Dynamic Systems & Control follows page 48

MECHANICAL
ENGINEERING
THE MAGAZINE OF ASME
No. 03
139
Technology that moves the world

BRAVE NEW ROAD

Autonomous vehicles will transform society in unexpected ways.

WITTENSTEIN alpha

BORN IN THE USA
WITTENSTEIN

Since our origination as Alpha Gear in 1984, WITTENSTEIN alpha has set the bar for excellence in motion control systems—right from the heart of the Midwest. Today our North American headquarters sits on a six-acre campus in Illinois, where we exceed customer expectations daily:

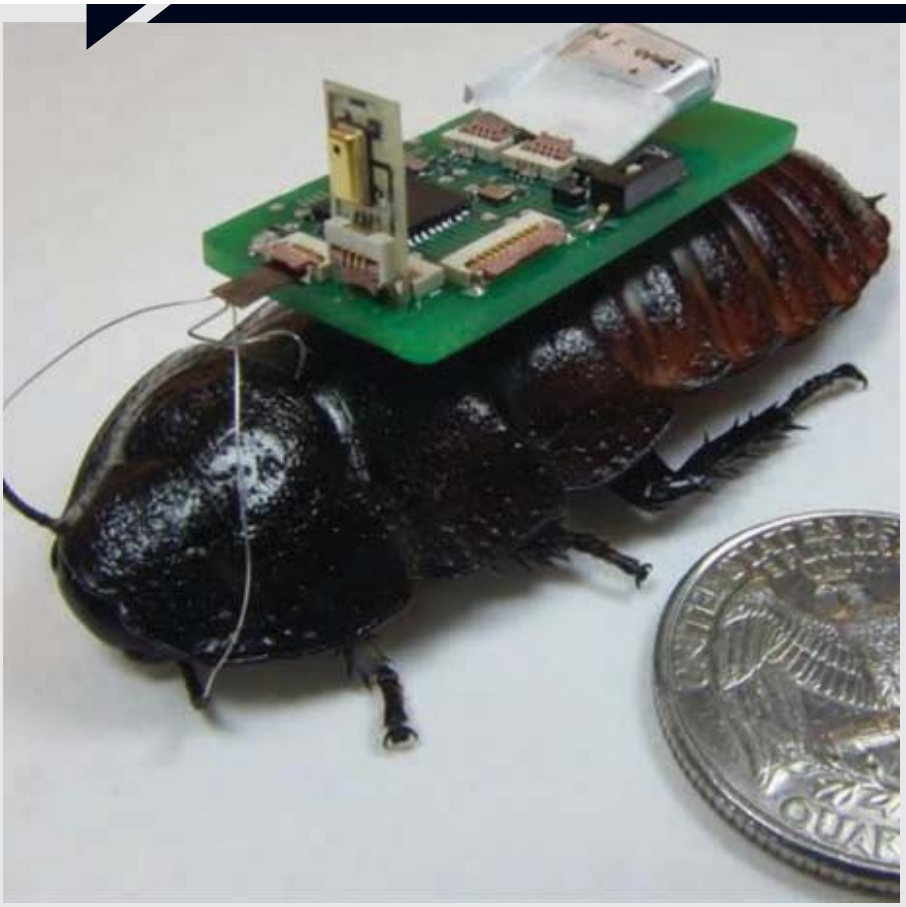
- Ship more than 5,000 products each month, and average 99% on-time delivery**.**
- Deliver engineering and technical support that helps optimize application performance.
- Provide on-site service and maintenance for WITTENSTEIN alpha gearheads.

The quality of WITTENSTEIN alpha gearheads is renowned. Today that quality is more accessible than ever. **For providers near you, email info@wittenstein-us.com.**

WITTENSTEIN – one with the future

www.wittenstein-us.com

WITTENSTEIN | alpha



BIOBOTS TO THE RESCUE

NORTH CAROLINA STATE UNIVERSITY researchers have a plan that has the makings of a Grade B horror movie, but it's actually a serious approach to defining and even identifying the parameters of immediate disaster response. The researchers are using cockroaches to penetrate collapsed structures or dangerous areas, pairing them with new software, hardware, and aerial drones to gather digital information they believe will produce maps of compromised areas.

BREAKING THE MOLD: 3-D PRINTING FOR SANDCASTING

MOST 3-D PRINTERS BUILD objects that are intended to be the finished product. But a startup called Viridis3D uses printers for sandcasting, the process of making molds into which molten metal is poured to create parts. The system fully automates the simultaneous creation of molds and patterns out of sand.

For these articles and other content, visit asme.org.

CASTING A WIDE NET

DRONES CAN BE FUN, useful, or even make life safer by assisting security efforts. But drones can also be dangerous in the wrong hands. One team of engineers is working to defuse that danger with its "dronecatcher" technology.

VIDEO: DESIGNING MEDICAL DEVICES WITH ADDITIVE MANUFACTURING

ROBERT C. COHEN, VICE PRESIDENT and general manager of R&D for Stryker Orthopedics, discusses the best practices medical device manufacturers must consider before adopting additive manufacturing.

DETERMINING DRUG EFFICACY IN ADVANCE

RESEARCHERS AT THE DANA-FARBER Cancer Institute have created a device to determine whether cancer drugs will work on individual patients before they begin potential treatments.

NEXT MONTH ON ASME.ORG

IMPROVING HYDROGEN STORAGE
Tesla and Chevrolet are gaining traction for their electric-powered cars, but hydrogen still may have its place. Toyota, for one, is developing a hydrogen-fueled car and new research may help it become more efficient.

VIDEO: INNOVATIONS IN ULTRASOUND
Jeff Geersten of GE Healthcare discusses new developments in the field of ultrasound technology, which has many new and intriguing applications.

TABLE OF CONTENTS

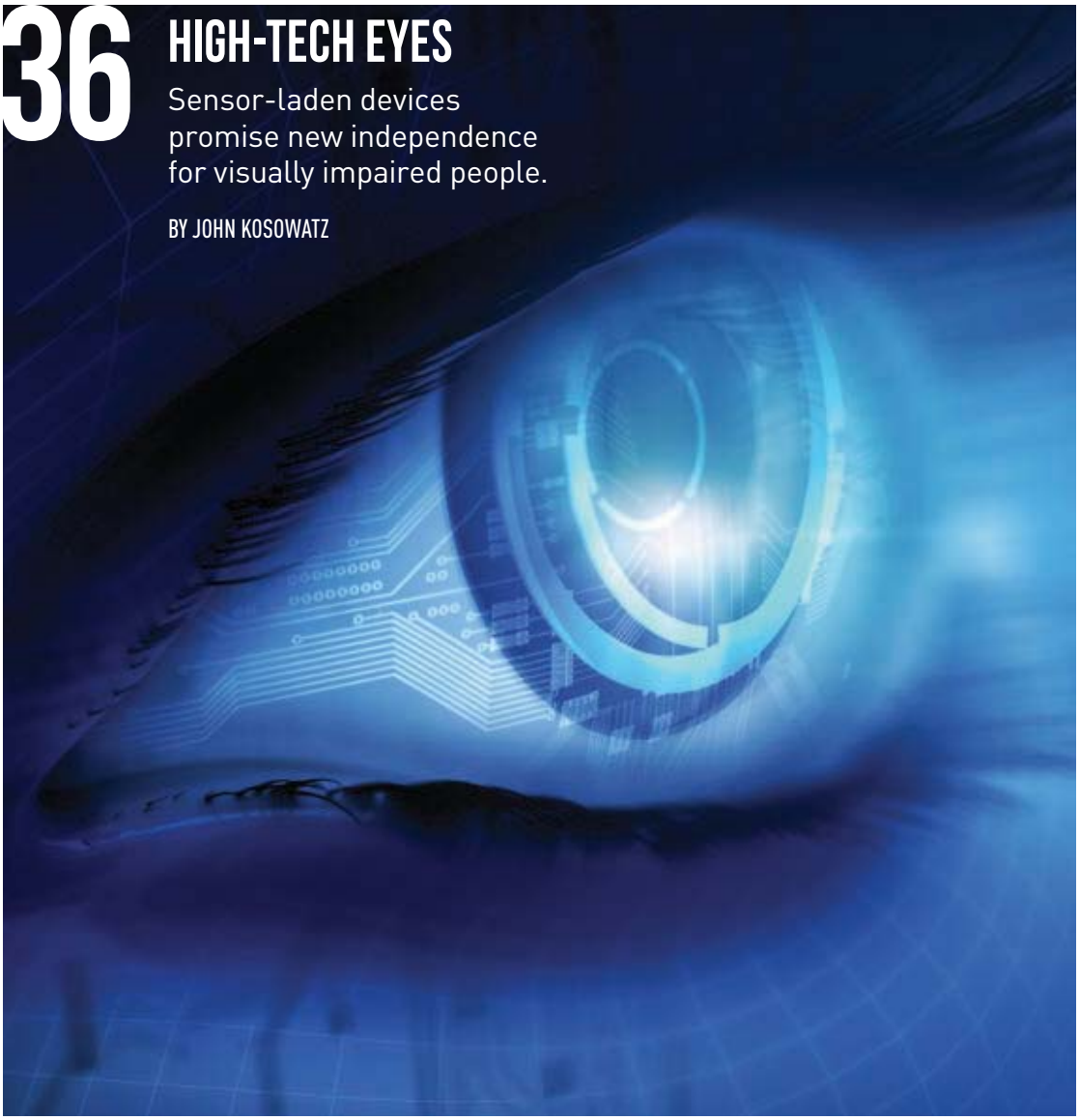
03 139

FEATURES

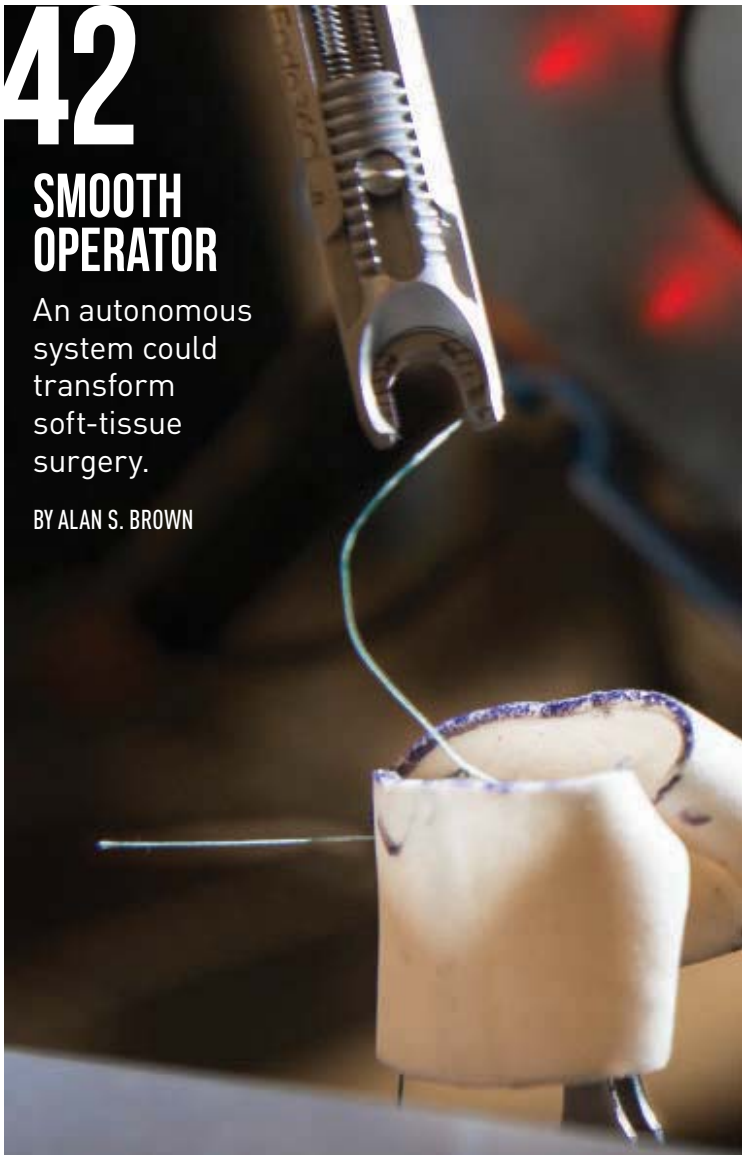
ON THE COVER

30 BRAVE NEW ROAD
Autonomous cars will reshape our society in unexpected ways.

BY BRIAN DAVID JOHNSON



ASME
SETTING THE STANDARD



42 SMOOTH OPERATOR

An autonomous system could transform soft-tissue surgery.

BY ALAN S. BROWN

22 CHEMISTRY SET

Hot Labs and cold plasma.

BY ALAN S. BROWN

73 GLOBAL GAS TURBINE NEWS

GE's Advanced Manufacturing Works and the run-up to Turbo Expo 2017.

DEPARTMENTS

88 SOUNDS OF SCIENCE

Engineering students build funky musical instruments.

BY JAMES G. SKAKOON

Contact *Mechanical Engineering*

Mechanical Engineering
memag@asme.org
p. 212.591.7783 f. 212.591.7841
Two Park Avenue, New York, NY 10016

For reprints contact Rhonda Brown
rhondab@fosterprinting.com
219.878.6094

asme.org
on.fb.me/MEMAGAZINE
memagazineblog.org

Published since 1880 by the **American Society of Mechanical Engineers (ASME)**. *Mechanical Engineering* identifies emerging technologies and trends and provides a perspective on the role of engineering and technology advances in the world and on our lives. Opinions expressed in *Mechanical Engineering* do not necessarily reflect the views of ASME.

Give me the place to stand, and I shall move the earth
—Archimedes

ASME offices

Headquarters
Two Park Avenue, New York, NY 10016
p. 212.591.7722 f. 212.591.7674

Customer Service
150 Clove Road, 6th floor, Little Falls, NJ 07424-2139
In U.S., Mexico & Canada toll-free
1-800-THE-ASME (1-800-843-2763) f. 973-882-5155
International 646-616-3100
e-mail: CustomerCare@asme.org

Washington Center
1828 L Street, N.W., Suite 810, Washington, DC 20036-5104
202.785.3756

Int'l Gas Turbine Institute – igti.asme.org
Int'l Petroleum Technology Institute – asme-ipti.org
11757 Katy Freeway, Suite 380, Houston, TX 77079-1733
p. 281.493.3491 f. 281.493.3493

Europe Office
Avenue De Tervueren, 300, 1150 Brussels, Belgium
p. +32.2.743.1543 f +32.2.743.1550
dogrum@asme.org

Asia Pacific LLC
Unit 09A, EF Floor, East Tower of Twin Towers;
No. B12, JianGuo MenWai DaJie; ChaoYang District;
Bejing, 100022 People's Republic of China
p. +86.10.5109.6032 f. +86.10.5109.6039

India Office
c/o Tecnova India Pvt.Ltd.; 335, Udyog Vihar, Phase IV;
Gurgaon 122 015 (Haryana)
p. +91.124.430.8413 f. +91.124.430.8207
NehruR@asme.org

Mechanical Engineering (ISSN 0025-6501) is published monthly by The American Society of Mechanical Engineers, Two Park Avenue, New York, NY 10016-5990. Periodicals postage paid at New York, N.Y., and additional mailing offices. POSTMASTER: Send address changes to Mechanical Engineering, c/o The American Society of Mechanical Engineers, 150 Clove Road, 6th Floor, Little Falls, NJ 07424-2139. Return Canadian undeliverable addresses to P.O. BOX 1051, Fort Erie, On, L2A 6C7. PRICES: To members, annually $38 for initial membership subscription, single copy $13; subscription price to nonmembers available upon request.

INJECTION MOLDING THAT CRUSHES CONVENTIONAL MANUFACTURING WISDOM.

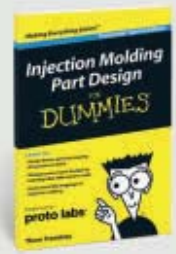
At Proto Labs, we have the automation and capacity to deliver low-volume production runs in just 15 days or less. We call this a game-changer.

DIGITAL MANUFACTURING FOR THOSE WHO NEED PARTS TOMORROW.

proto labs®

Real Parts. Really Fast.®

3D PRINTING | CNC MACHINING | INJECTION MOLDING



FREE BOOK

Request your Injection Molding for Dummies book at **go.protolabs.com/ME7ED.**

John G. Falcioni
Editor-in-Chief

LOOKING DOWN THE ROAD AT AUTONOMOUS VEHICLES

It's an exciting time of change for the auto industry, for car buffs, and for many engineers who've had a lifelong love affair with their vehicles—both behind the wheel and under the hood.

New technologies are bringing the utopian vision of self-driving cars cruising through smart cities into sharper focus. As work on that front continues, technology integrators are making today's vehicles more efficient and safer.

Drivers are already benefitting from advances in entertainment systems and safety and breakdown-rescue equipment. Some new cars sport automatic maintenance reminders; navigation systems that display real-time maps, weather, and road alerts; and security systems that include theft-alert and automobile-tracking mechanisms. There have also been significant breakthroughs in vehicle efficiency, with features such as fuel-management instruments and tachographs.

Just as we relate differently to our smartphones than we did to the rotary telephones of decades past, we relate differently to today's computerized and connected cars. For one, the ability for home mechanics to tinker with their cars is severely limited. But automakers and consumers have shown excitement over the new bells and whistles, and the market for services, devices, and connectivity in vehicles could exceed $39 billion by next year.

As makers of autonomous vehicles enter the market, however, they threaten to further redefine the relationship between car and driver.

Big-name players in this burgeoning space, such as Google, aren't the only ones getting into the act. Startups such as nuTonomy are advancing the self-driving vehicle landscape in quiet but exponential ways.

The MIT spin-off partnered with Uber's competitor Grab and began publicly testing self-driving cars last August on a 2.5 km square business district in Singapore.

NuTonomy's cofounder and CEO Karl Iagnemma, who also directs MIT's Robotic Mobility Group, said the new technology behind self-driving cars is not automotive but robotics-based, as it uses formal mathematical logic to design and verify its software. From an engineering perspective, he said, what matters are the interfaces that make a passenger interact with the car.

"How I tell the car to nudge forward a couple of feet because there's a puddle there and I don't want to get my feet wet is important," Iagnemma said. That's part of the robotics-like artificial intelligence process that his company is focusing on.

We can only speculate what the world will look like and how society will change if—or dare I say *when*—autonomous vehicles proliferate. So we decided to commission Brian David Johnson, a former Intel futurist and now futurist and fellow at the consulting firm Frost & Sullivan, to write our cover story this month and provide some learned context. His article, "Brave New Road," begins on page 30.

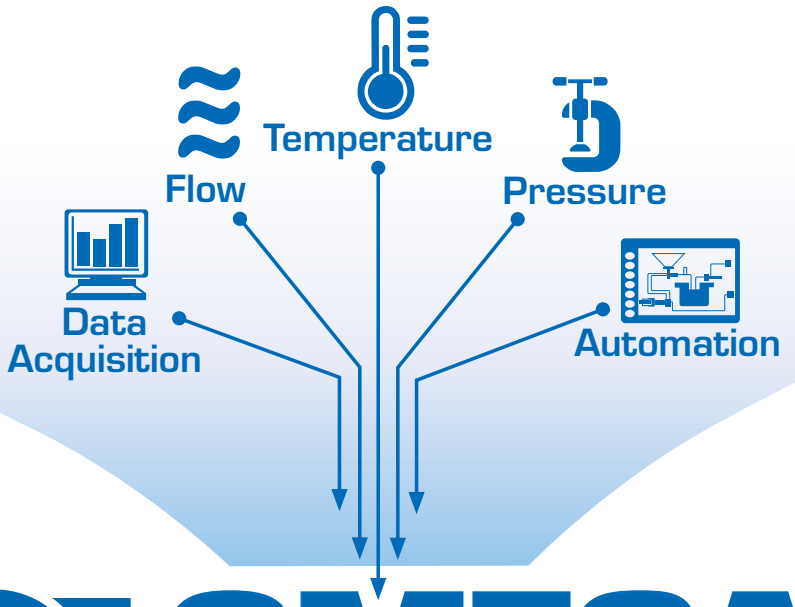
Of course, if you're Stefano Domenicali, the CEO of Automobili Lamborghini, who I met at the same MIT EmTech conference that Iagnemma attended, you don't worry about the future of driverless cars. "My customers want to feel the road," he told me. "The driving experience itself is as important as the destination. I am not worried about cars with no drivers." ME

FEEDBACK

Are you more excited or worried about autonomous vehicles? Email me.

falcionij@asme.org

Your Source for Process Measurement and Control



OMEGA®

100,000 Products
Customized Solutions
Expert Technical Support
Easy Online Ordering
Fast Delivery

NEW

Coriolis Flow Meters

PLATINUM™ Universal Benchtop Digital Controllers

Pressure Transmitters for Industrial & Mobile Applications

High Speed Data Loggers

omega.com

1-888-826-6342

LETTERS & COMMENTS

NOVEMBER 2016

Reader Jakuba pooh-poohs the amount of useful power from new micro-dams.

« A reader argues for the positive effects of manufacturing jobs, another questions the reliability of renewables.

CALCULATED EFFECTS

To the Editor: "By the Numbers: Jobs and Manufacturing" (Trending, October 2016) contains some misleading information that needs to be corrected. The writer states that the $800 billion trade deficit is "a small fraction of the $5.9 trillion worth of goods produced...." I suppose it depends on one's definition of "small fraction," but I consider 13.6 percent to be a nontrivial amount, and one that needs to be aggressively addressed rather than summarily dismissed.

Also, the writer's concept of normalizing manufacturing output with number of workers—and assigning increased worker productivity values to the output resulting from automation—is wholly off base. One cannot simply credit workers with improvement in productivity due automated (robotic) output. Yes, factory productivity is improved, but there is no evidence that worker functionality, or output, has improved.

I would argue just the opposite: Improvements in automation have reduced human productivity, per se. (I would be interested is seeing a clear definition of "worker productivity" in today's automated environment.) After all, can we say that a one-person operations manager should take credit for the entire output of a totally automated factory? I think not. By the writer's calculation, that manager would be a "superhuman."

Lastly, the writer does not include the positive effects of creating more jobs in those sectors ancillary to factories, such as construction, maintenance, additional housing, and the commercial and consumer aspects of a factory-town economy.

The net effect, in terms of jobs and economic gains, of returning manufacturing to this country would be considerable, rather than trivial as suggested by the writer.

Art Spero, *Shenandoah Valley, Va.*

A TRICKLE AT BEST

To the Editor: I disagree with the evaluation in the November 2016 Trending article ("New Hydro from Old Dams"). The actual output from these new dams would be negligible on the scale of the U.S. electricity consumption, and several could not be built or retrofitted for environmental concerns, fish migration among them.

According to the Energy Information Administration, in 2015 the capacity factor for hydroelectricity in the U.S. stood at 28.5 percent for an actual output of 29 GW. The U.S. Department of Energy is counting on harvesting a capacity factor of 33.7 percent from small dams in remote locations where it makes no economic sense to tie them to the grid, which is a must. The actual capacity factor represents the "good" dams erected on the most suitable rivers.

The proposed piddle-power dams will run at lower CF, perhaps 20 percent, and cost more per GW actually produced than the old ones did. Thus, it is not a 50 GW gain but only about a 10 GW gain from new and retrofitted dams that might never pay for themselves.

I have personal experience with such small-scale hydropower. My father built a hydropower dam on the brook at our house and charged several neighbors for the dc electricity that lit their kitchens. As soon as the utility wires reached the village, he keenly abandoned his money-maker, and pay his monthly bill instead of cashing checks.

Stanislav Jakuba, *West Hartford, Conn.*

DISTRIBUTED CHAOS

To the Editor: In the October 2016 Energy column on the reliability of the traditional grid, Michael E. Webber raised some legitimate concerns.

But in my life I've never seen any of the examples he listed, like cold snaps or coal delivery, be much more than an inconvenience for a few days. Even the big Northeast blackout a few years back was sorted out in a few days.

I lived through Hurricane Hugo in South Carolina in 1989. My power was out for nine days and that required significant replacement of almost a third of the state's power grid.

Now consider the possibility twenty or thirty thousand homes had relied on solar panels on their roofs. All of them would have been trashed. How long do you think it would take to replace that many—particularly since many of the homes would not be able to support them after the storm?

It would take months if not years to recover.

We need to keep those kinds of scenarios in mind as we look at renewables and how they affect the grid.

Michel Whitaker, P.E., *Beaufort, S.C.*

FEEDBACK Send us your letters and comments via hard copy or e-mail memag@asme.org (subject line "Letters and Comments"). Please include full name, address and phone number. We reserve the right to edit for clarity, style, and length. We regret that unpublished letters cannot be acknowledged or returned.

Your Source for Process Measurement and Control

Data Acquisition | Flow | Temperature | Pressure | Automation

OMEGA®

Handheld Thermometers

NEW

HH911T and HH912T
Starts at
$280

- For Lab and Industrial Apps
- Superior Accuracy ±(0.04% Irdgl + 0.3°C)
- 2000 Hour Battery Life
- Single or Dual Input
- Accepts Type J, K, T or E Thermocouples

Visit omega.com/hh911t-hh912t

Compact Rugged Pressure Transmitters

PX119 Series
$99

NEW

- All Stainless Steel Construction
- 15 to 5000 psi Ranges Available
- Choice of Gage or Absolute

Ideally suited for material handling, and industrial and mobile equipment applications where space constraints require a small body size.

Visit omega.com/px119

Coriolis Mass Flow Meter

Mass Flow, Density, Temperature and Volume Flow Meter

NEW

FMC-5000
Starts at
$4590

- Rugged Meters with No Moving Parts Results in Minimal Maintenance

Ideally suited for petroleum, petrochemical, chemical, pharmaceutical, pulp and paper, food and dairy, and more.

Visit omega.com/fmc-5000

Multi-Use PDF Temperature and Humidity Data Loggers

NEW

OM-22-23-24
Starts at
$72

- Plug-and-Play Multi-Use Temperature Data Logger with USB 2.0 Interface
- Accurate Thermistor Temperature Sensor

Ideal for a wide range of test and measurement, quality control, and environmental monitoring applications.

Visit omega.com/om-22-23-24

8 or 16 Channel Universal Input Touch Screen Data Logger

OM-DAQXL
Starts at
$1495

NEW

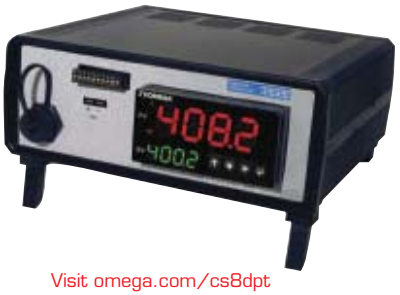
- 7" Touch Screen TFT Display
- Measures Voltage, Current, Thermocouples, RTDs, Thermistors, Strain Gage, Frequency and Pulse
- Fast Sampling Rate– 125 Samples/Sec (1 Channel)

Visit omega.com/om-daqxl

PLATINUM Series Universal Benchtop Digital Controllers

CS8DPT
Starts at
$595

NEW



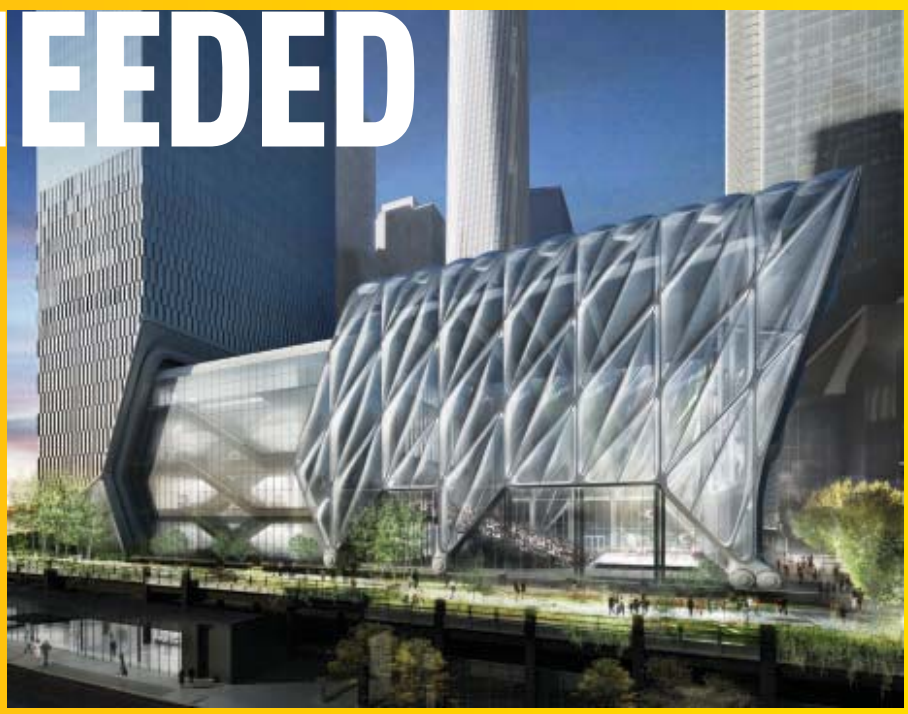
- Universal Inputs: Thermocouple, RTD, Thermistor, Process Voltage/Current, and Strain
- Optional RS232/485 and Ethernet Communications
- High Accuracy

Visit omega.com/cs8dpt

•100,000 Products •Customized Solutions
•Expert Technical Support •Easy Online Ordering •Fast Delivery

omega.com 1-888-826-6342

EXPAND AS NEEDED



ENGINEERS DESIGN A MASSIVE, MOVEABLE BUILDING TO LEVERAGE A CROWDED CITY'S MOST PRECIOUS COMMODITY.

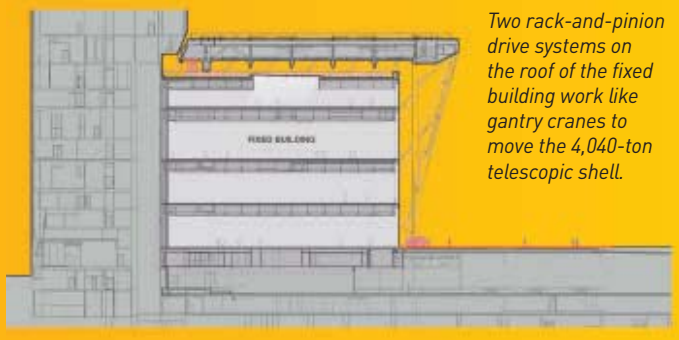
Like most people trying to do big things in a crowded city, the architects and engineers at Diller Scofidio + Renfro had a problem with space.

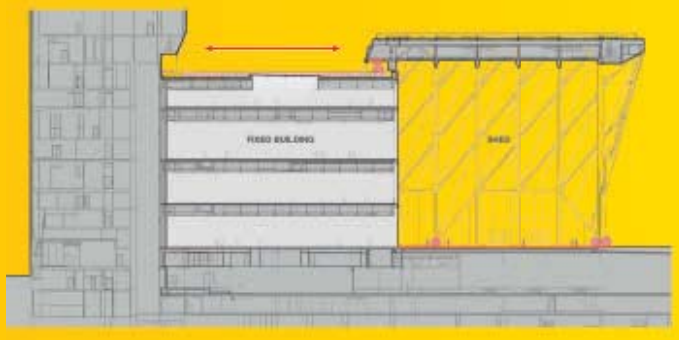
DS+R was designing a high-profile cultural center for the emerging Hudson Yards development in New York City. The main building allowed only 10,000 square feet of performance space, not quite big enough to accommodate large-scale events. But the property also included 20,000 square feet of open public space that was approved for outdoor performances. The architects wanted to incorporate that land into the building design, thereby doubling the center's year-round performance space.

The company's answer: The Shed, a moveable building that combines classic engineering and unique design elements.

The Shed, which will be run by a nonprofit by the same name, includes a six-level fixed building and a lightweight, transparent shell that measures 135 feet by 125 feet and is 115 feet tall. When retracted, the shell will cover the fixed building, and in warm weather, promoters can project movies onto The Shell's eastern wall or hold concerts in the plaza. In bad weather, the shell can be extended over the plaza to create a cavernous temperature-controlled hall that holds 3,000 people.

DS+R has a history of designing buildings that transform space, said Robert Katchur, an associate at the firm and





Two rack-and-pinion drive systems on the roof of the fixed building work like gantry cranes to move the 4,040-ton telescopic shell.

project leader for The Shed. "But we've never done anything on this scale," he said, adding that up to 20 engineers had worked on the project at times. "This felt like a new opportunity."

The main challenge in designing such a large structure that could move efficiently and quickly across a 113-foot span of steel tracks was making it as light as possible.

To control the weight, the team designed a lattice structure with a clear skin made from ethylene tetrafluoroethylene (ETFE). The plastic is about 100 times lighter than glass, so it doesn't require as much steel for support. DS+R plans to cover the lattice with multiple layers of ETFE to trap air and provide insulation properties similar to those of double-paned windows. The structure was also designed to deflect the strong winds that can whip off the nearby Hudson River.

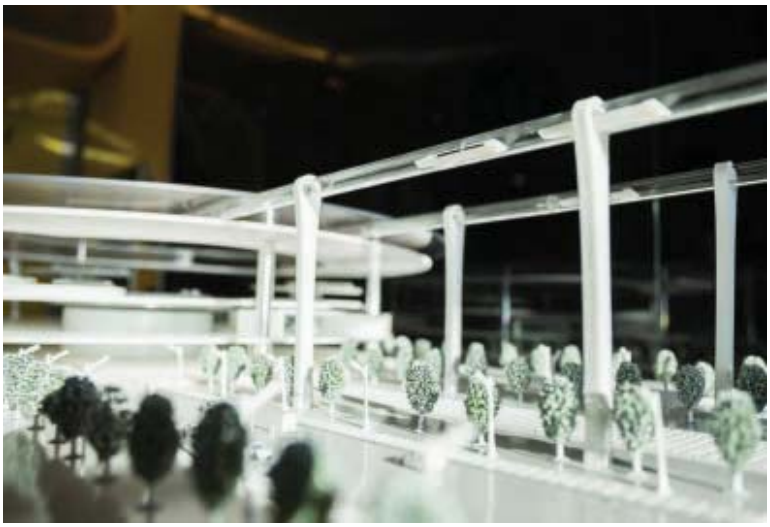
"The lattice serves as a structural expression that keeps the building light and maneuverable," Katchur said. Still, by the time The Shed opens in spring 2019, the structure will weigh 4,040 tons, about as much as 100 fully loaded 18-wheeler trucks.

To maneuver such a massive structure, the team designed a system that works the same way as the gantry cranes used to unload shipping containers from cargo ships. Two rack-and-pinion drive systems will sit on the roof of the fixed structure. Six motors with a combined 180 horsepower—about as much as a compact car—will drive the system.

The shell itself rests on six six-foot steel wheels attached to integral bearing shafts, which provide far less resistance as the wheels roll than a plain bearing system, Katchur said. At a quarter mile an hour, it will take about five minutes for the shell to expand fully.

"We worked very hard to make the structure expressive and beautiful," Katchur said. "But a lot of the design was driven by function and engineering." ME

JEFF O'HEIR



An architectural model of the Hyper Tube and its 600 mph vehicle.

KOREA INVESTING IN HYPER TUBE

The Korea Railroad Research Institute, a government-run technology organization based in Uiwang, reported in January that it signed an agreement to work with Hanyang University and other research groups to develop and build a near-supersonic train capable of reaching speeds of up to 600 miles per hour.

A vehicle that fast could travel from Seoul to Busan, on the southern coast of Korea, in under half an hour. At present, the quickest train trip between those cities takes nearly three hours.

According to a KRRI official quoted in the *Korea Times*, the train would operate inside a low-pressure tube, which would reduce losses due to wind resistance. The concept is similar to one proposed by technology entrepreneur Elon Musk, which Musk called the Hyperloop.

The Korean project is known as the Hyper Tube Express.

A memorandum of understanding was signed between KRRI and Hanyang University, the Electronics and Telecommunications Research Institute, the Korea Transport Institute, the Korea Institute of Machinery & Materials, the Korea Institute of Civil Engineering and Building Technology, and the Ulsan National Institute of Science and Technology.

The railroad research institute reported that it will test core technologies of the system while developing a blueprint for the supporting infrastructure, such as the tubes. KRRI will oversee the system engineering for three years and has already committed 24 billion won (about $21 million) for nine years. The project is endorsed by Korea's ministry for science, information technology, and planning. ME

LONG-LASTING WIRELESS BRAIN IMPLANTS

DUST-SIZE SENSORS powered by ultrasound could open the door to communicating inside the body.

This wireless, battery-less implantable sensor could one day improve brain control of prosthetics. The device measures 3 mm long and is powered by ultrasound. *Photo: University of California, Berkeley*

Inspiration came to Michel Maharbiz in the spring of 2013 as he stood in a parking lot. Why not use ultrasound to power implantable devices, record and communicate brain activity, and—potentially—stimulate nerves within the human body?

By that summer, his team at the University of California, Berkeley had published a paper depicting mathematically how the tiny devices would operate.

By August 2016, they'd built the dust-sized wireless sensors, implanted them in rats' muscles and peripheral nerves, and published their neural-dust research findings in the journal *Neuron*.

Brain implants are used for people with Parkinson's disease, epilepsy, or clinical depression. They're also being studied to help those who have suffered a stroke or head injury.

