine Velas, should be able to both produce and accelerate an electron beam. This capability will supply future hydrodynamics experiments with up to 10 times more image data than currently possible and provide more information with fewer experiments in support of the National Nuclear Security Administration's Stockpile Stewardship Program.

Contact: Nathaniel Pogue (925) 422-9192 (pogue1@llnl.gov).



Promising Nerve-Agent Antidote

Nerve agents like sarin, venomous agent X, or Novichok block the transmission of messages from the brain and spinal cord or central nervous system (CNS) to the peripheral nervous system (PNS), which controls vital processes such as breathing and heart rate. Unfortunately, current nerve-agent antidotes only protect the PNS as they cannot cross the blood–brain barrier (BBB)—leaving the CNS vulnerable. Effective antidotes must be able to cross the BBB and use small molecule-based oximes that can efficiently restore acetylcholinesterase (AChE) activity—a crucial neurotransmission enzyme nerve agents target.

Scientists from Livermore's Forensic Science Center (FSC) developed a promising and multifunctional antidote, LLNL-02, to counteract exposure to nerve-agent poisoning. LLNL-02 is a novel CNS-permeable oxime reactivator, making it the first antidote of its kind to achieve both BBB penetration and AChE reactivation.

To identify potential candidate compounds, researchers used computational modeling predictions and synthetic chemistry. The computational predictions were then validated with detailed in vitro and in vivo assays, and after two years, the team's efforts led to the discovery of LLNL-02. FSC Director Audrey Williams says, "LLNL-02 is a promising, versatile compound that demonstrates a path forward for protecting against bioterrorism and chemical weapons." The research, performed in conjunction with the U.S. Army Medical Research Institute of Chemical Defense, appeared in the July 30, 2021, issue of *Scientific Reports*.

Contact: Carlos Valdez (925) 423-1804 (valdez11@llnl.gov).

Commentary by Huban Gowadia

Dedication to Innovation and Mission

THIS issue of *Science & Technology Review* highlights the strength of the Laboratory's innovations, the profound impact our science and technology (S&T) has on our national security, and the Laboratory's values: ideas, impact, integrity, inclusiveness, and zeal. Despite the pandemic, we carried out our missions, including S&T research to protect our nation's infrastructure from cyberthreats, paving the path toward a low-carbon future and climate resilience, exploring new battery technology that can enhance human health, and supporting early-career staff as they break new ground in S&T.

This issue's feature article, beginning on p. 4, showcases how we are fortifying our nation's critical infrastructure against cyberattacks, and enhancing our national security at a time when cyberthreats are increasingly in the spotlight. Our immune infrastructure framework presents a paradigm shift. Instead of focusing only on keeping the adversary out, which is impractical when defending against nation-state adversaries, it accepts that cybersecurity breaches may occur and focuses on ensuring that our critical infrastructure continues to operate despite that compromise.

By bringing together network analysis, artificial intelligence, and collaborative autonomy, we are innovating capabilities to defend our critical infrastructure—electric, water, transportation, and cyber–physical systems. We are focused on a layered defense: understanding the systems, keeping the adversary out, detecting and responding to intrusions, and operating through compromise. In addition to defending against cyberattacks, these tactical layers help the nation's critical infrastructure become more resilient to physical attacks and natural hazards, including the effects of climate change as extreme weather events become more common.

The Laboratory is also supporting climate resilience by developing pioneering tools to sequester carbon dioxide (CO_2) deep underground. Carbon capture and storage is one of the long-term solutions needed to reach carbon neutrality and mitigate climate change. By harnessing our expertise in geochemistry, engineering, seismology, hydrology, and computational geoscience, Livermore has created the first open-source, scalable, portable, and exascale-ready simulation software supporting industrial-scale carbon sequestration: GEOSX, which will improve the planning, management, and security of geological repositories by simulating how fluids flow and rocks break deep underground. As open-source code, and through partnership with industry, GEOSX will help expand future CO_2 sequestration projects worldwide.

Other projects with potential global impact are focused on developing nuclear-powered batteries. Our engineering and materials scientists are utilizing technology originally developed for national security and astrophysics applications to create 3D nuclear-powered batteries. These devices could serve as tiny, high-density power sources with decades-long lifetimes for use in biomedical implants, such as pacemakers, and could benefit the lives of patients.

Like everything we do at the Laboratory, these projects would not be possible without our exceptional workforce. Each year, the Department of Energy's (DOE's) Office of Science Early Career Research Program (ECRP) recognizes exceptional researchers at U.S. academic institutions and DOE's national laboratories by awarding them with highly competitive funding to support their projects and further facilitate their promise. Since the program's inception in 2010, Lawrence Livermore has received more ECRP awards than any other National Nuclear Security Administration laboratory. Spread across the Engineering, Computing, Physical and Life Sciences directorates, and the National Ignition Facility and Photon Science Principal Directorate, the projects these staff lead reflect the Laboratory's diverse programs and the zeal the ECRP recipients bring to realizing innovative ideas.

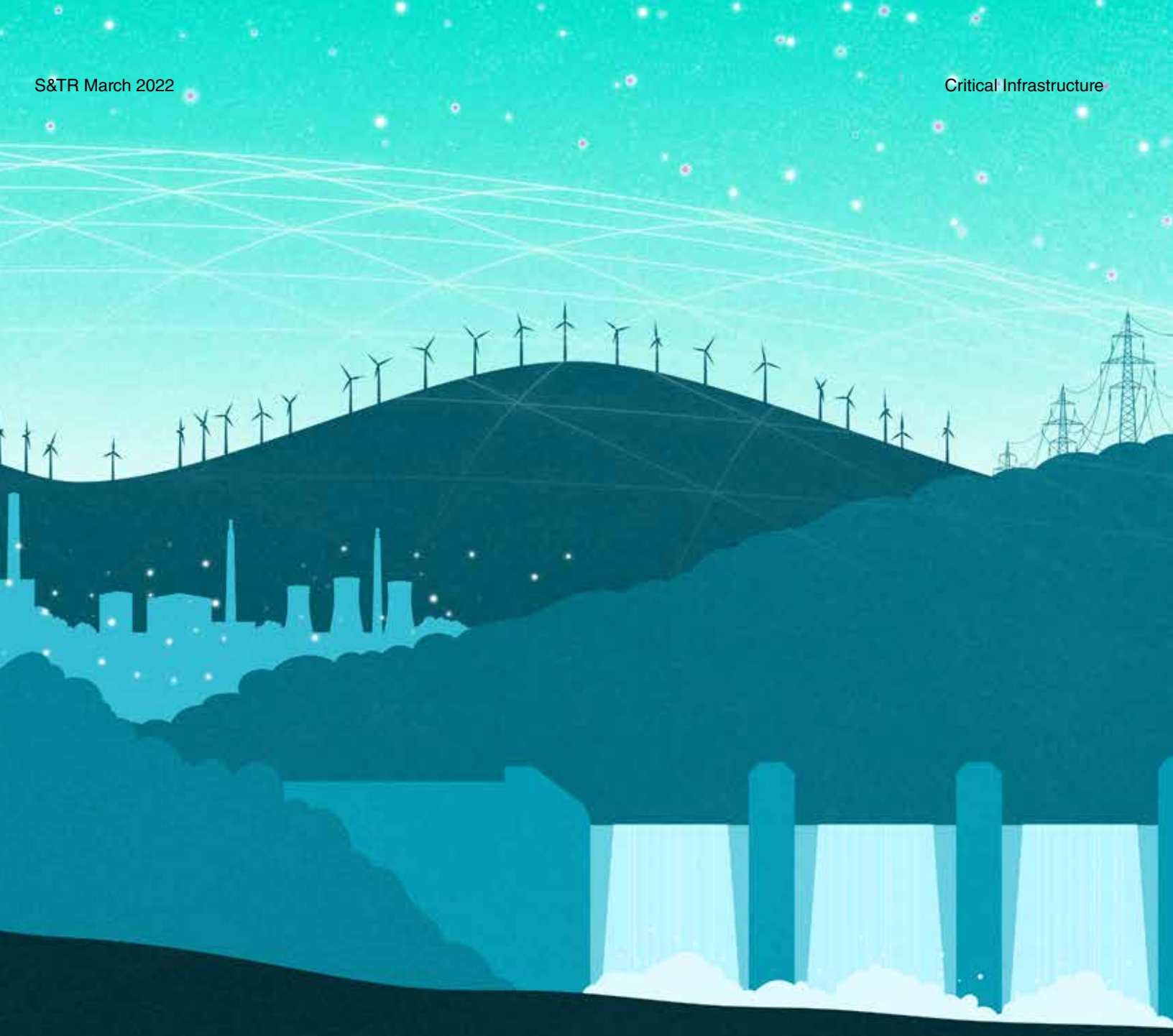
ECRP funding allows recipients to push the boundaries of their fields, build their networks, increase inclusivity, and inspire the next generation of leaders. They are a true testament to our high-caliber S&T efforts, and the diligent support provided by our Program Development Support Office.

By conducting this work during the ongoing pandemic, our teams have demonstrated resilience—never slowing down the pace of S&T innovation. The stories in this issue reflect that dedication to the Laboratory's mission. The Laboratory remains at the forefront of S&T, and we continue to deliver on our national security mission while living our values.

■ Huban Gowadia is principal associate director for Global Security.

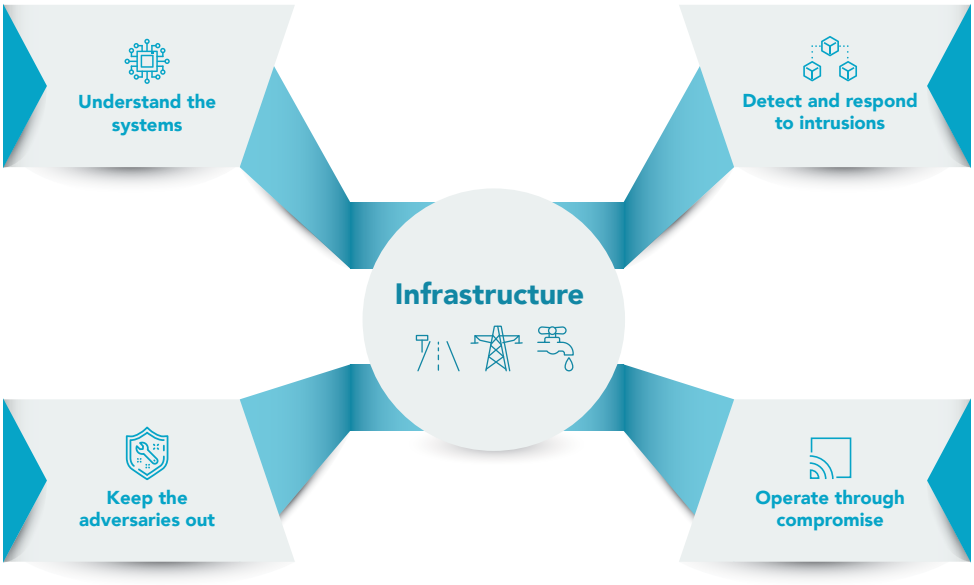
Defending U.S. Critical Infrastructure from NATION-STATE CYBERATTACKS

Researchers combine cyberdefense expertise, network analysis, artificial intelligence, and collaborative-autonomy algorithms to defend the nation's industrial control systems.