Implants within the spinal cord stimulate nerves that help with chronic pain and for issues like sleep apnea. Other implants stimulate muscles to allow them to operate.

In the future, a patient with a neural implant may be able to use a prosthetic limb in the same ways humans use their natural limbs: without thinking consciously about how they want the arm or leg to move.

> **"I CAN TAKE A SPECK OF NOTHING AND PARK IT NEXT TO A NERVE... AND READ OUT THE DATA."**
> **MICHEL MAHARBIZ, UNIVERSITY OF CALIFORNIA, BERKELEY**

Before his sudden inspiration, Maharbiz had been toying with a problem that has long dogged neural technology researchers. Conventional implants used to record brain activity or stimulate nerves are composed of long, thin wires topped with electrodes and connected at sites within and outside the body. The wired implants literally emanate from the patient, said Maharbiz, an associate professor of electrical engineering and computer sciences at Berkeley.

What's more, they quit functioning after about five or six years, with some failing much earlier than that due to the effects of their environment.

continued on p. 15 »

Join us for this free webinar

MECHANICAL ENGINEERING WEBINAR SERIES

Using Acoustic Technologies for Leak Detection in Fluid-Filled Pipes

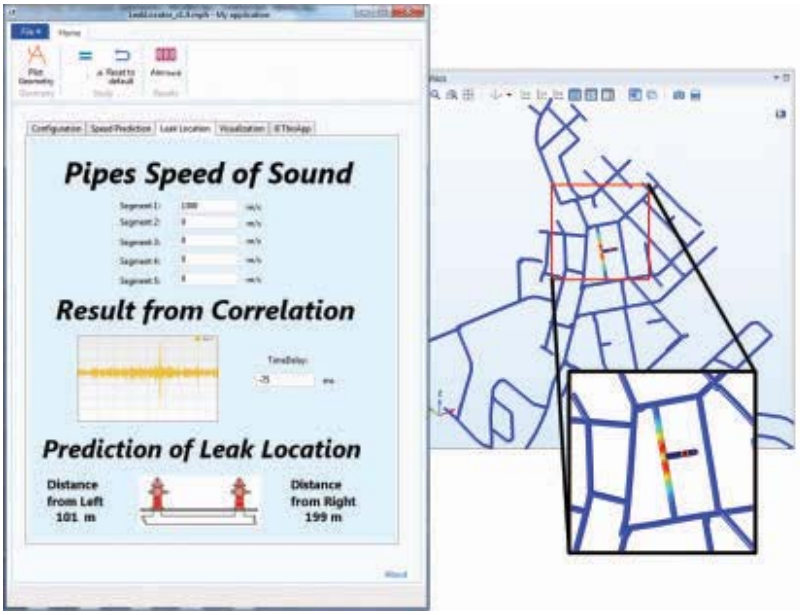
Date: March 23rd, 2017, 2:00 pm EDT

Register today at: https://goo.gl/1mxwgZ

If you are interested in modeling sound propagation in fluid-filled pipes, then tune into this webinar with guest speaker Sebastien Perrier of Echologics Engineering.

The prediction of speed of sound is important to accurately locate leaks in buried pipe networks, such as water mains. Sound propagation is influenced by parameters such as pipe materials and dimensions, which are network dependent. Knowing these parameters is critical for leak detection using acoustic technologies.

In this webinar, Sebastien Perrier will discuss how Echologics Engineering implemented a finite element simulation framework using COMSOL Multiphysics® and deployed it using apps. You will also get a live demonstration of how to model the acoustical behavior of pipes and estimate the variation in speed of sound. At the end of this webinar, there will be a Q&A session.



A sound propagation analysis of a leak noise on a pipe network. The plot shows the pressure in the surrounding area of a leak.

Sponsored by:

COMSOL

SPEAKERS:

SEBASTIEN PERRIER
R&D Acoustical Scientist
ECHOLOGICS ENGINEERING

VALERIO MARRA
Marketing Director
COMSOL

MODERATOR:

CHITRA SETHI
Managing Editor
ASME.org

Register today at: https://goo.gl/1mxwgZ

WHERE TO BUILD MICROHYDRO?

AN OPEN-SOURCE TOOL enables engineers and communities to analyze sites for small hydropower generators.

Small-scale hydropower generators rely on the natural flow of a river or stream unaided by reservoirs that regulate the water delivered to the system. Such run-of-river generators are vulnerable to seasonal changes in water volume, droughts, floods, and climate change. Engineers, communities, and governments need to be able to predict those medium- to long-term changes to make the best use of microhydro. But the modelling tools available are too often only useful with large data sets that are lacking for many small waterways and in developing countries.

A microhydropower generator operating in the Cascade Range of central Oregon.
Photo: Oregon State University

Now, engineers at Oregon State University in Corvallis have developed a kit of open-source tools to work with scarce data and improve what is available. The result is a tool suite that analyzes potential sites for run-of-river hydropower systems anywhere in the world.

The important factors needed to understand a site's hydropower potential are how much water flows through it and the elevation drop, said Kendra Sharp, a mechanical engineering professor at Oregon State who heads the university's Microfluidics and Micro-hydro Lab.

"The elevation drop is easy—you have digital elevation tools for any region in the world," Sharp said. "Water is harder. In order to get the water part, we had to develop climate tools [to measure things like] precipitation and temperature."

Sharp worked with colleagues David Hill, a professor of civil engineering at Oregon State, and Thomas Mosier, a consultant to the World Bank in Washington, D.C., and a former student of water resources and mechanical engineering at OSU, to develop what they call the "hydropower potential assessment tool." That open-source tool and the results from a field test on a microhydropower generator in Oregon were presented in the November 2016 edition of *Renewable Energy*.

Using existing data tools as their starting point, the team refined the resolution of the temperature and precipitation models available from 50 square km to 1 square km. After discovering the climate conditions, the new software suite develops a hydrologic model that shows the amount of water available for a hydropower system. "Then we combine water availability and elevation, giving you hydropower potential," Sharp said.

The models rely on data that is available online and on measurements taken at or near each site. Elevation is easy to find online for most places in the world. Historic climate data may also be easy enough to find for many places.

"If not, you can use our climate downscaling tool (the one that downscales precipitation and temperature grids to 1 km spacing) to generate the needed input," Sharp said.

The models also require streamflow observations for calibration, which may not be readily available. The U.S. Geological Survey provides stream-gauge data for U.S. sites. But in developing countries, stream-gauge data should come from a local stakeholder or a remote sensing system such as the Moderate Resolution Imaging Spectroradiometer.

"While inputting a greater number of stream-gauge data observations is likely to lead to improved calibration and model performance, you can run this with data from just one (or more) sites. The model will be most accurate if your calibration data comes from a point where the upstream landscape characteristics reflect the characteristics of the region of interest," Sharp said.

The software suite can also make predictions about the future of a waterway by plugging in climate-change data. The models can show what may happen to a waterway as the world produces greenhouse gases at their current rate, or slower or faster over time.

The tools are not "super plug-and-play," Sharp said, but they are available online and researchers are encouraged to adapt them to their needs and share their work. The tool suit is available for download at globalclimatedata.org. ME

ROB GOODIER is the editor of EngineeringForChange.org.

continued from page 12 »

BIOENGINEERING: DUST

"This is one of the big challenges of neural technology: how to build an implant that will last for a long time in the body," Maharbiz said. "The cells start ripping apart the implant and wires are rubbing on areas inside the body, and you may get a fibrous mass that grows around the implant."

The researchers call their devices neural dust. They're about the size of a grain of sand and are comprised of a piezoelectric crystal that converts ultrasound vibrations from outside the body into electricity to power a minuscule transistor that rests on a part of the brain, a nerve, or muscle fiber.

The sensors are unique not only because of their size, but also because ultrasound is used both to power the device and communicate measurements. Ultrasound technology is already widely used in the medical field, and ultrasound vibrations can penetrate nearly anywhere in the body, unlike radio waves, Maharbiz said.

"We can make these tiny, free-floating implants for communicating and recording brain activity and we're already doing nerve stimulation with them," he added. "We can implant them into people and have them last for 20 years or more."

But the duties of the neural dust of the future may be much broader in scope, said neuroscience graduate student Ryan Neely, who worked on the project.

"The original goal of the neural dust project was to imagine the next generation of brain-machine interfaces, and to make it a viable clinical technology," Neely said. "If a paraplegic wants to control a computer or a robotic arm, you would just implant this electrode in the brain and it would last essentially a lifetime."

The devices open the door to communicating all kinds of information about what's happening in a patient's body, Maharbiz said.

"Having access to in-body telemetry has never been possible because there has been no way to put something super-tiny super-deep," Maharbiz said. "But now I can take a speck of nothing and park it next to a nerve or organ, your GI tract, or a muscle, and read out the data."

Implants take about a decade to become commercialized and receive FDA approval, and Maharbiz expects the neural dust to be no different.

Once approved, the dust will become vital to many patients' lives. Certainly it is not the kind of dust they'll want to sweep under the rug. **ME**

JEAN THILMANY is an independent writer.

GUIDANCE IN THE AIR

Inventors were **working on drone technology** before the **Wright brothers' first flight**.

Drone delivery is becoming a big deal, especially with Amazon planning to deliver packages via unmanned aerial vehicles. But autonomous vehicles have been invented and patented for more than a century, often with an eye for delivering bombs, not books.

The original idea to remotely control different kinds of vessels likely belonged to Nikola Tesla. His patent for the invention, No. 613,809 (1898), primarily pertains to a remotely controlled boat ("waves or disturbances are conveyed to the vessel in order to control it") but it also notes that the invention applies to other "vehicles." Remember, this was before the Wright brothers' first powered flight at Kitty Hawk.

An early patent which more clearly pertains to an actual airplane controlled by a radio is Patent No. 1,304,314 (1919) for a "wireless controlled flying torpedo."

L. B. Sperry later invented and patented a "mechanically piloted" airplane with a gyroscope for stabilization. This might be the first truly autonomous UAV. Two Sperry patents, 1,418,605 (1922) for an aerial torpedo and 1,670,641 (1928) for a "mechanically-piloted dirigible device," are part of a flying bomb project, which was of interest to the military in World War I but never deployed.

Others continued to work on UAVs after the war. An early invention for a UAV deployed from a manned aircraft is disclosed in Patent No. 1,818,708 (1931).

In World War II, the U.S. Army procured drones from the Radioplane Co. on Hollywood Boulevard in California. Reportedly, Norma Jeane Mortenson (later rechristened as Marilyn Monroe) was a technician there. One of Radioplane's patents is No. 2,257,277 (1939) for a drone with a parachute that can be remotely deployed for easier landings and recovery.

L.B. SPERRY'S PATENT FOR A "MECHANICALLY PILOTED" AIRPLANE WITH A GYROSCOPE FOR STABILIZATION MIGHT BE THE FIRST FOR A TRULY AUTONOMOUS UAV.

The first UAV patent I can find where the UAV has a camera for transmitting images back to the controller is the U.S. Navy's Patent No. 2,649,262 (1945).

During the Vietnam War, the Teledyne Ryan Aeronautical Co. manufactured jet-powered drones launched and controlled from C-130s. One Teledyne patent, No. 3,703,998 (1972), pertains to a jet-powered drone with wings that fold for storage and transport inside an aircraft bomb bay.

Of course, probably the most well-known drone is the Predator built by General Atomics Aeronautical Systems Inc. One patent for the Predator is No. 5,918,832 (1999).

Today, numerous initiatives exist for UAVs. One is to fly longer. AeroVironment Inc. specializes in long-range solar-powered and, as disclosed in Patent No. 8,011,616 (2011), hydrogen-powered UAVs.

Another idea is to deliver mail using drones as disclosed in pending U.S. Patent Application No. 2014/0254896 by the Zhou brothers—Tiger, Dylan, and Andrew. Now Amazon and others are hoping to deliver packages using UAVs. Amazon's pending Patent Application is No. 2015/0120094.

Who first had that idea? Tesla again. Tesla's 1898 patent concludes as follows:

"The invention which I have described will prove useful in many ways. Vessels or vehicles of any suitable kind may be used, as life, dispatch, or pilot boats or the like, or for carrying letters, packages, provisions, instruments, objects, or materials of any description, ... but the greatest value of my invention will result from its effect upon warfare and armaments, for by reason of its certain and unlimited destructiveness it will tend to bring about and maintain permanent peace among nations."

Alas, Tesla's prediction of peace among nations has yet to be realized. ME

KIRK TESKA is the author of Patent Project Management and Patent Savvy for Managers, is an adjunct law professor at Suffolk University Law School, and is the managing partner of Iandiorio Teska & Coleman, LLP, an intellectual property law firm in Waltham, Mass.

COMPANIES LAUNCH HYDROGEN CONSORTIUM

A group of 13 energy, transportation, and industrial companies announced the formation of the Hydrogen Council in January during the annual World Economic Forum in Davos, Switzerland.

The Hydrogen Council is comprised of Air Liquide, Alstom, Anglo American, BMW Group, Daimler, ENGIE, Honda, Hyundai, Kawasaki, Royal Dutch Shell, the Linde Group, Total, and Toyota, which collectively represent total revenues of more than $1 trillion and employ 1.72 million people worldwide.

The CEOs of the member companies declared that they are determined to position hydrogen technologies as one of the key means for reducing carbon emissions over the next several decades.

Member companies confirmed their ambition to accelerate their investment in the development and commercialization of the hydrogen and fuel-cell sectors. That additional investment is predicated on receiving policy support from government stakeholders.

"We cannot do it alone," Benoît Potier, CEO of Air Liquide, was quoted in a press release announcing the launch of the consortium. "We need governments to back hydrogen with actions of their own—for example, through large-scale infrastructure-investment schemes. Our call today to world leaders is to commit to hydrogen so that together we can meet our shared climate ambitions and give further traction to the emerging hydrogen ecosystem." ME

DUTCH TRAINS RUN ON WIND POWER

The Dutch railway company NS transports 600,000 passengers a day on 5,500 train trips, which requires 1.2 billion kWh of electricity a year. In January, the company announced that all its electrical demand was met by wind power.

A partnership between NS and Eneco, the Rotterdam-based electric utility, was launched in 2015, with the aim of making the railway system carbon-neutral by 2018.

Although the Netherlands generates 7.4 billion kWh from wind-power production, the demand for renewable electricity exceeds that level.

Eneco was able to secure enough wind power from neighboring countries, in addition to building some new wind farms, to meet the renewable energy goal for Dutch railroads a year early. ME

Q&A
ADDISON STARK

WHILE GROWING UP ON A FARM in eastern Iowa during the 1990s bioeconomy boom, Addison Killean Stark saw first-hand how biofuels could transform farmers' lives and our energy system. Now, as an Acting Program Director at the Advanced Research Projects Agency—Energy, he's combining biomass and carbon sequestration to create a revolutionary new form of electricity generation. To hit the carbon targets in the Paris agreements and avoid the worst effects of climate change, he said, we need electricity generation that "actually removes CO_2 from the atmosphere."

ME: What led you to want to work with biomass and redesign power plants?
A.S: While I was at the University of Iowa for my undergraduate, I got involved in energy technology and energy policy. They had a coal power plant they were able to retrofit to use oat hulls—the outer grassy husk of the oat kernel—from a nearby Quaker Oats production facility. Since then it has always been in the back of my mind: How can you more broadly utilize this type of approach?

ME: How can you generate electricity and simultaneously pull carbon dioxide out of the atmosphere?
A.S: The approaches to do that are two-fold. You can build direct air capture plants, [which are] effectively chemical plants. All numbers point to that being an extremely expensive approach. A biological plant, however, is a carbon-capture plant that builds itself and runs itself cheaply and is all powered by solar. If you then [combust the biomass] in a power plant, you can have electricity generation and still sequester your CO_2 instead of just having to pay for it.

ME: How do we get there?
A.S: [We need] further development of direct biomass combustion or gasification technologies to enable cocombustion of biomass and coal. [We need] biomass pretreatment technologies such as torrefaction that makes biomass more like coal. We also need to [engineer and] grow plants that have chemical components in them that are closer to coal so they're optimized for their combustion properties.

ME: What's your blue-skies vision of how it would work on the ground?
A.S: You can imagine power plants that are either within a few hundred miles of large resources of agricultural waste or dedicated energy crops that are being harvested. These dedicated energy crops would be these plants that have been optimized for high lignin content, high energy density. Out in the field, the farmer will harvest the food component [of the plant] and sell it into food markets, but also utilize biomass pretreatment technologies in the field. The farmer will then ship biocoal to centralized power plants. There, it will be utilized together with coal to make electricity, and you would have the sequestration of the CO_2 underground.

ME: There's been such a struggle to get coal with carbon capture and sequestration actually implemented at power-plant scale, with projects falling through all over the world. Is this really practical?
A.S: Under policy scenarios in which society decides to capture CO_2 and sequester it or put a price on carbon, this technology has to exist.

ME: In other words, we're not there yet, policy-wise, but the technology's going to be ready?
A.S.: I believe so, yes.

ME: You're a fairly young engineer and you're taking on this huge world-changing challenge. What advice would you have for student engineers who also hope to tackle important challenges in the world?
A.S: Find that topic that you really are passionate about. I've found an area that I'm truly both passionate about as a major societal, technical challenge, but also is intellectually stimulating to me. Having those two pieces together is what makes it so exciting. ME

DAN FERBER

CHINA CAR SALES RECORD

In spite of fears of an economic slowdown, sales of automobiles in China hit a record mark in 2016. According to the China Association of Automobile Manufacturers, more than 28 million cars were sold in China in 2016, a 13.7 percent increase over the year before.

China is the world's largest auto market.

The number of cars manufactured in China also increased, to 28.12 million units. Chinese manufacturers exported 708,000 vehicles last year, and that figure is expected to reach 750,000 in 2017.

The data was first reported by the Xinhua News Agency.

Year-over-year growth in sales has fallen over the past several years. The manufacturing association forecasts that auto sales will expand to 29.4 million vehicles in 2017, a 5 percent increase. ME

BIG NUMBER

56 hours

DURATION OF THE FLIGHT OF A COMBUSTION-POWERED UNMANNED AERIAL VEHICLE.

ONE ANTICIPATED ADVANTAGE OF DRONE AIRCRAFT over piloted ones is the ability to stay aloft for days, maybe longer. In late November, a UAV built by Vanilla Aircraft of Falls Church, Va., took off from an airfield in Las Cruces, N.M., and stayed in the air for more than two days and nights, setting a National Aeronautic Association duration record for its class. According to a Department of Defense press release, the VA001 drone is designed to carry a 30-pound payload at 15,000 feet for up to 10 days without refueling. After 56 hours, the drone landed with its fuel tank still half full.

SELF-DRIVING MINING TRUCKS

AT OPEN MINING SITES, it may actually be safer to hand the keys over to autonomous vehicles following GPS-guided routes.

Walk around a surface mine with 30-ton, 2,600-horsepower trucks hauling material, and you might hope the drivers paid attention to your whereabouts. But if the site used autonomous mining trucks, there might be no drivers—and you'd be perfectly safe.

Although human drivers can do the job, autonomous trucks are able to drive an exact route every time without getting bored, tired, or taking time off. That elimination of human error and regular training improves safety and increases a mine's productivity.

Mining engineers began experimenting with autonomous equipment in the mid-1990s, but it has taken time for the technology to catch up with the idea. Today, however, both Caterpillar and Komatsu manufacture autonomous mining trucks that are used at sites around the globe.

The driverless trucks offer mining companies some clear advantages. "They need fewer people at the site, plus when they're operating 24/7 there's never a case of human error because of fatigue," said Michael Murphy, chief engineer of mining and technology solutions for Caterpillar. What's more, Murphy added, "human drivers can veer slightly off course from time to time. The autonomous vehicles just do the job, over and over."

The new equipment relies on advances in computing power and memory, two-way radio communication and research from the Defense Advanced Research Projects Agency on autonomous vehicles.

To navigate around the site, each autonomous mining truck employs both radar and lidar (light detection and ranging, devices) to sense objects around the vehicle. These, combined with high-precision GPS, create an overall picture of location, speed, and possible obstacles.

That information feeds into a centralized computer at the site's control center. The computer replaces the driver's job. It reads the truck's navigation system and selects the best route from A to B. It also directs the truck to a particular shovel. After the truck is loaded, it proceeds to a particular dumping point. Each dump location is recorded so that two loads aren't dropped into the same pile.

The computer is programmed with scheduling and assignment algorithms designed to maximize productivity and meet each day's loading goals. Because of this, the routes from shovels to dumping points are extremely precise, with the trucks running the same paths over and over again. An onboard inertial navigation system acts as a backup, sending an alert if there's a discrepancy between the guidance technologies.

The computer functions as a kind of mine air-traffic control, keeping track of everything going on within the mine's perimeters. "If a light vehicle is moving near an autonomous truck, the system calculates if it will get in the truck's path and when, slowing it down to avoid a collision," Murphy said.

The system is sensitive enough to detect a human in a truck's path—or even a kangaroo, which happens frequently at mining sites in western Australia.

Automobile engineers have visited with the Caterpillar team to pick their brains on autonomous vehicles, Murphy said. But the trucks have a different mission than an autonomous car, he added. "Our trucks are designed to move 100 million tons of material a year safely and efficiently, but getting people around securely is more important." ME

JOHN MORELL writes about technology and business from Woodland Hills, Calif.

E-FEST GOES GLOBAL THIS MONTH

THE WORLD HAS NOW TO MOVE forward without the U.S. on the road towards climate-risk mitigation and clean-technology innovation.

— *Hans Joachim Schellnhuber, director of the Potsdam Institute for Climate Impact Research, in a statement released November 9, 2016.*

ASME this month will launch a series of global events aimed at college students and designed to highlight the latest breakthroughs, changes, and opportunities happening in the world of engineering.

The E-Fests (short for Engineering Festivals) focus on design, advanced manufacturing, and robotics.

The three regional events, each taking place over three days and two nights, feature a variety of hands-on activities including hackathons, keynote speakers, technology and innovation lightning chats, career-briefing and networking sessions, mentoring opportunities, leadership and professional development workshops, social activities, and entertainment.

"ASME has created E-Fests as a vehicle to better prepare post-secondary students and early career engineers to be a part of today's diverse and multidisciplinary engineering community," said Noha El-Ghobashy, executive director of the ASME Foundation.

E-Fest Asia Pacific, will take place from March 3 to 5 at the LNM Institute of Information Technology in Jaipur, India. E-Fest West is scheduled from March 17 to 19 at the University of Nevada, Las Vegas. E-Fest East is from April 21 to 23 at Tennessee Tech University in Cookeville, Tenn.

The festivals will also serve as the new venues for the regional rounds of ASME's premier student competitions: the Human Powered Vehicle Challenge, the Student Design Competition, the Innovative Additive Manufacturing 3-D (IAM3D) Challenge, and the Old Guard Competition.

For more information on the E-FESTS and the student competitions, visit http://efests.asme.org. ME

DARPA FUNDS SURPRISING SYSTEMS

ENGINEERS NOT ONLY BUILD CHEMICAL systems, they also use them. This month, we look two labs at the Southwest Research Institute that have made unique chemical systems. One destroys poison gas with an internal combustion engine and dirt. The other makes industrial quantities of cold plasma.

A portable system can destroy up to 10 tons of chemical warfare agents using an internal combustion engine, diesel fuel, and dirt. *Photo: Southwest Research Institute*

BURNING CHEMICAL AGENTS

THE LAB Chemistry and Chemical Engineering Division, Southwest Research Institute, San Antonio, Tex. Darrel Johnston, senior program manager.

OBJECTIVE Develop new ways to manage and destroy chemical-warfare agents and other hazardous materials.

DEVELOPMENT A truck-mounted portable system treats hazardous waste using diesel fuel, dirt, and an internal combustion engine.

Destroying most chemical warfare agents is surprisingly easy, but it takes huge facilities to annihilate every molecule and ensure that no toxic by-products formed during the destruction process escape into the environment.

Now Darrel Johnston, an engineer at Southwest Research Institute in San Antonio, is developing a portable system that breaks down poison gases using dirt, diesel fuel, and an internal combustion engine. It handles a wide range of chemicals and can fit on one or two tractor-trailers.

Johnston dreamed up the idea years ago while managing a poison-gas destruction plant in the Pacific Ocean. Most poison gases are hydrocarbons that release energy when burned, and Johnston wondered if he could use them to generate electricity.

When the Defense Advanced Research Projects Agency requested proposals for portable systems, Johnston decided to try it. He turned to an experimental internal combustion engine SwRI was developing to boost fuel economy. It ran one cylinder rich (too much fuel) to produce syngas, a combination of hydrogen and carbon monoxide fuel. Recirculating syngas into the other three conventional cylinders acted like octane to boost their performance.

Johnston used the engine to deliver syngas into the three cylinders running simulants (safe chemicals that resemble poisons). This drives the temperature high enough to destroy 99 percent of the simulants.

The remaining exhaust goes to a reactor with a column of suspended soil particles

at 400 °C. Heat and contact with the hot particles breaks down any remaining simulants, while the calcium in the soil adsorbs the acid gases synthesized by the heat and converts them to safe materials. In fact, the calcium bonds so tightly to fluorine and chlorine, which could form potentially toxic gases, that the resulting soil can be safely buried, Johnston said.

The reactor works best with limestone and gypsum soils, two forms of calcium readily available almost anywhere in the world, Johnston said. SwRI and DARPA are planning tests on actual chemical warfare agents this winter. ME

Generating high volumes of cold plasma could make it possible to repair aircraft coatings in the field and sterilize hospital rooms. *Photo: Southwest Research Institute*

GIANT AIRBORNE PLASMAS

THE LAB Surface Engineering and Materials Chemistry Section, Materials Engineering Department, SwRI, San Antonio, Tex. Vasiliki Zorbas Poenitzsch, principal scientist.

OBJECTIVE Develop plasma deposition systems for applying coatings and synthesizing nanoparticles and other bulk materials.

DEVELOPMENT Open-air cold plasma systems generate orders of magnitude more ionic species.

A new open-air cold system generates enough plasma to apply thick coatings to metals and alter material surfaces rapidly in open air. Called the High Power Impulse Plasma Source (HiPIPS), it was developed by SwRI's Vasiliki Zorbas Poenitzsch.

Plasmas, which are clouds of hot ions and radicals, typically live in vacuums confined by magnets. Over the past decade, researchers have created jets of cooler plasma in open air, but they generate only a trickle of ions and radicals.

"Comparing them to HiPIPS is like comparing a squirt gun to a fire hydrant," said DARPA deputy director Tyler McQuade, who funds the project. HiPIPS generates four orders of magnitude more ions and six orders of magnitude more radicals.

Poenitzsch did this by using pulsed dc generators, which produce two to three times higher peak power densities than other power supplies. This produces massive amounts of plasma.

But could those pulses ignite and sustain plasma in flowing air? To find out, Poenitzsch built a plasma jet head and applied pulsed power voltage to an electrode. As gases flowed past, the high voltage broke them down into ions and radicals. The power supplies reduce power just prior to arcing, which prevents those lightning-like sparks from disrupting the carefully sustained plasma.

Poenitzsch has tested HiPIPS with argon, a neutral carrier than can modify plastic or metal surfaces to improve adhesion or water resistance.

She has also worked with nitrogen, which is more reactive. Aiming a jet of cold nitrogen plasma at a wire of pure titanium would entrain the titanium atoms and deposit them on a surface as titanium nitride. This durable, corrosion-resistant material could be used for field repairs to coatings on aircraft landing gear damaged by rocks or other debris.

Poenitzsch has already built plasma jet heads large enough for industrial processes like roll-to-roll plastics processing. She plans to work with hydrocarbon gases to make coatings, such as the diamond-like carbon films used to protect aircraft canopies.

McQuade envisions portable HiPIPS units that can blow cold plasma into a field hospital to kill bacteria prior to surgery. ME

ALAN S. BROWN

MEASURING MICROSCOPIC MOVEMENT

Engineers can now create ever-smaller microelectromechanical systems (MEMS) for use in making sensors, biomedical devices, control systems, accelerometers, tiny robots, and countless other products.

What they can't always do is measure the motion of the parts of these miniscule systems in a highly accurate way.

Now physicists at the National Institute of Standards and Technology (NIST) have come a step closer to solving the problem.

They've created a device that precisely measures subatomic motions shorter than the diameter of a hydrogen atom. The team also developed a fabrication process for mass-producing the device.

The new device, also called a nanomechanical plasmonic resonator, suppresses the noise of mechanical motion to a level 1.5 orders of magnitude less than that of comparable plasmonic systems and four times lower than laser Doppler vibrometers, the current standard for measuring the movement of MEMS, the team said.

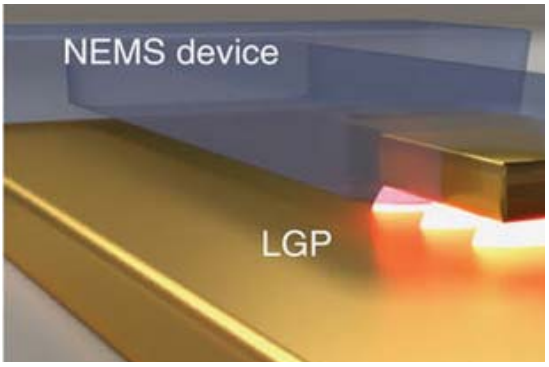
This proof of concept could eventually allow engineers to develop new applications and solutions to sense hazardous materials, deploy airbags more quickly and accurately, perfect the movement of nanorobots, and detect extremely weak sound waves.

"Mechanical engineers will be on the forefront of engineering components at the nanoscale," said Brian Roxworthy, who, with fellow NIST physicist Vladimir Aksyuk, recently published the findings in *Nature Communications*.

"This will give them a new tool to conduct highly sensitive motion measurements," Roxworthy said.

To fabricate their device, Roxworthy and Aksyuk used silicon nitride to build can-

Localized gap plasmon (LGP) resonators are embedded into arrays of silicon nitride nanostructures in this plasmonic NEMS device.



tilever mechanical resonators that look like tiny diving boards. They embedded the cantilevers with gold nanoparticles and positioned them above a gold sheet.

The physicists then used a sacrificial layer of chromium that they later removed with a wet-chemical etch to create a tiny air gap between the gold nanoparticles and the gold sheet. This allowed the cantilevers to vibrate.

The air gap—15 nanometers in width or about 10,000 times as thin as a human hair—was so narrow that light from a laser could not pass through. But the light's electric field does cause plasmons—groups of trapped electrons that move along the boundary between the gold nanoparticle's surface and the air in the gap—to vibrate like a plucked guitar string at frequencies that depend on the gap diameter.

The cantilever's motion is driven by ambient thermal energy. It changes the width of the air gap, which in turn changes the frequency at which the plasmons oscillate. This in turn alters how laser light is reflected. The scientists detected those changes using an optical microscope and a photodetector connected to an electronic spectrum analyzer.

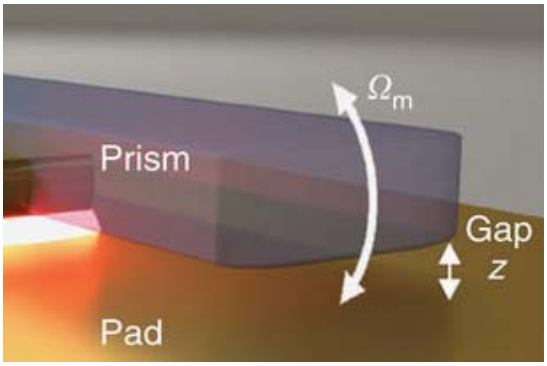
By using this method, the team was able to bypass the optical diffraction limit, which typically limits the resolution of light-based measurements of motion. This allowed them to detect motions much smaller than the wavelength of the laser they used.

"What's new in our device is that we can perform highly sensitive measurements at scales that are much smaller than the diffraction limit," Roxworthy said. "And [we can] make chip-level devices."

To that end, the physicists used lithography to print 25,000 of these devices on a single computer chip. This fabrication approach is scalable and designed to facilitate practical applications of the motion-measurement technique. For example, the team's plasmonic resonators could be adapted to measure the movement of mass-produced devices such as MEMS accelerometers and gyros used in sensors that detect motion and orientation in cars and smartphones.

The NIST system could be ready for mainstream use in about three to five years, Roxworthy said. ME

JEFF O'HEIR



URANIUM AND COAL: RIVALS OR PARTNERS?

ALVIN M. WEINBERG, DIRECTOR, OAK RIDGE NATIONAL LABORATORY, OAK RIDGE, TENN.

A renowned physicist makes the case that rather than choosing one or the other, the United States should find ways to make coal and nuclear power work together.

LOOKING BACK

The case for what would become the Department of Energy was first being made when this article was published in March 1967.

The rivalry between fossil fuels and uranium is good and in the best American tradition. It is good for coal to be put under the kind of economic pressure that forces it to improve mining methods and come up with technological advances like unit trains. It is good for uranium to be asked sharp, no-holds-barred questions by its competitors in the fossil fuels industries.

Nonetheless, it seems that something is still lacking in this competitive relationship. Nuclear energy has its government champion—the U.S. Atomic Energy Commission and the Joint Congressional Committee on Atomic Energy; coal has its government champion—the Department of the Interior. Neither of these two vigorous and well-run agencies can be faulted. Yet a more fundamental question deserves serious consideration: Should there not be some home in government for energy itself—not nuclear, or coal, or oil, or solar, or water—but all forms of energy which, after all, is the ultimate raw material?

That some such feeling must exist in Washington is suggested by the energy study that has been going on for several years in the Office of Science and Technology under the leadership of Ali Cambel, formerly head of the Department of Mechanical and Astronautical Sciences at Northwestern University. This study will look at the entire energy picture. There is much reason to believe that the broad responsibility for energy suggested by the outlook of such studies might well become the job of some yet-to-be organized government agency.

In suggesting alterations to existing government structures, one necessarily treads on the most treacherous political ice. However, if a person is deeply convinced of the increasing role of energy in our society, this is an important order of business of our government, namely, the reexamination of the alignment and structure for dealing with broad problems of energy. Out of such a reevaluation process may come a more rational way of coping with the ever-growing and even insatiable demands that society has for energy. In this way the full potentials of both uranium and fossil fuels may be exploited for the benefit of all.

Every source of energy will be required in an energy-exploding economy. Each source will eventually find those spheres of use which capitalize on its strengths and minimize its weaknesses. Competition between various sources of energy will tend to keep everyone honest much to the benefit of the society that must use energy at an increasing rate. **ME**

A NUCLEAR PIONEER

Alvin M. Weinberg had been the director at Oak Ridge for a dozen years when his article in *Mechanical Engineering* magazine was published. After studying biophysics at the University of Chicago in the 1930s, Weinberg was pressed into service as part of the Manhattan Project, the wartime effort to design and build an atomic weapon. His team was tasked with developing a reactor that could transmute uranium into plutonium. Weinberg is also credited for proposing the pressurized water reactor, which became the industry standard, though through his long career he advocated the development of other designs and had an experiment molten-salt reactor built at Oak Ridge in 1964.

Weinberg with John F. Kennedy in 1959.
Credit: Ed Westcott/DOE

April 3–7, 2017, Denver, Colorado

Pressure Vessels, Piping and Pipelines MasterClass Series

Register Today for Practical Training this April Led by ASME PVP Experts and Code Authorities

What Past ASME MasterClass Attendees Have to Say:

"... very informative and quite practical to help improve my day-to-day failure analysis investigation."
– Michael Adeosun, GE Power

"... provided a good balance of technical depth and practical experience. It gave me a better understanding of Materials Behavior with Failure Modes."
– Bob Courtney, Fixed Equipment Reliability Engineer, PBF Energy

* Accredited by IACET

ASME Training & Development is accredited by the International Association for Continuing Education and Training (IACET). ASME Training & Development complies with the ANSI/IACET Standard, which is recognized internationally as a standard of excellence in instructional practices. As a result of this accreditation, ASME Training & Development is authorized to issue the IACET CEU.