IN the news with increasing frequency are cyberattacks against critical infrastructure that supplies electricity, natural gas, water, transportation, and communication systems with the intent to disrupt these vital services. The first known cyberattack by a nation-state took place against Estonia in 2007. In response to the removal of a Soviet war monument in Tallinn, Russian-based attackers targeted state and commercial services, flooding them with junk digital traffic that rendered government, banking, and media websites inoperable. Then, in December 2015, hackers using malware compromised Ukraine's electric grid, disrupting electricity to hundreds of thousands of people. Subsequent attacks followed and in 2017, malware used against Ukraine spread globally, infecting banks, media outlets, and infrastructure in Germany, France, Italy, Poland, Russia, the United Kingdom, and Australia. Cyberattacks against electrical grids, natural gas pipelines, municipal railways, wastewater plants, and water utilities have also made headlines in the United States. Hackers have successfully extorted ransom money, collected intelligence, and disrupted critical infrastructure around the world, which, over the last several years, has become a digital front line in the conflict between nation-state adversaries.

For many years, Lawrence Livermore National Laboratory has been conducting



The Immune Infrastructure Program's vision is a strategic, layered defense that works to protect the nation's critical infrastructure from cyberattacks.

research on cybersecurity, as well as defending its systems and networks from cyberattacks. The Laboratory has developed an array of capabilities to detect and defend against cyberintruders targeting information technology (IT) networks and worked with government agencies and private-sector partners to share its cybersecurity knowledge to the wider cyberdefense community.

The proliferation of microprocessor-based industrial control systems (ICS) in recent decades has also exposed vulnerable points in critical infrastructure. In 2020, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) identified 16 critical infrastructure sectors from the chemical industry to water and wastewater facilities, whose incapacitation would weaken national security and compromise public health and safety. With the rise of cyberattacks against critical infrastructure, Livermore has increased its focus on protecting the operational technology (OT) systems, which control and monitor utilities, transportation, communication, and manufacturing processes, as well as other industrial apparatus society relies on and requires.

Cyberthreats to critical infrastructure range from unsophisticated hobbyist hackers to organized crime syndicates and expert nation-state actors. Cyberattackers of any stripe may find and exploit well-known vulnerabilities, discover new ones, or create weaknesses where none previously existed. The least threatening adversary may be no more than teenagers with laptops breaking into an ICS to snoop around. Those looking for opportunities include organized criminal organizations using ransomware to extort money. The highest level of adversary can stealthily manipulate software, hardware, and networks using a full suite of capabilities to enter otherwise secure systems. Typically, these adversaries tend to be nation-states with deep expertise and resources whose motives are not necessarily financial—but intend to disrupt infrastructure or plot a future attack. Players at this level can manipulate the software supply chain by injecting malignant code into legitimate products or place insiders within companies and service providers to gain intelligence. "The vast majority of day-to-day threats are from lower-tier adversaries, and commercial industry does a decent job of defending against these threats," says Nate Gleason, program leader for the Laboratory's Cyber and Infrastructure Resilience Program. "We focus on protecting against national security-level threats to our critical systems, which generally means nation-state actors."

Layered Defense

The Laboratory has developed the immune infrastructure framework to protect critical infrastructure from these national security threats. Its goals are to create technologies and approaches that enable intelligent, self-healing, and resilient infrastructure by applying concepts from biological immunity to protect IT and OT networks from cyberattacks and physical disruptions. The Laboratory's design of an immune infrastructure framework departs from current cyberdefense strategies, which stress creating a robust, digitally secure perimeter to keep adversaries out—now an impractical defense against high-capability adversaries. "With lower level adversaries, we can keep the bad guys out of our systems," asserts Gleason. "When faced with more sophisticated actors, we have to assume that they will inevitably find a way to compromise our systems, so we must minimize the consequences of that intrusion and make it as difficult as possible for them to achieve their goals."

The immune infrastructure framework is comprised of four layers: understanding the systems, keeping the adversary out, detecting and responding to intrusions, and operating through compromise. Development of this approach leverages the Laboratory's ability to pull together multidisciplinary expertise in cybersecurity, data science

and machine learning, power-grid engineering, infrastructure, and systems analysis to address this predicament.

Understand the Systems

The Laboratory has developed a portfolio of capabilities that enable cyberdefenders to understand the asset inventory, which includes networks, hardware components, and software, as well as how an adversary might assess the system to successfully attack it. "Layer One focuses on understanding what's in networked systems in order to defend them," says Jovana Helms, associate program leader for Civilian Cybersecurity. Critical infrastructure such as the electricity grid or a water management system includes tens of thousands of networked, electronic devices that control a physical system and communicate with each other, forming a cyber–physical system. Some Layer One capabilities are designed to understand network software, hardware, and the connections between them; others are providing continuous network and device monitoring and creating digital twins of networks so that modeling and simulation can determine critical system nodes.

Livermore's Network Mapping System (NeMS) software is a longstanding capability that produces a comprehensive representation of Internet-based computer network environments. This tool, which has been licensed by public- and private-sector users, discovers and characterizes the devices, such as switches, routers, and hosts, and their connections on a network, allowing cyberdefenders to see how the system network is operating. It also determines where the IT network touches the OT network, so that cyberdefenders can monitor vulnerable points. "We don't want any unsupervised touch points between these two networks," says Helms.

The Laboratory Directed Research and Development (LDRD) Program has funded the development of a tool that goes one step further. The Industrial Control System Intelligent Device Characterization Tool (ICS ID ChaT) uses machine learning to analyze OT networks and characterize ICS devices on the network. The software identifies where the devices sit, who the manufacturers are, and what they do. "ICS ID ChaT's objective is to understand system behavior by analyzing network traffic to discover which components are on the network, their model numbers, and in the future, their firmware—the software permanently etched into a device by the manufacturer," says Helms. "It goes beyond existing network mapping by using machine learning to scan and infer what ICS devices are actually in these systems."

While ICS ID ChaT addresses existing cyber–physical systems, Livermore researchers are also working to secure the IT and ICS supply chain, a significant point of weakness in currently networked infrastructure systems. "A single firmware update can allow an adversary to compromise hundreds of devices," says Helms. Firmware updates to any device or system that manages an industrial process typically contain proprietary code written by the device vendor, as well as code from third-party software libraries from other companies, and sometimes,

Software Bill of Materials

Filesize 1183 kb
Executable Code

5 included components

Statically Linked Libraries 5		**55%**
libc v2.24	711 functions	45%
gcc v6.3.0	60 functions	4%
zlib v1.2.9	38 functions	2%
pcre v8.44	28 functions	2%
openssl v1.1.1d	27 functions	2%

Unidentified Code 45%

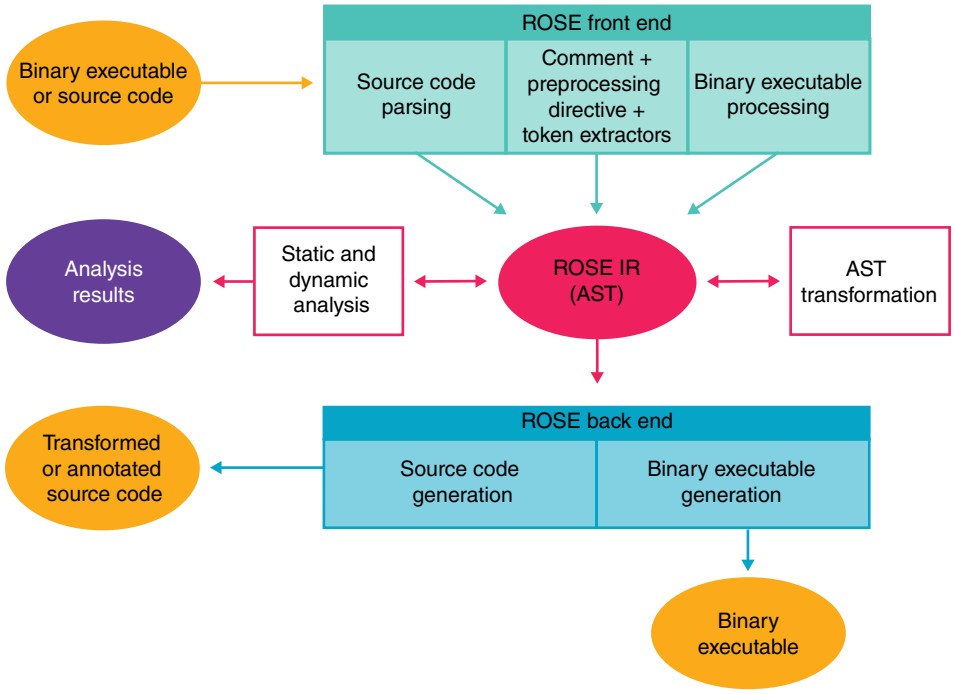
The Software Bill of Materials, much like the Nutrition Facts label on food packaging, provides cyberdefenders with information about the source of each piece of code in a software program, firmware, or automatic updates. Knowing exactly what code contains and where it came from will help cyberdefenders identify suspicious or malicious code.

even open-source code. Adversaries have successfully infiltrated and slipped malicious codes into firmware updates. A masterful example is the SolarWinds hack, discovered in 2020, which delivered a backdoor update to 18,000 corporate and institutional customers who use its network-monitoring software that gave hackers unfettered access to their networks. "We are developing tools that conduct automated software and firmware analysis, which helps us understand what's in software and crucially, firmware."

For the Valyrian Steel Project, a name drawn from the *Game of Thrones* television series, Laboratory researchers are developing a tool, Longclaw, which creates a software bill of materials (SBOM) or ingredients list for code that identifies where each component of code originated. The Department of Homeland Security–funded Longclaw tool extracts the code from a binary sequence and determines the libraries and functions that make up that code. "Knowing what libraries and functions are in software and firmware enables rapid and targeted response when a new vulnerability is discovered," says Helms. "Sometimes, the weak link is buried in the second or third layer of the software supply chain, so having SBOMs allows us to quickly recognize which systems have the vulnerability and how proliferated it is."

A third element of Layer One is modeling the physical process and the network controlling it to target vulnerable points. Sophisticated adversaries can launch attacks against dozens of components or points, while most utilities only have the computing power to model one or two components at best. Squirrel, part of the LDRD-funded Quantitative Intelligent Adversary Risk Assessment Project, is an algorithm that helps find these points by solving the inverse problem: For a given type of cyberattack and its consequence, such as shutting down components of an electrical transmission grid, Squirrel identifies the critical failures that lead to the consequence, and tells system operators which nodes of the network they should harden. The Laboratory is partnering with utilities to analyze their systems using Squirrel. One such run on a partner's grid revealed close to 200 weak nodes. Squirrel, however, also determined that protecting just 25 of those nodes would have eliminated all critical failures—a valuable insight that system operators can use to prioritize their limited resources for hardening their systems.

With funding from the Department of Homeland Security, Livermore has also launched the Night's Watch Project, bringing together several industry partners to demonstrate the Laboratory's infrastructure cyberdefense capabilities. Through efforts like these, the Laboratory is working to share these tools with electric and natural gas utilities and put them to use where they belong—defending the nation's critical infrastructure.



ROSE is a robust, open-source, compiler-based infrastructure for building source-to-source program transformation and analysis tools for static analysis, optimization, and other applications.

Keep the Adversary Out

Layer Two research provides tools to secure the hardware and software supply chain and keep the adversary out of systems. "Just because an adversary will inevitably find a way to penetrate a cybersecurity perimeter doesn't mean we should make it easy for them to do so. The idea with the layered approach is that each subsequent layer is there if the previous layer fails," says Helms. Researchers are building automated tools to increase the efficiency of device evaluation, enable cyberdefenders to verify the integrity of software and firmware updates, and develop self-verifying devices. "We have a software assurance focus, which tries to ensure that there are no flaws in the code the adversary can use to infiltrate the system," says Bob Hanson,

associate program leader for National Security Infrastructure at the Laboratory.

The Valyrian Steel Project also plays a key role in Layer Two. "It's very hard to assess large software programs even when they update monthly," explains Hanson. "Valyrian Steel focuses on automating software assurance analysis." Longclaw can also run analytics to detect suspicious features and evaluate the quality and security of the code, not just identify its contents.

ROSE, a Livermore-developed, open-source compiler for building source-to-source program analysis, is another essential Layer Two tool. With ROSE, cyberdefenders can perform automatic binary analyses of software updates in search of malicious code and scale their analysis to hundreds or thousands of pieces of software without requiring a high degree of user sophistication. FUNPAC (Firmware Updates Need Proof of Accompanying Code) is an LDRD-funded project to develop formal verification techniques for firmware. Using the ROSE compiler infrastructure, FUNPAC analyzes vendor-annotated binaries to determine if firmware conforms to security requirements. FUNPAC is designed so that grid devices such as processors, voltage converters, and regulators with limited computing power can verify that a firmware update does not contain malicious code before installing it.

Cybersecurity Testing for Resilient Industrial Control Systems (CyTRICS) is DOE's program for cybersecurity vulnerability testing, digital subcomponent enumeration, and forensic assessment. CyTRICS leverages best-in-class test facilities and analytic capabilities at six DOE national laboratories and strategic partnerships with key stakeholders including technology developers, manufacturers, asset owners and operators, and interagency partners. DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) funds CyTRICS. Lawrence Livermore is a participating laboratory in CyTRICS; performs testing on high-priority digital components in OT and ICS; brings its specialization in software analysis to the program; and leads efforts to automate testing, analysis, and SBOM generation for energy-grid devices.

Detect and Respond to Intrusions

In the Dragonglass Project, another *Game of Thrones*–themed name, Livermore researchers are building intelligent detection capabilities to automatically respond to unknown threats for the immune infrastructure framework's Layer Three. State-of-the-art detection algorithms look for signatures of network compromise. This approach works for detecting less-sophisticated adversaries, but not against the highest tier where adversaries deploy tactics that defenders are not likely to have seen before. To anticipate these unknown or unfamiliar tactics, researchers are using deep-reinforcement learning (DRL), a form of machine learning. By running a large number of transmission and distribution simulations, these algorithms can learn what a healthy system looks like and use that data to identify any behavior that could disrupt the health of the system.

"We're trying to teach the system to defend itself against attacks using deep-reinforcement learning," says Jean-Paul Watson, senior research scientist in Livermore's Center for

(a) Dragonglass uses a digital twin of a system to gather information, detect unusual behavior, isolate compromised components in a system, or counter suspicious commands.

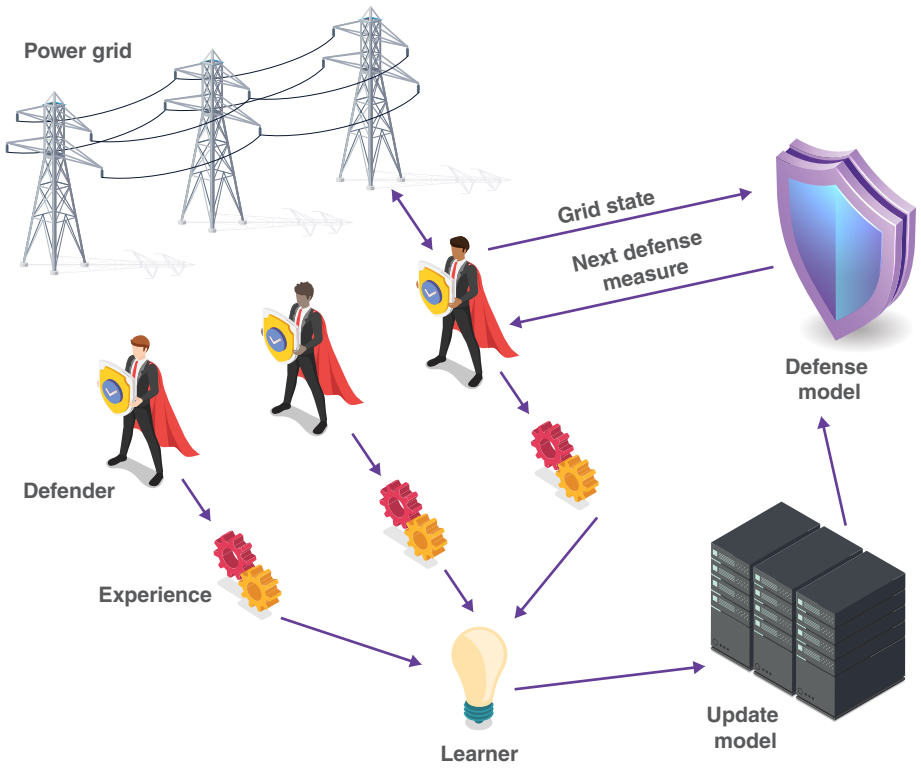
(b) Longclaw creates a Software Bill of Materials by extracting code and determining the libraries and functions within it, as well as where it originated.

(c) FUNPAC (Firmware Updates Need Proof-Accompanying Code) provides formal verification techniques by analyzing vendor-annotated binaries to establish that firmware conforms to security policy before it is installed.

Applied Scientific Computing (CASC). "We are developing a simulator for each side of the system: one that captures the physics and one that looks at the control systems' points of contact with the physical systems." Using training sets of information about what normal behavior, as well as what attacks look like on the grid, this system acts like an immune system by learning how to recognize an attack, isolate or eliminate it, and return and restore normal system functioning.

To train the algorithms to identify abnormal activities, Dragonglass uses a digital twin of a system. When unusual behavior is detected, the algorithms gather information about the event and automatically respond. For example, by closing or opening relays or countering suspicious commands, the algorithms can isolate parts of the physical system that are compromised. The algorithm can also ignore normal actions, investigate abnormal actions, make corrections, and alert human operators. DRL algorithms developed for the Dragonglass Project also have climate-change relevance: they can be used to reroute power flows around sections of the grid affected by storms or wildfires. Elements of the Dragonglass Project, which address the electric grid, are funded by DOE's Grid Modernization Laboratory Consortium, and DOE CESER funds oil and natural gas applications.

The Laboratory's Skyfall Facility is a test bed that simulates an electrical grid where researchers can run Dragonglass's DRL and other detection algorithms to evaluate their effectiveness. (See *S&TR*, December 2018, pp. 16–19.) Livermore has also partnered with the University of Toledo, where a portion of the University's campus electrical grid has been heavily instrumented, and can provide real-time electric grid operational data to help train the software. Schweitzer Engineering Laboratory manufactures equipment for electric-grid controls and, as a partner in the Dragonglass Project, provides data on how their equipment behaves under normal operating conditions.



Dragonglass uses deep-reinforcement learning to monitor a control system, determine what normal and abnormal operations look like, build a model capable of recognizing a cyberattack or a natural catastrophe, take action to eliminate the threat, and keep the system running.

Operating through Compromise

A motivated, technically sophisticated cyberattacker will inevitably find a way into a cyber–physical system despite the preceding layers of protection. Layer Four research develops capabilities to facilitate infrastructure operations despite an attack on a part of the system. "Modern infrastructure is full of digital components," says Colin Ponce, a computational mathematician at CASC. "The nation's critical infrastructure is geographically diffuse, yet connected, and programmable. In these network-connected systems, all of the devices relay their data to a central control system, which performs analysis and sends out commands. The problem is that if a cyberattacker infiltrates the control center, they have the means to shut down the entire system."

To counter this vulnerability, Livermore researchers are deploying collaborative autonomy to decentralize control of physical systems. (See *S&TR*, June 2018, pp. 12–15.) Instead of all functions relying on a single, central control center or machine, low-power edge devices—such as solar inverters, smart meters, and vehicle chargers—distributed throughout the network can perform independent analysis, verify, and communicate with neighboring devices or nodes to reach consensus

on the next steps to take—the central axiom of collaborative autonomy. "Using collaborative autonomy, many devices can self-organize into a collective whole to reliably conduct monitoring and operations. No single device or control point can precipitate system or network failure," says Ponce. "We are leveraging the distributed nature of the system and using it to our advantage."

Livermore researchers are developing algorithms that allow distributed energy resources (DER) such as solar inverters and smart meters to share input data with their neighbors, and verify, for example, the voltages of different devices based on known data patterns to determine if they are normal. The underlying method uses "gossip" or update-and-share algorithms to propagate information about what the network is communicating from one component to another like a rumor. Each device then verifies its neighbors' computations mathematically.

The robust DERMS (Distributed Energy Resource Management System) Project is an effort to apply collaborative autonomy to keeping solar inverters, which convert the variable direct-current output of a photovoltaic (PV) solar panel into an alternating current that can be fed into an electrical grid, responsive to cyberattack. In a PV grid, multiple inverters are controlled centrally, so the adversary only has to compromise one device or central controller to gain control over multiple solar inverters. An adversary could destabilize the grid by telling all inverters to, for example, power down simultaneously. Funded by the Department of Energy's (DOE's) Office of Solar Technologies, Ponce's team has inserted a verification step into software that manages the inverters. When an operator (or adversary) sends a control command to DERMS, it is then relayed to the inverters, which uses collaborative autonomy to assess and decide whether to accept or reject it.

Managing DERs through collaborative autonomy also helps grids become more resilient to climate change. A grid composed of multiple DERs can be managed as a group, keeping itself running if one DER crashes during extreme weather events. DERs could also match variable loads with demand, for example, reconciling intermittent PV availability with charging batteries for electric vehicle fleets, to smooth out uneven supply and demand.

For electric utilities, a black start—restarting the power grid from a total blackout—is the most challenging responsibility. Typically, a black start requires a large power plant to anchor the restart of the rest of the grid. But if an adversary has compromised that larger plant, the grid cannot restart. Federally owned Plum Island, in waters near Long Island, New York, is the site of government facilities equipped with an instrumented electric grid researchers can utilize to test out cybersecurity infrastructure solutions. Livermore researchers have been conducting an experiment there, the Plum Island Blackstart Project, to execute a black start using collaborative autonomy via DERs using batteries on a PV system without a central controller. DOE's Grid Modernization Laboratory Consortium funds the project. "We installed software on the Plum Island system to collaboratively manage the DERs and were able to successfully execute a black start. The technology works," Ponce explains. "We can now use DERs as a control verification framework or as a redundant control system that kicks in if the central controller is compromised. These algorithms are applicable to industrial control systems, water, communications, manufacturing—anything that's too big to see in its entirety at a glance."