Join an elite group of ASME PVP and Code experts who lead this week-long ASME PVP MasterClass learning event with a variety of courses discussing practical applications of current technologies and standards that establish safety rules governing the design, fabrication and inspection of pressure vessels, piping and pipeline systems, featuring:

- Bases and Application of Piping Flexibility Analysis to ASME B31 Codes (MC110)
- Piping Vibration Causes and Remedies - a Practical Approach (MC111)
- Piping Failures - Causes and Prevention (MC117)
- Design by Analysis Requirements in ASME Boiler and Pressure Vessel Code Section VIII, Division 2 – Alternative Rules (MC121)
- **NEW!** Fatigue Analysis Requirements in ASME BPV Code Section VIII, Division 2 – Alternative Rules (MC123)
- **NEW!** Inspection Planning Using Risk-Based Methods (MC124)
- **NEW!** Bases and Application of Design Requirements for High Pressure Vessels in Section VIII, Division 3 of the ASME B&PVC (MC127)
- Run-or-Repair Operability Decisions for Pressure Equipment and Piping Systems (MC132)
- Onshore Pipeline Design and Construction - A Practical Approach (MC139)
- Pipeline Defect Assessment (MC140)
- **NEW!** Pipeline Stress Corrosion Cracking Management (MC141)
- **NEW!** Integrity Management of Natural Gas Pipelines Using the ASME B31.8S Standard (MC142)
- **NEW!** Pipeline Integrity Issues, Mitigation, Prevention and Repair Using ASME B31.8S Standard (MC143)
- **NEW!** Practical Application of ASME Boiler and Pressure Vessel Code Section VIII Division 1 (MC147)
- **NEW!** Fracture Mechanics and Other Methods for Fatigue and Fracture Analysis of Pressure Equipment (MC150)
- **NEW!** Design by Rule Requirements in ASME Pressure Vessel Code Section VIII Division 2 (MC151)

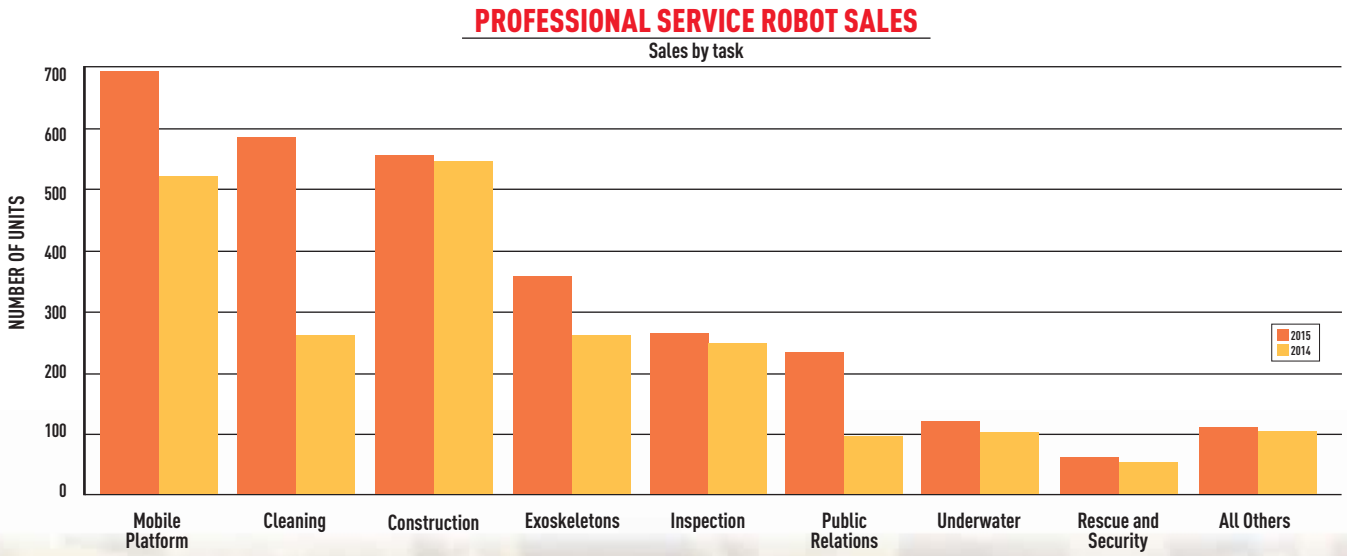
For program details and to register, type in any browser: go.asme.org/pressuretechtraining

ASME SETTING THE STANDARD

The American Society of Mechanical Engineers® (ASME®)

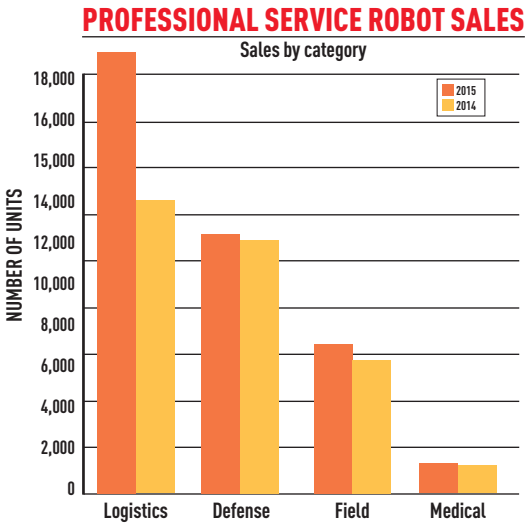
BY THE NUMBERS: ROBOTS ON THE RISE

Automation for the service sector is a multibillion-dollar business.



The impact of robots on the manufacturing sector has been well documented. According to the International Federation of Robotics, a trade association in Frankfurt, Germany, the number of industrial robots in operation will increase to 2,600,000 by the end of 2019, a jump of nearly a million in just four years.

But professional service robots are increasing at an even faster rate. Those robots, which the IFR defines as ones used in commercial, nonmanufacturing tasks that show some degree of autonomy, range from power-assist exoskeletons to humble mobile barn cleaners. Annual sales of professional service robots rose by 25 percent in 2015, the latest year for which complete data is available. That year, companies and individuals purchased 41,100 service robots worth $4.6 billion.



Between 2016 and 2019, the IFR expects the world to deploy an additional 330,000 professional service units worth $23 billion.

The IFR published the data in its report, *World Robotics 2016.*

Robots used in logistics systems led the way, accounting for more than half of all professional service robots sold in 2015. Those robots have enough autonomy to plan routes, avoid obstacles, and work safely around people, even under crowded conditions. Warehouses use them to stock or retrieve goods. In factories, they easily adapt their routes to accommodate changes in manufacturing processes.

Logistics robot sales reached $780 million in 2015, including 15,500 units for warehouses and 3,400 for factories. The IFR projects that sales of logistics robots will rise to 175,000 units worth $5.3 billion between 2016 and 2019. In 2015, more than 80 percent of all logistics systems were built in the U.S.

The IFR warns that its data may vastly underestimate the number of logistics robots in the world, since many rollouts are not reported. Amazon, for example, has built and deployed more than 30,000 robots for its warehouses since 2012.

Less numerous, but more valuable, are medical robots. Those robots, which are used in diagnosis, surgical assistance, and rehabilitation, range from mobile disinfection robots that reduce infection rates in hospitals to da Vinci surgical robots that enables surgeons to perform precision tasks more accurately. While only 1,300 medical robots were sold in 2015, they were worth $1.5 billion. By 2019, the IFR projects that sales of medical robots will top $7 billion.

Some 27 percent of all professional service robots are used in defense applications, such as surveillance and bomb disposal. Defense sales in 2015 included 9,400 unpiloted aerial vehicles and 1,500 unmanned ground vehicles.

"The demand for service robots is seeing a historic breakthrough," Joe Gemma, president of the International Federation of Robotics, said. "In addition to the already established business with professional service robots, the personal and domestic segment is increasingly dynamic. Growth forecasts between 2016 and 2019 are just excellent." **ME**

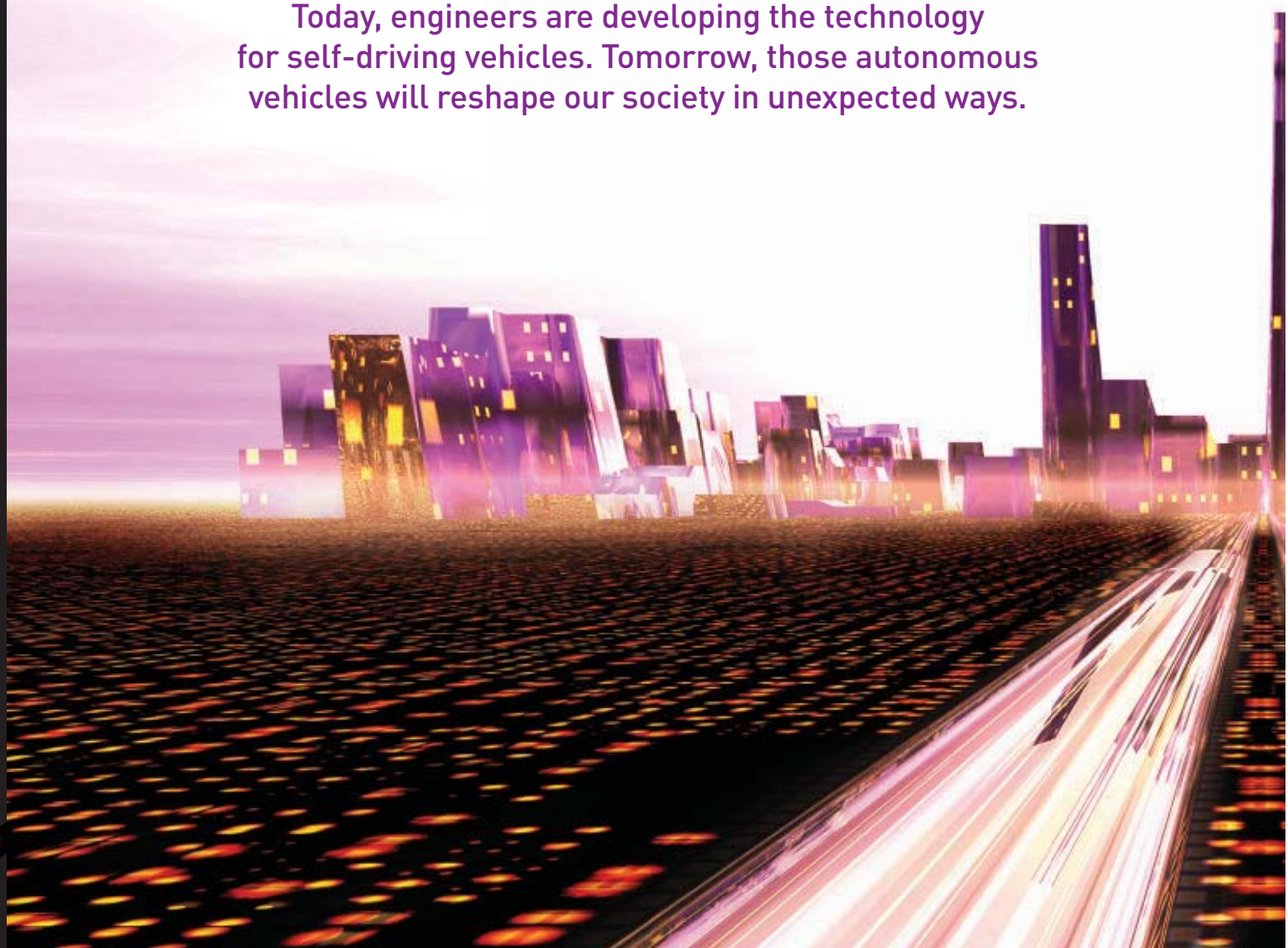
ALAN S. BROWN

An army of more than 45,000 robots augments the human workforce at Amazon's warehouses.

F30

BRAVE NEW ROAD

Today, engineers are developing the technology for self-driving vehicles. Tomorrow, those autonomous vehicles will reshape our society in unexpected ways.



BY BRIAN DAVID JOHNSON

Autonomous cars used to exist only in culture, not in technology. You could find self-driving cars springing from the imagination of science fiction writers and filmmakers or in the musings of Silicon Valley visionaries. But they were tropes, not technologies. A self-driving car just wasn't the kind of thing one could expect to see on the road in a lifetime.

No more. Vehicles that can drive themselves without a human hand on the wheel or foot on the brake pedal are a technological reality today and soon will be cruising through your neighborhood, if they aren't already there.

Indeed, according to one estimate, 10 million self-driving cars will be on the road by 2020.

For many, this now-inevitable triumph of technology is neither needed nor wanted. People love their cars. They enjoy the freedom a vehicle gives them to commute to work, run personal errands, and escape on family vacations. Car culture is so embedded in our society—and our emotions—that one in four people name their car and many more talk to them on a daily basis. If you have the physical, mental, and financial strength to drive a car you love, then the driverless future seems like an unnecessary, even frightening, prospect.

As a futurist, I look at technological, economic, and cultural changes to understand what it will feel like to live a decade or more in the future. That sounds like an abstract and ethereal thing to do for a living, but the future is local and is built every day by the actions of people. I'm trained to look for change where it happens first—at the margins, on the fringes, in places where the present state of technology isn't really working out for people the way it ought to. Those are the people and places that need change and see disruptive new technologies not as a burden, but as an opportunity.

By thinking about what people on the fringes could do with that opportunity, you can begin to map out some potentially surprising ways a new technology like self-driving cars could reshape our society.

The engineering community is building this future, and is focused on making autonomous vehicles safe and efficient and attractive to use. That is incredibly important. But it's also important not to

This delivery droid operated by Just Eat autonomously delivers takeout orders to hungry Londoners.

lose track of the social implications of this new technology—and every new technology—when it reaches the market and comes into wide use.

If many people think they aren't ready for autonomous vehicles, which have been foreseen for decades, wait until they grapple with the changes they didn't anticipate.

REGAINING INDEPENDENT MOBILITY

When I talk about people on the fringes, that makes it sound like leather-clad youths with spiky green hair. But I'm thinking more of people with gray hair: I believe the group that will experience the most unexpected impact from self-driving cars is the elderly.

For one thing, the Baby Boom generation that is now aging into retirement is used to having things its own way. Their entire lives, popular culture and Madison Avenue have sold Boomers on the idea that they could have it all, and that they had a birthright to the freedom of the open road. Think *American Graffiti*, Jan and Dean, or *Thelma and Louise*. Even when the so-called Me Generation starts to lose its eyesight, it will insist on keeping that independence, no matter the cost.

AARP, for one, recognizes the size of the potential market. "About 36 million current older drivers still hold valid licenses. About 80 percent of them live in car-dependent suburbs or rural areas, not cities with public transit. And nearly 90 percent say they intend to age in place," wrote David Dudley in *AARP Magazine* in 2015. "For those whose independent living is closely tied to their ability to drive safely, self-driving tech is a future that can't come soon enough."

By 2030, the number of Americans over 65 is expected to reach 72 million.

AARP's interest is important for another reason: The elderly vote, and if they want self-driving cars, lawmakers will quickly tackle some of the thorniest policy hurdles—such as regulation, local traffic laws, and insurance.

But an elderly-led adoption of autonomous vehicles will look different from what the technology's biggest backers have been touting. For one thing, the epicenter for the self-driving future would not be Silicon Valley with its tech millionaires and billionaires, or Las Vegas with autonomous tourist minibuses, or Pittsburgh, where Uber is now testing driverless taxis. Instead, the

first place to incorporate autonomous vehicles into its mainstream may well be The Villages, a 70,000-resident retirement community in Florida.

If so, that would change the type of vehicle to be rolled out. Instead of some sleek sedan, think of a self-driving golf cart!

The Villages already has around 100 miles of golf-cart trails, and for residents it is the preferred mode of transportation in the community. From an infrastructure standpoint, kitting out a retirement community with the sensors, lane markers, and other technology needed to have a meaningful fleet of autonomous vehicles is far simpler than doing the same for a city like Boston, with narrow and windy streets that follow precolonial deer trails. What's more, since they aren't intended for the open road, golf carts can be lighter and slower than street-legal cars, and that translates into a dramatically lower barrier to entry—and reduced stakes in case of mishap.

However, the really interesting changes are what happens after people on the fringe adopt the new technology. An elderly population freed from (what is to them) the burden of driving would be given a new lease on independence. Forget about doctor's appointments made on time or the absence of stress about faltering reflexes: Think about the impact on social activity. Would new hobbies develop? Would volunteering or even paid work increase? Perhaps the over-65 set would find themselves attending night clubs—or maybe "afternoon clubs"—that would bring together a wider variety of retirees in a time in life when company and companionship matters the most.

We won't know until the technology reaches them. But I suspect the impact of autonomous vehicles on the lives of elderly people will be profound.

REIMAGINING THE SUPPLY CHAIN

Vehicles carry more than people—the other passengers are the things in the international supply chain that can stretch from a factory in Vietnam or a farm in Chile to your front door. But increasingly, semitrailer trucks do more than simply carry goods from point A to point B.

I learned that lesson while I was in the back of a minivan on the A6 autobahn racing from Stuttgart and Frankfurt. I didn't want to look at the speedometer as my driver, Anatoly, gunned and revved the minivan from lane to lane like something out of James Bond movie, so instead I focused on the seemingly endless stream of long-haul trucks that shared the road with us.

In a rare moment of calm as we slowed down for some construction, I asked Anatoly why there were so many trucks on the highway.

"People don't warehouse anymore," Anatoly replied, taking his eyes off the road to glance back at me. (Why do I ask my drivers so many questions?) "Back a decade ago, all the big companies had warehouses where they stored goods. Then they would deliver them from storage when people placed an order. But today nobody does that. Everything is just-in-time delivery. Most of what is on this road is not people—it's things, it's stuff. Stuff is going for a ride on the autobahn."

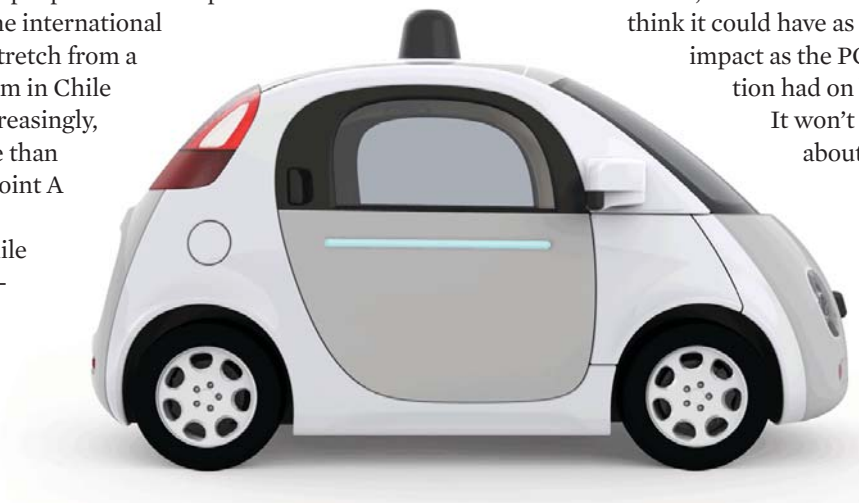
He shook his head as we hit a bump. "It's very hard on the roads and bridges."

Highways are the new warehouses, but within the limits placed by human labor. After all, a giant warehouse can be staffed by a handful of workers, but each 40-foot container on the back of a tractor-trailer has a human driver.

Or to put it in the frame of a futurist, overland cargo is a fringe use of human-driven vehicles. And self-driving delivery is a disruption that could have all sorts of advantages.

In an age of autonomous vehicles, smart cities and roads, intelligent logistics, and artificial intelligence, the human-imposed limit on the number of hours a day a shipment can stay on the road disappears. We can automate, iterate, and designate exactly where we want our stuff and how to get it there. Goods may never have to leave the road—or sea lanes or air routes—from the factory gate to the front porch.

"Autonomous transport of goods will allow us to completely reimagine the future of the global supply chain," Abe Ashkenazi, the CEO of APICS, a global supply chain trade association, told me recently. "We think it could have as much impact as the PC revolution had on business. It won't be just about moving



Google's self-driving car is a street-legal vehicle. But autonomous golf carts might be more practical.

This truck didn't need a driver for its 120-mile beer delivery in October 2016.

things from point A to point B. The whole system will change." In response, the vehicles will change, too.

The necessity of putting a driver in the front with a view of the road has restricted the design of passenger cars and freight-carrying trucks. But autonomous delivery vehicles won't be subject to that constraint. A self-driving vehicle constructed to deliver a week's groceries or an IKEA sofa won't have to look like the common delivery van—or each other, either.

There's evidence today for what our tomorrow might look like. Just Eat is a company in the United Kingdom that receives takeout orders via an app and sends the food to the customer using a delivery droid. It's essentially an autonomous vehicle, but it doesn't look or act anything like a car. The six-wheeled hauler is more like a large insulated picnic basket, with a hissing on-board air-conditioning unit. The machine is so unassuming that after a few days of rolling along the sidewalks of London, local residents stopped giving it a second thought.

RECLAIMING THE INFRASTRUCTURE

Like the Just Eat droid, future autonomous cargo vehicles not only will shed their human drivers, but even the form factor of being trucks. Acting as both transport and storage, they will be efficiently designed for the single-minded purpose of getting goods into the hands of consumers as directly as possible.

But the roads—suffer the roads. It will be a brave new world for our roads, quite a dystopian future of wear and tear that was never imagined by the engineers who designed them half a century ago. The effect on our infrastructure as the rolling supply chain hammers the road hasn't even begun to be addressed.

In another way, though, autonomous vehicles may also help extend the life of the built infrastructure.

Back in 2012, I was sitting on a Tempe, Ariz., bus bench with writer and futurist Bruce Sterling, who is best known for championing the cyberpunk movement of the 1980s and the ubiquitous device design trend that followed—that is, the world we are living in now. We had ducked out of the annual Emerge event at Arizona State University and were musing about autonomous cars and staring out across the desert spring landscape.

"I think the thing that I'm really excited to see is what the cars will do at night," Sterling said in his scratchy Texas accent.

"I spend a lot of time staring out of hotel room windows at night," I replied. "I travel constantly and I love watching cities at night."

Sterling's flair for science fiction narrative got excited. "You can imagine standing in your hotel room, watching all of the driverless cars moving themselves back into place for the next day. All of them empty. All of them getting ready for the next rush hour."

"It's like a front-row seat to the midnight ballet," I added, imagining the cars easing down the street, dodging each other with a dancer's ease, in no hurry, but beautifully efficient.

A midnight ballet may sound a bit strange, but if we dramatically shift the metaphor we use to think about our cars and roads, might we not begin to see new patterns and new ways to imagine these vehicles?

"It's not about cars at all," Shahar Waiser explained

to me at a recent event. Waiser is the co-founder of GetTaxi, a ride-sharing service that allows customers to order a taxi via an app or website. What has set GetTaxi apart from its competition in the 70 cities where it operates across Israel, Russia, United Kingdom, and United States is how it works not only with travelers but businesses as well.

"We are changing how corporations think about moving people and goods," Waiser said. "We are optimizing our system to have fewer cars on the road, but with increased utilization. We are trying to not only do business but also make the cities cleaner and less congested. Autonomous vehicles will only increase that."

It won't just be cars deadheading home, as Sterling suggested. Delivery runs can be made at night. Self-driving cargo pods can take the most industrial and blighted routes, leaving the parkways and stateliest streets for cars with human passengers. And the roadsides themselves will be transformed, as preprogramed cars won't be swayed by flashing neon or large signs proclaiming deep, deep discounts.

That sort of perspective shift has happened to other landscapes. Rivers and waterfronts were the industrial highways of previous centuries, but now we see them as pastoral. Perhaps, as we drive on them less, we will be more inclined to see our roads and city streets as works of architecture or public art.

To the extent that self-driving cars will be perfect-driving cars, we may reclaim the streets for strolling on or playing hopscotch.

The cultural effects of technological change are often the most surprising. It's not good or bad, it is just what's been happening as long as we have been humans.

And so, the most interesting changes that will be brought by autonomous cars will be the cultural shifts. What will happen when we have an entire generation of children who have never known a time when cars did not drive themselves. What will their children think and their children's children?

Whole infrastructures that we take for granted today as critical will recede into the distance. Try explaining to a seven-year-old that at one point the entire world's overland transportation was powered by horses.

There will be a time when stop lights and road signs recede away like so many stables and barns.

The future of autonomous cars will certainly change our lives in both dramatic and subtle ways, but the ways that will be most interesting are the things that are forgotten, the things that the next generation deem useless and frivolous. It's exactly the shedding of this baggage that will allow the next generation and their children to be unencumbered by the past.

As I said at the beginning, it's important for the engineering community to think through the scenarios of how new technology can affect the course of society. Engineers are the ones building this future, and the technology choices they make will determine the other choices the rest of us can make when using the technology. It's not enough to perfect the technology. Engineers have to be mindful of the way their technology impacts an all too imperfect world. ME

BRIAN DAVID JOHNSON is futurist in residence at the Center for Science and the Imagination at Arizona State University in Tempe and a futurist and fellow at the consultancy Frost & Sullivan.

HIGH-TECH EYES

New independence for people with visual impairments

By JOHN KOSOWATZ

J.R. RIZZO HAS KNOWN since he was a teenager that his retinas were deteriorating and he would someday be blind. So it was understandable that he became fascinated by animals with naturally poor eyesight—bats come immediately to mind, but any number of fish and mammals get around just fine in environments that seem murky at best.

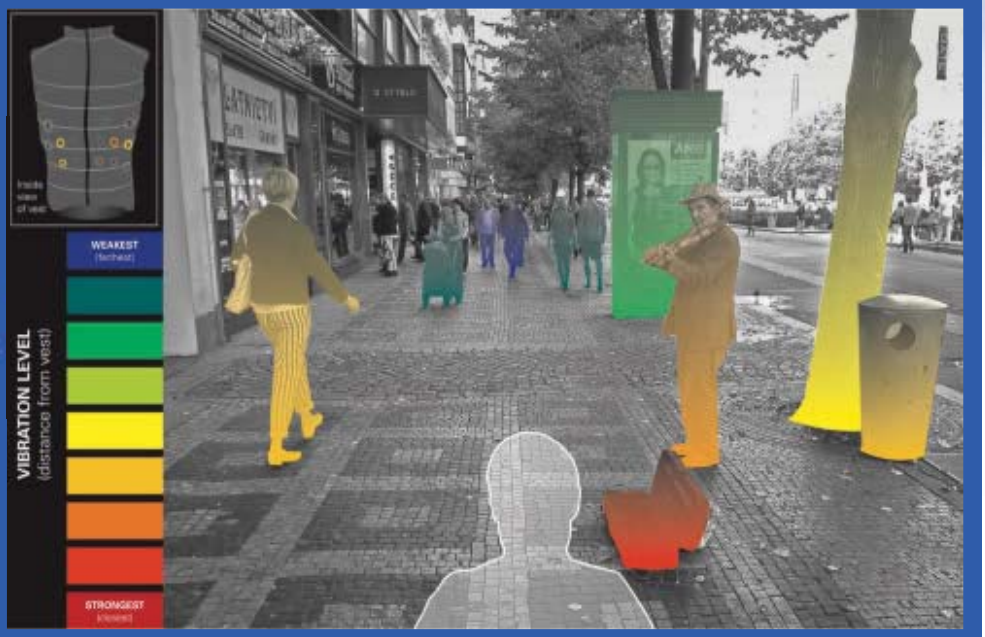
As Rizzo read up on those animals, he noticed that many had something in common. "Multisensory integration," Rizzo said, explaining that these animals relied on other senses in addition to eyesight to understand their position in the world.

"It was amazing to me, from a species standpoint, how something with very poor vision used different sensory input," Rizzo said. "Dolphins use echolocation. What could that mean for humans?"

Rizzo, who is now legally blind, is an assistant professor of rehabilitative medicine at New York University and one of a number of technologists working to answer that question. They are using high-tech sensors, visual detection software, and mobile computing power to develop new means to enable visually impaired people to navigate a world designed for—and by—sighted people.

It's a big advance. Until just recently, navigational aids for the blind and visually impaired had changed little from a white cane or a guide dog.

While those aids can provide a welcome degree of mobility, they are unable to pick up critical clues from the surroundings, such



The Eyeronman system, developed by NYU's Visuomotor Integration Laboratory and Tactile Navigation Tools, combines a sensor-laden outer garment or belt with a vest studded with vibrating actuators (left). The sensors detect objects in the immediate environment (above) and relay their locations via buzzes on the wearer's torso.

as reading a sign or detecting an onrushing object, that sighted people take for granted.

Already a number of smartphone apps help blind people perform basic tasks: identifying denominations of money or reading labels on a product package. By adapting technology developed for robots, automobiles, and other products, researchers and developers are creating wearable devices that can aid the visually impaired as they navigate through their daily routines—even identifying people and places.

"We want to give people information they can no longer see," said Yonatan Wexler, executive vice president of research and development at OrCam, a computer vision company in Jerusalem.

Point and Hear

OrCam spun off from Mobileye, an Israeli firm that pioneered advanced collision-avoidance systems for vehicles. Its cofounders, industrial engineer Ziv Aviram and computer scientist Amnon Shashua, had hoped to apply the advanced computer-vision algorithms they had developed for cars to a more personal level.

"There's a huge number of people whose sight is a problem," over 14 million in the U.S. alone, said Wexler. "What they miss is information—a lot of information that comes through the eyes."

Before Wexler and his team could apply the Mobileye technology to the challenge of vision impairment, they needed to build a platform almost from scratch. In 2010 when the company was founded, "We thought the technology was about to mature," he said. But to achieve their goal, "We had to develop the technology."

Wexler pointed out that research into teaching computers to see goes back to the 1970s, but visual perception was "still an open problem. We see innately, but you really don't realize how complex the act of seeing is."

At the time, one of the devices on the market most similar to what they were trying to produce was the IntelReader, Intel's handheld device with a camera and processor that "reads" printed material, converting it into digital text and then reading it aloud to the user. But Wexler said it was bulkier than what they were seeking

and took too long to read back the text.

"When you look at something, the brain starts reading," he said. "We wanted to read any text on any surface. There was no technology that could do that, so we started to develop our own reading capability."

It took OrCam's team of programmers, computer engineers, and hardware designers five years to develop the firm's MyEye device, which attaches to the temple of a pair of eyeglasses. The hardware features a front-facing camera and a bone conduction speaker in an arm extending toward the wearer's ear. A cable connects the device to a pocket-size computer that uses its own algorithms for computer vision and an i.MX 6Quad processor to interpret visuals and process them in real time.

The user activates the device by pointing a finger or pushing a button. The vision system scans the field of view, and if it recognizes an object or a location, the computer announces the name through the speaker.

Much like the human eye, the MyEye works best in lighted environments, but the firm claims a flashlight is adequate in darkened areas. The system comes preloaded with a set of objects it can recognize, but the user can easily add to the library by shaking the device to add an item or waving a hand to add a face or a place. The device instructs the user on how to store items in memory, including things such as credit cards and faces of friends and family.

Wexler said the team worried about privacy, so OrCam is designed specifically not to be a recording device. It does not store images, only signatures.

"It reads and tells the user what is has read, and then forgets about it," he said. "So if it is hacked, [the hacker] will not find anything to harm the customer."

Navigating by Smartphone

Kris Kitani, assistant research professor in the Robotics Institute at Carnegie Mellon University, has been watching OrCam's progress. "They are headed in the right direction," Kitani said. "You can get a lot of information from a camera."

Kitanti is part of a team at Carnegie Mellon that last year released an open-source platform to develop Navcog, a smartphone app that taps into sensors and Bluetooth beacons to enable visually impaired users to move about without traditional assistance.

For now, the app only works on the Carnegie Mellon campus, where beacons are installed throughout halls and pathways. The app analyzes data pulled from the beacon and signals the user through smartphone vibrations or voice through earbuds, but developers want to push it further.

The system, which Kitani and his team developed with help from researchers at IBM, works a bit like GPS for vehicles. But GPS has a positional accuracy of about 10 feet, which is much too coarse for pedestrians to use.

"We want to develop accurate localization, as opposed to the resolution from an automobile-based GPS system," Kitani said. "That's fine for cars. But with a blind person, you have issues like, 'What part of the sidewalk are you walking on.' "

> **"We see innately, but you really don't realize how complex the act of seeing is."**
>
> **— Yonatan Wexler, OrCam**

Developers can access cognitive assistance tools through the IBM Bluemix cloud computing service. The toolkit includes an app for navigation, a map editing tool, and localization algorithms to help blind people identify in real time where they are, as well as what direction they are facing and local environmental information. A computer-vision navigation tool can turn smartphone images of the localized environment into a 3-D space model to improve localization and navigation.

Team leader Chieko Asakawa, a visiting faculty member at Carnegie Mellon and an IBM fellow, said, "To gain further independence and help improve the quality of life, ubiquitous connectivity across indoor and outdoor environments is necessary." Asakawa is herself visually impaired.

The team is working to expand the app, aware that relying on Bluetooth beacons can be limiting. Kitani believes one key to developing the network beyond the

Carnegie Mellon campus is the eventual availability of low-cost beacons.

Looking ahead, he said the team wants to add a smartphone-based navigation system working with a camera.

> **"Ultrasound operates at the speed of sound, but you still need to wait for the chirp off of the echo."**
>
> **— J.R. Rizzo, New York University**

"One of the things about using computer vision in the wild is that the same object can look radically different at different times of the day," Kitani said. "And any kind of technology using computer vision needs a level of robustness."

Sensor Vest

Back in New York, Rizzo is developing a system that could be independent of beacons and other markers. At NYU's Visuomotor Integration Laboratory, where Rizzo is the director, and at his startup, Tactile Navigation Tools, Rizzo and his team is fitting outerwear with transmitters and sensors that detect oncoming objects along with their shape, location, and speed.

Rizzo first worked on the idea in medical school, as choroideremia began taking more of his eyesight.

He teamed up with a partner and technical advisor, who is a neuroscientist. Together, the pair worked within NYU's School of Business to develop a business plan and meet business advisors and potential investors. They recruited a range of engineering, computer, and technical experts to help in the system's development, offering equity stakes in the company to keep payroll low and direct seed money into research and development.

"The design has evolved substantially," Rizzo said. "But it is an intuitive-based system. We're creating a stable foundation for sensory schemes, and a foundation that can be modified for each individual user."

In visually impaired people, studies have shown the portion of the brain normally used to process visual information instead processes auditory information. That plasticity allows visually impaired people to train themselves to recognize objects based on sound cues. Sound waves bouncing off a wall, for instance, are perceived as distinct from those reflecting off a car, and those differences become part of an auditory library.

Rizzo's system, which he calls Eyeronman, turns that passive listening into active scanning. At present, the system consists of a vest and belt studded with ultrasound, infrared, and laser ranging sensors or lidar.

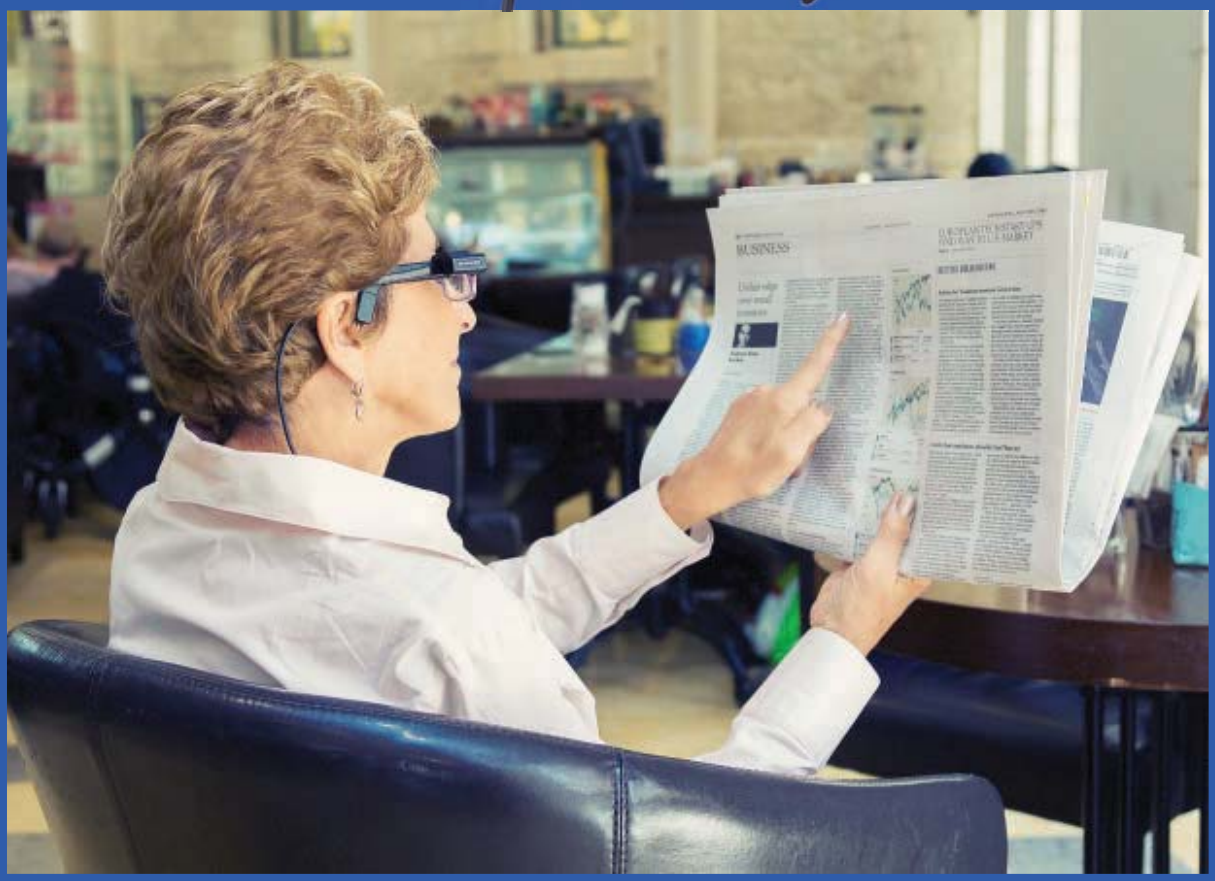
"It is sensor fusion," he said. "Using sonar, buttressed by lidar, and integrated into something meaningful."

When someone wearing the vest walks down a sidewalk, the sensors detect objects in a wide cone up to 18 feet away, and converts the data into a series of vibrations via actuators in the vest. If a dog is running toward the wearer from the left, the lower left panel of the vest will start to buzz. When the dog stops or sits, the buzzing will slow to a gentler vibration.

Right now, Eyeronman works well only if the wearer is moving slowly enough for the data to be read accurately. To get the system capable of processing data at a normal walking speed will require overcoming some technical challenges.

"Ultrasound operates at the speed of sound, but you still need to wait for the chirp off of the echo," Rizzo said. He added that his team has had to work to minimize crosstalk and outside noise from sensors.

Still, "When people put this vest on, nothing is average," he said. "You turn the system on and have people walk an obstacle course, and people understand. They pick this up almost instantly. You can now walk in one direction and put your torso in another direction" and recognize objects.



The MyEye system developed at OrCam identifies objects or text for the user. The camera attached to the temple of the glasses frame (top) scans the field of view. When the wearer points at an object or block of text, the image is sent via a connecting cable to a pocket-size computer, which processes the image and relays its contents by speech through a speaker at the wearer's ear.

Rizzo calls the system a "game changer" and hopes to start commercial production sometime in 2018.

The system also has applications beyond the visually impaired.

"If we create an omnidimensional spatial perception, it has application to a number of vertical markets," Rizzo said. The system could be mounted on fire-retardant clothing for use by fire departments. Police or military units could use a version incorporated into bullet-proof vests.

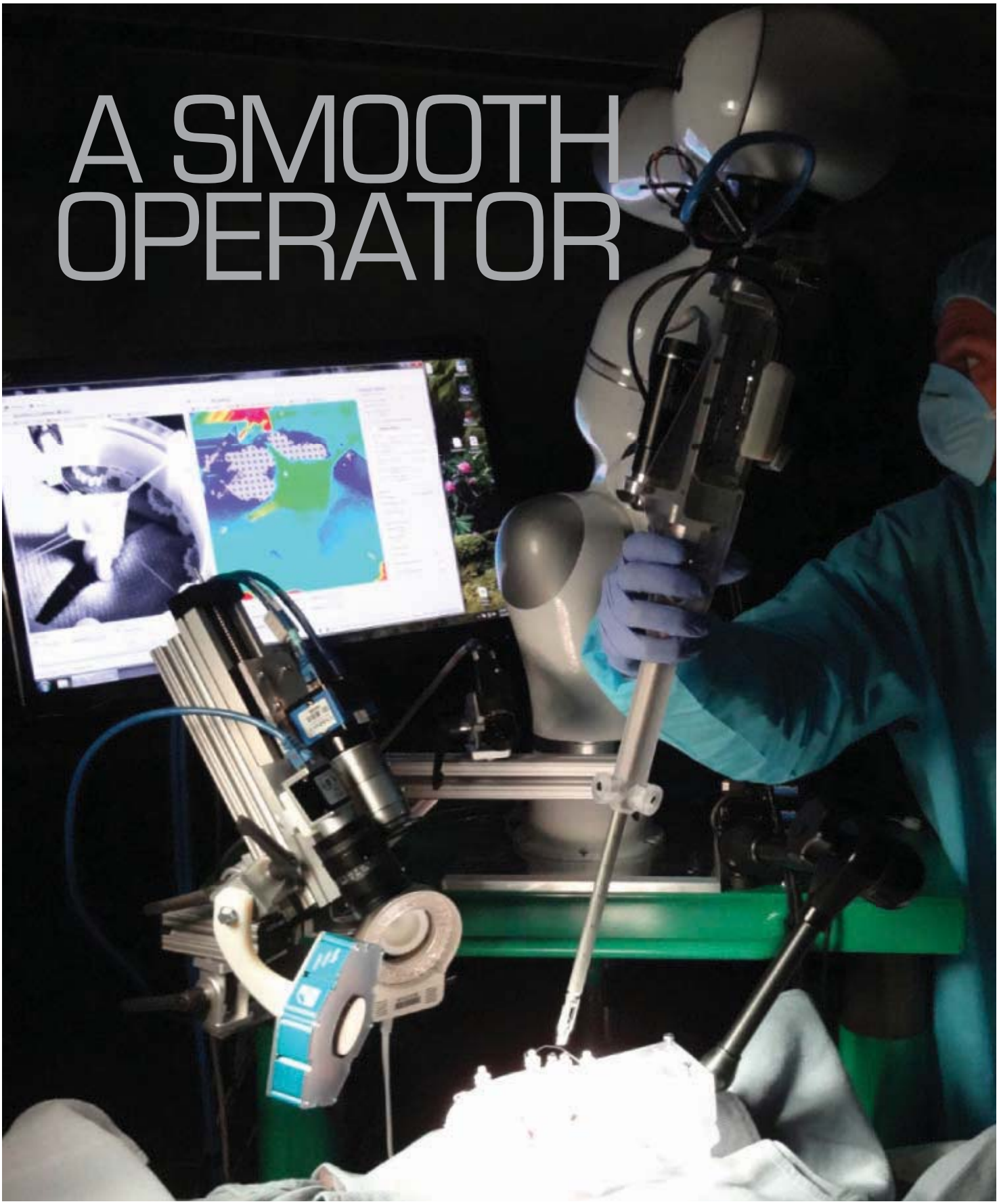
For now, the system needs to be on the outermost article of clothing, but Rizzo said eventually it could be worn as a discreet harness. "An external shell just makes sense right now," he said.

Rizzo is also thinking of more data streams that could be delivered to users via his vest. Cloud-based software, for instance, could deliver voice messages through a 4G, Wi-Fi multi-modal system.

That would be a development to bring technology for the visually impaired squarely into the 21st century. **ME**

JOHN KOSOWATZ is senior editor at ASME.org.

A SMOOTH OPERATOR



A new surgical robot could transform soft-tissue surgery.

ALAN S. BROWN

The surgeons and nurses filed into an operating room at the Children's National Medical Center in Washington, D.C. Led by associate chief surgeon Peter Kim, they quickly put the patient, a pig, under anesthesia and prepared to operate. Scalpels gleamed in the bright lights. Yet the suturing needles to sew the patient back up were nowhere in sight. Instead, a robotic arm with a long shaft hovered over the patient. The Smart Tissue Autonomous Robot, or STAR, would be doing the sewing today.

You can think of it as driverless surgery.

STAR is Kim's vision of the future of surgery. Surgeons, he argues, vary greatly in training, dexterity, experience, and decision-making. This is the reason why 30 percent of the world's 232 million soft tissue surgeries result in complications. By embedding the knowledge of the best surgeons in digital systems, autonomous and semiautonomous robots could deliver universal access to the best surgical techniques.

In addition to his surgical duties, Kim is also vice president of the hospital's Sheikh Zayed Institute for Pediatric Surgical Innovation. He guides what the medical field calls "translational research," applying new science to improve human health. To make his vision a reality, Kim recruited a team of engineers to build a robot that could perform soft tissue surgery.

After years of testing on plastic pads and dead tissues, STAR was ready for prime time. And today it would try to prove that it could, at least by some measures, do a better job of stitching those severed tissues together than experienced surgeons.

To make his case, Kim chose a complex surgery called circular anastomosis. It involved stitching together two severed ends of an intestine. To heal properly, every one of the sutures had to be perfect. Make them too far apart or too loose and they will bleed. Tie them too closely or too tightly and they will strangle and kill the tissue.

Because the anatomy of a pig resembles that of human beings, surgeons are comfortable working with them. The doctors rapidly severed the pig's intestines, extended them through a cloth covering, and stretched them open for

The STAR robot forms sutures by using a moveable head to shoot a curved needle through tissue.
Credit: Children's National Medical Center

easy access.

Then STAR went to work. Its U-shaped stitching head pushed a curved needle through adjacent intestinal walls and tied off the knot. Then it went on to the next.

Robots in the surgical suite are nothing new. The best known of them, Intuitive Surgical's da Vinci, is more than 15 years old and has performed 2 million operations worldwide. Its multiple hand-like effectors, which look like a prop from the movie "Alien" and require a team of surgeons to operate, act as extensions of the surgeons' hands. They can perform incredibly precise maneuvers, but humans make every decision and control every move.

Autonomous robots are smarter, and they are beginning to edge their way into the operating room. These robots are savvy helpers. They locate and machine bone for hip and knee implants, make the slices in Lasik vision surgery, target radiation at tumors, and provide guidance during back surgery. They rarely, if ever, operate independently. They work exclusively with solid objects, such as bones or eyes, which remain stationary during surgery.

In contrast, soft tissues vary in shape, size, and location from patient to patient, and they are, by definition, pliant. Stitch them together and each stitch will alter their shape. Sometimes, the sewn seams cover the previous stitch or hide the location of the next stitch. Other times, leaking blood obscures the tissue.

While all surgeons have excellent hand-eye coordination, their most important skill is making good decisions while navigating this complex and changing environment. An autonomous robot must not only manipulate a needle and thread, but follow—and react to—the shifting shapes that it creates in real time.

This is the Grand Prix, the Super Bowl, and the World Cup of surgical robot challenges all rolled into one. An autonomous robot that masters these challenges would change the game.

"Just imagine having the best technology and technique available any time and any place for any surgeon and for any patient," Kim said. "Having these intelligent systems working with surgeons will ultimately decrease complications and save lives."

STITCHING

Kim pitched those benefits to recruit Alex Krieger, who led the STAR engineering team. The German-educated mechanical engineer came to the United States to automate a Bosch AG automotive facility, but was drawn to bioengineering while earning his Ph.D. at Johns Hopkins. There, he was part of a team that developed a nonmetallic robot that could work within the high magnetic fields of an MRI machine. They went on to found a company that was acquired and commercialized the technology. After five years of corporate life, he was ready for a new challenge.

Despite his experience in medical robotics, Krieger was unprepared for soft-tissue surgery: "It was so bloody, and there were flaps of tissue obscuring everything. It was a mess, and so difficult to see what was going on or where the next stitch would go."

Yet Krieger knew how to attack it. "As an engineer, you try to break difficult tasks down to small, manageable pieces."

Before he could build a robot, he needed to learn how surgeons went about their business. Fortunately, he worked in a hospital filled with some of the nation's top pediatric surgeons. He asked question after question: What was a surgical plan? How did they prepare the surgical area? Did they move right to left or left to right? Did they stitch outside-in or inside-out? How did they manage corners? Robots, even autonomous ones, do not improvise, so Krieger needed an answer to each question to program the robot effectively.

Some questions were harder to answer than others. Sutures vary with type, spacing, and tension, depending on the organ or tissue. Surgeons study some rules of thumb, but they also learn to recognize when a stitch feels right. Since surgeons don't take precise measurements of tension, Krieger could not find hard data for his robots. Fortunately, his wife, an optometrist, remembered a reference on eye surgery that contained the force tables he needed.

Surgeons also linearize circular tissues like intestines, tying them to the abdominal wall to form the straight, easy-to-stitch straight lines of a triangle. It also keeps the rest of the tissue away from the work surface. The STAR team replicated this by placing a ring over the patient. Once they elevated the intestines out of the abdomen so the robot could see them more clearly, they tied them onto the ring.

Then Krieger tackled suturing. It involved looping thread, pushing a curved needle through tissue, and knotting lines of stitches. Autonomous robots find this challenging and rarely get even half the stitches right.

Krieger needed a simpler method. He considered surgical glue, staples, and tape. Ultimately, he settled on the Endo360°, a suturing tool developed for laparoscopic, or minimally invasive, surgery. With its pistol grip, trigger, and long, thin shaft, it looked like the wand of a power washer—with levers, knobs, and cables to orient the moveable head. Once in position, the surgeon flicks a switch and the head shoots a surgical needle through folds of skin to make the stitch.

"It works like a nail gun," said Simon Leonard, a Johns Hopkins University computer scientist who worked on the project. "We just aim and shoot. We don't need to build a robot with the dexterity to move a needle to right place and push it through."

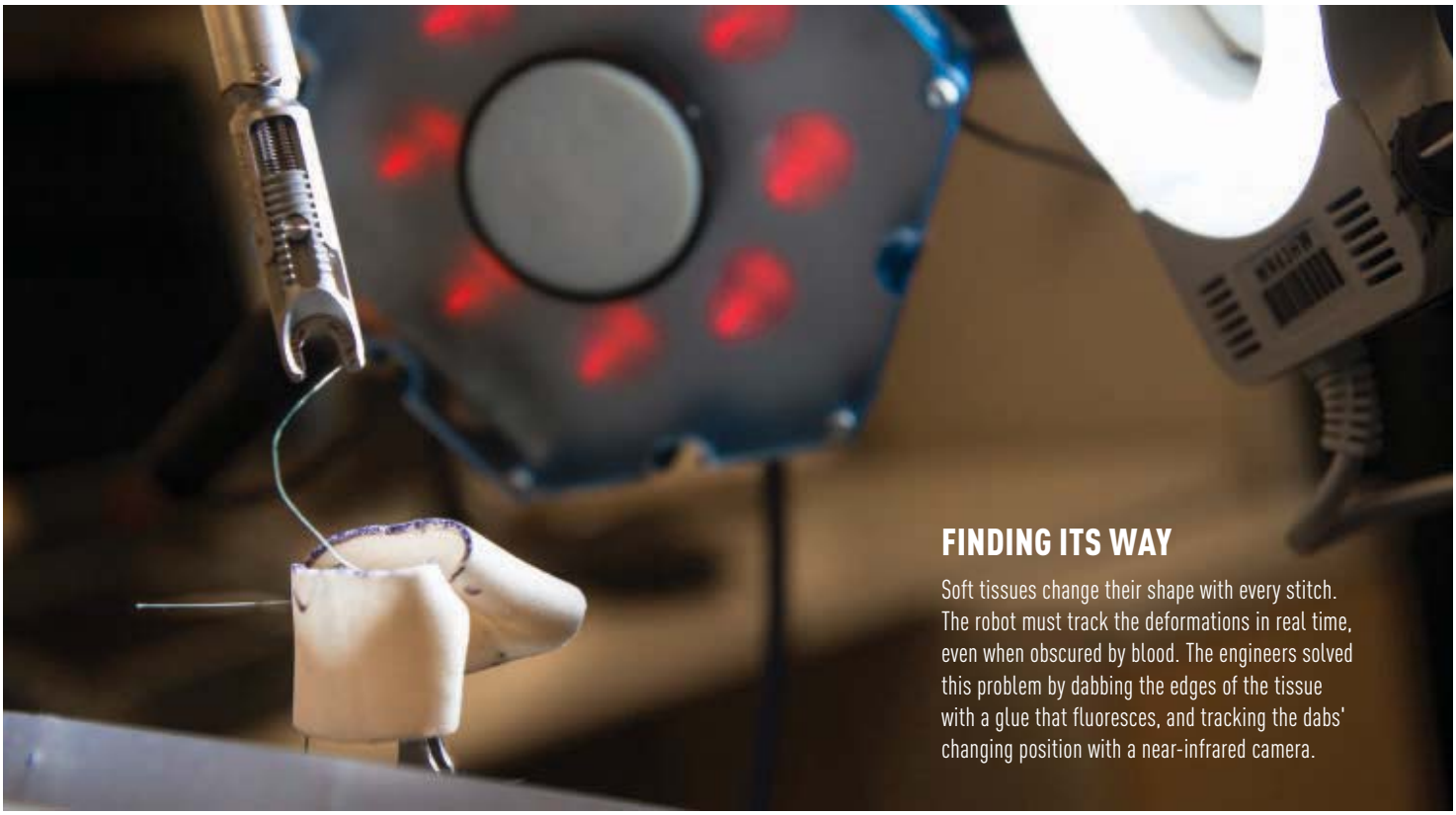
The engineers replaced the Endo360° manual controls with motorized devices and attached it to a human-safe robot from Germany's KUKA. They spent weeks straightening and calibrating the tool, since its length magnified every imperfection.

> This is the Grand Prix, the Super Bowl, and the World Cup of surgical robot challenges all rolled into one.

STAR also needed eyes that could resolve locations in three dimensions and follow blood-soaked tissue as it changed during surgery. The team opted for two separate cameras and a clever trick.

The first was a plenoptic camera, which uses an array of small microlenses that work like a bug's eye. Each microlens sees the image from a slightly different angle. Computer algorithms reconstruct those vantage points into a single 3-D image. The camera has a wider focus than a single lens and it is compact enough to hover above an operating table. Even then, it took months to calibrate the camera to the millimeter accuracy needed to control the long Endo360°.

Still, the camera was not fast enough to track tissue deformation accurately in real time. The



FINDING ITS WAY

Soft tissues change their shape with every stitch. The robot must track the deformations in real time, even when obscured by blood. The engineers solved this problem by dabbing the edges of the tissue with a glue that fluoresces, and tracking the dabs' changing position with a near-infrared camera.

Photo: Children's National Medical Center

engineers finessed the problem. They dabbed drops of an FDA-approved fluorescent glue onto the edges of the tissues. When illuminated, it fluoresced brightly in the near-infrared range, even when covered with blood or other tissues.

A near-infrared camera imaged the dabs, and a computer drew imaginary lines between them. Instead of trying to track the deformation of the tissue, the computer followed the dots and changes in the imaginary lines. It could do this in real time with capacity to spare.

"That was key to solving the problem of tissue recognition and tracking," Krieger said.

Yet neither the plenoptic nor the NIR camera were accurate enough to determine the depth of a stitch. The STAR team solved that by mounting a force sensor between the jaws of the Endo360°'s stitching head. The sensor told STAR when the head was at the right depth, and provided the feedback needed to slide along tissue and into the difficult-to-suture corners.

At that point, STAR was ready to start sewing.

SURGERY

STAR started its surgical career by working on rubbery pads with small protrusions. Surgeons use them to learn to stitch together wounds or tissues.

"Since the protrusions are all one height, it simplified the problem," Krieger said. "There was no blood, no crazy deformations. We could begin testing before we finalized the vision system."

To prove the robot could adapt to unexpected patient movements during an operation, the engineers shifted the pads randomly during testing. STAR successfully tracked the location of its target and repositioned its arm to make the stitch.

The experiments showed that STAR had the potential to complete one stitch every seven seconds on patients—faster and more consistently than humans, Krieger said.

The engineers had thought STAR would do as well on animal cadaver tissue—until their tools broke. "We didn't have the right cleaning procedure," Krieger said. "The tool tip gunked up and the cables controlling the head broke because we were putting too much force on them."

Up and running again, their sutures began pulling out. Cadaver tissue, it turned out, was not as consistent as the practice pads. Some tissues were thick, others fatty, and others thin and flimsy. Over time, the team learned to optimize its stitching for different types of tissues.

Live tissue proved more resilient and durable than cadaver tissue and easier to work with. The force sensor enabled the team to make perfect stitches along the intestinal flaps. The cam-

eras positioned the Endo360º accurately and tracked each twist and turn as it stitched.

STAR worked exactly as the team envisioned, though it did need some human help. Surgeons sliced the intestine and prepared it for surgery. They double-checked each stitch's location and helped manipulate the thread. But Kim estimates that 60 percent of the operation was fully autonomous, and described these interventions as "minor adjustments." He likened them to holding an infant's hand while it is learning to walk, and said STAR could have done all the stitching autonomously.

Either way, STAR more than lived up to Kim's high standards. It outscored surgeons with seven years training on stitch location and stitch tension. Such consistency is important, because a surgeon who makes only one imperfect stitch out of 20 has failed his or her patient.

STAR's only drawback was time. It took nearly an hour to complete the surgery. This was simply a matter of making sure each stitch was perfect, Leonard said: "This had never been tried on real-life animal, and we played it very safe." At full speed, he added, the robot could have stitched five to 10 times faster than a human.

"We were able to show the potential for robots to do significantly better than a human surgeon," Krieger said. He argues that automating stitching after surgery leaves surgeons with more time for higher-value tasks. Krieger wants to begin using the robot clinically and to expand its repertoire to include hysterectomies and stomach operations.

Engineers prepare for surgery. The ring-like device elevates the intestines and secures it to form easy-to-stitch triangular lines.
Photo: Children's National Medical Center

The team plans to integrate additional sensors onto their robot to give surgeons better surgical information. Using a combination of force sensors and sophisticated multispectral cameras that see more than visible light, future robots might advise surgeons about tissue health, thickness, strength, and blood circulation. This would quantify knowledge that surgeons now learn only through experience.

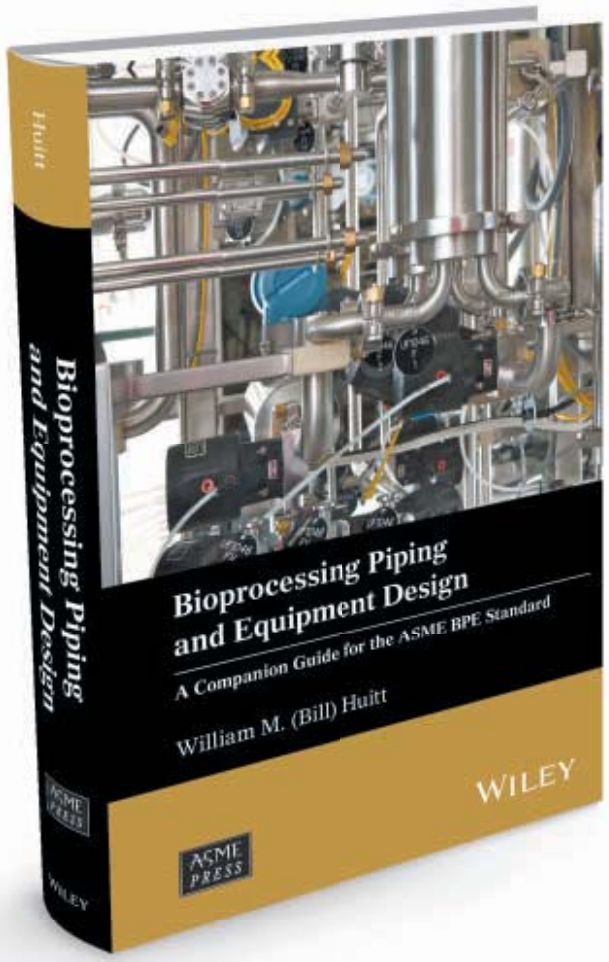
STAR will help the team explore better ways for surgeons to collaborate with machines to provide safer and more consistent outcomes than either could alone, said Ryan Decker, a senior engineer on the team. Humans, he explained, are very good at segmenting objects, such as identifying the edge of a severed colon that has changed shape and is obscured by blood. They also excel at identifying new features in an environment, and generating hypotheses about the world around them.

Robots are a long way from emulating those intellectual skills, but they surpass humans in their ability to do precise work quickly and repeatably. For highly defined tasks, like measuring the distance between stitches or the force on a knot, robots leave humans in the dust.

"Our goal is to create a framework for human-machine collaboration that achieves something better than the sum of those parts," Decker said.

STAR is only the start. **ME**

ALAN S. BROWN is associate editor at *Mechanical Engineering* magazine.



FEATURED

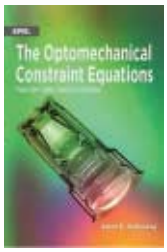
BIOPROCESSING PIPING AND EQUIPMENT DESIGN: A COMPANION GUIDE FOR THE ASME BPE STANDARD

WILLIAM M. (BILL) HUITT

ASME Press Book, Two Park Ave., New York, NY 10016. 2016.

This companion guide to the ASME Bioprocessing Piping and Equipment (BPE) Standard is co-published with John Wiley & Sons, the well-known commercial publishing house. Huitt draws on many years' of experience and insights from first-hand involvement in the field of industrial piping design, engineering, construction, and management, which includes the bioprocessing industry. His goal is to explain why dimensions and tolerances, process instrumentation, and material selection play such an integral part in the manufacture of components and instrumentation. Also, Huitt recognizes that a standard provides a set of requirements, but not the logic underlying it. "This book is meant to close that gap of ambiguity to a large degree," Huitt wrote, "and make clear not only the standard itself but also its intent."

544 PAGES. $130; ASME MEMBERS, $104. ISBN: 978-1-1192-8423-9

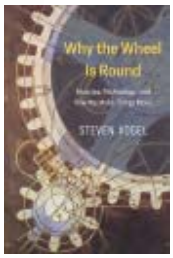


THE OPTOMECHANICAL CONSTRAINT EQUATIONS: THEORY AND APPLICATIONS

Alson E. Hatheway
SPIE Press, P.O. Box 10, Bellingham, WA 98227-0010. 2016.

Optical instruments are increasingly electronic—just try buying a film camera—but they are all still designed and manufactured with the input of mechanical engineers, who may not always be familiar with the fundamental equations of optics and how to apply them to physical systems. Hatheway's book is intended to enable engineers to manage the mechanical design process. He starts with a comprehensible primer on basic optics and develops that to the optomechanical constraint equations: "Seven equations that control the position, orientation, and size of images in both simple and complex optical systems." The book concludes with example applications of these equations to real-world design, analysis, and manufacturing problems.

140 PAGES. $55. ISBN: 978-1-5106-0175-8



WHY THE WHEEL IS ROUND

Steven Vogel
University of Chicago Press, 1427 E. 60th Street, Chicago, IL 60637. 2016.

The wheel is a foundational invention, but it didn't match up well with the linear power sources of the ancient world—or many of the modern ones. Vogel, a professor emeritus of biology at Duke, provides a lucid but comprehensive account of the ingenious ways engineers throughout history have harnessed linear power, such as human muscles and draft animals, to rotating mechanisms. It's hard to come away from his account without being impressed by human ingenuity. Vogel even provides diagrams and instructions for making models of some of the inventions he investigates, from a motorized potter's wheel to a tabletop ballista he claims is suitable for beaning sleeping students with ping pong balls.

344 PAGES. $35. ISBN: 978-0-2263-8103-9

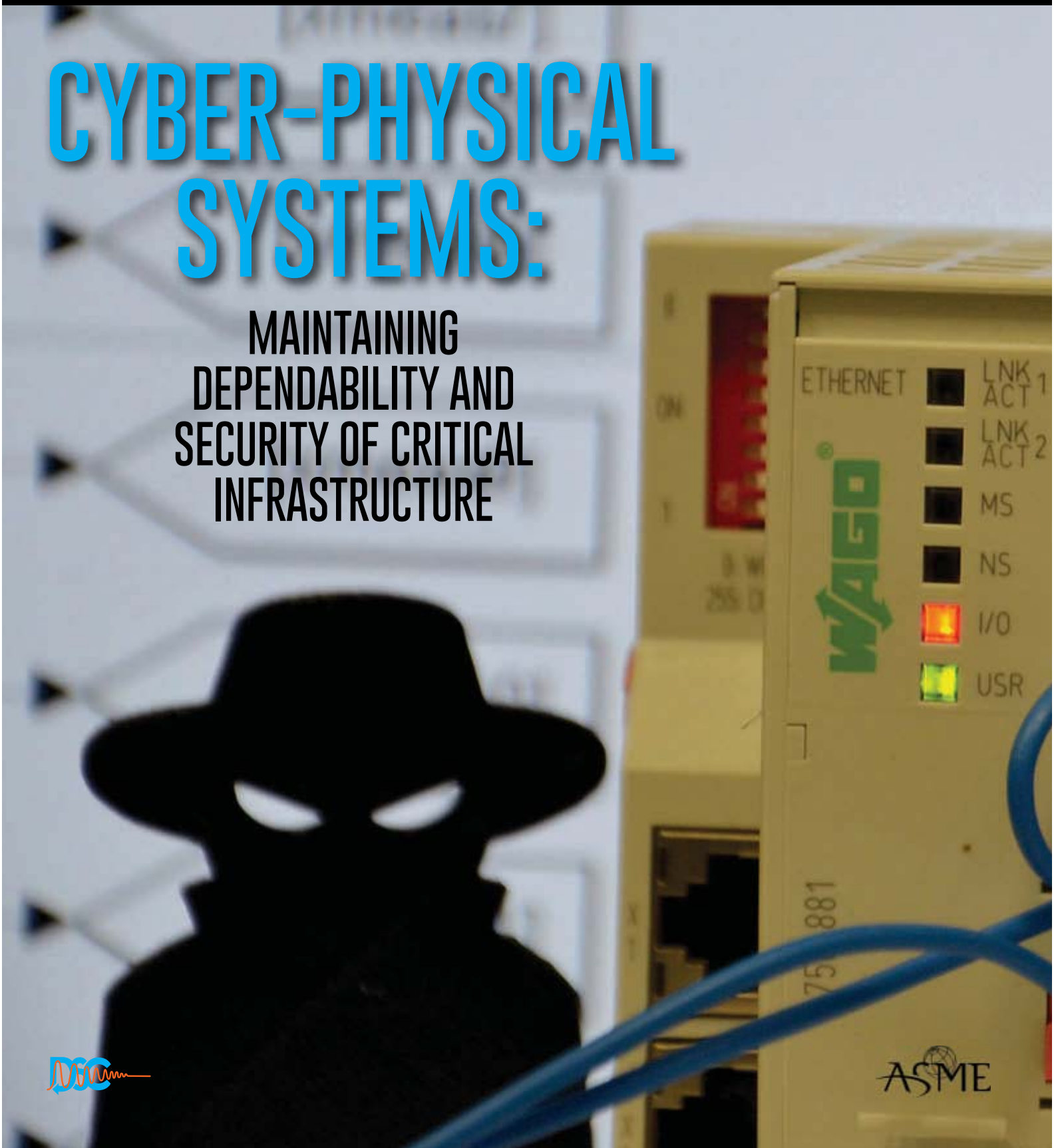
A forum for emerging systems and control technologies.

DYNAMIC SYSTEMS & CONTROL

MARCH 2017 VOL. 5 NO. 1

CYBER-PHYSICAL SYSTEMS:

MAINTAINING DEPENDABILITY AND SECURITY OF CRITICAL INFRASTRUCTURE



Cyber-physical Systems

Since the advent of ARPANET and Modicon's Modbus, industrial plants found in military and civilian applications have benefitted greatly by the synergy of computers, communications, and control systems. Norbert Wiener's earlier vision of "cybernetics," at least as it pertained to machines, has borne fruit. From electricity distribution to water management to specialized shipboard plants and automotive systems, higher levels of efficiency and performance have been reached by the adoption of technology and methodology developed for Cyber-Physical Systems (CPS). Given society's growing reliance on CPS, the current issue turns its light on the intrinsic vulnerabilities of these impactful (often, critical) systems.

In the first article, following a comprehensive introduction to CPS, Ed Zivi presents the product of his pioneering effort in developing an undergraduate course in the field. While it imparts the fundamentals, the curriculum is flexible enough to adapt to the demands of an ever-changing technological environment. The second article, by Brian Connett and Bryan O'Halloran, discusses the need for a framework and architecture that allow the system defenses to access maximum information, optimized to the characteristics of a cyberattack. Attributes of a detected anomaly include timing, medium, intention, and value. The authors take the System of Systems approach to model any "cyber conflict" and to enable the most effective defensive posture against anomalies across the network of communication nodes. In the third article, Anastasis Keliris and Michail Maniatakos consider cyberattacks as an emerging threat for Industrial Control Systems (ICS). It is typical for contemporary ICS components to utilize Commercial-Off-The-Shelf hardware and software, rendering them prone to vulnerabilities and exploitation techniques that afflict IT systems. The authors analyze the design process of an Advanced Persistent Threat for ICS and, consequently, gain an understanding of the methodologies, resources, and tools available to "black hat" actors. Then, using such information, defenders can identify weak points and more efficiently protect the ICS against cyber-attacks. The authors of the fourth article, Brien Croteau and Deepak Krishnankutty, summarize work produced in the Eclipse Research Cluster on cyber-physical domain attacks that may occur at multiple levels of the system's hierarchy. Demonstrated solutions leverage the physical constraints of the plant and expand to non-traditional inputs and measurements providing heterogeneous surfaces that are more resilient to typical cyberattacks. The article covers one approach based on IC-level side-channel power monitoring and another using add-on trusted sensors for automotive systems.

We greatly appreciate the authors whose hard work and dedication to their fields have contributed the content for this issue of the *Dynamic Systems and Control* magazine.

If you have any ideas for future issues of this magazine, please contact the Editor, Peter Meckl **(meckl@purdue.edu)**.

Kiriakos Kiriakidis, Ph.D.
Levi DeVries, Ph.D.
Guest Editors, *DSC Magazine*

COVER IMAGE: MOMA LAB @ NYU ABU DHABI

TEACHING CYBER-PHYSICAL SYSTEMS

BY EDWIN ZIVI
PROFESSOR OF SYSTEMS ENGINEERING, UNITED STATES NAVAL ACADEMY

In response to ever-present cyber threats, the U. S. Naval Academy thrust in cyber security studies includes a new major, Cyber Sciences, and construction of a new facility, Hopper Hall, to house the assembled multi-disciplinary teaching and research team. An essential component of this initiative is Cyber-Physical Systems (CPS) dependability and security of critical infrastructure and mission-critical systems. To address this need, a new senior-level engineering undergraduate technical elective has been offered and evolved over the past five years. Key concepts, design, content and teaching experiences are presented herein. Targeted primarily to Systems Engineering majors, this course builds on a foundation of linear control system design and embedded computer hardware / software integration to explore fundamental CPS concepts, attributes and risks. The course contains three primary themes: (1) fundamentals including the evolution of CPS including shipboard engineering plants, (2) a simulation-based case study of the dynamic interdependencies associated with cyber intrusions into a vinyl acetate industrial plant control challenge problem and (3) hands-on Controller Area Network (CAN) and CANopen real-time embedded control networks. The long-term objective is to provide an integrative teaching, learning and research environment for multidisciplinary advances targeting unification of key CPS enabling technologies including: (1) control theory, (2) computer science (3), communications, (4) embedded systems and (5) cyber security. The discussion commences with an introduction to CPS concepts and a survey of CPS research needs.

INTRODUCTION TO CYBER-PHYSICAL SYSTEMS

As defined by the National Science Foundation, "*Cyber-physical systems (CPS) are engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components*" [1]. The President's Council of Advisors on Science and Technology assesses that cyber-physical systems "*are now a national priority for Federal R&D. Improved methods are needed for the efficient development of these systems. These methods must assure high levels of reliability, safety, security, and usability*" [2]. CPS "scientific and technological importance as well as its potential impact on grand challenges in a number of sectors critical to U.S. security and competitiveness" [3] has been established along with strategic challenges and driving sectors including: (1) Defense, (2) Energy, (3) Transportation, (4) Manufacturing, (5) Buildings and Infrastructure, and (6) Healthcare. Potentially catastrophic failures of highly vulnerable national infrastructure such as the terrestrial power grid [4] and mission systems could have disastrous consequences.

The Editorial of the Editor in Chief of IEEE Transactions on Automatic Control special issue on CPS states that "*The control of Cyber-Physical Systems presents enormous challenges and requires approaches drawn from Systems and Control, such as those in traditional control, hybrid control systems, discrete event systems, networked control, and also approaches drawn from Computer Science, such as abstraction and verification, Networks, and many other areas depending on the applications of interest. The large scale and heterogeneity of components in CPS introduce grand research challenges. Robustness, resilience, reliability, safety and security issues for changing and reconfiguring dynamical systems must be addressed and these are novel research areas of great importance. The integration of different technologies and scientific*

domains presents new and challenging fundamental problems underlying the theoretical foundations for this class of systems" [5].

CYBER-PHYSICAL SYSTEMS RESEARCH NEEDS

The Networking and Information Technology Research and Development (NITRD) program identifies the following research needs: "*A new systems science is needed to provide unified foundations, models and tools, system capabilities, and architectures that enable innovation in highly dependable cyber-enabled engineered and natural systems. Better understanding of system complexity is also necessary in this research area to aid in improved management and decision support. Specific technical areas for emphasis include:*

- *Unifying foundations for modeling, predicting, and controlling systems that exhibit combined cyber (logical/discrete/digital) and physical (continuous/analog) system behaviors*
- *New approaches for supervisory control of systems that must interact on an ad hoc basis*
- *Scientific and engineering principles, metrics, and standards that integrate the disciplines of real-time embedded systems, control, communications/networking, security, and human-machine interaction*
- *Technology to close the design and productivity gap between modeling, programming, and runtime execution of cyber-physical systems*
- *Principles for reasoning about and actively managing properties of complex, multiscale, real-time cyber-physical system interactions, including safety, security, reliability, and performance*
- *Design methods and systems technology for autonomy, human interaction, and management of control authority*
- *Open systems approaches for composition, integration, and coordination of cyber-physical Systems*" [6].

At the heart of this effort is the search for effective and efficient mathematical formulations, methods and tools that bridge the semantic and temporal gaps between physical and cyber systems [7]. More specifically, time is an essential attribute of the physics-based differential equation modeling and control synthesis of dynamic systems wherein time is critical to the correctness of the solution. However, in computer science and communications, discrete mathematic formalisms such as finite state machines predominate wherein time is typically treated as a measure of responsiveness and is rarely associated with correctness. Embedded systems represent the preliminary fusion of control theory and computer engineering wherein invariant time steps and bounded latencies enable the application of digital control theory [8]. The emergence of CPS systems composed of complex computer architectures, operating systems, middle-ware, communications networks and protocols and cyber intrusions require new hybrid continuous-time and discrete-event-driven mathematical formalisms [9], [10]. The final essential ingredient is the incorporation of cyber security into CPS design, analysis, and implementation and maintenance considerations including: (1) threat modeling, (2) vulnerability analysis and (3) life cycle cyber security risk management [11], [12] . The key differences in Information Technology (IT) and CPS security are highlighted by the **Figure 1** comparison of key attributes [13].