Transitioning to Operations

In the immune infrastructure roadmap, the first step to building and testing the components of the infrastructure protection framework will be followed by a proof-of-concept pilot at a cyber–physical demonstration site. Livermore has taken the first steps toward this goal at Site 300, a Lawrence Livermore experimental facility 24 kilometers from the Laboratory's main site. Site 300's core mission is assessing the operation of nonnuclear components of weapons systems, and its large open space provides an ideal place to build a pilot-scale ICS. Planning has begun. "Our vision is to bring together equipment vendors and asset owners so they can see how to incorporate immune infrastructure technology and this layered framework in their own devices," Gleason says. "They will receive firsthand experience incorporating these technologies while we identify the best solutions."

—Allan Chen

Key Words: Center for Applied Scientific Computing (CASC); collaborative autonomy; climate change; cyber–physical system; cybersecurity; Cybersecurity and Infrastructure Security Agency (CISA); Department of Energy (DOE) Grid Modernization Laboratory Consortium; distributed energy resources (DER); Distributed Energy Resource Management System (DERMS); DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER); Department of Homeland Security; electricity grid; industrial control system (ICS); immune infrastructure; information technology (IT); Laboratory Directed Research and Development (LDRD) Program; Network Mapping System (NEMS); operational technology (OT); photovoltaic (PV); resilience; Skyfall; software bill of materials (SBOM).

For further information contact Nate Gleason (925) 423-6278 (gleason6@llnl.gov).

GEOSX

SIMULATES CARBON DIOXIDE STORAGE SOLUTIONS

SINCE the Industrial Revolution, atmospheric carbon dioxide (CO_2) levels have continued to rise. While oceans, plants, and soils can sequester some of this CO_2 naturally, they cannot capture and remove it all, causing the excess to make its way into the atmosphere. Long-term storage solutions are needed to address the surplus—a contributor to climate change—and help the world achieve carbon neutrality. Carbon sequestration, or the capture and storage of CO_2 in deep geologic formations, may offer promising solutions for preventing the release of CO_2 into the atmosphere and reducing its contribution to global warming as a greenhouse gas. Once captured from stationary sources, such as power plants and other large industrial facilities, CO_2 can be compressed to a dense, fluid-like state and injected deep underground into permeable, porous geologic strata for long-term isolation and storage.

In support of Lawrence Livermore's mission to improve the nation's energy security, the Laboratory has taken the lead on developing subsurface modeling and simulation software to support CO_2 storage efforts, partnering with TotalEnergies and Stanford University in a cooperative research and development agreement (CRADA) to develop an open-source tool: GEOSX. The GEOSX software is an innovative, first-of-its-kind technical achievement, supporting industrial-scale

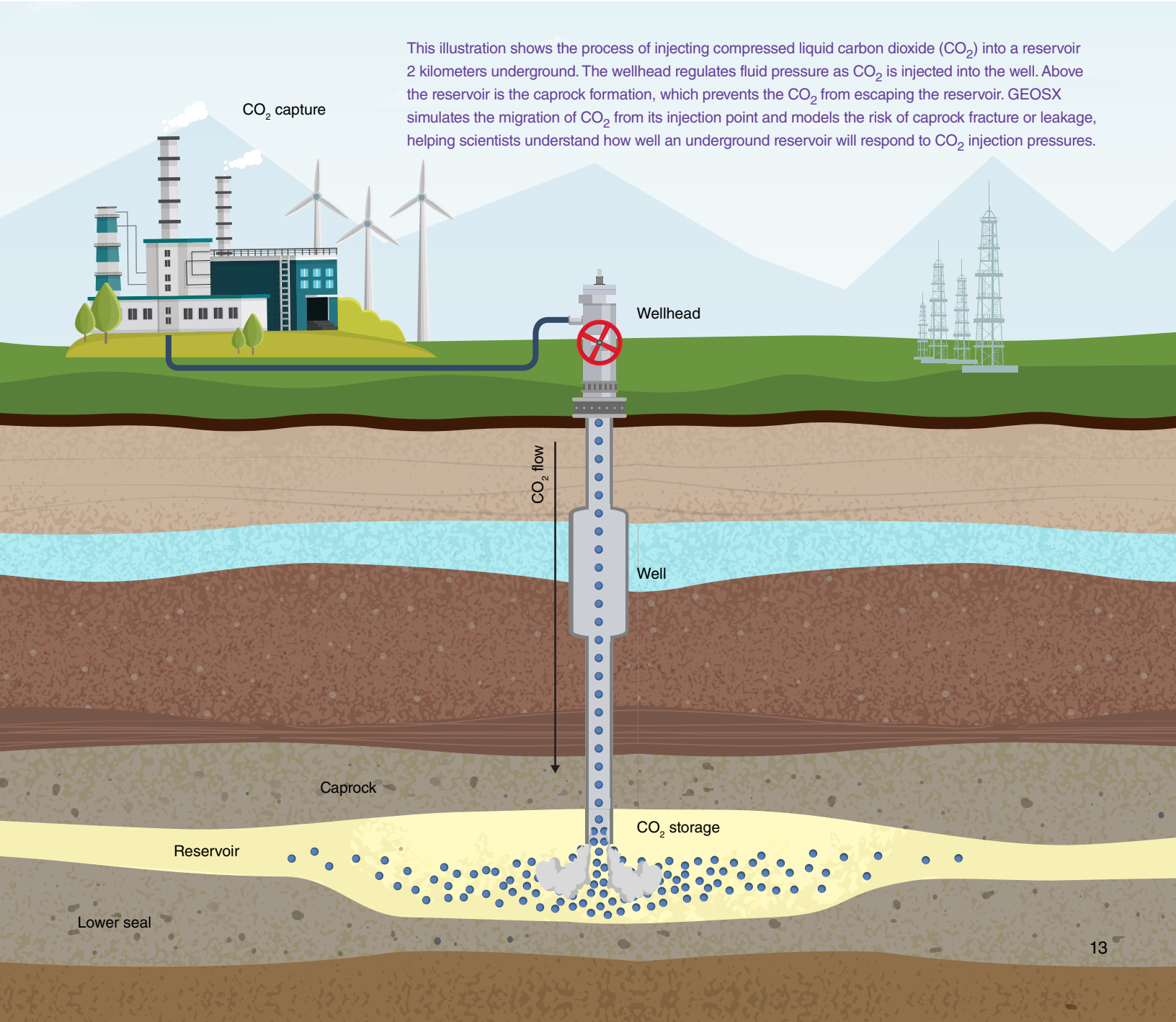
carbon sequestration. This effort further cements Livermore's leadership in computational geosciences—including the simulation of subsurface processes.

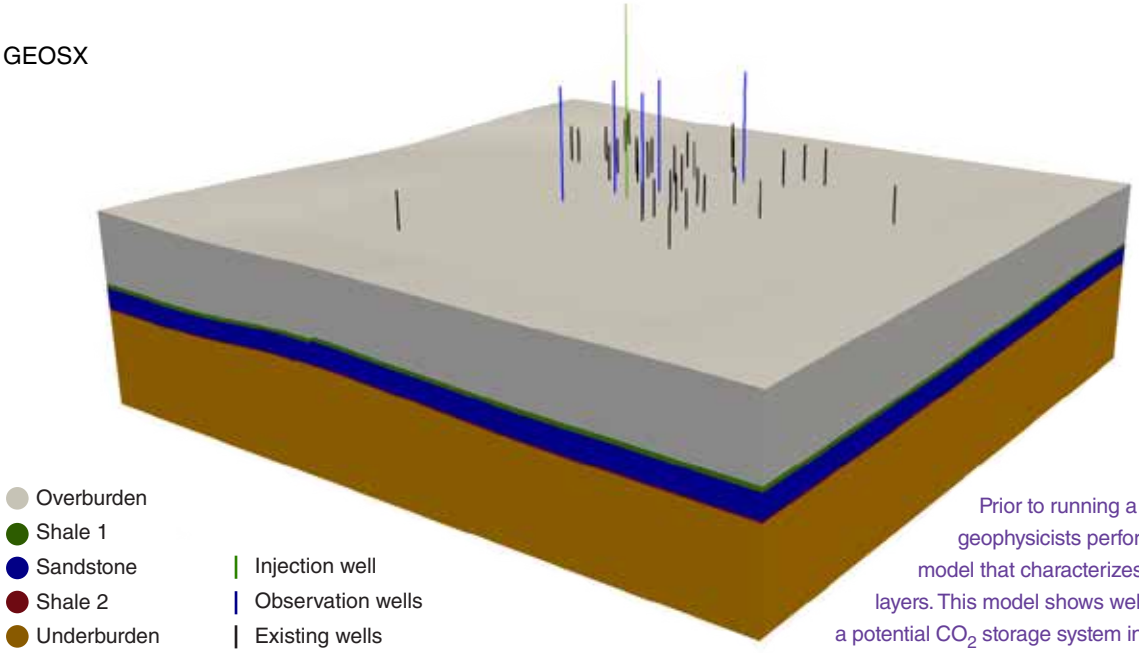
GEOSX and its predecessor, GEOS, were developed from the ground up with the help of experts from across the Laboratory, combining a range of disciplines including engineering, seismology, hydrology, computational geoscience, and oil- and gas-industry expertise to build a tool that can take advantage of advanced computing platforms. GEOSX lead architect Randy Settgast explains, "The code focuses on achieving performance scalability on current and next-generation high-performance computing (HPC) systems—through a portable programming model and scalable algorithms—making GEOSX ready for exascale-class systems as they come online."

How Rocks Break

In practice, GEOSX will improve the management and security of geological repositories and support planning for the widespread implementation of CO_2 storage at an industrial scale by simulating how fluids flow and rocks break deep underground. To do this, GEOSX provides 3D behavioral predictions of underground reservoirs—rock strata approximately 2 kilometers below the subsurface that either currently hold substances such as brine, oil, or gas, or have

This illustration shows the process of injecting compressed liquid carbon dioxide (CO_2) into a reservoir 2 kilometers underground. The wellhead regulates fluid pressure as CO_2 is injected into the well. Above the reservoir is the caprock formation, which prevents the CO_2 from escaping the reservoir. GEOSX simulates the migration of CO_2 from its injection point and models the risk of caprock fracture or leakage, helping scientists understand how well an underground reservoir will respond to CO_2 injection pressures.





Prior to running a GEOSX simulation, geologists and geophysicists perform a site survey to create a geologic model that characterizes subsurface properties and rock layers. This model shows well locations and key geologic layers for a potential CO_2 storage system in the Gulf of Mexico.

the potential to store CO_2. The chosen reservoir, also referred to as the storage formation, must have a caprock, an essential top barrier that prevents buoyant CO_2 from rising towards the surface once it is injected into the reservoir. GEOSX models whether the caprock can maintain the seal and if the reservoir is at risk for fracturing or leaking.

To store CO_2, a well is drilled down to the reservoir so fluids can be injected into the storage space. Prior to drilling, GEOSX assists scientists with creating detailed well designs, which take into account the well's physical make up and mechanical components, in addition to the surrounding rock, fluids, and gases. When a well is drilled and formed with steel casing and cement, operators generally have limited information about potential fractures or other pathways for fluid leakage that they may create. To prevent potential leakages, GEOSX provides simulations for how a wellbore will react to pressure from CO_2 fluid injection and any underground chemical reactions that could degrade well integrity. The need to understand and predict the behavior of hundreds to thousands of deep wells presents an urgent challenge, especially given the large volume of storage required for CO_2 sequestration to have a meaningful impact on climate change. "Modeling the subsurface is incredibly challenging because so many disparate factors operate at different scales. GEOSX takes a unique, algorithmic approach by coupling analysis of finite elements and volumes and allowing the user to integrate multiple physics solvers with different time steps or mesh regions within a simulation," says Settgast.

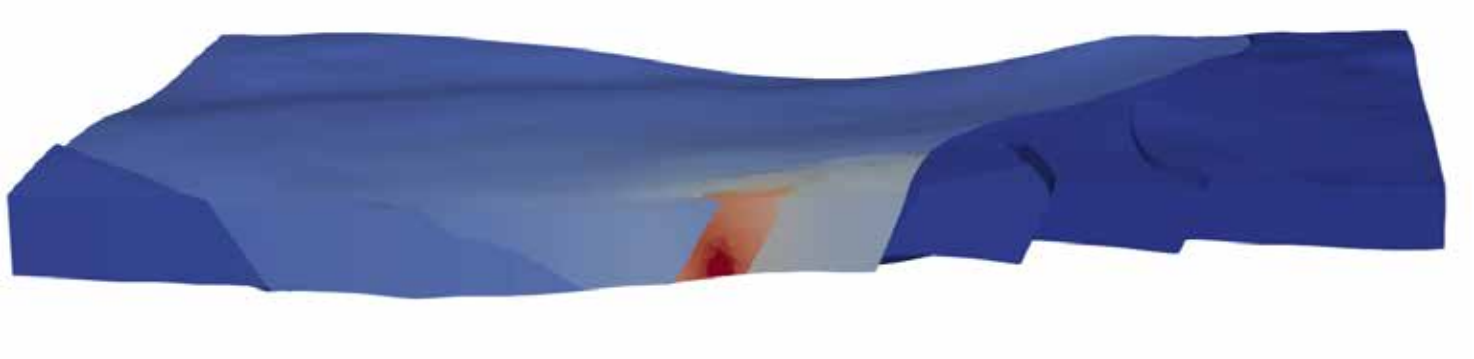
The GEOSX team has performed prospective simulations for several potential storage projects, including offshore fields in the Gulf of Mexico near Texas, and a new commercial venture underway in the North Sea off the coast of Norway. GEOSX reservoir engineer Joshua White notes, "Reservoirs in Texas and neighboring Gulf Coast states are predicted to lead the United States in terms of potential CO_2 storage. Texas has an estimated capacity to store approximately 1,800 gigatons or 1.8 billion metric tons of CO_2. This amount of storage, if completely filled, could hold up to 2,500 years of Texas's CO_2 emissions."

Solving the Puzzle

Prior to running a GEOSX simulation, geologists and geophysicists perform a site survey to characterize subsurface rock properties and layers. From this data, a computational model is built, mapping out several kilometers underground. GEOSX then uses a set of governing equations to predict how a given reservoir will react to high-pressure fluid injection. Starting from where the CO_2 is initially injected near the well to where it migrates in the reservoir, GEOSX models a timescale of indefinite storage from the first few seconds to hundreds or even thousands of years into the future. The resulting simulation evaluates factors ranging from the fluid dynamics of water and CO_2 to mechanical processes such as subsurface faults, rock deformations, and fractures. Ultimately, these data reveal how successfully a given reservoir could store CO_2.

To generate a storage timescale, the software works to simulate reservoirs piece by piece, looking at one small section at a time and modeling how each section interacts with others nearby. Settgast explains, "If we want to simulate a subsurface volume 10 kilometers in length by 10 kilometers in width and 2 kilometers high, we break it into smaller pieces that are easier to model, coupling the individual pieces to create the larger model." White adds, "It is like designing just the wing of an airplane versus the entire airplane—once you know how to model one piece, you can continue to build from there. This meshed model approach breaks the governing equations up into discrete elements, which produces a finite set of equations to be solved rather than an intractable number."

This GEOSX computer simulation indicates the pressure distribution in a faulted reservoir under the Gulf of Mexico. The dark red areas indicate about 2 megapascals of increased fluid pressure (more than 20 times Earth's atmospheric pressure) near the well due to CO_2 fluid injection, suggesting that the reservoir can handle high rates of fluid injection without risking caprock damage.



Exascale Simulations

Releasing GEOSX as open-source code aligns with the Laboratory's Rapid Application Development via an Institutional Universal Software Stack (RADIUSS) Project, an HPC ecosystem created to expand software usage across the Laboratory and the open-source community through a set of libraries and tools. The open-source model and platform portability of the code support both GEOSX and RADIUSS's mission to facilitate collaboration with external partners and the broader research community.

GEOSX depends on software packages, or multiple applications, within the RADIUSS software stack supporting its portability and memory management within supercomputer systems. Portability allows users to operate GEOSX on systems ranging from standard laptops to supercomputers and exascale platforms. Settgast says, "GEOSX has already been used on Livermore's top-ranked supercomputers Sierra and Lassen and will run on exascale systems such as Oak Ridge National Laboratory's Frontier and Livermore's El Capitan, which are some of the first exascale systems." He adds, "We are moving from petaflops (a unit of computing speed equal to 10^{15} floating-point operations per second) to exaflops (10^{18}), which have 1,000 times more computational power per second."

Currently, the code is included in the Subsurface Project, the Department of Energy Exascale Computing Project aimed at creating an exascale subsurface simulator. The effort couples Livermore's GEOSX code and its ability to predict geomechanical stressors with Lawrence Berkeley National Laboratory's Chombo-Crunch code, which predicts geochemical stressors. Together, the two codes form a multiphysics framework for addressing exascale computing challenges associated with the prediction of subsurface wellbore behavior and CO_2 storage. Algorithmic advancements and support from the Exascale Computing Project will enable GEOSX to scale and run larger problems on the latest exascale platforms, modeling complicated physics at unprecedented resolution. This capability, in turn, will lead to better understanding of subsurface properties and characteristics, advancing current CO_2 storage simulations. To validate GEOSX, the code has been compared against analytical solutions, other numerical simulators, experimental data, and field-observation data sets. The team has also incorporated uncertainty quantification, which plays an important role in engineering workflows, to evaluate GEOSX's predictions. "Uncertainty is another reason for focusing on development of a high-performance simulator so we can run these ensemble simulations as quickly as possible," says White. Current verification and validation benchmarks are available on the GEOSX website.

Drawing on more than two decades of experience in simulation and HPC research, Livermore, TotalEnergies, and Stanford University will enable GEOSX to become a tool that researchers all over the world can use to accelerate the development of CO_2 sequestration solutions. White says, "This project is a great opportunity to combine Livermore's expertise in earth sciences, energy systems, and high-performance computing. We are hopeful that GEOSX's framework can play an important role in our transition towards a low-carbon future."

—Shelby Conn

Key Words: Carbon dioxide (CO_2), carbon sequestration, carbon storage, computational geosciences, cooperative research and development agreement (CRADA), exascale, Exascale Computing Project, GEOS, GEOSX, high-performance computing (HPC), Rapid Application Development via an Institutional Universal Software Stack (RADIUSS), reservoir, Stanford University, Subsurface Project, TotalEnergies, wellbore.

For further information contact Joshua White (925) 422-3939 (white230@llnl.gov).

Mission Fulfillment with Exponential IMPACT

THE Department of Energy's (DOE's) Early Career Research Program (ECRP) aims to bolster the nation's scientific workforce by providing support to exceptional researchers at U.S. academic institutions and DOE's national laboratories during their early career years. Annually, ECRP provides research funding to full-time staff in their first 10 years post-doctorate. These highly competitive, five-year awards, funded by DOE's Office of Science, provide recipients with approximately $500,000 per year to cover their salary and research expenses.

Demonstrating the exemplary caliber of Livermore's early career staff, Lawrence Livermore has received more ECRP awards than any other National Nuclear Security Administration (NNSA) laboratory since the program's 2010 inception and is currently tied

for fourth among all DOE national laboratories. "The diversity of Laboratory divisions and programs our awardees represent—Engineering, Computing, Physical and Life Sciences, and the National Ignition Facility, among others—and the diversity of DOE program offices that support Livermore's awards is impressive," says Eric Schwegler, director for Sponsored Science in the Laboratory's Deputy Director for Science and Technology Office. "ECRP awards make a real difference because they give recipients the freedom to explore new ideas, the means to attract additional talent, and the opportunity to develop their professional networks at a critical stage in their career, which truly benefits the Laboratory and enhances its ability to fulfill its mission."

Yongqin Jiao

Geobiologist and 2011 DOE Office of Biological and Environmental Research ECRP recipient Yongqin Jiao uses systems biology to examine how microbes sense, respond, and adapt to environmental cues to discover foundational design rules that govern complex biological-systems behaviors. Jiao then applies these rules to redesign organisms with traits that support clean energy and environmental solutions. "Microbes play a major role in how uranium and other radionuclides affect the environment," says Jiao. "Their metabolisms can alter their chemical states and restrict their movement, but how or why they do that has been a mystery."

Jiao's ECRP project focused on *Caulobacter crescentus*—a gram-negative bacterium widely distributed in nutrient-limited, freshwater lakes and streams—to determine how it detects, accumulates, and catalyzes the formation of uranium-containing minerals. "By figuring out how this tiny bacterium interacts with uranium, we developed a conceptual model of uranium speciation, minerology, and biochemical cycling to help us understand what's happening at contaminated sites and enable bacteria to perform environmental remediation," she says.

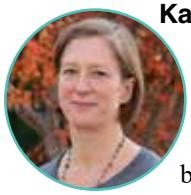
Under the ECRP, Jiao also published several papers, hired four postdoctoral researchers (three of whom have remained at Livermore), and landed a spin-off Laboratory Directed Research and Development–funded project initiated by one of the project's postdoctoral staff members. Perhaps most importantly, the project sowed seeds of a burgeoning scientific community of systems and synthetic biologists at the Laboratory. "Receiving the ECRP Award allowed me the freedom to pursue a research topic with real-world impact that integrated my deep knowledge of geobiology with cutting-edge, systems-biology tools," says Jiao. "We also established a strong scientific foundation that supports our exploration of other microbe–metal interactions including biotechnology for rare-earth element extraction so we can capitalize on selective metal binding and mineralization mechanisms that microbes and biomolecular systems use."

Michael Schneider

Once completed, the Vera C. Rubin Observatory's Legacy Survey of Space and Time (LSST) performed atop Cerro Pachón in Chile will scan the entire visible southern sky every three nights for 10 years with the largest digital camera ever constructed for ground-based optical astronomy. The 3-billion-pixel camera will produce massive amounts of data to advance understanding of dark energy, dark matter, galaxy formation, and asteroids potentially headed for Earth. Michael Schneider, Lawrence Livermore astronomer, astrophysicist, and 2017 DOE Office of High Energy Physics ECRP recipient says, "The LSST will generate a 500-petabyte database of images and a 15-petabyte catalog describing nearly 40 billion individual stars and galaxies. The information contained in one petabyte is the equivalent of a stack of more than 223,000 DVDs. That's a lot of data. Our research centers on big data, high-performance computing, statistical machine learning, artificial intelligence, and analysis. We used hierarchical Bayesian models to develop a distributed algorithm that measures cosmic shear (the gravitational lensing of galaxies), mitigates sources of systematic errors in the measurements, and produces more reliable inferences of dark-energy properties. We are exploring how to incorporate machine learning in our Bayesian pipelines to produce scientifically reliable algorithms."