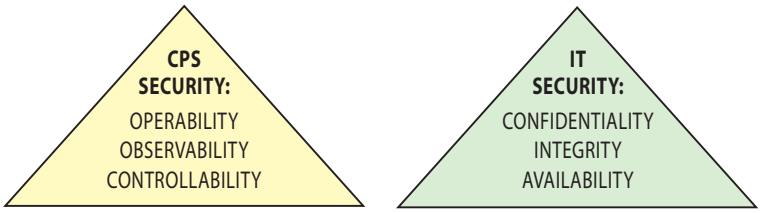


FIGURE 1 **Comparison of IT and CPS Security Attributes.**

Operability quantifies the ability to operate throughout specific scenarios including disruptive events. Observability and controllability can be defined from two perspectives:

1. Using linear control theory [14]
2. The aspiration of continuous situational awareness and control authority.

CYBER-PHYSICAL COURSE OBJECTIVES

The course is designed for a student population that is primarily composed of multi-disciplinary Systems Engineering majors who have taken:

- A first year cyber security course
- Second year C/C++ embedded computer hardware software integration and mechatronics courses
- Third year courses in linear system analysis, modeling and control design including embedded hardware-in-the-loop experiments
- Third year courses in electrical engineering and applications of cyber engineering.

Primary CPS learning objectives are:

- Characterize their essential role in critical infrastructure and mission-critical systems
- Characterize system and network vulnerabilities, resilience, and behavior under disruptive conditions
- Investigate Supervisory Control and Data Acquisition (SCADA) systems and vulnerabilities
- Analyze dynamic interdependence and performance of CPS feedback control systems stability and performance
- Analyze, instrument and quantify performance of Controller Area Network (CAN) based systems including CANopen application layer systems integration and device profiles.

Part 1–Cyber-Physical Fundamentals

The course fundamentals begin with an assignment to extract key observations from the Peabody award-winning [15] 60 Minutes "Sabotaging the System" investigation [16] followed by a literature search to determine the defining attributes of Cyber-Physical Systems. Arguably, the best short answer comes from the NSF, which coined the phrase: "Cyber-physical systems (CPS) are engineered systems that are built from and depend upon the synergy of computational and physical components" [17] among a variety of opinions. Perhaps the most notable variations center on whether the inclusion of networks is an essential or merely pervasive ingredient [18]. An early laboratory small group exercise has students reallocate engineering and damage

control responsibilities for conventional naval vessels under condition 1 "battle stations" to achieve the in-transition Navy crew size reductions of approximately 50%. The central focus of this exercise is to determine the necessary attributes of CPSs which are subjected to temporal and spatial bursts of disruptive events. These attributes lead to the following definitions:

- **Reliability:** Duration or Probability of failure-free performance, Mean Time to Failure (MTBF) (MIL-STD-721C)
- **Availability:** Probability a system is operable and committable for a specific mission (MIL- STD-721C)
- **Dependability:** Ability to operate throughout a distribution of likely disruptive scenarios. In response to an ONR control challenge problem[19] design-oriented metrics for operability and dependability have been formulated and applied to early trade space design studies for resilient systems [20], [21].

A central challenge to deploying resilient CPSs involves the appreciation for the multi-disciplinary challenges and the lack of a unified framework for CPS analysis, design and implementation [22]. At this point, students embark on a two-day in-class exercise to learn from Prof. Edward Lee's excellent recorded presentation: "*Cyber-Physical Systems: A Rehash or A New Intellectual Challenge?*" [23]. Prof. Lee clearly distinguishes between the properties of mathematic models such as linearity and determinism and the properties of actual systems. This divergence between the idealized, nominal system and actual behavior of CPSs leads to brittle systems with complex and subtle failure modes. Lee identifies four major challenges for CPSs:

1. Determinate CPS models
2. Open minds about languages and tools
3. A semantics of time
4. A discipline of "model engineering".

Moving from idealized, nominal systems toward more resilient systems introduces two ways to deal with faults and failures:

1. Fault-masking systems, which hide faulty behavior, often through redundancy
2. Fault-recovery systems that incorporate special procedures, such as retrying a failed operation.

These ideas are explored through the examples from computer networking, including token passing rings such as the ANSI X3 family of Fiber Distributed Data Interface (FDDI) network specifications which support both fault-masking and fault-recovery capabilities. Implementing counter-rotating rings can provide redundant data paths for fault masking. Moreover, disruption of links on both rings allows FDDI network nodes to perform fault recovery through constructing a new ring by wrapping around the failed segments. FDDI networks provide low-latency communication services with an upper bound specified by the token rotation time [24]. However, token passing rings such as FDDI have a serious vulnerability: any node to link state change causes the network to shut down and restart. The evolution of Ethernet from a linear bus to a switch-based star topology and the emergence of real-time Ethernet is investigated in various use cases including industrial control shipboard machinery control systems [25].

Part 2 – Cyber-Physical Case Study

A significant part of the course focuses on a case study in industrial control of a Vinyl Acetate (VAc) chemical plant. This chemical control challenge problem, "*…process model contains 246 states, 26 manipulated variables, and 43 measurements. Parts of the model, e.g., the azeotropic distillation tower, are highly nonlinear.*" [26] The VAc chemical plant is shown pictorially in **Figure 2.**

As a preliminary investigation, an Internal Model Controller (IMC) is developed for a simplified input-output model of unstable VAc polymerization reaction [28]. This introduces IMC control where the stable portion of the process plant is added as a feed forward term to a conventional Proportional, Integral plus Derivative (PID) controller. This exercise helps the students focus on the heart of this complex dynamically interdependent chemical plant and appreciate the dynamics of a gaseous phase exothermal process whose reaction rate rises exponentially with respect to temperature.

This problem-based learning project seeks to craft a cyber-intrusion to maximize production degradation while avoiding detection by the plant operators. VAc process control studies provide 26 single-input-single-output control loops providing a representative closed-loop control system model [29], [30]. The numerically-stiff simulation model contains time constants that vary from 10 of seconds to days. A MathWorks MATLAB Simulink simulation-based wrapper around the MATLAB and C simulation developed by the "Damn Vulnerable Chemical Plant" (DVCP) initiative [31], [32], [33] provides a rich environment for simulating cyber intrusions. In particular, the Simulink interface provides facilities to:

FIGURE 2 Vinyl Acetate Chemical Plant [27].

1. Insert disturbances
2. Change control set points
3. Insert false sensor data
4. Insert false controller commands
5. Modify the feedback controllers.

Initial experiments introduced by **Table 1** process disturbances subject to the itemized constraints were simulated for 12-hour scenarios.

These initial studies provided two interesting results:

1. Insight into the dynamic interdependencies within the VAc production process
2. Forensic investigations as to why three of the simulations crashed.

For example, the time histories associated with the third disturbance, loss of fresh HAc (Acetic Acid) feed stream, are shown in **Figure 3**. Note that the HAc tank level controller progressively requests increased HAc in feed. When the HAc tank is depleted after approximately 31.4 minutes, the simulation predicts a negative fluid level and is no longer mathemati-

cally valid. These observations reinforce Edward Lee's distinction between the behavior of mathematical models and real systems.

The VAc polymerization process is very sensitive to the concentration of oxygen. The upper **Figure 4** plot highlights the response to injection of false O_2 feed rate commands, shown as a dashed line compared to the controller's initial proportional gain followed by integral gain requests for increased supply of O_2. The lower **Figure 4** plot shows the rapid response in reactor exit flowrate. Note the overshoot in both the controller response and the exit flowrate once control authority is regained.

Eventually, a variety of simulated cyber-attacks were performed as summarized in **Table 2**.

Part 3–Controller Area networks

Controller Area Networks provide an appropriate "fieldbus" for implementing real-time embedded microcontroller systems for a wide range of applications including the transportation, manufacturing and energy sectors. As shown in **Figure 5**, CANopen is one of several application layers which build on CAN physical and data link layers.

CAN provides low latency, lightweight message delivery mechanism of small data packets where the highest priority message is granted

DISTURBANCES	CONSTRAINTS
1. Step change in C_2H_4 concentration in fresh C_2H_4 feed	1. O_2 concentration in reactor feed (< 8 mol%)
2. Loss of column feed	2. Pressure in the gas loop (< 140 psia)
3. Loss of fresh HAc (Acetic Acid) feed stream	3. Peak reactor temperature (< 200 C)
4. Loss of fresh O_2 stream	4. Liquid levels in the vessels (10-90%)
5. Organic product composition analyzer off-line	5. Reactor feed temperature (> 130C)
6. Column bottom composition analyzer off-line	6. FEHE hot effluent temperature (> 130C)
7. Gas recycle composition analyzer off-line	7. HAc concentration in decanter (< 0.06 mol%)
	8. VAc concentration in column bottom (< 0.01 mol%)

TABLE 1 VAc Process Disturbances and Constraints.

first access to the data bus. All nodes remain bit-synchronized, allowing on-the-fly bus arbitration, error detection and message acknowledgement. CAN coverage begins the low-level topics including: data frame format, dominate and recessive bus state signaling, signal propagation, characteristic impedance, cable termination and cyclic redundancy checks. Graphics, animation, and captured waveforms are used to reinforce these topics. Modern microcontrollers typically include a pair of CAN interfaces as part of the internal peripheral device suite.

Once CAN low-level concepts are established, the CANopen [34] application layer is added for hardware-in- the-loop experimentation. CANopen Magic from the Embedded Systems Academy [35] is used as a rapid prototyping network system integration, network management, logging and rich Graphic User Interface (GUI). The Microsoft Windows-based CANopen Magic computers are networked to pre-programmed Peak PCAN-MicroMod Evaluation Kits [36] shown in **Figure 6**.

The MicroMod device is pre-programmed to conform to the CAN in Automation CiA DS-401 generic I/O device profile. Therefore, once the students complete the physical connections and the accompanying MicroMod electronic data sheet is loaded, CANopen Magic is ready to manage, configure, interact with and control the MicroMod field device. **Table 3** identifies the MicroMod DS-401 generic I/O functions where Transmit Process Data Objects (TPDOs) are produced by the

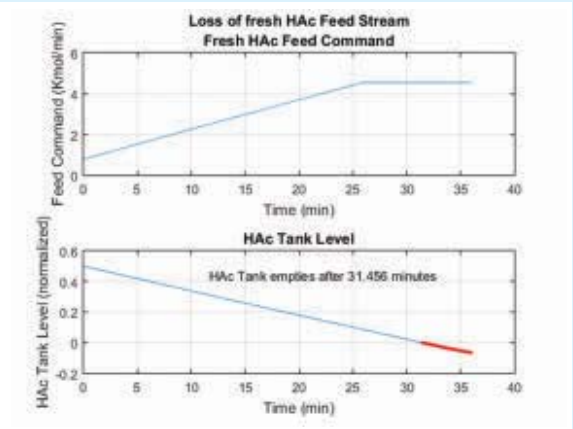


FIGURE 3 Loss of Fresh HAc (Acetic Acid) Feed Stream.

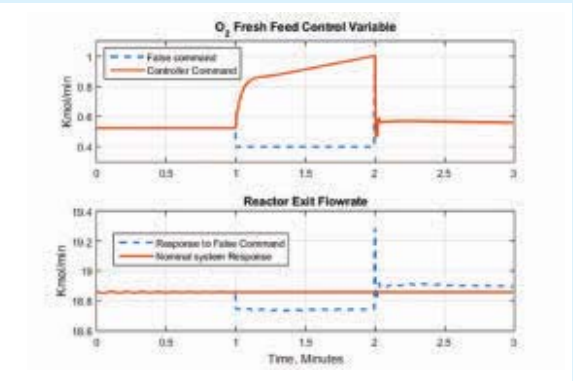


FIGURE 4 Interval Attack on O_2 Fresh Feed Rate Control.

MicroMod and Receive Process Data Objects (RPDOs) command are sent to the MicroMod.

Once the CANopen control networks are operational and the students have acclimated to the new concepts and the rich CANopen Magic GUI, DC motors are interfaced to the MicroMod devices through motor driver and velocity measurement electronics. Initially the CANopen Magic GUI is used to send open-loop PWM motor commands to the MicroMod and provide a graphical display of motor performance.

Finally the in-house mbed [38] LPC1768 microcontroller [39] interface board [40] shown in **Figure 7** is added to each standalone CANopen motor control network.

Initially, the mbed device is programmed to automati-

CYBER-PHYSICAL ATTACK	OBSERVATIONS
Control authority attacks with false actuator commands	These attacks break feedback loops tripping process alarms, large transients occur if the controller regains control
False sensor data injection	These attacks also break feedback loops risking tripping process alarms
Modifying process set points	These attacks can be effective but are likely to be noticed by plant operators
Coordinated control authority and false sensor data injection	Most effective and more difficult to detect

TABLE 2 VAc Process Attacks and Observations.

REFERENCES

1 National Science Foundation Cyber-Physical Systems Solicitation 16-549, https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286, visited March 20, 2016.

2 Leadership Under Challenge: Information Technology R&D in a Competitive World, President's Council of Advisors on Science and Technology (PCAST) report, August 2007, http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-07-nitrd-review.pdf .

3 Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology, President's Council of Advisors on Science and Technology (PCAST) December 2010. https://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-nitrd-report-2010.pdf .

4 M. Amin, Toward Self-Healing Energy Infrastructure Systems, IEEE Computer Applications in Power, pp. 20-28, Vol. 14, No. 1, January 2001.

5 P. Antsaklis, "Goals and Challenges in Cyber-Physical Systems Research," Editorial of the Editor in Chief, IEEE Transactions on Automatic Control, Volume 59, Issue 12, December 2014.

6 CPS Vision Statement, Networking and Information Technology Research and Development (NITRD) CPS Senior Steering Group 2012, https://www.nitrd.gov/nitrdgroups/images/6/6a/Cyber_Physical_Systems_(CPS)_Vision_Statement.pdf, last visited December 19, 2016.

7 Edward A. Lee and Sanjit A. Seshia, Introduction to Embedded Systems, A Cyber-Physical Systems Approach, Second Edition, http://LeeSeshia.org, ISBN 978-1-312-42740-2, 2015.

8 Astrom and Wittenmark, Computer-controlled systems: theory and design (2nd ed.), Prentice-Hall, Inc. Upper Saddle River, NJ, USA, ISBN:0-13-168600-3, 1990.

9 CHESS: Center for Hybrid and Embedded Software Systems, https://chess.eecs.berkeley.edu/, last visited December 19, 2016.

10 Cyber-Physical Systems Virtual Organization, http://cps-vo.org/, last visited December 19, 2016.

11 DoD Defense Directive 8500.01 Cybersecurity, http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf

12 Risk Management Framework (RMF) for DoD Information Technology (IT), http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf, last visited December 19, 2016.

13 Krotofil, Rocking the pocket book: Hacking chemical plants for competition and extortion," Hamburg University of Technology, presented at BLACK HAT August 2015. https://www.blackhat.com/docs/us-15/materials/us-15-Krotofil-Rocking-The-Pocket-Book-Hacking-Chemical-Plant-For-Competition-And-Extortion-wp.pdf

14 J. Dorf, and R. Bishop, Modern Control Systems, 11th Edition, Prentice Hall, Upper Saddle River, NH, 2008.

15 60 Minutes: Sabotaging the System (CBS), http://www.peabodyawards.com/award-profile/60-minutes-sabotaging-the-system, last visited December 19, 2016.

16 60 Minutes: Sabotaging the System (CBS), www.cbsnews.com/news/cyber-war-sabotaging-the-system-06-11-2009/

17 Cyber-Physical Systems (CPS) Solicitation 17-529, https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286, last visited December 19, 2016.

18 Cyber-Physical Systems, http://cyberphysicalsystems.org/, last visited December 19, 2016.

19 E. Zivi., "Design of robust shipboard power automation systems," International Federation of Automatic Controls (IFAC) Annual Reviews in Control, vol.29, no.2, 2005, pp. 261 – 272, ISSN 1367-5788, DOI: 10.1016/j.arcontrol.2005.08.004. http://www.sciencedirect.com/science/article/B6V0H-4HD8BMV-1/2/a37972b711869c686548e3007980e183, last visited December 19, 2016.

20 A. Cramer, S. Sudhoff, E. Zivi, "Performance Metrics for Electric Warship Integrated Engineering Plant Battle Damage Response," IEEE Transactions on Aerospace and Electronic Systems, Volume: 47, Issue: 1, 2011, Pages: 634 - 646, DOI: 10.1109/TAES.2011.5705696.

21 A. Cramer, S. Sudhoff, E. Zivi, "Metric Optimization-Based Design of Systems Subject to Hostile Disruptions," IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, Volume: 41, Issue: 5, 2011, Pages: 989 - 1000, DOI: 10.1109/TSMCA.2010.2093887.

22 E. Lee, "Cyber Physical Systems: Design Challenges," International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing (ISORC), Orlando, FL, May 6, 2008.

23 E. Lee, "Cyber-Physical Systems: A Rehash or a New Intellectual Challenge?," DAC 2013, Austin June 2012, http://ieee-ceda.org/activities/distinguished-speaker-series, last visited December 19, 2016.

24 K. Sevcik, M. Johnson, "Cycle Time Properties Of The FDDI Token Ring Protocol," IEEE Transactions On Software Engineering, Vol. SE-13, No. 3, March 1987.

25 A. Manfredi, P. Read, "Twenty Five Years of Shipboard Control System Networks," ASNE Automation and Control Symposium, At Biloxi, MS, December 2008.

26 R. Cheng, D. Kedar, T. McAvoy, "A Nonlinear Dynamic Model of a Vinyl Acetate Process," Ind. Eng. Chem. Res., 2003, 42 (20), DOI: 10.1021/ie020859k, March 12, 2003, pp 4478–4487.

27 S. Rathore, https://www.scribd.com/doc/236423736/Vinyl-Acetate-Monomer, Published Aug 10, 2014.

28 B. Burgett, Process Control, Prentice Hall, Upper Saddle River, NH, 2008, pp 305-310.

29 W. Luyben, B. Tyreus "An Industrial Design/Control Study for the Vinyl Acetate Monomer Process,", Computers Chem. Engineering. Vol. 22, No. 7–8, 1998, pp. 867–877.

30 W. Luyden, "Design and Control of a Modified Vinyl Acetate Monomer Process," Ind. Eng. Chem. Res., 2011, 50 (17), DOI: 10.1021/ie201131m, August 7, 2011, pp 10136–10147.

31 M. Krotofil, "Damn Vulnerable Chemical Process (DVCP)," European Network for Cyber Security (ENCS), Moscow, Russia June 29, 2015.

32 M. Kritofil, "Rocking the pocket book: Hacking chemical plants for competition and extortion," White Paper, Black Hat 2015, August 2015, https://www.blackhat.com/docs/us-15/materials/us-15-Krotofil-Rocking-The-Pocket-Book-Hacking-Chemical-Plant-For-Competition-And-Extortion-wp.pdf, last visited December 19, 2016.

33 DVCP-TE-master.zip from https://github.com/satejnik/DVCP-VAM, last visited December 19, 2016.

34 CAN in Automation website, https://www.can-cia.org/, last visited December 19, 2016.

35 CANopen Magic website, http://www.canopenmagic.com/, last visited December 19, 2016.

36 PEAK-System PCAN-MicroMod Evaluation Kit product webpage, http://www.peak-system.com/PCAN-MicroMod-Evaluation.221.0.html?&L=1, last visited December 19, 2016.

37 PCAN-MicroMod CANopen User Manual, https://www.peak-system.com/produktcd/Pdf/English/PCAN-MicroMod-CANopenFW_UserMan_eng.pdf, last visited December 19, 2016.

38 ARM mbed website, www.mbed.org, last visited December 19, 2016.

39 NXP OM11043 ARM mbed LPC1768 Board, http://www.nxp.com/products/microcontrollers-and-processors/arm-processors/lpc-cortex-m-mcus/lpc-cortex-m3/lpc1700-cortex-m3/arm-mbed-lpc1768-board:OM11043, last visited December 19, 2016.

40 J. Bradshaw, C Library for mbedWSE project based single board computer for hardware peripherals, https://developer.mbed.org/users/jebradshaw/code/mbedWSEsbc/, last visited December 19, 2016.

cally send PWM motor commands using the same message format as previously demonstrated in CANopen Magic. The laboratory apparatus is now ready for various Cyber-Physical Systems experiments including:

1. mbed-in-the-middle attacks where the mbed intercepts PWM commands from CANopen Magic and reverses the duty cycle commands to the MicroMod and motor speed messsages from the MicroMod.

2. PI motor closed-loop control commanded and monitored by CANopen Magic.

3. Red on blue competitions between CANopen network managers and CAN intruders. A sample CANopen Magic PI motor closed-loop control GUI screen shot is included as **Figure 8**.

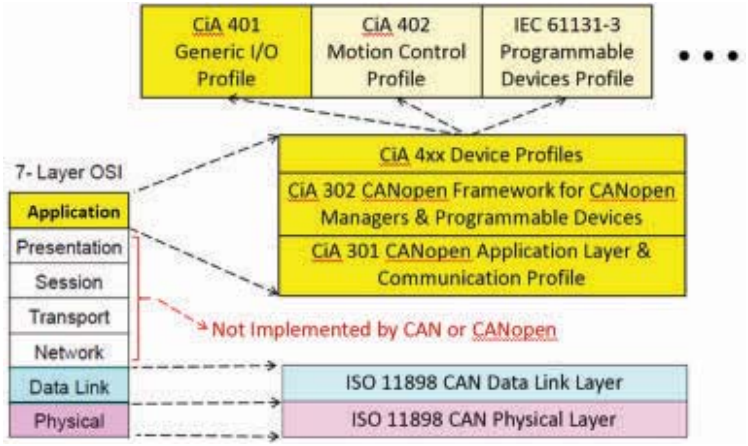


FIGURE 5 CAN and CANopen Network Layers.

MICROMOD CANOPEN GENERIC I/O MESSAGES Comm Obj Message	PEAK MICROMOD CANOPEN #	TYPE	I/O DEFINITIONS
TPDO 1	1	Unsigned byte	Digital In 0..7
RPDO 1	1	Unsigned byte	Digital Out 0..6
TPDO 2	4	Unsigned int	Analog In 0..3
RPDO 2	4	Unsigned byte	PWM Out 0..3
TPDO 3	4	Unsigned int	Analog In 4..7

TABLE 3 MicroMod Generic I/O Message Definitions [37].

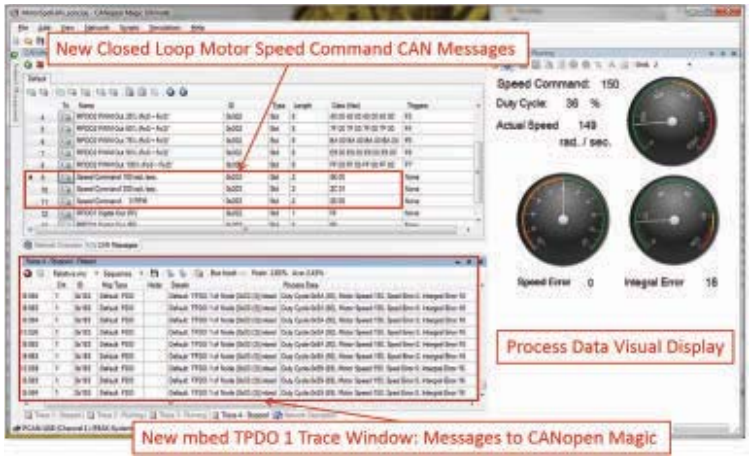


FIGURE 8 CANopen Magic PI Motor Closed-Loop Control GUI.

CONCLUSION

The course described herein presents fundamental concepts within the rapidly expanding field of Cyber- Physical Systems, has been tailored to and is well received by U. S. Naval Academy Systems Engineering senior level engineering students. For more information, contact the author at zivi@usna.edu. ■

FIGURE 6 Peak PCAN-MicroMod Evaluation Kit.

FIGURE 7 mbed LPC1768 Microcontroller Interface Board.

ABOUT THE AUTHOR

Edwin L. Zivi received the B.S. degree in Engineering Science and Mechanics from the Virginia Polytechnic Institute and State University, Blacksburg, in 1975. He received the M.S. and Ph.D. degrees in mechanical engineering from the University of Maryland, College Park, in 1983 and 1989, respectively.

Ed's present position is Professor of Systems Engineering at the United States Naval Academy, Annapolis, MD where his teaching and research focus on the design and implementation of resilient control systems. Ed manages the Systems Engineering Cyber Systems major elective track and developed the current course offerings. Ed leads the development of Cyber-Physical Systems at the Naval Academy and is presently developing a new Internet-of-Things (IoT) major elective.

Prior to 1998, he was a Senior Research Engineer and Technical Advisor at the Naval Surface Warfare Center, Annapolis, MD. In one project, he served as technical director for the NAVSEA Standard Monitoring and Control System leading the project from inception through full-scale land-based testing. His research focuses on resilient Cyber-Physical Systems, integrated electrical power systems and early-stage trade-space design methods and tools. The Office of Naval Research has been Ed's primary sponsor throughout his 40-year career.

ACKNOWLEDGEMENTS

The Cyber-Physical Systems research and pedagogical developments described herein were made possible through long-term support of the Office of Naval Research and the U. S. Naval Academy. Former Assistant Research Professor Yonggon Lee assisted with the development of the CANopen hardware and software prototyping environment. Joe Bradshaw and his Technical Support Division team assistance is also gratefully acknowledged.

MODELING CYBER CONFLICT TO INFORM CRITICAL INFRASTRUCTURE DEFENSE

Imagine a naval strike group patrolling in the middle of a territorially challenged and electromagnetically controlled area of the world. The threats to that group are varied and wide ranging which require the group to employ all available defensive and offensive tools. While the physical kinetic threat to the group can be detected as an external event, it is not always easily detected when that threat presents itself inside the control network of the strike group. In this scenario, it is possible that the lurking threat is exercising data collection among the ships, or simply lying in wait to take over the navigation system without the users knowing. No known architecture or decision framework exists to inform a critical infrastructure or cyber-physical system (CPS) when it is best to defend against a possible

BY BRIAN CONNETT
CDR, USN, PHD STUDENT
BRYAN O'HALLORAN
ASSISTANT PROFESSOR

NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIFORNIA

attack. In addressing systems of systems (SoS) or families of systems (FoS), designers implement characteristics to describe the robustness of the system in terms of availability, reliability, reparability, etc. This approach may not be appropriate for the given scenario or those similar. Therefore, a framework and architecture must be introduced that supports the defense of a system to access most information, while being optimized to the characteristics of an attack. Often, those characteristics are not readily accessible, so an architecture is developed to analyze the attributes of an anomaly's timing, medium, intention and value. Here, the reader will find a methodical recommendation that develops the way defense of a cyber critical infrastructure can be most effective. First, historical background motivates the current political theme, followed by modeling theory that has been published. Classical systems engineering foundations are reviewed to adapt modeling environment to the current cyber conflict problem in a way that allows a systems owner to posture most effectively against anomalies across the network of communication nodes. Finally, the focus of both this paper and the authors' research is defining the attributes, and the common knowledge expected to be used throughout this field of research. Those attributes form the landscape upon which future research can be conducted.

BACKGROUND

The U.S. Critical Infrastructure Protection program of 1996 [1], and amplification in the Patriot Act of 2001, defines critical infrastructure as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." According to Presidential Policy Directive (PPD-21) [2] and the Department of Homeland Security (DHS) there are 16 critical infrastructure sectors. Those systems and assets within critical infrastructures were created and existed in a seemingly safe space away from exploitation or attack by adversaries with ill-intent. With increased complexity of CPS, vulnerability to cyber-physical attacks shows significant increase, if only validated by open source reporting like that of the attack on the Iranian Nuclear program, called Stuxnet [3]. In addition to the daily open-source reporting of infiltrations, this increase in activity is clearly demonstrated by the Federal Aviation Administration (FAA) Federal Registry report and Government Accounting Office (GAO) report citing belief

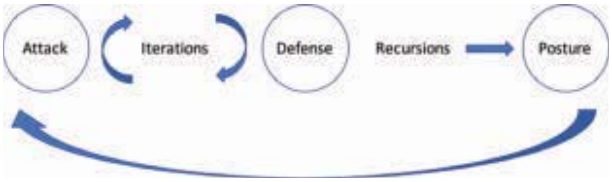


FIGURE 1
Integration Systems Model – Cyber Conflict.

that commercial aircraft contain significant risk for cyber-attacks through a common network of the avionics and entertainment system [4, 5]. Further, security breaches of well-known establishments emphasize the capability of such attackers. As a result, critical infrastructure has become a target.

Knowing that CPS exploits exist, with characteristics of patience, stealth, replication ability and the robustness never experienced before, system owners are obligated to maintain a high level of response-action posturing to protect their own resources. Regardless of the posturing, limited systems resources exist in computing, logic, and exploitation definitions, and contribute to an aggregated failure against multi-pronged attacks from multiple simultaneous attackers. Even when aligned in an apparent show of up-to-date defense, there exists the danger of unknown vulnerabilities and penetrations against such defenses. The key to success is having the knowledge to align critical infrastructure architecture in a manner that is responsive to the capability, willingness and timing of the attacker.

MODELING, ARCHITECTURE AND FRAMEWORK

Models currently exist that primarily demonstrate the dynamics of cyber-physical systems. In particular, Derler, et al., present a significant approach in "dynamics, the evolution of a system state in time"[6]. This model provides insight into the inherent difficulties of simply modeling the dynamic nature of systems of CPS. Few models, empirical or theoretical, exist to examine the value of both knowing attacker capabilities in the cyber realm and the strength of one's own system. Axelrod and Iliev [7] present a mathematical model that analyzes how the timing of using a cyber exploitation depends on the stakes involved and the characteristics of the exploitation itself. The reader is encouraged to reference this work in depth to understand three major assumptions of this model, leading to a balanced equation that defines value of an attack on a system. The implication of this model is that a protection posture can be estimated, and can quickly turn into a balanced engagement between the attacker and defender. The difficulty therein lies of knowing when to fortify a critical infrastructure against an impending attack.

To establish a framework that informs decision makers of when to defend critical infrastructures, critical architecture elements for several parameters are estimated. Understanding these parameter estimations uniquely positions the decision maker to posture having revealed the vulnerabilities of those parameters being estimated, an attacker's persistence, and stealth. A scalable framework designed to deliver optimal solutions to its user requires a broad-based methodology that can capture all aspects of the impending problem and the possible solutions. To that end, our current research works toward laying the foundational framework in four specific attributes, and tied into the aforementioned modeling efforts. The attributes of timing, intent, value of attack, and mediums will allow both a qualitative and quantitative tractability in the decision at hand.

As the framework is developed, consider the work of Langford who delivers a discourse on the differences in systems engineering versus systems engineering integration [7]. As relevant as it is in the classroom, the practices on integration from his industry point of view are even more relevant when applied against this problem of defending the critical infrastructure. Specifically, he highlights that the "usual desire for integration is for interoperability of objects and processes to achieve some effect in their intended operational environment," yet it is exactly this desire to integrate the parts of a system into a whole which make our modern cyber and physical systems vulnerable. Continuing to use Langford's emphatic position that systems engineering is quite different from systems integration, integration should not be relegated to that effort which results in a whole by following some set of best practices. "For systems engineering, a best practice is iterative development and improvement. For systems engineering integration, a best practice is successive approximation based on recursive thinking." [7] This approach to systems design and systems integration will be applied in a similar manner to the design of a proactive response to anomalies, rather than an iterative and reactive response. **Figure 1** is based on Langford's "high-level summary of the systems engineering process model" [7] where he addresses the "type of thinking required … as the service progresses through development and into integration." Similarly, the cyber conflict framework and architecture introduced in this research claims the same progression. The attack of the critical system is interactive with the defense of the same system through iterations. The iterative relationship is the ultimate integration of understanding the attributes of the models described in Axelrod and Illiev [7], and help to develop the measures of success in the approach. Once the engagement is complete, or has settled to a steady state manageable for continued operations, the overall effectiveness of the integration of defenses is indicated by a forward-looking recursion to demonstrate the learned behavior within the decision framework. The recursive relationship forwarded to consequential posture of the system indicates the level of that learned behavior. The life-cycle of an attack and defend engagement is indicated by the closed-loop review arrow.

FRAMEWORK AS A DECISION MAKING TOOL

Decision making in defense of a critical infrastructure under a possible cyber-attack is rooted in the system owner's desire to maintain attributes of a system that are often found in broadly defined terms such as reliability, resilience, and stability. It is under these attributes that measurements of success can be assigned. While attributes found in these loosely-defined terms are generally understood, these attributes are not characteristics of this research being considered. Instead, the reader is encouraged to think of the optimal solution to an attack in terms of redundancy, which here describes the grouping of mechanisms (synthetic or natural) that replicate ability. As a result, failure of one means of ability will be recovered and continued

by the next. To increase the broad applicability of redundancy, this architecture decision framework is agnostic to how the physical or logical redundancy is presented.

The functions of redundancy encompass two sets of approaches to defending the SoS or the FoS, namely an iterative-based set versus a recursive-based set. These sets are respectively assigned to decision making based on rules or prior knowledge. The iterative process is purely reactive and allows an anomaly to have an initial effect on the system before the rules have an opportunity to adjust. Considering the Axelrod and Iliev model introduced earlier, a recursive (knowledge) based ruleset that does not wait for an anomaly to present itself, is introduced that considers the four attributes introduced in this piece as information to invoke redundant procedures throughout the SoS. This framework combines both of these approaches. This is a developing framework, yet it still needs to be stimulated by the attributes in some manner from an external source. The assumption of the ability to acquire the stimuli is made here, and will be left to other research to understand why or how that information is obtained. Still, we must start by aligning the work of Axelrod and Iliev to match the premise of response action being introduced.

Two attributes of the attacker, stealth and persistence, are most relevant in this framework. An exploitation or anomaly in a CPS or critical infrastructure will likely have some aggregation of these characteristics. Stealth is defined by earlier authors as a conditional probability describing that an exploitation will be able to transit a CPS undetected given that the attacker has activated the capability (Pr (exploitation surviving | activated)), and Persistence is defined as a conditional probability describing that an exploitation will not be detected given that the attacker has not activated the capability (Pr(exploitation surviving | not activated)) [8]. While this is consistent with the previous works, we will consider this as an attacker's 'intent', and for the research presented here persistence will be a redefined

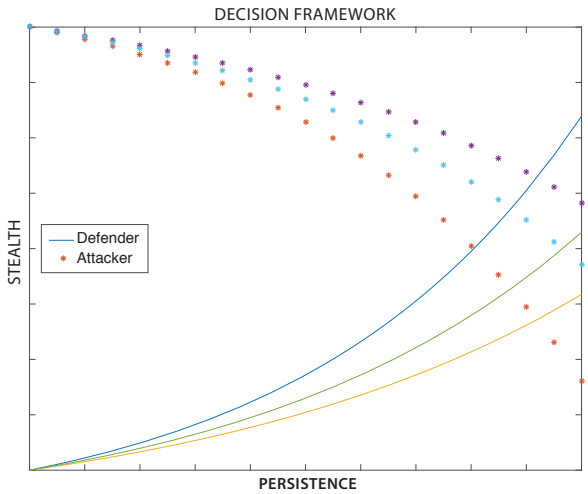


FIGURE 2 Decision Framework based on Threshold.

trait parameter to match the framework goal. Specifically, persistence will be the conditional probability describing that an exploitation will be able to transit a CPS undetected given that the attacker has increased its number of attempts at exploiting a system (Pr (exploitation surviving | increase in attempts to exploit)).

The next attribute informing the architecture framework is the value of the attack. Notionally, the value of the attack is a relatively-weighted item that fits into categories of destruction, data extraction, and behavior and social modifications. Because of the assumptions of stimuli introduced from a known external source, the weight of these values will be dictated by the current intelligence picture relative to the systems being targets. There are numerous examples cited throughout the government, industry and private

MEDIUM	PERSISTENCE	VALUE	STEALTH
Network Failure	M:1	0.05	1.00
Power Failure	M-(x_1) : 1	0.20	0.80
Malicious – Low	M-(x_2) : 1	0.40	0.60
Malicious – Med	M-(x_3) : 1	0.60	0.40
Malicious – High	M-(x_4) : 1	0.80	0.20
Kinetic Effect	1 : 1	1.00	0.05

TABLE 1 Taxonomy of Cyber Conflict.

sectors that build a growing intelligence picture with regard to cyber conflict. Specifically related to the fragility of critical infrastructure are examples of the electric grid blackout (2003) in the Northeast United States of America and Southern Canada, the ongoing failures of the Metropolitan transit lines in Washington, D.C., United States, private information breaches among super chains such as supermarket and retail product provider, Target, and hints at weak protection of avionics in commercial airliners that have received attention in recent memorandums from the U.S. Federal Aviation Administration. Still, knowing that these weaknesses exist, the weight of an attack value is dependent upon external source analysts.

The third attribute, when combined with the previous two attributes, reveals a taxonomy of attacking vectors that will ultimately inform the overall timing of the defense posture in the recursive methodology desired at the beginning of this work. The medium from which an attacker can deliver anomalies into a system is varied, but for the purpose of discussion, **Table 1** lists persistence, stealth and value for a range of mediums. As research to support the architecture framework matures, and modeling of the frameworks develops, arbitrary values will be modified to realize the potential effect of these attack characteristics. The mediums described are listed as those attack vectors that are expected to be encountered, from least destructive to most destructive. The persistence is described as an attempt-to-realization ratio. For example, in a Network Failure the attacker will be able to attempt access to a system many times before being caught (M:1), whereas a Malicious attack will have less attempts before being detected (M-(x_n):1). Finally, an attack with a kinetic effect will be attempted one time, and by the nature of its effect, will be known immediately (1:1). The last two columns are arbitrarily weighted values assigned to the attack in order to quantify the overall utility of the system and the stealth of an attacker. These are arbitrary values, and will be adjusted during modeling efforts using simulation techniques to measure various effects.