The ECRP funding has given Schneider and his team the freedom to think about longer-term payoffs and situated Lawrence Livermore at the vanguard of dark-energy research. "We can tackle bold, even controversial approaches that some might argue are too impractical or impossible," he says. "We're making technical advances and integrating novel machine-learning tools to create more efficient computational pipelines. The ECRP Award also means we could mentor four doctoral projects, fund two postdoctoral team members, and attract more talent and additional funding streams."

Kathryn Mohror



As supercomputers continue to achieve phenomenal speeds and scientific simulations produce massive amounts of data, moving and storing all of that data creates workflow bottlenecks. "My ECRP project solves this

YONGQIN JIAO

Geobiologist Yongqin Jiao used her 2011 Early Career Research Program (ECRP) Award to study how the bacterium *Caulobacter crescentus* detects, accumulates, and catalyzes the formation of uranium-containing minerals that could have environmental applications and established a strong foundation for exploring other microbe–metal interactions for rare-earth element extraction.

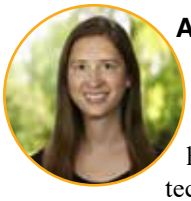
MICHAEL SCHNEIDER

Astronomer, astrophysicist, and 2017 ECRP recipient Michael Schneider has developed hierarchical Bayesian models that incorporate machine learning, high-performance computing (HPC), big data, and artificial intelligence to interpret the massive amounts of data produced by the Vera C. Rubin Observatory's Legacy Survey of Space and Time and advance understanding of dark energy, dark matter, galaxy formation, and near-earth asteroids.

problem by characterizing the data management needs of scientific simulations and developing strategies to make data movement and storage more efficient," says Kathryn Mohror, computer scientist and group leader for the Parallel Systems Group in the Laboratory's Center for Applied Scientific Computing, and 2019 Office of Advanced Scientific Computing Research ECRP recipient. Currently, storage systems and input–output (I/O) middleware on supercomputers manage all data in the same manner. "My approach breaks away from the 'same size fits all' model and tailors data management based on the type of data," says Mohror. "For example, simulations typically perform an operation called 'checkpointing' to save the state of a simulation in case of a failure, like autosave in Microsoft Word. We can cache checkpoint data on temporary compute-node storage and delete it when no longer needed. This simple step results in much higher I/O bandwidth for checkpoint operations and significantly faster simulation times."

The most challenging aspect, according to Mohror, is that people think I/O should "just work" rather than devote time and energy into getting I/O right. "We often focus on how fast the programs run, but the reason we use supercomputers is to obtain the scientific results," she says. "If we don't manage the data efficiently, we're leaving a lot of performance on the table." By making simulation data operations more efficient, scientists can analyze mission-critical results faster.

Mohror's ECRP Award has played a role in her establishing university collaborations, guiding students in their theses, hiring a postdoctoral researcher, heading high-performance computing (HPC) workshops, and serving in leadership and I/O expert roles across the HPC community. "The additional funding has also made it much easier to implement and deliver my vision for HPC data management," she says.



Andréa Schmidt

Neutrons—uncharged elementary particles with a mass about the same as protons—can be used to "look through" objects containing hydrogen, such as fuel or water, but this imaging technique requires an extremely bright neutron source. Andréa Schmidt, the electromagnetics section leader of the National Security Engineering Division at Lawrence Livermore and recipient of the 2021 Office of Fusion Energy Sciences ECRP says, "Right now, if we want to look through an engine to evaluate how it's working, we would have to construct a transparent engine out of quartz instead of metal. But you can't run a quartz engine at normal temperatures and pressures. "Instead, our group is developing a z-pinch device called a dense plasma focus to make a bright enough flash of neutrons to reveal objects' interiors."

KATHRYN MOHROR

Computer scientist, group leader for the Parallel Systems Group in the Center for Applied Scientific Computing at Lawrence Livermore, and 2019 ECRP Award recipient, Kathryn Mohror has delivered innovative, faster, and more efficient data management methodologies for HPC and served as a leader in the HPC community through her project.

ANDRÉA SCHMIDT

Andrea Schmidt, the electromagnetics section leader of the National Security Engineering Division and recipient of a 2021 ECRP Award, has combined computer simulations with experiments on a novel megajoule-class z-pinch device and diagnostics to develop a brighter neutron flash source that can be used to look inside cargo, suitcases, and suspicious packages.

For her ECRP project, Schmidt will combine world-class computer simulations with experiments on a newly commissioned dense plasma focus (DPF) platform, the Megajoule Neutron Imaging Radiography, and diagnostics that, at a fundamental level, will reveal where the plasma current in the DPF flows, facilitating the development of a brighter flash of neutrons. "We can also use neutron pulses to interrogate unknown objects—cargo, suitcases, waste drums, and suspicious packages. Anything we can do to make neutron sources brighter or more portable will open the door to exciting basic, applied, and new operational concepts that support the Laboratory's missions," says Schmidt.

Schmidt's ECRP Award has brought attention to the Laboratory's DPF group, strengthened her ties to the DOE Office of Science, and provided additional opportunities for her team to publish its research. "We have the opportunity to develop future technologies that will impact many areas of national security," says Schmidt. "Applications include ensuring the credibility of the nuclear deterrent without nuclear testing, screening cargo for illicit materials, or learning how fuel flows in engines and fuel cells."

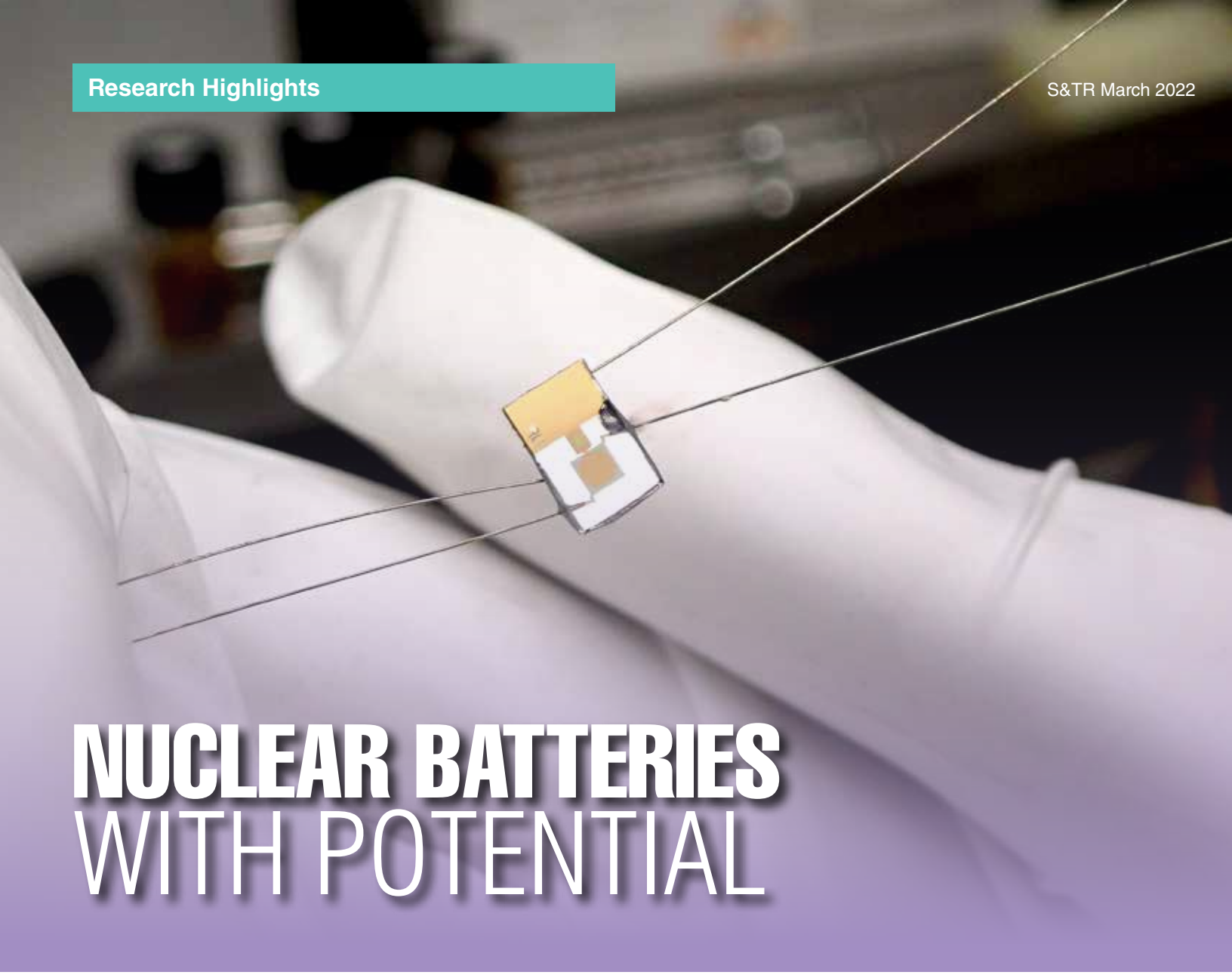
Support for Fantastic Ideas

The Laboratory's Program Development Support Office (PDSO) assists early career staff in preparing competitive proposals submitted for the ECRP each year. PDSO holds proposal writing classes, a roundtable discussion with previous recipients, and a town hall where applicants can share concepts and provide feedback. "Our early career staff have fantastic ideas with the potential to revolutionize science and change the world. We help them write more effective proposals by working to refine their logic, address points reviewers look for, and ensure compliance with sponsor requirements," says PDSO Director Chris Hartmann. "Livermore ECRP recipients, as well as their peers and colleagues, demonstrate exceptional ingenuity, discipline, and dedication to tackling provocative scientific questions in support of the Laboratory's mission and national security. The ECRP awards empower the recipients and their teams to have a truly exponential impact on the Laboratory's mission fulfillment."

—Genevieve Sexton

Key Words: Bayesian model, biochemical cycling, biomolecular systems, *Caulobacter crescentus*, checkpointing, cosmic shear, dark energy, dark matter, data management, dense plasma focus (DPF), Department of Energy (DOE) Office of Science Early Career Research Program (ECRP), high-performance computing (HPC), input-output (I/O), Legacy Survey of Space and Time (LSST), Megajoule Neutron Imaging Radiography, neutrons, uranium, z-pinch device.

For further information contact Patricia Falcone (925) 422-0557 (falcone2@llnl.gov).



NUCLEAR BATTERIES WITH POTENTIAL

FROM small traditional alkaline batteries that energize flashlights to larger lithium-ion ones that drive electric vehicles, batteries come in many shapes and sizes for various applications. At Lawrence Livermore, engineering and material experts are researching, developing, and prototyping 3D nuclear batteries—tiny, high-density power sources useful for remote applications, such as in biomedical implants, where operating at low power for longer periods of time (up to decades) is essential.

Nuclear batteries contain radioactive substances that emit energetic alpha or beta particles through radioactive decay. Semiconductors within the device capture and convert the decay energy into electricity. The radioisotope and the semiconductor materials as well as the type of battery—alpha versus betavoltaic—dictate the overall power performance.