Finally, the fourth attribute determines the optimal timing of both the attacker and the defender. Using the taxonomy of the cyber conflict, a mathematical model will be derived to determine at what point it is best for a target defender to employ the recursive knowledge-based ruleset desired and illustrated in **Figure 2**. In **Figure 2**, a series of curves are used to demonstrate the dynamic nature of applying defensive measures. As stealth and persistence are measured along the axes, the posture of both the attacker and defender can be estimated. The model derivation will reveal an optimal time to employ the rules of the framework.

Figure 2 is a theoretical representation of what the authors believe will represent that decision timing for both the attack and defender. All measurements within the graph are unitless and are meant to give an illustration of a relative magnitude of those attributes discussed. The solid curves of the graph show a relative magnitude value of defending against an attack, whereas the starred curves show a relative magnitude value of the attack. When stealth is at its highest, a deployment of defensive measures will have the smallest effect since it is not known if the anomaly exists. When persistence is greatest, it is known that an anomaly exists in the system, but now with lower stealth value. The intersection of the curves indicates when it can be both the best time to attack and to defend. The multiple curves show how the weighted values of the frameworks taxonomy can dictate that threshold of action. This is when the architecture framework lends itself to a decision framework.

CONCLUSION

Cyber physical systems are vulnerable to various anomalies. Some of those anomalies exist naturally, but when those anomalies are introduced by an actor with malicious intent, the intention and outcome can be devastating. In defense of the cyber-physical system there exist many methods and techniques to respond to an attack as it happens. The resources required to counter an attack can certainly be effective, but exist as a reactive measure. This paper presents a combination of known models and system design techniques that results in an architectural framework that is predictive. In turn, the prediction of the models serves as a decision tool for the physical systems owners. Further research of this predictive modeling and architectural framework will build upon current community contributions. Overall, the contributions from this community will address the tipping point of cyber conflict within the critical infrastructure of our hyper-connected society. Physical threats to the military, industry and private sector control systems are not easily detected, nor mitigated. Without architecture or frameworks in place to confront the issue, system owners will continue to struggle against the threat. When optimized within decision algorithms, data will exist to illuminate what process can be implemented in defense. Using classical systems engineering fundamentals, modeling & simulation, and proven mathematical approaches, this research seeks to support such implementation. ■

ABOUT THE AUTHORS

Commander Brian Connett, U.S. Navy, is currently stationed at the U.S. Naval Postgraduate School in Monterey, CA pursuing his Ph.D. in Systems Engineering. In particular he is examining concepts of cyber-physical systems and the complexity of decision making regarding its security. His education includes a M.S. in Systems Engineering, a M.S. is Space Operations both from the U.S. Naval Postgraduate School and the B.S. in Information Systems from Drexel University, Philadelphia, PA.

A career naval officer, Brian has recently been a junior faculty member at the U.S. Naval Academy in Annapolis, MD leading midshipmen in the classroom as a controls systems and cyber operations instructor. Prior to this classroom mission, his naval experiences include assignment to the U.S. Naval Air Forces, Navy Information Operations Command, Special Boat Team TWENTY and USS Lake Erie (CG70). His personal decorations include the Meritorious Service Medal, the Defense Meritorious Medal, the Navy and Marine Corps Commendation, and the Navy and Marine Corps Achievement Medal.

Bryan O'Halloran is currently an Assistant Professor in the Systems Engineering department at the Naval Postgraduate School. Previously he was a Senior Reliability and Systems Safety Engineer at Raytheon Missile Systems and the Lead Reliability and Safety Engineer for hypersonic missile programs. He holds a Bachelor of Science degree in Engineering Physics and a Master of Science and Doctorate of Philosophy in Mechanical Engineering from Oregon State University. His current research interests include risk, reliability, safety, and failure modeling in the early design of complex cyber-physical systems.

REFERENCES

1 W. J. Clinton, "Executive order 13010 on the presidents commission on critical infrastructure protection," United States of America, White House, 1996.

2 B. Obama, "Presidential policy diective - critical infrastructure security and resilience. PPD-21," United States of America, Washington, D.C., 2013.

3 K. Zetter, "WIRED," Crown Publishers, 03 11 2014. [Online]. Available: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/. [Accessed 16 11 2016].

4 Federal Aviation Administration, "Airworthiness Standards: Transport Category Airplanes," FAA, Washington, D.C.., 2014.

5 U.S. Government Accountability Office, "Air traffic control: FAA needs a more comprehensive approach to address cybersecurity as agency transitions to NEXTGEN," Government Accounting Office (GAO), Washington, D.C., 2015.

6 P. Derler, E. A. Lee and A. S. Vincentelli, "Modeling cyber physical systems," in *Proceedings of the IEEE*, 2012.

7 G. O. Langford, Engineering Systems Integration: Theory, Metrics, and Methods, CRC Press, 2016.

8 R. Axelrod and R. Illiev, "Timing of cyber conflict," in *Proceedings of the National Academy of Sciences*, 2014.

9 Federal Bureau of Investigation, "The Cyber Threat," 27 03 2012. [Online]. Available: https://www.fbi.gov/news/stories/2012/march/shawn-henry_032712. [Accessed 15 11 2016].

10 U.S. Senate and U.S. Congress, "Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act of 2001)," Unites States of America, Washington, D.C., 2001.

DEMYSTIFYING ADVANCED PERSISTENT THREATS FOR INDUSTRIAL CONTROL SYSTEMS

BY ANASTASIS KELIRIS
PHD CANDIDATE
MICHAIL MANIATAKOS
ASSISTANT PROFESSOR
ELECTRICAL AND COMPUTER ENGINEERING
NEW YORK UNIVERSITY ABU DHABI

Cyberattacks are an emerging threat for Industrial Control Systems (ICS) that, given the tight coupling between the cyber and physical components, can have far-reaching implications. It is typical for contemporary ICS components to utilize Commercial-Off-The-Shelf (COTS) hardware and software, rendering them prone to vulnerabilities and exploitation techniques that afflict IT systems **(Figure 1)**. In an effort to demonstrate the ICS cyber threat landscape, we discuss a comprehensive methodology for designing an Advanced Persistent Threat (APT), which is a stealthy and continuous type of cyberattack with a high level of sophistication suitable for the complex environment of ICS. Retracing the steps and studying the objectives an attacker would take into consideration when designing a cyberattack enables us to demonstrate the potential impact of these attacks and identify critical entry points, vulnerable flows, and services of ICS. Finally, leveraging the generated intelligence, we discuss defensive strategies that can assist in thwarting such attacks.

FIGURE 1 The modernization of Industrial Control Systems exposes them to novel threats and cyber-attacks.

ICS are systems that monitor and control physical processes in industrial environments. Over the past decade, components used in ICS are under modernization with the inclusion of Information and Communication Technologies (ICT), towards increased efficiency and controllability, reduced downtime, and lower costs. The vision for the future of industrial automation is interconnected cyber-physical systems of systems, where components communicate with each other, have computational capabilities and are able to make decisions in a decentralized manner [1].

Despite the numerous benefits of this modernization trend, an immediate and pressing consequence is its negative impact on the cyber-security posture of ICS and the underlying physical processes. In order to enable the transition of ICS into the information age, contemporary ICS components utilize COTS hardware and software, such as ARM or Intel microprocessors and real-time versions of commercial operating systems [2]. **Figure 2** depicts the internals of an industrial controller, which include an ARM processor, COTS integrated circuits for control and communication, RJ45 sockets (Ethernet) for communication over common ICT protocols, as well as several memory chips.

The use of COTS components facilitates development and reduces commissioning time, but at the same time enables malicious actors to readily port ICT vulnerabilities to ICS environments, rendering ICS prone to the same vulnerabilities and exploitation techniques that plague ICT. ICS systems often control national critical infrastructure such as critical manufacturing, chemical plants, power grids, oil and gas systems, and nuclear plants. Taking this into consideration, the implications of cyber-security breaches can be far-reaching, including significant financial losses, environmental disasters, and loss of life.

ICS CYBER-ATTACKS

Cyber-attacks targeting ICS are not only theoretical; several real attacks against ICS have been reported and studied to date. At the same time, the majority of cyber-security-related incidents are believed to remain unre-

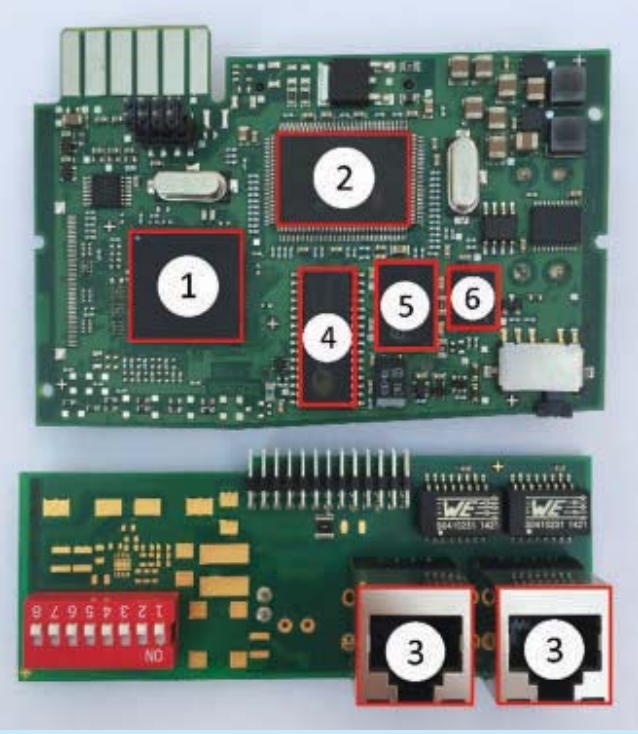


FIGURE 2 Printed Circuit Boards of disassembled industrial automation controller, demonstrating the pervasive use of Commercial-Off-The-Shelf components in Industrial Control Systems. 1) ARM microprocessor, 2) Ethernet Integrated Switch, 3) RJ45 sockets, 4) Non-volatile SRAM, 5) Synchronous DRAM, 6) NOR Flash memory.

ported, since this would hurt the public image of vendors, industries, or even governments [3]. A prominent example of an ICS-targeting cyber-attack is Stuxnet, a nation-state-sophisticated attack against an Iranian uranium enrichment plant in 2009 [4]. More recent examples include an attack on a German steel mill in 2014 [5] and a partial blackout of the Ukrainian power grid in 2015 [6]. The common factor of these attacks is their physical world impact, demonstrating that cyber-attacks are no longer contained in the cyber realm. The forensic information gathered from known cyber-attacks indicates that, currently, the involved threat actors are highly motivated, sophisticated, and well-funded organizations or nation states. However, as more and more ICT and COTS components are deployed in ICS and the entry bar for threat actors is lower, we can expect the volume of cyber-attacks against industrial environments to increase.

DESIGNING AN ADVANCED PERSISTENT THREAT

One of the most complex and evasive categories of cyber-attacks are Advanced Persistent Threats (APTs) [7]. These attacks are a*dvanced* in the sense that the attack strategies and exploitation techniques they utilize are tailored, highly sophisticated, span multiple attack vectors, and are stealthy. They are *persistent* in the sense that they establish a strong foothold within the target infrastructure, pursue their objectives over extended periods of time, and adapt to defense mechanisms deployed to thwart them.

In an effort to highlight the dangers that ICS face from the cyber domain and stress the importance of ICS cyber-security, we guide the reader through the steps an attacker would follow while designing an APT for industrial environments. This structured approach enables us to demystify APTs, identify critical entry points, and generate intelligence that can be leveraged by ICS stakeholders to better protect their infrastructure from cyber-attacks.

The overall design flow of an APT can be broken down in five interdependent steps, namely, 1) Reconnaissance, 2) Vulnerability discovery, 3) Payload design, 4) Payload delivery, and 5) Attack persistence. **Figure 3** shows the progression and interdependencies between the different steps.

The APT design process begins with *Reconnaissance*, which is continuously undertaken throughout the lifetime of a cyber-attack campaign. During reconnaissance, the attacker collects and analyzes information regarding all aspects of the target system. The gathered information is then used during *Vulnerability* discovery. In this step, the attacker's aim is to discover potentially exploitable vulnerabilities in subsystems, devices, or services of the target system. The actual payload is developed during *Payload design*, where the attacker takes into consideration the available delivery mechanisms and objectives of the campaign, in addition to information gathered during reconnaissance. If the final payload does not fulfill the campaign's objectives, the APT design process can revert to the vulnerability discovery step. Moving forward, in the *Payload delivery* step the adversary uses exploitation techniques to exploit the discovered vulnerabilities and establish a delivery mechanism for the actual attack (i.e., the payload). The feasibility of delivering a payload within the target system is informed by the findings of the reconnaissance. If effective delivery mechanisms are not found, the design process reverts to the vulnerability discovery step. The final step is *Attack persistence*. During this step, the attacker identifies any corrective or defensive actions taken by the ICS operators to thwart cyber-attacks, through information from the continuously ongoing reconnaissance step. The attacker adjusts the existing payloads and payload delivery mechanisms accordingly, or develops new attack vectors, in an effort to bypass any deployed security mechanisms and ensure persistence of the cyber-attack.

The above-described design process is repeated during the

FIGURE 3 Design flow for developing an Advanced Persistent Threat for Industrial Control Systems.

lifetime of a cyber-attack campaign, ensuring persistency and successful fulfillment of the campaign's objectives. A more extensive analysis of each step is presented below.

RECONNAISSANCE

Reconnaissance is the process of gathering information regarding a target system or organization, with the purpose of extracting critical information that can enable an attack. Examples of such information include data regarding the users of a facility (e.g., business role, contact details, personal information), business strategies, network structure, hardware devices, configuration details, and software services [8].

A first source of information is any publicly available information. This can be in the form of publicly available websites, corporate documents, press releases, vendor success stories, or reports that the target organization is legally bound to release publicly (e.g., environmental impact reports). Further information can be obtained from network interfaces. Reconnaissance of ICS networks can borrow techniques, tools, and methodologies from ICT (e.g., the Network Mapper – Nmap [9]). Moreover, field devices may be directly routable from the public internet, either because of system requirements, or as a result of misconfigurations. In this case, information regarding ICS field devices can be extracted from device search engines such as Shodan [10].

One important objective of reconnaissance is to *fingerprint* software services and hardware devices deployed within the target system, i.e., identify specific software services or physical devices. In the context of ICS, fingerprinting translates to identifying the specific hardware and software of field devices. Common ICT tools capable of fingerprinting (e.g., Nmap and p0f) might not always provide adequate information. However, it is possible to leverage variations between ICS device implementations for the purposes of fingerprinting. For example, information regarding field device make and model can be extracted over commonly used industrial protocols. Such an approach has proven to be able to fingerprint ICS devices via the Modbus protocol by carefully crafting packet requests. The technique effectively exploits the different implementations of the non-standardized Modbus protocol by vendors, combined with the lack of built-in authentication mechanisms, and was validated on real field-deployed ICS devices indexed by Shodan [11].

VULNERABILITY DISCOVERY

Leveraging the information gathered during reconnaissance, the attacker can focus on discovering vulnerabilities in the target process workflow, or the field-deployed devices themselves. During vulnerability discovery, the attacker typically has two options: 1) use existing, known vulnerabilities, or 2) study the system and discover new, previously unseen vulnerabilities, also known as 0-day vulnerabilities[1].

In search of known vulnerabilities, the attacker could make use of readily available vulnerability scanner tools such as Nessus, Nikto, etc. [12]. These scan the target system to find versions of software services and operating systems for which known vulnerabilities have been publicly disclosed. In addition to the use of scanner tools, the adversary could discover vulnerabilities by querying vulnerability and disclosure databases such as the Open Source Vulnerability Database and the U.S. National Vulnerability Database. For ICS vulnerabilities discovered in field devices, the U.S. Department of Homeland Security maintains the ICS-CERT database [13].

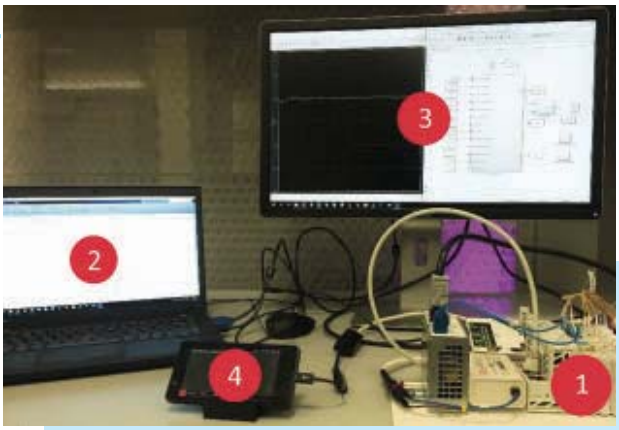


FIGURE 4 Hardware-In-The-Loop setup for studying ICS cyber-security at NYU Abu Dhabi 1) Programmable Logic Controller (PLC), 2) Host computer executing software simulation, 3) Software simulation model, 4) Smartphone used to deploy cyber-attacks.

When known vulnerabilities cannot be found, or the campaign's objectives do not allow their use, 0-day vulnerabilities may be developed. 0-day discovery typically requires highly sophisticated technical analysis. Example methods include fuzzing[2] of network services or hardware equipment, and reverse engineering the firmware[3] of hardware devices. To facilitate the vulnerability discovery step, the attacker could obtain physical copies of the field devices used in the target organization, and replicate the target environment. To avoid the high cost of entire ICS facility replication and the inaccuracy of purely software simulations, a hybrid approach can be followed with Hardware-In-The-Loop testbeds. This setup adopts the benefits of both software simulations and hardware testbeds. At the same time, it enables realistic testing of vulnerabilities and keeps the cost low because of the reduced hardware requirements [14]. **Figure 4** depicts the Hardware-In-

[1] *A 0-day vulnerability is a type of vulnerability that is not reported prior to it being used, effectively allowing the program's authors zero days to create a patch or workaround to counteract it.*

[2] *Fuzzing is an automated or semi-automated method for software testing. During fuzzing, unexpected or random data are provided as inputs to a program. The program is then monitored for exceptions, crashes, or memory leaks indicating the existence of a software bug.*

[3] *Firmware is the intermediate layer between hardware and software, enabling low-level control and communication between the two. Embedded devices typically include firmware.*

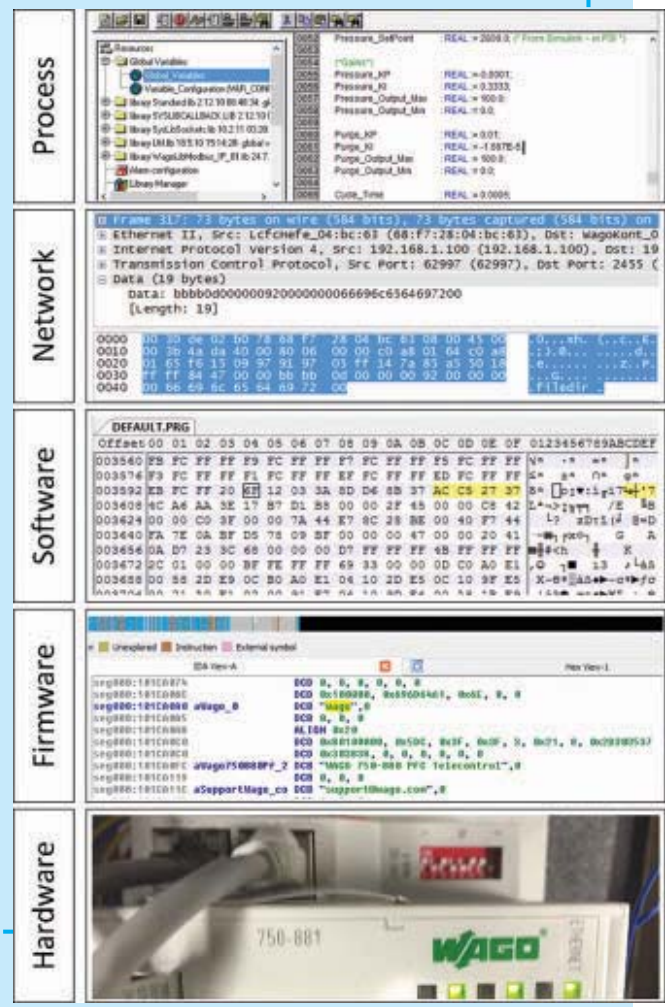


FIGURE 5 **Hardware-In-The-Loop testbeds allow security assessments across all layers of an ICS**

The-Loop setup developed at NYU Abu Dhabi for studying ICS cyber-security. By using this setup, it is possible to perform vulnerability assessments across all different layers that constitute an ICS system – the hardware, firmware, software, network, and process layer (**Figure 5**).

PAYLOAD DESIGN

The cyber-attack's objectives and, by extension, the payload, may change throughout the evolution of a campaign. The payload design step is thus variable and adjusts to the needs and objectives of the campaign. A payload's goal in the initial phase of a campaign may be, for example, to exfiltrate critical data, or strengthen the foothold of the attacker within the target system. At a later stage, the payload may be directed at the field level and aim to change certain operational parameters of the ICS environment. The latter requires an in-depth understanding of the ICS process and the potential presence of interlocks deployed in the system [15]. These types of attacks can be characterized as *process-aware*, since they are cognizant of details specific to the target ICS. By carefully analyzing the information from reconnaissance it is possible to construct a model of the ICS, identify the critical components of a system, and subsequently design a process-aware payload that can introduce arbitrary modifications to the process, including destroying the system [16]. Furthermore, under certain constraints, payloads may be automatically generated [17].

PAYLOAD DELIVERY

Following design of the payload, the attacker can study possible attack delivery mechanisms, including the discovery of exploitation techniques. In the case of known vulnerabilities, it is possible that an exploit already exists and can be readily utilized. Exploitation frameworks, such as

REFERENCES

1 L. Sha, S. Gopalakrishnan, X. Liu, Q. Wang, "Cyber-Physical Systems: A New Frontier," IEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing, 2008.

2 K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, A. Hahn, "Guide to Industrial Control Systems (ICS) Security," NIST Special Publication 800-82 Revision 2, 2015.

3 "Industrial hacking - the untold story," Computer-Weekly.com, August 10, 2015.

4 N. Falliere, L. O. Murchu, E. Chien, "W32.Stuxnet Dossier v1.4," White paper, Symantec Corp., 2011.

5 T. de Maizière, "The State of IT Security in Germany 2014," German Federal Office for Information Security Report, 2014.

6 "Inside the cunning, unprecedented hack of Ukraine's power grid," WIRED, March 3, 2016.

7 G. Locke, P. D. Gallagher, "Managing Information Security Risk: Organization, Mission, and Information System View," NIST Special Publication 800-39, 2011.

8 A. Basta, N. Basta, M. Brown, "Computer security and penetration testing," Cengage Learning, 2013.

9 L. Gordon, "Nmap network scanning: The official Nmap project guide to network discovery and security scanning," Insecure, 2009.

10 R. Bodenheim, J. Butts, S. Dunlap, B. Mullins, "Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices," International Journal of Critical Infrastructure Protection 7, pp. 114-123, 2014.

11 A. Keliris, M. Maniatakos, "Remote field device fingerprinting using device-specific Modbus information", IEEE International Midwest Symposium on Circuits and Systems, 2016

12 "Vulnerability Scanning Tools", Open Web Application Security Project, June 15, 2016

13 "The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)," Department of Homeland Security, 2016.

14 A. Keliris, C. Konstantinou, N. Tsoutsos, R. Baiad, M. Maniatakos, "Enabling Multi-Layer Cyber-Security Assessment of Industrial Control Systems through Hardware-in-the-Loop Testbeds," 21st Asia and South Pacific Design Automation Conference, 2016.

15 M. Krotofil, J. Larsen, "Rocking the pocket book: Hacking chemical plants", DEF CON, 2015.

16 A. Keliris, H. Salehghaffari, B. Cairl, P. Krishnamurthy, M. Maniatakos, F. Khorrami, "Machine Learning-based Defense Against Process-Aware Attacks on Industrial Control Systems", IEEE International Test Conference, 2016.

17 S. McLaughlin, P. McDaniel, "SABOT: Specification-based payload generation for Programmable Logic Controllers." Proceedings of the 2012 ACM conference on Computer and communications security, 2012.

18 "Exploit frameworks", Digital Bond, http://www.digitalbond.com/scadapedia/exploit-frameworks/ Accessed: Nov. 2016.

Metasploit and CANVAS, can be of assistance to the attacker during this step [18]. These frameworks maintain databases of exploits, which they utilize to automatically exploit known vulnerabilities. In the case of a 0-day vulnerability, the attacker needs to develop new exploits. This can include modifying the firmware of field devices, using the network as a payload delivery mechanism (through the internet or the target's intranet), and using techniques to infiltrate and bridge air-gapped networks. Finally, physical devices programmed to automatically deploy an attack may play the role of Trojan horses. Users of the target facility could be tricked to deliver the attack (e.g., by dropping infected USB thumb drives in parking lots), or bribed/extorted to deploy a malicious node within the organization's secure perimeter. An attractive option that can act as a malicious physical implant is a smartphone. Contemporary smartphones incorporate a wide range of sensors, have advanced computational and communication capabilities, and can thus be orchestrated to automatically craft and launch a sophisticated cyber-attack [16].

ATTACK PERSISTENCE

After effective attack vectors have been discovered and verified, secondary campaign objectives may include ensuring and strengthening the attacker's foothold within the target system, increasing the quantity and quality of exfiltrated information, identifying new attack vectors, and developing contingency scenarios to ensure the cyber-attack is carried out successfully. During the attack persistence step, the attacker monitors information from the reconnaissance step and identifies any existing or newly-deployed security mechanisms within the target that can thwart or detect the cyber-attack. Depending on the findings, this could lead to modifying payload delivery mechanisms or payloads to maintain a stealthy presence and avoid attribution, while ensuring fulfillment of the campaign's objectives.

DEFENDING AGAINST ICS CYBER-ATTACKS

By analyzing the design process of an APT for ICS, we gain an understanding of the methodologies, resources, and tools available to threat actors. This information can be utilized to identify weak points of an ICS environment, and generate intelligence that can be used to address these weaknesses and better protect an ICS against cyber-attacks.

As humans are usually the weakest link of a system, personnel working in ICS facilities should be aware of the dangers their system faces from the cyber domain. This knowledge could render them more vigilant, and enable them to identify anomalies in the ICS process that can be indicators of a cyber breach. From a device perspective, strong authentication mechanisms should be used for field devices, and their firmware should be frequently updated. Vendors should promptly develop firmware updates to address known vulnerabilities. In addition, logs of the devices could be audited in a periodic fashion to identify any anomalous behavior. With regards to securing the network infrastructure of an ICS, best practices for network security should be enforced. These could include the use of firewalls, Intrusion Detection or Prevention Systems (IDS/IPS), and network separation between corporate and field networks. Finally, direct routes from the public internet to field devices should not be allowed.

A new field of research for securing ICS relates to process-aware defense mechanisms. These mechanisms analyze information directly from the field and try to detect anomalies specific to the physical characteristics of an ICS process. A unique characteristic of ICS is their cyber-physical nature; thus, effects that originate from cyber domain actions can have observable effects in the physical world. Despite the fact that attackers can alter the behavior of cyber components, they are unable to modify the underlying physical laws that govern these systems. Leveraging this observation, it is possible to design effective defense mechanisms that intelligently draw information from the physical world to detect anomalous behavior and assist in securing our critical infrastructure [16]. ■

ABOUT THE AUTHORS

Anastasis Keliris was born in Larnaca, Cyprus. He received his B.Sc. and M.Sc. degrees in Electrical and Computer Engineering from the National Technical University of Athens in Greece with Honors. Currently, he is a PhD candidate at the Tandon School of Engineering of New York University and is affiliated with the Modern Microprocessors Lab at NYU Abu Dhabi. His research interests include security of embedded systems with a focus on industrial control systems and critical infrastructure.

Michail Maniatakos is an Assistant Professor of ECE at NYU Abu Dhabi and a Research Assistant Professor at the NYU Tandon School of Engineering. He is the Director of the MoMA Laboratory (nyuad.nyu.edu/momalab). He received his Ph.D. in 2012 from the Electrical Engineering department at Yale University. His research interests, funded by industrial partners and the US government, include robust microprocessor architectures, privacy-preserving computation, as well as industrial control systems security. He has authored several publications in IEEE transactions and conferences, holds patents on privacy-preserving data processing, and serves in the technical program committee for various conferences. Michail is currently the faculty lead for the Embedded Security Challenge held yearly at various NYU global sites.

ACKNOWLEDGEMENTS

The authors wish to acknowledge Hossein Salehghaffari, Brian Cairl, Prasanth Krishnamurthi, Farshad Khorrami, and Ramesh Karri for their contributions to the presented work. Part of this work has been supported by the Office of Naval Research (#N000141512182, Program Manager: Sukarno Mertoguno) and the NYU Abu Dhabi Global PhD fellowship.

CYBER-PHYSICAL

BY CDR BRIEN CROTEAU
DEEPAK KRISHNANKUTTY
PHD STUDENTS
UNIVERSITY OF MARYLAND, BALTIMORE COUNTY

The Eclipse Research Cluster at University of Maryland, Baltimore County (UMBC) led by professors Nilanjan Banerjee, Chintan Patel, and Ryan Robucci is seeking to address cybersecurity challenges by employing a diverse set of specialty areas including: Computer Science, Computer Engineering, and Electrical Engineering. This group is looking at leveraging physical relationships to provide diversity of measurement and reporting to not only improve anomaly detection but also make decisions about how to keep critical functions operating even if only in a degraded mode.

Cyber-physical domain attacks can occur at multiple levels of a system hierarchy. This group plans to demonstrate solutions at multiple levels that use physical constraints of a plant or system and expand into non-traditional inputs and measurements to provide heterogeneous surfaces which should be more resilient to traditional cyber attacks. Two systems this article will cover include an IC-level side-channel power monitoring system and add-on trusted sensors for automobiles.

Many of the control systems that regulate our critical infrastructure such as power systems or water treatment have back-end controllers located close to the physical entities they are measuring or controlling. Cárdenas et all, breaks a typical control application into three levels. "In the first layer the physical infrastructure is instrumented with sensors and actuators. These field devices are connected via a field area network to programmable logic controllers (PLCs) or remote terminal units (RTUs), which in turn implement local control actions (regulatory control). A control network carries real-time data between process controllers and operator workstations. The workstations are used in area supervisory control, planning the physical infrastructure setpoints. The higher level is the site manufacturing operations, which is in charge of production control, optimizing the process, and keeping a process history."[1]

The controllers at the lowest level of such a scheme usually contain micro-controller or Field Programmable Gate Array (FPGA) chips that can be reprogrammed to perform maintenance or allow for future upgrades. These also represent a critical vulnerability, in that if an attacker can modify the firmware running on these controllers they can discover much about the rest of the system or possibly launch sophisticated attacks that can be hard to trace back to rogue low-level controllers. One famous example of an attack on a supervisory control and data acquisition (SCADA) system took place against the Maroochy Shire Council's sewage treatment in Queensland, Australia in 2000 where a disgruntled contractor who helped install the system later caused 800,000 liters of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel, killing marine life and turning creek water black with an unbearable stench [2]. This group of researchers at UMBC propose there may be additional measures that can be taken to protect against some attacks like this.

VULNERABILITIES

A critical aspect of a secure system is the identification of system components wherein trust can be established. A common view considers hardware as the workhorse that is driven by software to carry out a specific task (**Figure 1a**), however in reality software exists within a virtual world running inside a hardware layer (**Figure 1b**). All contact that software has to the outside physical world has to pass through and be affected by the hardware layer and smart security designers can use this to measure and limit vulnerabilities.

SECURITY RESEARCH AT UMBC'S ECLIPSE LAB

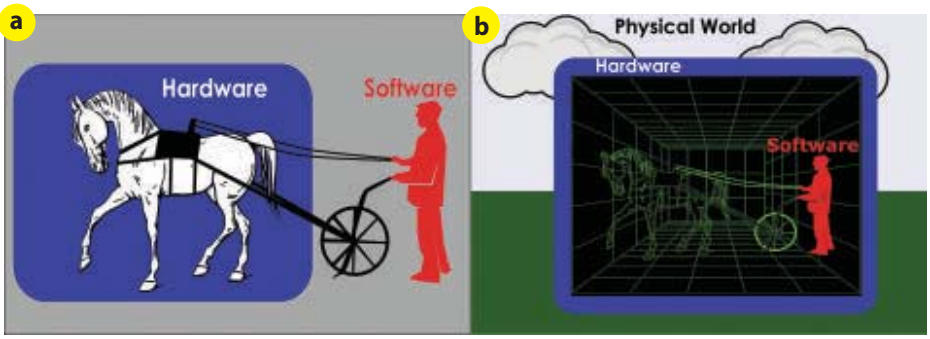


FIGURE 1 Comparison of different views on the relationship between hardware and software: (a) depicts hardware driven by software (b) depicts software running inside the hardware. This group leverages the second view point where hardware forms the interface from software and the outside physical world.

This suggests security should be grounded in hardware.

Vulnerabilities take on many forms; one way to categorize them is to look at which ones correspond to each layer of abstraction for the electronic computing device being studied. As seen in **Figure 2**, at the lowest level, the individual integrated circuits can be subjected to side channel attacks which can use outputs that were never intended by the designers to obtain information about information passing through the chips. They can be subjected to malicious hardware modifications (trojan attacks) during the design and manufacturing process. At the higher level, the various hardware components that are part of the entire system are vulnerable to introduction of counterfeit components as well as other supply chain issues as the system might be put together by multiple untrusted entities. At the firmware layer, there is the potential for back-door vulnerabilities including additional code being inserted or modified during manufacturing or after deployment. At the network layer when several of these devices are connected together, the possibility of some nodes being compromised and needing to counter the injection or flooding of malicious data must be considered.

Many vulnerabilities arise from the increasing globalization of electronics supply chains, wherein components are made, sold, and stored for future use due to current economic realities in the electronic industries. The US Department of Defense has launched an initiative to combat the pervasive growth of counterfeit parts due in large part to how the nature of the electronics manufacturing industry has fragmented with the pressures of a global economy [3]. In 2014 DARPA announced its Supply Chain Hardware Integrity for Electronics Defense (SHIELD) program [4] to invite research into hardware root-of-trust for a cryptographic key enclosed in a physically fragile tiny semiconductor 'dielet' anti-tamper component, that will self-destruct upon any attempts to physically remove, modify, or open it [5]. One promising avenue of verification involves the idea of Physical Unclonable Functions (PUF) which is "the exploitation of inherent and naturally occur-

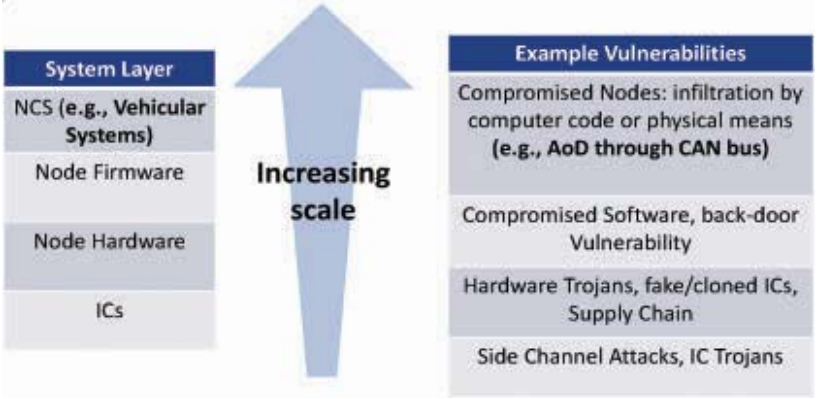


FIGURE 2 Spectrum of vulnerabilities listing examples of how attacks differ depending on what level is targeted.

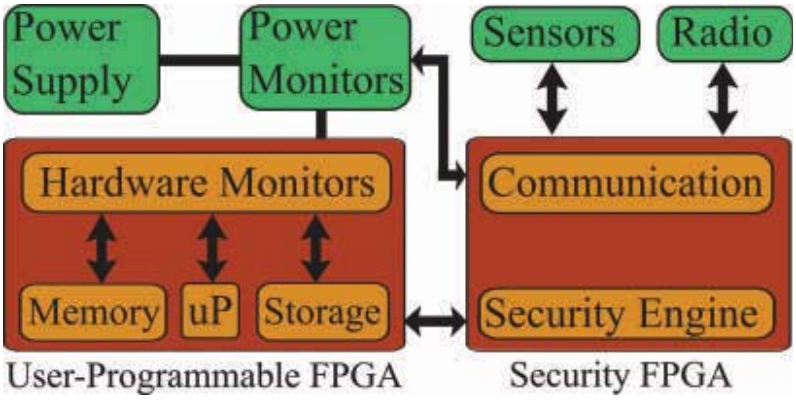


FIGURE 3 Concept of separating user-programmable computing functions from a secure processing core which is harder to modify and controls access to power and communications.

ring physical disorder (fingerprint) of the device as its unique signature, e.g., silicon manufacturing variations. A PUF is a (partially) disordered physical system: when interrogated by a challenge (or input, stimulus), it generates a unique device response (or output)." [6]

Also of primary concern is the globalization of the design chain. A subset of the steps involved in design and production of integrated circuits include the following: Design, Register-Transfer Level (RTL) conversion, Logic Gates synthesis, Scan Chain insertion, Clock Tree insertion, Place and Route layout, IO Pad design, Reticle assembly, Foundry fabrication, Die slicing, Packaging and Delivery. The various steps in producing integrated circuits may take place in far-ranging companies and locations throughout the world.