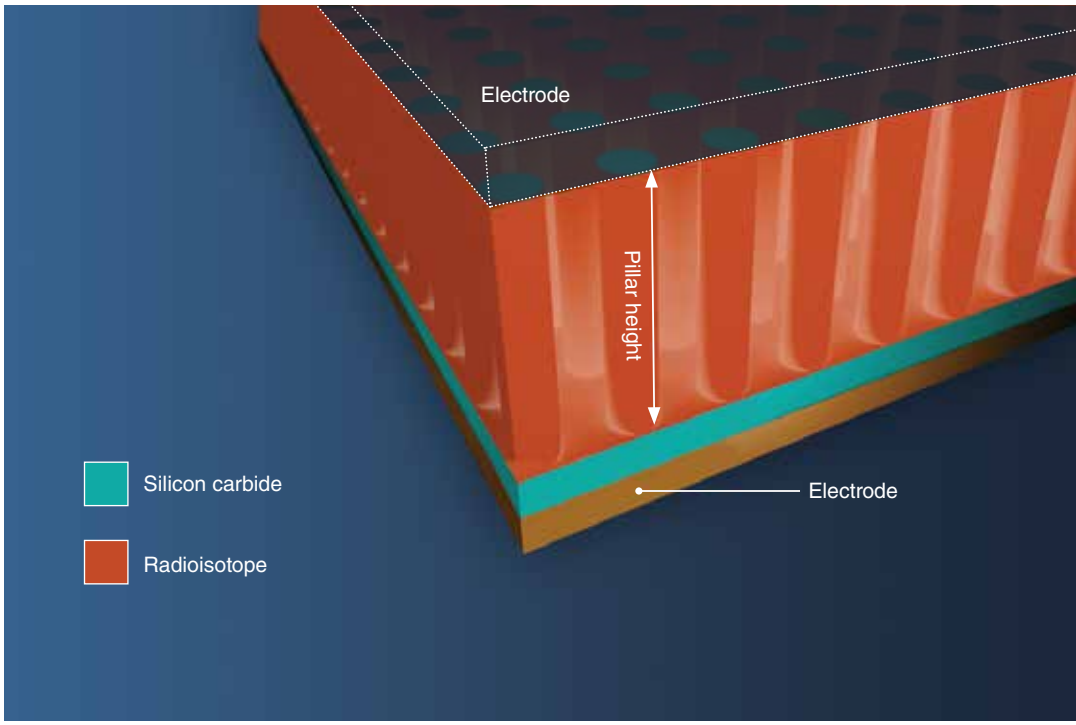
Bolstered by Livermore innovation in advanced microfabrication, engineering, materials science, and nuclear chemistry, Livermore researchers are exploring an extensive battery design portfolio that includes different radioisotopes as well as semiconductor materials in various states—solid, gas, and liquid. Electrical engineer and deputy program manager for the Laboratory's Energy and Homeland Security Program Rebecca Nikolic says, "We are investigating different media to determine the most robust and economical approach for various applications."

Pillars of Success

"Research into 3D low-power batteries began more than 10 years ago, leveraging semiconductor technology developed through the Laboratory's work on neutron detectors for national security applications," says Livermore nuclear engineer Joshua Jarrell. (See *S&TR*, March 2014, pp. 12–15.) The semiconductor platform comprises small silicon pillars that transfer charged particle signals to an electrode. The research team incorporated this platform into an advanced 3D battery prototype wherein

silicon-carbide pillars, surrounded by promethium-147, capture the decay energy emitted from the radioisotope to generate electricity. (See, *S&TR*, April/May 2017, pp. 21–23.)

Extensive characterization testing of the battery has revealed surprising material behavior. "Using an electron beam gun at Livermore, we irradiated both silicon and silicon-carbide diodes at different energies and varying fluxes and fluences to accelerate material aging without the radioisotope present," says Jarrell. The results were counterintuitive. Although silicon carbide is known for being radiation hard—more resistant to damage from ionizing radiation—than silicon, above 100 kiloelectronvolts, silicon outperforms its competitor. Jarrell continues, "The results suggest that silicon may in fact be a better semiconducting material for promethium-based betavoltaics." The team is also evaluating what other radioisotopes could be incorporated into this design. Nikolic says, "Although promethium was used to develop a viable 3D battery, supply chain issues and increased costs associated with it meant that we needed to identify alternatives."



A Livermore-developed 3D nuclear battery design features pillars made from silicon carbide surrounded by a radioisotope such as promethium-147. Beta particles emitted from the radioisotope interact with the semiconductor to generate electric current.

Different Media, Multiple Possibilities

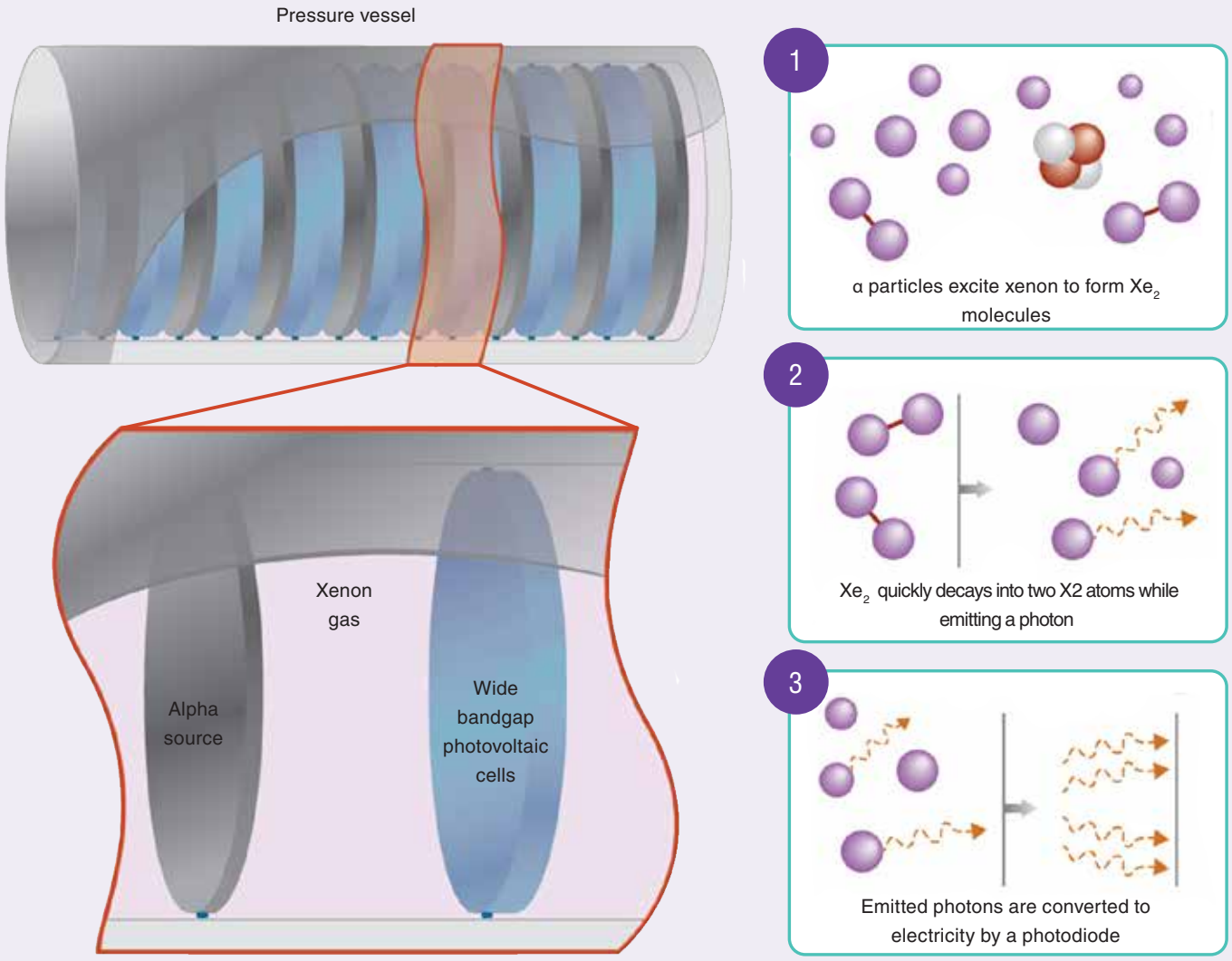
Livermore's broad materials science research includes development of polycrystalline transparent ceramics—materials composed of small, chemically identical crystalline grains. One of the team's proposed battery designs incorporates an innovative solid-state polycrystalline transparent ceramic photocell. In addition, promethium is replaced with strontium, which has a much higher energy beta-particle emission.

To prevent radiation damage to the semiconductor photocell, the ceramic is inserted between the strontium-90 source and the photocell. The ceramic absorbs the higher energy beta particles and emits photons benign to the semiconductor. Alternating layers of the structure can be sandwiched together to further enhance power density. "This technology is promising because it is radiation hard to sources useful for nuclear batteries," says Jarrell. "We have many variables to consider, including gamma-ray emissions produced during decay. To overcome this challenge, we need to identify better shielding options."

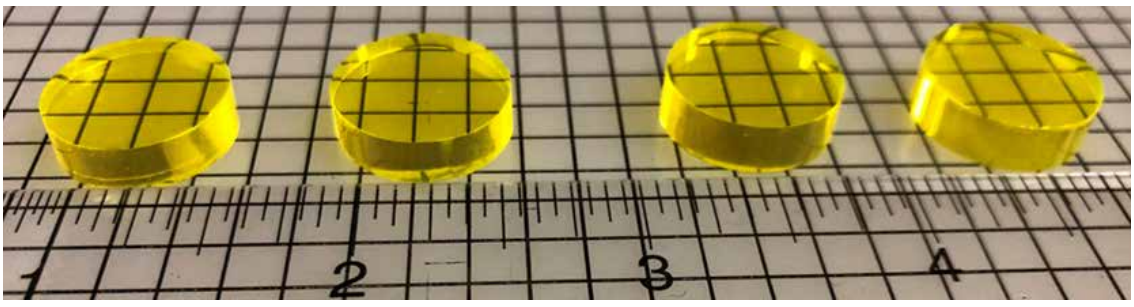
Another battery design has roots in Livermore's work with rare-event detectors—such as those in development to detect dark matter for the first time—wherein particles interact with xenon atoms to create photons and electrons that provide measurable signals of the incident particle. For 3D nuclear batteries, the team uses a high-pressure xenon gas to create a scintillation signal from alpha-emitting radioisotopes. "The alpha particles transfer energy to the outer electron shells of the gas atoms as they pass through the xenon, creating excimers—unstable and short-lived molecules that emit ultraviolet photons when they separate. The photons bounce through the gas until a solar cell captures and converts that energy to an electric current," says Jarrell.

With this alphavoltaic design, the team can squeeze many thin layers of the battery structure into a small space to increase the power density. "The system must operate under vacuum to maintain high gas purity, which is essential for battery output, since the decay energy will seek any way to disperse itself besides interacting with xenon," says Jarrell. Maintaining the extremely high purity is a complicated procedure that requires exact pressures and temperatures. He notes, "We are looking at NASA-developed, small, lightweight, stainless-steel vessels to scale down the battery to a realistic size."

Inside a noble gas-based 3D battery, alpha particles pass through xenon (Xe), transferring energy to the gas atoms and creating excimers that quickly separate. This separation results in emission of a photon, which is then converted to electricity by a photodiode.



Researchers are testing the efficacy of transparent ceramic scintillators (samples shown here) for use in 3D batteries. In one battery design, a polycrystalline transparent ceramic photocell absorbs high-energy beta particles and emits photons benign to the semiconductor.