One approach to tackling these myriad of security issues facing users of programmable devices is to design with strong security measures from the start. A possible concept in this vein, shown in **Figure 3**, is to divide the computing functions of a programmable micro-controller/FPGA into two parts, one that contains the normal code and memory being used and modified regularly and a second that contains security and cryptographic information and would act as a monitor for malicious behavior. The secure core would be harder to re-program and would control access of the main portion to the communication channels to the outside world as well as monitor any information being leaked on side-channels, as described in the next section.

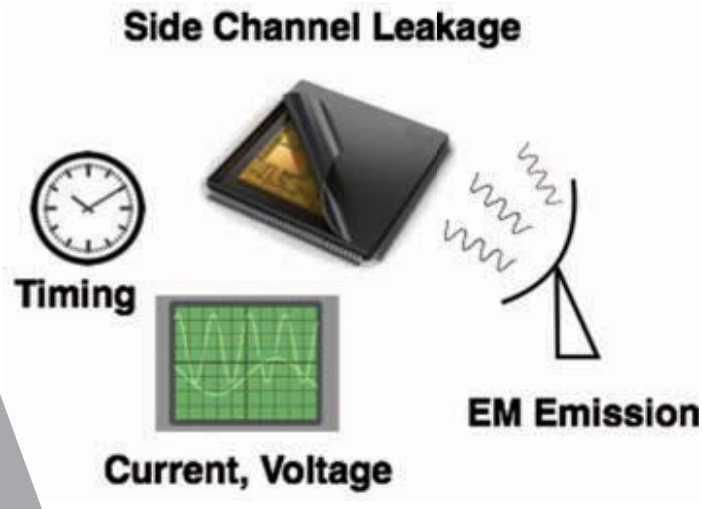


FIGURE 4 Different examples of side channel emissions that can be exploited to gather information about a chip or sensor.

SIDE CHANNEL LEAKAGE ANALYSIS

Side Channel Attacks allow an attacker to extract secret information from a target device by monitoring the power supply, electromagnetic radiation, or timing information of the device. Side-channels are conduits of information (Inputs/Outputs) not intended by designers that exist in a physical system and increase observability in such a way as to compromise security. Simple Power Analysis (SPA) involves direct interpretation of the power supply traces from the operation of interest. Other examples of side channel attacks include: Timing [8], Electromagnetic (EM) [9], Differential fault [10], Scan-based [11], Cache-based [12], Bus-snooping [13], and Acoustic [14]. Side-channel attacks have been proven to reveal the keys of popular encryption ciphers such as the Data Encryption Standard (DES) since Kocher et. al., published the seminal paper [7] on this topic in 1999. For much more background on this topic please read their 2011 update to that original work published in the Journal of Cryptographic Engineering (JCEN) titled "Introduction to differential power analysis" [8] which has an extensive list of references.

Ironically, though side-channels have become popular security exploits, they can also be leveraged to increase security. The next section demonstrates how power supply measurements are physically bound to IC operation and can be used to identify parameters of code execution for validation. This insight is further extended by identifying other physical side-channels in a typical cyber-physical control system and introduce monitors to observe and analyze them alongside the physical signals they are bound to. A vehicular system is used as an exemplary case study for a cyber-physical control system as presented in the subsequent section.

SIDE-CHANNEL POWER MEASUREMENT TESTBED

In the Eclipse lab at UMBC, a custom board (**Figure 5**) was designed and fabricated to measure power-consumption data during software execution. The board

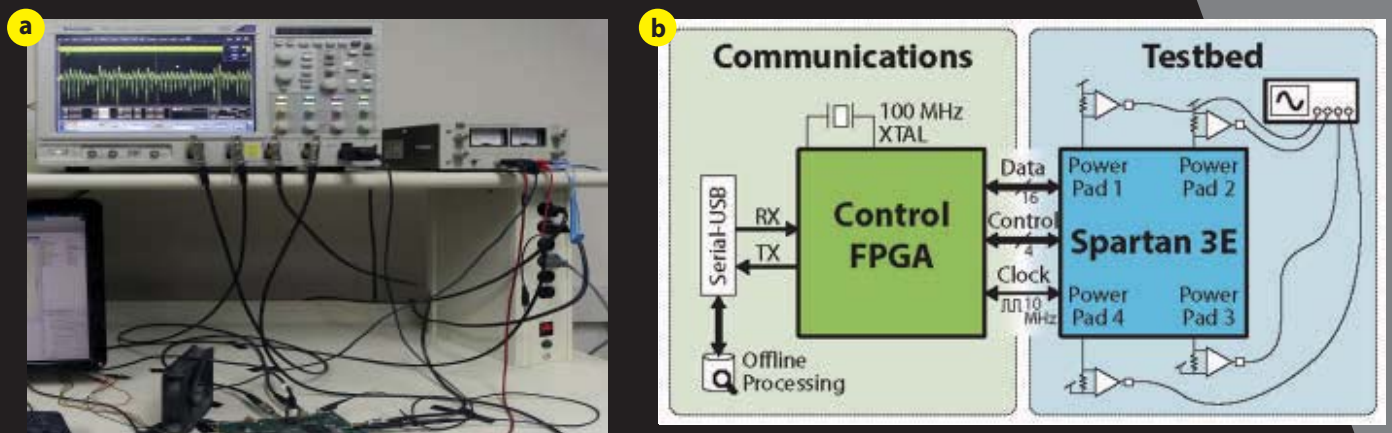


FIGURE 5 (a) Setup of FPGA side-channel power measuring device. (b) System level block diagram showing the relationship between the device under test and the control FPGA.

comprises of one control FPGA facilitating experimentation on a second FPGA, a Xilinx Spartan 3E which is the Device Under Test (DUT) instantiated as an openMSP430 [15] running at a clock-rate of 10 MHz. The control FPGA also functions as the communication device to convey debug and control data to the DUT. Four power-supply pins available on the DUT are used for power supply side-channel analysis by using 1 Ω-resistors in the supply path for each power pin. The voltage across each resistor due to the current consumption of the device is actively probed and amplified on-board and passed through coax cables to four channels on a Tektronix DPO7354C oscilloscope. From there, the data is collected and sent to a PC to be analyzed in custom MATLAB software.

The openMSP430 instruction set consists of instructions that use 1- to 6-clock-cycles per instruction [16]. A training set of power profile measurements was formed by averaging over 20,000 instances of each instruction. **Figure 6** shows the collection of power traces for all the 2-cycle and 4-cycle instructions. One can see that there are some differences between the power traces that can potentially be used to identify which instructions were executed, given a new power measurement.

Each collection of the same clock-cycle instructions was grouped based on hardware utilization, addressing mode (e.g., memory, register), computational operation, and status register updates. For example, all the 2-clock-cycle instructions were broken into three groups: One set involved operations where the source was memory and the destination was a register, second group involved a constant number (immediate memory) being operated on and going to a register while performing a subtraction operation (using the 2's-complement hardware), and the third group was an immediate to register operation without subtraction.

As a first step in matching instructions to a measured power trace, the intent would be to find out what pattern of clock-cycles best approximates the sample. As shown in **Figure 7**, the sampled waveform could be made up of {4,3,2}, {2,6,1}, or {2,3,4} cycle groups. In general, finding the best match is a problem with NP time complexity and thus it is impractical to calculate an exact solution. As an alternative, the UMBC group developed a dynamic programing scheme that uses nearest-neighbor comparisons against the templates to find candidate sequences that best match the input trace [17]. Once the number of clock-cycles is known for each segment, then they can be compared against the templates to find the group of instructions that best matched the trace. In laboratory tests using the FPGA setup, they have demonstrated 72-100% accuracy of matching the correct instruction group.

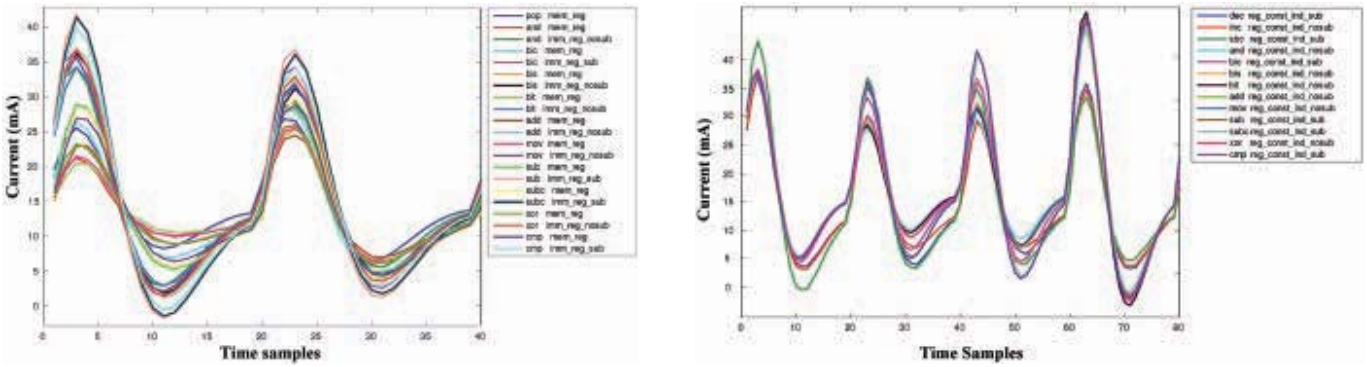


FIGURE 6 Averaged sampled power traces collected grouping 2-cycle and 4-cycle MSP430 instructions.

REFERENCES

1 Cárdenas, Alvaro A., Saurabh Amin, and Shankar Sastry. "Research challenges for the security of control systems." Proceedings of the 3rd conference on Hot topics in security. USENIX Association, 2008.

2 NIST Industrial Control System (ICS) Cyber Security presentation "Maroochy Water Services Case Study", Aug. 2008, http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_briefing.pdf

3 U. S. Senate Armed Services Committee Report:112–167, "Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain", 2012, http://www.armed-services.senate.gov/imo/media/doc/Counterfeit-Electronic-Parts.pdf

4 Bernstein, Kerry. DARPA Broad Agency Announcement DARPA-BAA-14-16 "Supply Chain Hardware Integrity for Electronics Defense (SHIELD)." 2014.

5 Koushanfar, Farinaz, and Ramesh Karri. "Can the SHIELD protect our integrated circuits?." In 2014 IEEE 57th International Midwest Symposium on Circuits and Systems (MWSCAS), pp. 350-353. IEEE, 2014.

6 Hussain, Siam U., Sudha Yellapantula, Mehrdad Majzoobi, and Farinaz Koushanfar. "BIST-PUF: Online, hardware-based evaluation of physically unclonable circuit identifiers." In 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), pp. 162-169. IEEE, 2014.

7 Kocher, Paul, Joshua Jaffe, and Benjamin Jun. "Differential power analysis." Annual International Cryptology Conference. Springer Berlin Heidelberg, 1999

8 Kocher, Paul, et al. "Introduction to differential power analysis." Journal of Cryptographic Engineering 1.1, 2011: pp. 5-27. http://link.springer.com/content/pdf/10.1007/s13389-011-0006-y.pdf

9 Quisquater, J.-J., and Samyde, D., "Electromagnetic analysis (ema): Measures and countermeasures for smart cards. In Smart Card Programming and Security," I. Attali and T. Jensen, Eds., vol. 2140 of Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2001, pp. 200–210

10 Biham, E., and Shamir, A. "Differential fault analysis of secret key cryptosystems." In Advances in Cryptology - CRYPTO '97, J. Kaliski, Burton, S., Ed., vol. 1294 of Lecture Notes in Computer Science. Springer Berlin Heidelberg, 1997, pp. 513–525.

11 Yang, B., Wu, K., and Karri, R. "Scan based side channel attack on dedicated hardware implementations of Data Encryption Standard." In Proceedings of the IEEE International Test Conference (ITC), Oct. 2004, pp. 339–344.

12 Page, D. "Theoretical use of cache memory as a cryptanalytic side-channel." Technical report CSTR-02-003, Department of Computer Science, University of Bristol, 2002.

13 Kuhn, M. "Cipher instruction search attack on the bus-encryption security microcontroller ds5002fp." Computers, IEEE Transactions on 47, 10, Oct 1998, pp. 1153-1157.

14 Asonov, D., and Agrawal, R. "Keyboard acoustic emanations." In 2004 IEEE Symposium on Security and Privacy (S&P 2004), 9-12 May 2004, Berkeley, CA, USA, 2004, pp. 3-11.

15 "MSP430x1xx Family User's Guide," (rev. f) ed., Texas Instruments, http://www.ti.com/lit/ug/slau049f/slau049f.pdf, 2006

16 O. Girard, "openmsp430," http://opencores.org/project,openmsp430, 2016 (accessed March 1, 2016).

17 N. S. Altman. "An introduction to kernel and nearest-neighbor nonparametric regression." The American Statistician, 46(3):175–185, August 1992.

18 D. Krishnankutty, R. Robucci, C. Patel and N. Banerjee (in press). "FISCAL : Firmware Identification using Side-Channel Power Analysis", VLSI Test Symposium 2017

19 Report by staff of U.S. Senator Edward Markey "Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk", 2014, https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf

20 Kulandaivel, S., Schmandt, J., Fertig M, Banerjee, N. Preseentation "Detection and Mitigation of Anomalous Behavior in Embedded Automotive Networks", 2016, http://ur.umbc.edu/files/2016/06/kulandaivelSekarSm.pdf

21 G. Singh, T. A. Chen, R. Robucci, C. Patel and N. Banerjee, "distratto: Impaired Driving Detection Using Textile Sensors," in *IEEE Sensors Journal*, vol. 16, no. 8, April15, 2016, pp. 2666-2673.

For the set of groups listed made from all the 2-clock-cycle instructions, classification accuracy of 100%, 95.3% and 79.4% for the three groups can be achieved [18].

CASE STUDY - USING TRUSTED SENSORS FOR SECURING VEHICULAR SYSTEMS

One application area which has generated a great deal of public interest is the sensor network in a typical automobile generally connected by the aging controller area network (CAN) bus. In 2014, Senator Ed Markey published a report that described the current threats facing modern vehicles and some responses from manufacturers about what steps they were taking to prevent malicious attacks. [19] Using the security monitor concept one could potentially add additional components between vehicle measuring units to control their access to the bus if malicious or abnormal behavior is identified. A UMBC project that involved installing trusted physical sensors to a vehicle is described below.

This initiative [20] installed some additional trusted sensors to an automobile in order to have another signal to compare CAN bus data against to detect and prevent anomalies or attacks. Textile capacitive sensors [21] were installed near the pedals of test vehicles which by using the proximity of the driver's leg to the sensor would provide a measurement of the physical movement corresponding to depressing the brake or accelerator pedal. An inertial sensor was placed on the steering wheel which measured the movement of the steering inputs. The data from these sensors was compared to similar data on the CAN network to corroborate the authenticity of the packets on the CAN bus. If the CAN network is compromised, these additional trusted sensors can act as an out-of-band detector of anomalies. The researchers envision, in near real time, being able to fuse information from the CAN bus and the external trusted sensors to alert the driver to CAN inconsistencies and possibly command an ability to operate in a degraded mode to maintain safe driving, but prevent further malicious behavior. In any case the inclusion of these additional sensors will make it more difficult for attackers to inject false data into the vehicle.

Figure 8 illustrates a potential configuration of an add-on heterogeneous

trusted sensor system in one portion of the vehicular system. The chain links represent physical and cyber interfaces that have bounded relationships. Green arrows represent identified side-channels being analyzed by monitors of security. Yellow arrows represent the aggregate information sent into the security unit. The security unit

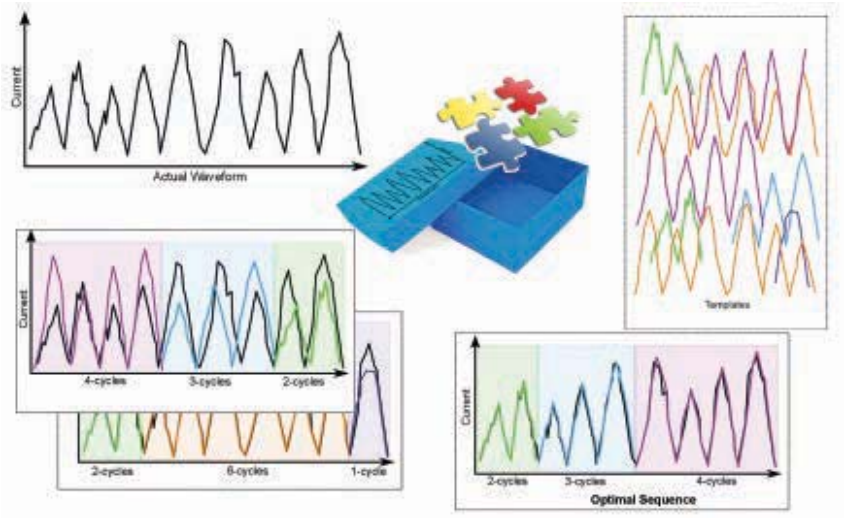


FIGURE 7 Dynamic Programming example. Given an arbitrary waveform one must first map the correct pattern of clock cycle groups before matching individual instructions.

would enforce limitations on components, such as the implementation of a secure core processor described above, in the event of suspicion of attack. By exploiting the physical relationships between pressing a brake pedal and the operator's leg position and the power consumption of a sensor and the instructions being run in it, this group proposes to provide new indicators that can be used to increase resilience to cyber attacks.

This concept describes an example for a small section of a typical vehicle system. This group's future research is seeking to expand this general approach of using the physical relationships of sensors to the properties they are measuring or actuators and the cause or effect of their action. Other potential examples include a microphone to determine if a fan is spinning or an inertial sensor to measure the physical deflection of a steering wheel. These inexpensive add-on trusted sensors will communicate to higher level controllers using out-of-band communication paths, and since they are unlike the nominal sensors it would take much more effort to compromise both as part of a malicious attack. The UMBC Eclipse research cluster (https://eclipse.umbc.edu/) is currently collaborating with several leading academic and government institutions, but continue to seek new potential partners. ■

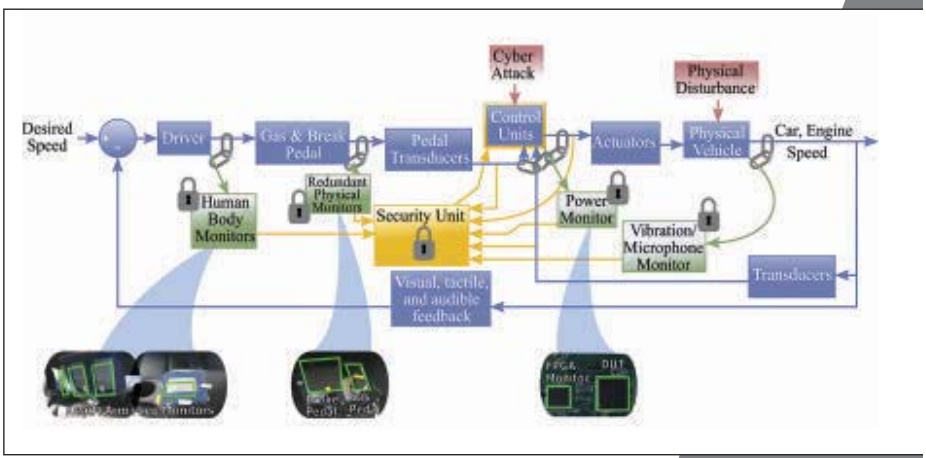


FIGURE 8 Diagram of trusted add-on sensors in a car application. Exploiting the physical relations and using heterogeneous sensors will increase cyber resiliency.

ABOUT THE AUTHORS

CDR Brien Croteau graduated in 1999 from the U.S. Naval Academy with a B.S. in Systems Engineering, completed a M.S. in Control Systems Engineering from Rensselaer Polytechnic Institute in 2000. He served as a Naval Flight Officer for 16 years flying in the EA-6B Prowler and EA-18G Growler aircraft and attended the U.S. Naval Test Pilot School in 2007. In 2016, he was selected to become a Permanent Military Professor and began a Ph.D. program in Electrical Engineering at University of Maryland Baltimore County. After completing that degree, he will join the Cyber Science department at the U.S. Naval Academy. His research interests are in the nexus between hardware security and higher-level control systems applications.

Deepak Krishnankutty received the B.Tech. degree in Computer Science and Engineering from the University of Calicut, Kerala, India, in 2006, and the M.Tech. degree in Computer Science and Engineering (Information Security) from the National Institute of Technology Rourkela (NITR), Rourkela, India, in 2009. In 2013, he joined the Department of Computer Engineering, University of Maryland Baltimore County, as a Ph.D. student after a 3 year stint as a lecturer in Kerala, India. His research interest is in the area of hardware security and its countermeasures.

ACKNOWLEDGEMENT

This work was supported in part by the U.S. Office of Naval Research under Award N00014-15-1-2179.

2017 AMERICAN CONTROL CONFERENCE

Seattle, WA, May 24–26, 2017

The 2017 AMERICAN CONTROL CONFERENCE will be held Wednesday through Friday, May 24-26, at the Sheraton Seattle Hotel in the heart of Seattle, Washington – the most visited city in the Pacific Northwest. The conference venue is near nightlife, restaurants, shopping, and entertainment, just a walk to all of Seattle's known sights such as the Seattle Waterfront, Pike Place Market, Space Needle, Seattle Aquarium, and the Washington State Ferries.

The ACC is the annual conference of the American Automatic Control Council (AACC, the U.S. national member organization of the International Federation for Automatic Control (IFAC)). National and international society co-sponsors of ACC include American Institute of Aeronautics and Astronautics (AIAA), American Institute of Chemical Engineers (AIChE), Applied Probability Society (APS), American Society of Civil Engineering (ASCE), American Society of Mechanical Engineers (ASME), IEEE Control Systems Society (IEEE-CSS), International Society of Automation (ISA), Society for Modeling & Simulation International (SCS), and Society for Industrial & Applied Mathematics (SIAM).

The 2017 ACC technical program will comprise several types of presentations in regular and invited sessions, tutorial sessions, and special sessions along with workshops and exhibits. Submissions are encouraged in all areas of the theory and practice of automatic control.

Details can be found on the conference web site at http://acc2017.a2c2.org

2017 Seattle ACC

TENTH ASME DYNAMIC SYSTEMS AND CONTROL CONFERENCE 2017

DSCC 2017

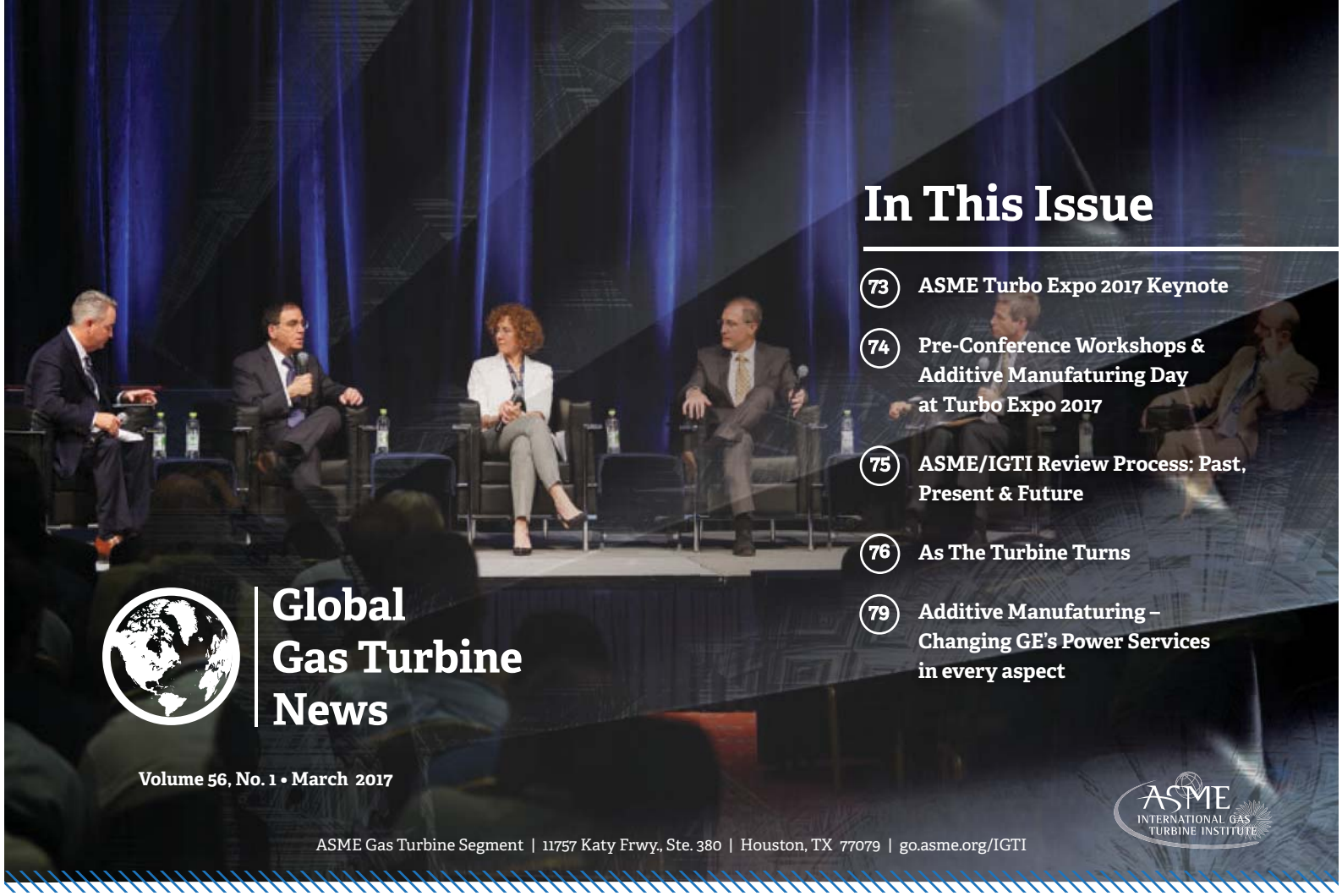
OCTOBER 11-13, 2017
SHERATON TYSONS HOTEL, TYSONS CORNER, VIRGINIA

The DSC Conference, organized and led by the members of the ASME DSC Division, provides a focused and intimate setting for dissemination and discussion of the state of the art in the broad area of dynamic systems and control from theory to industrial applications and innovations in education.

In addition to regular sessions, the conference program will also include contributed sessions, invited sessions, tutorial sessions, special sessions, workshops, and exhibits.

SUBMISSION OF PAPERS FOR REVIEW APRIL 12, 2017

VISIT HTTPS://WWW.ASME.ORG/EVENTS/DSCC FOR DETAILS



Global Gas Turbine News

Volume 56, No. 1 • March 2017

ASME Gas Turbine Segment | 11757 Katy Frwy., Ste. 380 | Houston, TX 77079 | go.asme.org/IGTI

In This Issue

ASME Turbo Expo 2017 Keynote

The keynote panel format, with moderators fielding questions from the audience and posing them to the panelists, was introduced in 2016. This year, we have some exceptionally high-profile industry experts lined up to be the moderators and panelists. Bringing their expertise and experience, they will make this a worthwhile part of the conference. Do not miss your chance to join over 2,000 turbomachinery colleagues, from around the world, who take part in this!

Keynote & Awards Program

"Disruptive Technologies & Accelerating the Pace of Innovation in Gas Turbines"

Monday, June 26th 10:15 a.m. – 12:15 p.m.

Crown Ballroom, Charlotte Convention Center

Graeme Wood said about advertising that "change has never happened this fast before, and it will never be this slow again." Despite approaching its 80th birthday, this could equally be applied to the gas turbine. Technology developments are propelling the industry forward at an ever faster pace, be it in design, manufacturing or maintenance. The theme of the conference will focus on the technologies that are disrupting and accelerating the development of the gas turbine. These include leaps in the areas of multi-disciplinary optimization, advanced manufacturing, automation and digitalization among others. The conference will open with keynote speeches from customers in the aircraft, power generation and oil & gas segments. These industry leaders will introduce their expectations for where technology developments will lead, and how they will help them face their future challenges.

Panelists:

Dag Calafell
Upstream Machinery Chief
Exxon Mobil

Karen Florschuetz
Vice President and General Manager
Americas Operations

Jean-Paul Ebanga
President & CEO
CFM International

Kevin Murray
PMC Engineering & Construction
Duke Energy

Moderators:

Mark Turner
Professor
University of Cincinnati

Paul Garbett
Head of Large Gas Turbine Engineering
Siemens Power & Gas Division

ASME IGTI Student Scholarship Program

The deadline to submit an application is June 15
In the 2017-2018 school year up to 20 scholarships at $2,000 each will be awarded. The scholarship is to be used for tuition, books, and other university expenses. The check will be made out to the university on the student's behalf.

Eligibility of the Applicants
The nominee must be pursuing an academic degree (bachelor's, master's, Ph.D., or equivalent degrees) in an engineering discipline related to turbomachinery. Students must be currently registered at an accredited university (either U.S. or international). The university must have a gas turbine or turbomachinery program.

Download the application and send in one pdf to ASME at igtiawards@asme.org.

The ASME R. Tom Sawyer Award

The R. Tom Sawyer Award is bestowed on an individual who has made important contributions to advance the purpose of the gas turbine industry and to the International Gas Turbine Institute over a substantial period of time. The contribution may be in any area of institute activity but must be marked by sustained forthright efforts. The RTS Award includes a US $1,000 honorarium and a plaque presented during ASME Turbo Expo.

The nomination must be complete and accompanied by three to five letters of recommendation from individuals who are well acquainted with the nominees' qualifications.

The completed reference form from a minimum of 3 people will need to be sent in with the nomination package. It is up to the "nominator" to submit all required information.

Your nomination package should be received at the ASME Office no later than August 15, 2017 to be considered.

ASME IGTI Awards
11757 Katy Freeway, Ste 380
Houston, TX 77079 USA
Email: igtiawards@asme.org

Dilip R. Ballal Early Career Award

An early career award is intended for those starting a professional career, which is typically after a relevant terminal degree: BS, MS, or PhD. A criterion of seven-years-from-degree will be used to define the nominee's eligibility. The nominee must receive the award prior to the completion of the seventh year beyond the terminal degree.

The recipient of the Early Career Award will be presented with the award at Turbo Expo. The award consists of a plaque, funds to support the travel and registration costs to Turbo Expo, free ASME membership registration for five years, and a US $2,000 honorarium.

Nomination packets are due to ASME on or before August 1, 2017. Send complete nomination to: igtiawards@asme.org.

For more information on the ASME IGTI Honors and Awards Opportunities, visit https://community.asme.org/international_gas_turbine_institute_igti/w/wiki/4029.honors-and-awards.aspx.

ASME 2017 Turbo Expo Pre-Conference Workshops

Pre-conference workshops will be held at the Westin Hotel (adjacent to the Charlotte Convention Center) on Sunday, June 25, from 8:00 a.m. to 5:00 p.m. Seize this opportunity to earn 7 Professional Development Hours (PDH's) and receive a certificate of completion. Consider attending one of the workshops and take advantage of the low registration fee. Registration is available online. For detailed information about the workshops visit:
https://www.asme.org/events/turbo-expo/program/workshops

New at Turbo Expo: Additive Manufacturing Day!

Wednesday, June 28
The ASME Gas Turbine Segment and ASME IGTI Committee Leaders and ASME Design Materials and Manufacturing Segment have formed an Additive Manufacturing Day (AM3D) at Turbo Expo to leverage the research that this next generation, strategic technology can provide to the gas turbine industry. For more information visit:
https://www.asme.org/events/turbo-expo/ .

The ASME IGTI Review Process:

Past, Present and Future

by Z. Spakovszky on behalf of the ASME IGTI Review Chair team

The final reviews of 2017 ASME Turbo Expo technical papers are coming to a close,

and the ASME IGTI leadership would like to thank the volunteers for all their time and effort devoted to ASME Turbo Expo. Our conference continues to grow and to convene a worldwide range of gas turbine experts with various backgrounds and cultures. It has become *the* global gas turbine technology event.

A key aspect in keeping the high interest and the reputation is maintaining technical paper quality. This requires effective communication and interaction between authors, reviewers and session organizers, including a shared *responsibility for the integrity of the review chain.* In this document we summarize the past, the present situation, and the vision for achieving this.

Many of you may remember the 'good old days' before the review web tool, when communications were handled by telephone calls, faxes, and postal mail. The Session Organizers had a substantive amount of (literally) paper work: abstracts, requests for reviews, draft papers, reviews, copyright forms, etc. When a paper review was complete, a package was put together and mailed to ASME IGTI. ASME IGTI staff, in turn, went through each package to be sure everything was in order and then forwarded the package to the Review Chair (one person) who did the final reviews. Sending and receiving was not only time and labor intensive, it was subject to mishap and delay.

The observation is that the advent of email and the development of the ASME IGTI web tool have greatly improved the efficiency of the review process. Opportunities exist, however, to further improve the process, review quality, and tools. As one example, prior to the web tool, when pen had to be put to paper, reviewers conscientiously responded to the review questions and one line reviews such as "this is a good paper" were hardly ever seen (who would spend the postage to return an empty form?). The web tool made the process more efficient and more convenient for the reviewers: radio buttons on originality, quality, and so on. have to be toggled and general comments can be optionally entered, but the unanticipated consequence was that the convenience came at the cost of deteriorating review quality.

For last year's ASME Turbo Expo in Seoul, South Korea, a review template was made available as a download from the web tool. The template was recommended, but not mandated, for use by roughly 3,500 reviewers. The idea was to guide the reviewers through the review process with the aim of improving quality and uniformity of the reviews across tracks and committees. The template required the reviewers to answer questions related to relevance, originality, impact and quality of the paper, following G. H. Heilmeier's catechism[1] used by industry, academia and government agencies for evaluating a research project. Most importantly, the template asked for specific statements why the paper was recommended for or against conference and journal publication so that in case of an appeal or objections to the review recommendation the review chain could be held accountable.

Our analysis of the 2016 ASME Turbo Expo reviews showed that 28% of the final papers (305 of 1087) had issues. For papers where the template was followed, the reviews were found to be of higher quality and the likelihood for inconsistency between the final recommendation of the session organizer and the individual reviewers was substantially reduced. This was the case for both conference and journal publication. In addition where there was a conflict between the majority vote of the reviewers and the recommendation of the session organizer or where a journal recommendation was made but not substantiated, the review team contacted the Session Organizers for more information. An overview of the review issues during the 2016 ASME Turbo Expo is given in the table

[1] Dr. G. H. Heilmeier (1936 – 2014) was an American engineering leader. He was one of the inventors of the LCD display and held many leadership positions in industry and government (e.g., Director of DARPA, CEO of Bellcore, VP of Texas Instruments). Among his long list of accolades, he received the 2012 Draper Prize (referred to as the 'Nobel Prize in Engineering') from the National Academy of Engineering.

Continued on page 78

"As the Turbine Turns...."

#29 March 2017

Lee S. Langston
Professor Emeritus
Mech. Engr. Dept.
University of Connecticut

Electric Power and Natural Gas Synergism

As an electrical power producer, natural gas fueled gas turbines driving generators are proving to be the most versatile and effective energy converter of any in the engineer's arsenal of prime movers. Continued research and development have and are making these gas turbine power plants even more effective, flexible and efficient.

Seven years ago [1] I started this quarterly Global Gas Turbine News column with an inaugural piece on the bright future of land-based gas turbines, fueled by natural gas. During the years since, as predicted in this first column, the number and use of these power plants has increased greatly. In 2010 the worldwide value of production (in 2015 US dollars) of electric power gas turbines was $13.5B while in 2015 it was $17.5B, an increase of 30% in five years [2] — and it's still growing.

Also, based on US Energy Information Administration (EIA) data, in 2015, 33% of the US four trillion kilowatt hours of electricity was generated using natural gas, most of which was used in gas turbine plants. Where I live in New England, 40-60% of our electricity currently comes from gas turbine/natural gas plants. The EIA projects that almost 60% of new US electric power generation capacity in the next 20 years will be provided by natural gas fueled gas turbine plants.

Gas Turbine Power Plants

These plants exist in natural gas burning simple cycle or combined cycle (possessing gas turbines whose exhaust powers a steam power plant), using gas turbines with outputs up to 510 MW and thermal efficiencies up to 44%. Combined cycle (CC) plants with a single gas turbine and steam turbine currently have an output as high as 764 MW and a current proven thermal efficiency up to 60-62%. (This proven performance makes CC plants the most efficient heat engines in mankind's thermodynamic history.)

Currently, gas turbine power plants have the lowest capital costs. They range from $700-$1,000/kilowatt, compared to coal-fired steam plants at about $2,000/kilowatt, fuel cell plants also at $2,000/kilowatt and nuclear at $5,000/kilowatt.

Gas turbine plants can operate under either base load operations or in quick start/fast shutdown modes. At my institution, the University of Connecticut at Storrs, we have a 25 MW power plant, fueled by natural gas, with a backup of fuel oil. It has three gas turbines that run in base load operation, supplying campus power (and heat and chilled water) since 2006.