Liquid Potential

In 2017, the research team made headway on a battery containing liquid selenium–iodine, a mixture that works well as a semiconductor and a photovoltaic but is highly caustic. (See *S&TR*, April/May 2017, pp. 21–23.) "Liquid selenium–iodine is like a bull in a china shop," says Jarrell. "The two substances are corrosive on their own, but when we combine, heat, and irradiate them, they become even more corrosive. It's really a nightmare environment. For this type of battery to work, it must be stable for decades and remain free from radiation leaks."

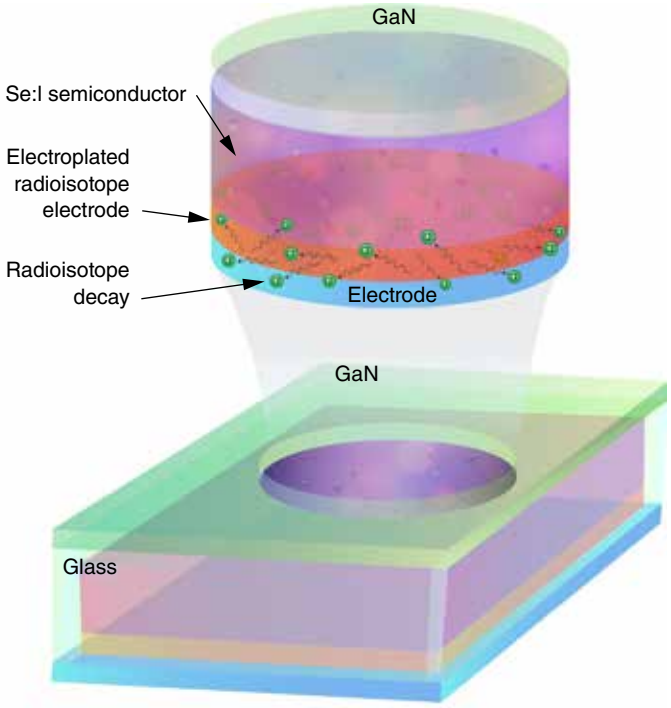
Leveraging the Laboratory's microfluidics capabilities and expertise, the team developed a novel housing structure for the radioactive and semiconductor materials. The selenium–iodine mixture is poured into a tiny cavity etched into a silicon chip. Once the mixture has been added, a layer of glass is chemically bonded on top of the chip. "One of the challenges with this design was making the glass window thin enough so that the alpha particles would pass through it rather than stop. The window is just a few tens of micrometers—thinner than a strand of human hair," says Jarrell. The whole microchip design is a few millimeters in size and about a millimeter thick.

The chips are undergoing characterization testing, and the team is working to scale up the design by adding multiple chips together in a single unit. The researchers are also investigating alternative methods for incorporating the radioactive material into the semiconductor. Currently, the work requires a special, sealed glovebox to add the selenium–iodine mixture to the chip. Jarrell notes, "We are exploring whether we can make and use a sealed source by electrodepositing it onto a surface, which would eliminate the need for the glovebox. The material can't physically go anywhere, but the radiation can still escape from the source to produce energy." The team is excited about the prospects. "We recently generated a small amount of power with this prototype, which is a big step in the right direction."

The Power of Nanonuclear

Since 2016, Livermore has hosted three collaborative workshops with external partners from industry, other government agencies, and academia to facilitate the exchange of scientific ideas in support of 3D nuclear battery development. The most recent workshop, held in 2020, focused on improvements in power density. Jarrell notes, "The goal was to see how much more power we could get from a specific volume."

In addition to their other battery designs, the Livermore team worked in partnership with City Labs, Inc., to enhance a commercially available tritium-based betavoltaic. "We demonstrated the ability to absorb low-energy beta particles more efficiently," says Jarrell. Chief Executive Officer of City Labs Peter Cabauy adds, "Lawrence Livermore was a valuable partner as a premier institution in understanding tritium and the regulatory requirements associated with using the material. The interaction with the Laboratory has also given us perspective on new applications and approaches."



This schematic shows the housing design of a 3D battery containing an electroplated radioisotope and a selenium–iodine (Se:I) semiconductor. A bonded glass and gallium–nitride (GaN) substrate sandwiches the materials together to improve power density.

Cabauy also notes that when most people think of nuclear, images akin to Homer Simpson and his power plant come to mind. "The reality is much different," he says. "When we talk about nuclear batteries, we mean extremely small, even millimeter-scale power sources that can provide power for decades. Imagine a rice grain–size battery placed in a tiny pacemaker that could work for the life of the patient." Their footprint may be small, but 3D nuclear batteries have big potential.

—Caryn Meissner

Key Words: alpha particle, alphavoltaic battery, beta particle, betavoltaic battery, neutron detector, nuclear battery, radioisotope, scintillator, selenium–iodine, semiconductor, silicon, silicon carbide, xenon.

For further information contact Joshua Jarrell (925) 423-7785 (jarrell2@llnl.gov).

In this section, we list recent patents issued to and awards received by Laboratory employees. Our goal is to showcase the distinguished scientific and technical achievements of our employees as well as to indicate the scale and scope of the work done at the Laboratory. For the full text of a patent, enter the seven- or eight-digit number in the search box at the U.S. Patent and Trademark Office's website (uspto.gov).

Patents

Composite 3D-Printed Reactors for Gas Absorption, Purification, and Reaction
Du T. Nguyen, Roger D. Aines, Sarah E. Baker, William L. Bourcier, Eric B. Duoss, James S. Oakdale, Megan M. Smith, William L. Smith, Joshuah K. Stolaroff, Congwang Ye
U. S. Patent 11,148,114 B2
October 19, 2021

System and Method for Curved Light Sheet Projection During Two-Photon Polymerization
Sourabh Saha, Shih-Chi Chen, Yina Chang
U. S. Patent 11,150,484 B2
October 19, 2021

Systems and Methods for a Triplet Network with Attention for Speaker Diarization
Huan Song, Visar Berisha, Andreas Spanias, Megan Willi, Jayaraman Thiagarajan
U. S. Patent 11,152,013 B2
October 19, 2021

***Reissued patent* Chemical Amplification Based on Fluid Partitioning**
Brian L. Anderson, Bill W. Colston, Christopher J. Elkin
U. S. Patent RE48,788 E
October 26, 2021

Magnetically Coupled Pressure Sensor
Jack Kotovsky, Taylor Bevis
U. S. Patent US 11,162,861 B2
November 2, 2021

Enhanced Colorimetric Apparatus and Method for Explosives Detection Using Ionic Liquids
John G. Reynolds, Lara D. Leininger, Thomas W. Myers
U. S. Patent 11,162,904
November 2, 2021

System and Method for All Optical Electrode Interface for Bioengineering Application
Susant Patra, Razi-Ul Muhammad Haque, Komal Kampasi
U. S. Patent 11,169,341 B2
November 9, 2021

Fabricating Structured Particles Through Rapid Hardening and Tailored Collection Methods
Congwang Ye, Roger D. Aines, Sarah E. Baker, Caitlyn Christian Cook, Eric B. Duoss, Joshua D. Kuntz, Elaine Lee, James S. Oakdale, Andrew J. Pascall, Joshuah K. Stolaroff, Marcus A. Worsley, Carlos J. Martinez
U. S. Patent 11,173,461 B2
November 16, 2021

Hierarchical Porous Metals with Deterministic 3D Morphology and Shape via De-Alloying of 3D Printed Alloys
Zhen Qi, Juergen Biener, Wen Chen, Eric Duoss, Christopher Spadaccini, Marcus A. Worsley, Jianchao Ye, Cheng Zhu
U. S. Patent 11,173,545 B2
November 16, 2021

Vacuum Manufacture of Cryogenic Pressure Vessels for Hydrogen Storage
Salvador Aceves, John Elmer, Francisco Espinosa-Loza, Guillaume Petitpas, James Smith, Michael Veenstra, Laus Szoucsek
U. S. Patent 11,181,236 B2
November 23, 2021

Compounds for Central Reactivation of Organophosphorous-Based Compound-Inhibited Acetylcholinesterase and/or Inactivation of Organophosphorous-Based Acetylcholinesterase Inhibitors and Related Compositions Methods and Systems for Making and Using Them
Carlos A. Valdez, Nicholas A. Be, Michael A. Malfatti, Heather Ann Enright, Brian J. Bennion, Timothy S. Carpenter, Saphon Hok, Hio Leong Lao, Tuan H. Nguyen
U. S. Patent 11,186,548 B2
November 30, 2021

System and Method for Modifying Material Surface
Selim Elhadj, Jae Hyuck Yoo
U. S. Patent 11,198,196 B2
December 14, 2021

MOMP Telonanoparticles, and Related Compositions, Methods and Systems
Matthew A. Coleman, Nicholas O. Fischer, Amy Rasley, Craig D. Blanchette, Todd Peterson
U. S. Patent 11,207,422 B2
December 28, 2021

Awards

Livermore scientists and engineers received three **2021 R&D 100 Awards**. ***R&D World Magazine*** lauded the Livermore engineering team in cooperation with California-based partner Opcondys, Inc., for developing power grid switches aimed at reducing carbon emissions. Laboratory scientists were also among a multi-institutional team awarded for a field-deployable instrument able to identify and gauge nuclear threats. In the third award, Lawrence Livermore computer scientists collaborating with a team based at the University of Tennessee, Knoxville, were recognized for software breakthroughs that manage supercomputing workloads.

Three Livermore physicists were selected as **fellows for the American Physical Society (APS)**. The honorees include **Tilo Doeppner** and **Tammy Ma** from the High-Energy-Density Division of the National Ignition Facility and Photon Science Principal Directorate, and **Xueqiao Xu** from the Physics Division of the Physical and Life Sciences Directorate. Their areas of expertise range from high-energy, laser-matter interactions and inertial fusion science to computational capabilities geared toward magnetic fusion energy experimentation. APS fellowships are awarded after peer nomination and an exceptionally stringent evaluation process.

Abstract

Defending U.S. Critical Infrastructure from Nation-State Cyberattacks

Livermore's immune infrastructure framework applies a new paradigm for protecting the nation's critical infrastructure, such as utilities and electrical grids, from cyberattacks, focusing on sophisticated nation-state adversaries capable and motivated to act. The layered defense approach looks to minimize the effects of intrusions, enabling continued operation or graceful degradation of our critical infrastructure systems. Four tactical layers comprise the immune infrastructure framework: understanding the systems, keeping the adversaries out, detecting and responding to intrusions, and operating through compromise.

Contact: Nate Gleason (925) 423-6278 (gleason6@llnl.gov).

U.S. Government Printing Office: 2022/670-075-20021

Celebrating 50 Years of Laser Research

Livermore's Laser Program, founded in 1972, marks its golden anniversary, celebrating significant accomplishments on the path to fusion ignition.

Also in this upcoming issue...

- *Solving the mystery of a local water leak with radioanalytical science*
- *Preparing the Laboratory's transuranic waste for safe shipment and disposal*

www.llnl.gov

Coming Next Issue

Science & Technology Review
Lawrence Livermore National Laboratory
P.O. Box 808, L-664
Livermore, California 94551

PRSRT STD
U.S. POSTAGE
PAID
San Bernardino, CA
PERMIT NO. 3330

Printed on recycled paper.