Many gas turbine plants are set to run intermittently, in some cases to start up to full load in a very few minutes. If the wind velocity suddenly dies in a wind turbine farm, a backup gas turbine plant can quickly pick up the grid electrical load. One 100 MW gas turbine plant we have in Waterbury, Connecticut, can quickly go online in late afternoon to take advantage of higher cost electricity rates.

Natural Gas Fuel

Natural gas as a fossil fuel (extensively dealt with by Smil [3]), is composed mostly of methane, CH_4. It is the most environmentally benign of hydrocarbon fuels, with impurities such as sulfur (hydrogen sulfide) removed before it enters pipelines. Methane has the highest heating value per unit mass (21,520 BTU/lbm = 50.1 MJ/kg, LHV) of any of the hydrocarbon fuels (e.g. butane, diesel fuel, gasoline, etc.).

Roughly 40% of the world's electricity is generated in Rankine cycle coal-fired power plants. On an energy input basis, coal produces more carbon dioxide – a greenhouse gas – than natural gas by a factor of about 1.8. In addition, if these coal plants, which operate at about a 30% thermal efficiency, were replaced by gas turbine CC plants at 60%, CO_2 emissions would be reduced by almost a factor of four, resulting in a substantial 75% reduction in CO_2 production [4], for 40% of the world's electricity.

Lastly, the US also has a robust and growing natural gas pipeline system (as long as 14,463 system miles for just the case of the Tennessee Pipeline Company). Pipelines are the most efficient means of bringing fuel to electric power gas turbine power plants. As Smil [3] notes, gas pipelines can have power transmission capacities of up to 10-25 GW. Contrast that to the electrical transmission lines leading away from power plants, where a single line can only have a maximum of 2-3 GW, an order of magnitude lower than that of a pipeline.

Renewables

As we are aware, for over a decade or two, there has been a concerted effort to replace nuclear and fossil fuel generated electricity with renewable sources (e.g., hydropower, wind and solar) that are sustainable and economically viable. Both Denmark and Germany have been leaders in the quest for renewables, using financial subsidies to support and grow renewable electrical generation.

According to EIA data, in 2015 the US generated 87% of its electricity by nuclear and fossil fuels (33% by natural gas), 6% by hydropower and just 7% by other renewables (about 70% of the 7% came from wind and 10% from solar). The EIA projects that this 7% contributed by renewables will grow in the future, especially by wind and solar.

This has led many writers of articles advocating renewables, to assign the role of natural gas fueled gas turbines as a "transitional technology," with an assumption that all or most electrical generation will be taken over by renewables in the future.

This assumption of a gas turbine/natural gas phase-out strikes me as if someone in the early days of the automobile, said that the gasoline powered car was "temporary and transitional," until the electric (or steam) powered car was perfected. When the sun doesn't shine and the wind won't blow, we all know we need reliable on-demand electric power at a reasonable cost. As Alonso, et al [5] point out, averaged over a year, wind/solar systems deliver 25% to 45% of their nameplate production capacity. Thus backup power plants (with rapid startups) or adequate energy storage facilities (which do not currently exist) would have to deliver the remaining 55% to 75% of electricity, based on the renewable nameplate deficit. Seasonal variability is another major impediment that adds to the unpredictability of an all-renewable scenario.

A recent econometric study of renewable electric power implementation was done by Verdolini, et al [6] of 26 OECD countries for 1990-2013. Their conclusion was that the use of fast-reacting fossil technologies (e.g., gas turbines) were more likely to result in the successful investment and use of renewables. The reliable and dispatchable backup capacity of fast-reacting fossil technology (i.e., gas turbines) to hedge against variability of electrical supply, was key to successful renewable use in the 26 countries studied.

Conclusion

As we highlighted in the first "As the Turbine Turns..." in 2010, the use of versatile electric power gas turbines fueled by natural gas will continue to grow in the world. In the US, with recent shale discoveries and fracking of natural gas, such use should increase, with or without the emphasis on renewables.

References

1. **Langston, Lee S., 2010, "A Bright Natural Gas Future", *Global Gas Turbine News*, February, p.3.**
2. **Langston, Lee S., 2016, "Clear Skies Ahead", *Mechanical Engineering Magazine*, June pp. 39-43.**
3. **Smil, Vaclav, 2015, *Natural Gas: Fuel for the 21st Century*, Wiley.**
4. **Langston, Lee S., 2015, "Gas Turbines – Major Greenhouse Gas Inhibitors", *Global Gas Turbine News*, December, pp. 54-55.**
5. **Alonso, Agustin, Brook, Barry W., Meneley, David A., Misak, Josef, Blees, Tom and van Erp, Jan B., 2015, "Why nuclear energy is essential to reduce anthropogenic greenhouse gas emission rates", *EPJ Nuclear Sci. Technol.*, 1, 3, pp. 1-9.**
6. **Verdolini, Elena, Vonda, Francesco, Popp, David, 20916 "Bridgine the Gap: Do Fast Reacting Fossil Technologies Facilitate Renewable Energy Diffussion?", National Bureau of Economic Research, Working Paper 22454, July, <http:/www.nber.org/papers/w22454>.**

ASME IGTI Review Process, continued from page 75.

below (note that several papers had multiple issues so the total does not add up to 305 papers or 28%.).

Review Issue or Inconsistency	No of Papers (%)
Author & reviewer same affiliation:	2 (0.2%)
Less than three reviewers:	7 (0.6%)
Reviewers with same affiliation:	22 (2%)
Journal recommendation issues:	26 (2.4%)
Recommendation conflict between SO and reviewers:	267 (25%)

Table 1: Review data from the 2016 ASME Turbo Expo held in Seoul, South Korea

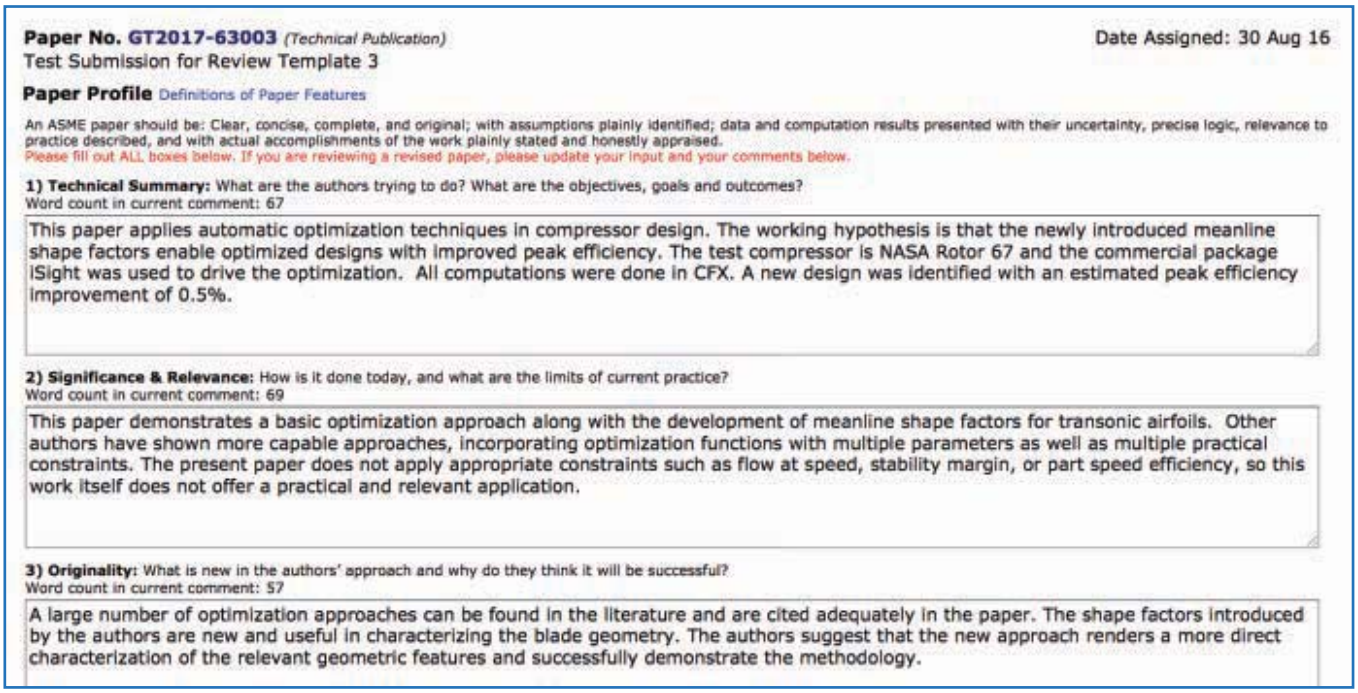
The review template was seen to improve the quality of the reviews in a substantive manner and to have major positive impact on the overall process, and the ASME IGTI leadership strongly supported the modifications to the web tool for the 2017 ASME Turbo Expo in which the review template is now embedded. To guide and to support the review chain in the new process the Review Chair team held a number of webinars and WebEx meetings with the ASME IGTI community. The slides discussed included a checklist for each level in the review chain plus example answers provided as part of the review template. The sample answers for the first three (of eight) questions are shown below in Figure 1, and the full set of slides can be found at **http://www.asmeconferences.org/TE2017/pdfs/ReviewProcessWebinarSlides.pdf.**

Because the ASME IGTI review process assesses journal quality, papers must receive thorough reviews from three independent reviewers, ideally one from academia, one from industry, and one from government. Compared to the time and energy spent by the authors on the research and the paper presentation, receiving a minimum of *200 words that substantiate the recommendations and comments of the reviewer* does not seem too much to ask.

Going forward, we will process the review data for inconsistencies in the same manner as for the past ASME Turbo Expo. We will also determine the impact of web tool changes on review quality. The final paper recommendations for the 2017 ASME Turbo Expo are coming soon and the Review Chair team of four is gearing up to perform final checks of over 1000 papers to ensure each paper was (i) processed properly, (ii) reviewed in a fair manner, and (iii) assessed for acceptance for conference and for any other recommendations following ASME and IGTI standards. Our prediction is that, with the new review template in place, there will be fewer conflicts and issues and the clearly documented reviews and recommendations will benefit both authors and organizers.

Looking further ahead, the ASME IGTI leadership is committed to enhancing the quality of the paper reviews, reinforcing the shared responsibility of the reviewers and session organizers, and improving communication between authors and organizers. We would like to express again our sincere thanks to everybody involved in the review chain and to those who have sent comments and suggestions. We look forward to seeing you in Charlotte this summer.

Figure 1:



Paper No. GT2017-63003 *(Technical Publication)* Date Assigned: 30 Aug 16

Test Submission for Review Template 3

Paper Profile Definitions of Paper Features

An ASME paper should be: Clear, concise, complete, and original; with assumptions plainly identified; data and computation results presented with their uncertainty, precise logic, relevance to practice described, and with actual accomplishments of the work plainly stated and honestly appraised.
Please fill out ALL boxes below. If you are reviewing a revised paper, please update your input and your comments below.

1) Technical Summary: What are the authors trying to do? What are the objectives, goals and outcomes?
Word count in current comment: 67

This paper applies automatic optimization techniques in compressor design. The working hypothesis is that the newly introduced meanline shape factors enable optimized designs with improved peak efficiency. The test compressor is NASA Rotor 67 and the commercial package iSight was used to drive the optimization. All computations were done in CFX. A new design was identified with an estimated peak efficiency improvement of 0.5%.

2) Significance & Relevance: How is it done today, and what are the limits of current practice?
Word count in current comment: 69

This paper demonstrates a basic optimization approach along with the development of meanline shape factors for transonic airfoils. Other authors have shown more capable approaches, incorporating optimization functions with multiple parameters as well as multiple practical constraints. The present paper does not apply appropriate constraints such as flow at speed, stability margin, or part speed efficiency, so this work itself does not offer a practical and relevant application.

3) Originality: What is new in the authors' approach and why do they think it will be successful?
Word count in current comment: 57

A large number of optimization approaches can be found in the literature and are cited adequately in the paper. The shape factors introduced by the authors are new and useful in characterizing the blade geometry. The authors suggest that the new approach renders a more direct characterization of the relevant geometric features and successfully demonstrate the methodology.

Sample answers to review template questions – each text box requires a minimum of 25 words, equivalent to 1 to 2 sentences.

Additive Manufacturing

Changing GE's Power Services in every aspect

Philip L. Andrew | P.E., ASME Fellow

Advanced Manufacturing Works Milestones: faster time to market innovative feature or design.

GE continues to invest in advanced manufacturing. The company sees it as an enabler for the differentiating technologies that are vital to the products its customers need in order to be successful in the power-generation market. As a recent example of this ongoing commitment, GE has invested $73 million to date in its Advanced Manufacturing Works (AMW) and will invest another $327 million across the GE Power Greenville campus over the next several years to drive innovation and foster development of best-in-class technologies that deliver more value for customers across the globe. The Advanced Manufacturing Works serves also other GE units such as Aviation and Transportation.

One mission of the Advanced Manufacturing Works is to bridge technology prototypes from GE's six global research centers and university affiliates into serial production—a typically-arduous journey that has not always been successful in the past and often relegates promising ideas to a perpetual conceptual-design status. The AMW provides for the development of novel production processes for familiar components, or standard production processes for new product features, without

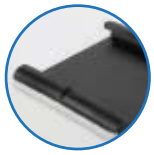
interfering with on-going serial manufacturing activities. An example of the former is the application of additively-printed sand-casting molds for reciprocating engine cylinder heads, incorporating novel, yet complex features that enhance fuel-efficiency. The end product is familiar, but the additive process speeds prototyping of difficult-to-manufacture features, and thus brings performance-boosting products to market sooner.

Rapid prototyping is a well-known means of getting products to the market quickly, but one of the more crucial benefit is in the creation of serial test article prototypes that enable the performance enhancement of products such as hydraulic turbines in a timely fashion. Several prototypes can now be built and tested in the development time period that formerly accommodated perhaps one design iteration. Customers benefit from power-generation products with differentiated performance, driven by optimization and robustness to operational conditions, yet consistent with a Fastworks development mindset.

AMW's Innovation Ecosystem

Another mission of the AMW is to house and facilitate collaborations with suppliers, universities, research labs, and machine tool manufacturers. One such effort is the development of the Laser MicroJet (LMJ) with Synova and Makino for implementing advanced film-cooling holes in turbine blades. Today's film-cooling design enhances gas turbine performance by minimizing required levels of parasitic cooling flow. Instead of machining the cooling holes into the airfoil base metal, then coating with thermal barrier coating, and finally clearing of any overspray, GE has developed an application of the LMJ to carry-out a post-coating laser ablation and drilling process to accomplish all three steps simultaneously, saving cost and cycle time. Film hole locational quality is enhanced by reducing the number of tooling set-ups of a given component. Further, the process enables holes at very shallow angles, enhancing the effectiveness of the film, and thus minimizing the amount of cooling air required.

Inside the AMW, suppliers value the opportunity to showcase their manufacturing technology in each of three, glass-walled pods which combine industrial floor-space with collaborative



engineering design areas. One such pod currently houses a robotics cell where a new mobile robot is being developed to tend to multiple production processes on the factory floor. The robot is co-developed with Clearpath Robotics and GE's Global Research branch in Detroit, Michigan. Locational sensors, GPS, and proximity sensors inform the robot of where it is, and where people are, so that its motion can be slowed or curtailed if encounters become too close. This approach may be one of the first instances where one mobile robot can do the work of several, displaced, stationary robots on the factory floor, while maintaining safety and positional accuracy.

Smart Repair

Behind the three pods, the AMW houses the more-strategic development projects, such as taking ceramic matrix composites (CMCs) to the next application space. GE currently offers CMC stationary shrouds, or ring segments, where the material system has accumulated more than 30,000 hours in the 7FA gas turbine fleet. These shrouds offer an increase of as much as 0.6 percent gas turbine output, up to 0.2 percent in heat rate reduction, and a

Continued on next page.

GE Power in Greenville, continued from previous page.

32,000 Factored Hour/1,250 Factored Start Maintenance Interval. Machining of CMC shrouds is another possible application of the previously-mentioned LMJ technology. Further applications of CMCs under development within the AMW are expected to add 500 ∞F in thermal capability to hot gas path components in addition to shrouds.

Other strategic technologies undergoing the transition to serial production via the AMW include methods of creating advanced cores for investment castings. Additionally, collaborative efforts between the Repair Technologies Center of Excellence team developing advanced creep-sensing technology (trademarked by GE as LIFESIGHT) and the AMW team enable an effective turbine blade conditioned-based maintenance program.

The company also achieved a new advanced manufacturing success resulting from GE and Alstom's combined commitment in "additive manufacturing" technology making the process cost-effective for serial production. An example is a new idea for a fuel nozzle, in which the additive part iterations can be produced in a month, as opposed to a year by conventional investment casting means. The additional design iterations are critical to ironing-out design/manufacturing issues prior to ramping-up to serial production rates. The time from design-finalization to serial-production may also be considerably reduced, from more than a year to several months.

The AMW deals with a wide variety of materials. In addition to additive metal applications and printed sand molds, printed polymer has proved to be invaluable in creating fixturing, especially fixturing compatible with CT scanning used to ensure the dimensional quality of cored components.

Disruptive innovation in Power Services

Last year's acquisition of Alstom Power offers the potential for a leap forward for GE, by combining complimentary technology development leadership from both entities, applicable to a broad range of products. To this end, the Advance Manufacturing Works will play a vital role in integrating the engineers and technologies to incubate the manufacturing technologies required to deliver the next-generation of products counted on by the power-generation industry.

In addition, GE Power Services recently achieved a commercial additive manufacturing and turbine engineering milestone for the energy industry by installing four different 3-D printed components—including the largest components of its kind—in a GE GT13E2 gas turbine at the Heizkraftwerk Berlin-Mitte Power Plant near Germany's capital city of Berlin. The natural gas-fueled district heating station is operated by Vattenfall Europe Wärme AG (VE-W), a subsidiary of Swedish utility Vattenfall AB.

Because these components are made with a lightweight configuration and can be engineered to include cooling channels and other customized features, they help the turbine run more efficiently and burn less gas, representing a new frontier in turbine engineering and production.

The components for Vattenfall's plant included the Combustor Zone 1 Segment, the world's largest 3-D printed part to be installed in a gas turbine. The Combustor Zone 1 Segment, which was manufactured at GE's plant in Birr, Switzerland, weighs 4.5 kilograms (9 pounds) and is the size of a laptop. The other 3-D components —stator heat shields, first-stage turbine vanes and AEV burner front panels—also were manufactured at the Birr facility.

"The installation of the components at Vattenfall's Berlin Mitte station represents a turning point in the global power generation industry," said Wolfgang Mueller, product line E-Class gas turbines leader for GE's Power Services. "We are demonstrating that it is possible to commercially manufacture customized large pieces for turbines in a much shorter period of time while increasing turbine efficiency."

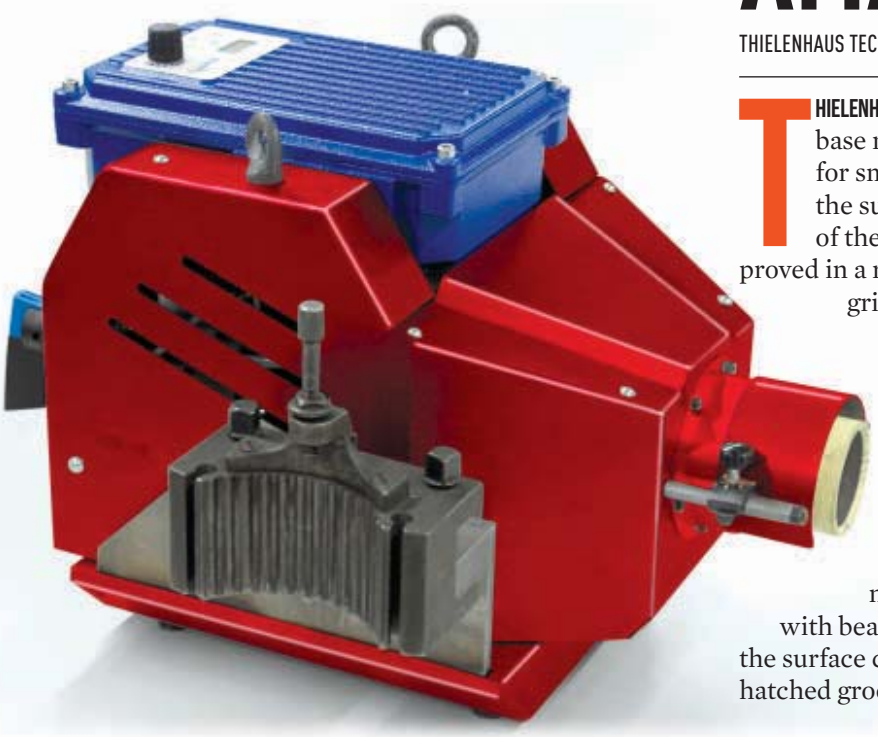
3-D printing creates a new disruptive business model for the global energy sector and marks a turning point in the traditional supply chain value stream, creating new competitive dynamics for the industry.

When the gas turbine's estimated 50 heat shields are 3-D printed instead of traditionally cast, they reduce cooling flow requirements by more than 40 percent, offering operators potentially millions of dollars in fuel-cost savings per year. A gas turbine typically consumes 10 kg of fuel every second and the amount of cooling air required affects the system's efficiency. The first-stage vane is one of the turbine's hottest-running components and its 3-D printed portion offers a 15 percent reduction in the need for cooling air, which is equivalent to approximately $3 million in annual fuel savings.

The Berlin-Mitte Power Plant project resulted from GE's long-term commitment to advancing "additive manufacturing" technology. GE continues to invest in the latest 3-D production systems. GE recently acquired the first commercial M400-4 Laser DMLM machine to be installed worldwide. The system is an ultra-fast quad laser that supports the production of complex metal parts and will significantly enhance GE's additive manufacturing production capacity at the Birr factory.

MICROFINISH ATTACHMENTS

THIELENHAUS TECHNOLOGIES GMBH., WUPPERTAL, GERMANY



THIELENHAUS MICROFINISH NOW OFFERS A RANGE of attachments to base machines for superfinishing applications and for small batch sizes. Those attachments enable the surface, roughness, waviness, and contact ratio of the components being worked on to be improved in a reliable manner using conventional turning, grinding, and milling machines. The attachments consist principally of an electric drive unit for high short-stroke movements and the oscillating tape or stone tool. The workpieces are held in the base machines between centers or, if no centering bore is present, tensioned from one side with a chuck or a collet. Using the attachments, surface roughnesses of Ra 0.01 µm with rolls and Ra 0.3 µm with bearing positions can be achieved. Alternatively, the surface can be given a structure with defined, cross-hatched grooves to improve its tribological properties.

LOAD CELL

STRAIGHTPOINT, HAVANT, UNITED KINGDOM

The Impact Block load cell is manufactured by Straightpoint in partnership with tree safety equipment pioneer DMM. Unlike crane-related or other typical rigging scenarios, in tree applications professionals do not always have an anchor point above the lifting point. If only the stem and canopy of a spruce tree remains, for example, a rope break may have to be attached to the bottom of the tree from where a rope and pulley will connect to the piece being cut. The Impact Block can fill gaps in knowledge about the forces put through rigging equipment and the weight of loads as they are cut away from trees. Utilizing wireless dynamic load monitoring electronics and strain gauge technology, real time data can be displayed on a handheld controller, tablet, or laptop at speeds up to 200 Hz.

TOOL HOLDER

SCHUNK, MORRISVILLE, N.C.

The TENDOturn uses a sealed hydraulic system to enable fast and accurate tool changes while providing the advantages of hydraulic expansion toolholder technology, even with applications on lathes and milling centers. The TENDOturn allows for a versatile clamping range by using intermediate sleeves, and the run-out and repeat accuracy is within 0.003 mm. The system also features vibration damping, which allows users to work at high precision. The company recommends the system for turn/mill centers and mill/turn centers, as well as for CNC rotary transfer centers for drilling, reaming, milling, turning, and thread tapping applications.

HARDWARE

IMAGER

FARO, LAKE MARY, FLA.

The new 9MP version of the Cobalt Array Imager is a higher resolution model of FARO's Cobalt platform. The company says the 9MP version is suited for automotive and aerospace manufacturers, where there is a need to capture fine details and features on edges and surfaces including stamped, machined, or engraved parts. The 5MP version released in 2016 is suitable for users who do not require high-resolution data capture. Both versions feature on-board processing, blue light technology, interchangeable lenses, high dynamic range, and automatic exposure. The company suggests using the 9MP in applications such as quality inspection, factory automation, and in-process verification.

PYROMETER

AMETEK LAND, SHEFFIELD, UNITED KINGDOM

The SPOT Aluminum Extrusion, Quench, and Strip pyrometer provides high accuracy and a three-in-one capability specifically for aluminum applications, including extrusion press exit, extrusion press quench zone, and aluminum strip mills. The pyrometer comes with pre-configured algorithms that make it suitable for use at the mill entry and exit positions in hot rolling mills. In addition, the pyrometer's algorithms can be customized and tuned for bespoke applications and specific aluminum grades. The instrument was designed specifically to work in low-emissivity environments where regular pyrometers might struggle to provide accurate and reliable readings. It has the ability to measure a temperature range from 200 °C to 700 °C and takes advantage of cutting-edge temperature detector design.

HANDHELD SCANNER

THOR3D, MOSCOW

The Drake 3-D scanner is a handheld, wireless system capable of capturing objects both small and large. The body of the scanning system contains a built-in computer, a 7-inch touchscreen, and a battery. Once the device captures 3-D data and compiles it in real time, the data is transferred over to a computer via Wi-Fi or USB for finalization and export. The system uses algorithms that enable the scanner to detect thin plastic walls and sharp edges. The white-light scanner has a minimum resolution of 40 µm, while its "maxi" setting enables the system to scan objects as large as automobiles.

VOICE COIL ACTUATOR

H2W TECHNOLOGIES, SANTA CLARITA, CALIF.

H2W Technologies now offers miniature versions of both its moving-coil and moving-magnet voice coil actuators. The NCM01-04-001-2IB is the company's smallest moving-magnet voice coil actuator, with an outside diameter of 0.40 in. (10 mm) and a length of 0.735 in. (18.8 mm). It has a stroke of 0.10 in. (2.5 mm) and generates a continuous force of 0.10 lbs. (0.45 N) and a peak force of 0.30 lbs. (1.35 N). The NCC01-04-001-1X moving-coil voice coil actuator has an outside diameter of 0.44 in. (11.1 mm) and weighs just 0.20 ounces (5.7 grams), while generating a continuous force of 0.06 lbs. (0.27 N) and a peak force of 0.18 lbs. (0.8 N). The bobbin has been constructed of plastic to prevent any damping forces that a metallic bobbin would create.

SPOOL VALVES

ASCO, FLORHAM PARK, N.J.

ASCO has added to its 362 and 562 Series of brass and stainless steel spool valves by introducing ⅜-inch and ½-inch pipe sizes. The new sizes provide design engineers with additional solutions for control valve automation, especially in the upstream, midstream, and downstream oil and gas markets. The ASCO 362 Series is a three-way valve made for single-acting process valve applications. The ASCO 562 Series is a four-way spool valve designed for double-acting process valves. The 362 and 562 Series valves are available in brass and 316L stainless steel constructions for corrosion resistance in harsh environments, and are offered in both pneumatic and solenoid models. A solenoid option with ATEX and UL hazardous location approvals is available, as are 0.55 W low-power versions.

SUBMISSIONS

Submit electronic files of new products and images by e-mail to **memag@asme.org**. Use subject line "New Products." *ME* does not test or endorse the products described here.

ROTARY ENCODER

LEINE & LINDE, SCHAUMBURG, ILL.

The Leine & Linde 1000 series rotary encoder with speed monitoring capabilities is intended for use in applications where secure speed feedback is critical in order to protect motors, machinery, or operators from risk of failure. The overspeed electronics on the 1000 series consist of a speed-detection system that senses rotational speed and direction. Those electronics control three separate relay switches which can be programmed for identification of critical speeds or errors in direction. In addition, a fourth relay can be set to detect overspeed conditions or be set to detect any functional error in the unit itself. Limits can be set for direction and for over and under speed up to 6,000 rpm.

ULTRASONIC ROTARY POSITIONERS

PI (PHYSIK INSTRUMENTE), AUBURN, MASS.

The U-622 high dynamics miniaturized rotary positioner features an ultrasonic piezomotor for superior positioning while reaching rotational velocities of up to 720° per second. Due to the self-locking ceramic motor, no heat is generated at rest. The U-622 is offered in widths of 20, 30, or 50 mm and heights of 10, 12, or 19 mm, which allows for easy integration into tight spaces of existing applications. With a rotation range of 360° and quiet operation, the stages provide a large dynamic range and are quick to step and settle. The U-62x series comes with integrated, direct-measuring, incremental encoders to ensure resolution down to one-thousandth of a degree and reliable position control and repeatability. Vacuum compatible versions to 10-6 hPa are available.

This free webinar is now available on-demand

MECHANICAL ENGINEERING WEBINAR SERIES

How Digitization Is Changing Manufacturing

Originally broadcast: Feb. 22nd

Tune in today at: https://goo.gl/pg5Fqu

Manufacturing vulnerabilities result in hours wasted troubleshooting, isolating the defect, disassembling to remove the bad parts, waiting for replacements and then reassembling and retesting the products. Frequently even the replacement parts are defective.

Join Beyond PLM's Oleg Shilovitsky, 1Factory's President and Founder Nipun Girotra, and Arena's Senior Director of Solutions Consulting George Lewis for a webinar that discusses how digitization is changing how manufacturers reduce risk, implement change more proactively to lower cost and accelerate time to market.

In this webinar, you'll discover the following:

- How modern cloud-based technologies create a new continuum for digital processes
- The importance of controlling quality at the source—even on the factory floor
- Value of an all-in-one product development platform to streamline product processes

Sign up for this webinar today and discover how you can simplify and speed up quality control tasks from inspection planning to data collection and analysis, enabling engineering, operations and manufacturing to control quality at source.

SPONSORED BY:

arena

SPEAKERS:

OLEG SHILOVITSKY
Entrepreneur and Blogger
BEYOND PLM

GEORGE LEWIS
Senior Director of Solutions Consulting
ARENA SOLUTIONS

NIPUN GIROTRA
President and Founder
1FACTORY

MODERATOR:

CHITRA SETHI
Managing Editor, ASME.org

Tune in today at: https://goo.gl/pg5Fqu

ADVERTISERINDEX

To purchase or receive information from our advertisers, visit the advertiser's website, or call the number listed below.

	PAGE	WEBSITE	PHONE
Arena Solutions	84		
ASME E-Fests	87	efests.asme.org	
ASME Training & Development	27	go.asme.org/pressuretechtraining	
ATI Industrial Automation	19	ati-ia.com/mes	919-772-0115
COMSOL, Inc.	C4, 13	comsol.com/application-builder	
Festo	15	festo.com/us	800-463-3786
Forest City Gear Co.	83	forestcitygear.com	815-623-2168
Omega Engineering, Inc.	7, 9	omega.com	888-826-6342
Proto Labs, Inc.	5	go.protolabs.com/ME7ED	
R+W America, Inc.	21	rw-america.com	
Siemens PLM Software	17	siemens.com/mdx	
Smalley Steel Ring, Inc.	24	smalley.com	
Tormach	25	tormach.com	
WIttenstein	C2	wittenstein-us.com	
Yaskawa America, Inc.	C3	http://budurl.me/YAI1005	800-YASKAWA

RECRUITMENT

Worcester Polytechnic Institute 85

Assistant/Associate/Full Professor, Fire Protection Engineering

The Fire Protection Engineering Program at Worcester Polytechnic Institute (WPI) invites applications for one tenure-track or tenured faculty position at the Assistant, Associate or Full Professor level.

We are seeking individuals who value innovation, creativity, diversity, inclusion and collaboration. Applicants at the tenure track level must show potential for an innovative and sustainable research and teaching career. Applicants at the tenured level must have a demonstrated record of outstanding research, excellent teaching and established leadership. The FPE program expects faculty to be involved in a balance of research, teaching and service.

The successful candidate is expected to have a PhD or equivalent degree in fire protection engineering or a closely-related engineering discipline. The candidate will be expected to develop an externally funded research program and teach graduate and undergraduate courses in and/or related to fire protection engineering alongside faculty from affiliated departments. A successful candidate would have a demonstrated record of accomplishment in a core area of fire protection / fire safety engineering, such as compartment fire dynamics, fire protection systems performance, fire performance of structures, wild land fires, fire risk analysis, or human behavior and fire. Full professors with leadership experience and a combination of academic and professional experience in fire protection engineering are encouraged to apply.

Additional information about the program, faculty, research and facilities can be found at https://www.wpi.edu/academics/departments/fire-protection-engineering

We are an Equal Opportunity Employer and do not discriminate against applicants due to race, color, age, religion, sex, sexual orientation, gender identity, national origin, veteran status or disability. We are looking for individuals who value creativity, diversity, inclusion, and collaboration.

To apply, visit: **http://apptrkr.com/931996**

WPI

EIGHT MEs IN 115TH CONGRESS

WHEN THE 115TH CONGRESS met in Washington, D.C., in January, a dozen members of the Senate and House of Representatives had engineering backgrounds, according to an analysis conducted by ASME's Washington office. Of that dozen, eight had earned degrees in mechanical or industrial engineering.

The mechanical or industrial engineers in Congress are:

Sen. Martin Heinrich (N.M.), *who earned his B.S. in mechanical engineering in 1995;*
Rep. Joe Barton (Tex.), *B.S. in industrial engineering, 1972;*
Rep. Chris Collins (N.Y.), *B.S. in mechanical engineering, 1972;*
Rep. Raja Krishnamoorthi (Ill.), *B.S.E. in mechanical and aerospace engineering, 1995;*
Rep. Daniel Lipinski (Ill.), *B.S. in mechanical engineering, 1988;*
Rep. Thomas Massie (Ky.), *S.M. in mechanical engineering, 1996;*
Rep. Brad Schneider (Ill.), *B.S. in industrial engineering, 1983;* and
Rep. Paul Tonko (N.Y.), *B.S. in mechanical and industrial engineering, 1971.*

Engineers from other specialties in Congress include **Sen. Steve Daines (Mont.), Rep. Tony Cárdenas (Calif.), Rep. Joseph Kennedy, III (Mass.),** and **Rep. Bruce Westerman (Ark.).**

The engineers in Congress represent both political parties.

To learn more about the demographics of the 115th Congress, visit http://www.rollcall.com/news/politics/party-diversity-gap-to-remain-in-115th.

THREE NEW PVP MASTERCLASS COURSES OFFERED IN EUROPE, U.S.

ASME Training and Development will present three new MasterClass courses as part of its Pressure Vessels and Piping MasterClass Series, which will be offered in Denmark, Italy, and the United States this spring.

Presented by a panel of leading PVP and ASME codes experts, ASME's PVP MasterClass Program consists of applications-based courses discussing technologies and codes that establish rules of safety governing the design, fabrication, and inspection of pressure vessels and piping systems.

James C. Sowinski, P.E., a consulting engineer for Equity Engineering Group Inc., is the instructor for "Design-by-Rule Requirements in ASME Pressure Vessel Code Section VIII Division 2." The two-day course is intended to impart practical knowledge and will focus on the design methods found in Part 4, including design loads and load case combinations, design rules for welded joints, and design rules for shells under internal pressure.

A second new course, "Practical Application of ASME Boiler and Pressure Vessel Code Section VIII Division 1," is intended to give participants a better comprehension of the practical application of code rules for the construction and certification of pressure vessels. The class will provide students with a detailed explanation of the requirements for materials, design, fabrication, toughness, examination, inspection, testing, and documentation of pressure vessels.

The instructor, **John P. Swezy, Jr.**, has more than 40 years of experience in steam- and combustion-driven prime mover electrical generation plants and associated engineering auxiliary systems.

"Risk-Based Inspection Planning Using ASME and API Standards" is the third new course being offered this spring.

That two-day course is intended to give attendees a detailed look at the risk analysis principles, guidance, and implementation strategies presented in the ASME Standard PCC-3, Inspection Planning Using Risk-Based Methods, as well as specific requirements from API 581, Risk-based Inspection Methodology.

The course will be taught by **Philip Henry**, P.E., a technical advisor for Equity Engineering Group.

The PVP MasterClass Series will be offered three times during the first half of 2017, beginning in Copenhagen, Denmark, where the series will be held this month, from March 13-17. The courses will also be offered from April 3-7 in Denver, Colo., and from June 19-23 in Milan, Italy.

For more information on the PVP MasterClass Series, visit http://go.asme.org/pressuretechtraining, or contact Jennifer Delda, program/business manager at deldaj@asme.org. ME

ASME BRIEFS CONGRESS ON ROBOTICS

Leaders in the field of robotics briefed members of Congress and their staff on the role of automation in advanced manufacturing during an ASME sponsored briefing in December.

The briefing, "Advanced Robotics in Manufacturing," was introduced by **Sen. Chris Coons** (Del.), co-chair of the Senate Manufacturing Caucus, and ASME President **Keith Roe**. **Chuck Thorpe**, senior vice president and Provost of Clarkson University and co-chair of the ASME Robotics Public Policy Task Force, was the moderator. Thorpe suggested that, contrary to widespread opinion, new robotics technologies are encouraging new skills and new jobs to form, especially for mechanical engineers.

One of the panelists, **Erik Nieves**, the founder and CEO of PlusOne Robotics, said that most manufacturing companies that employ robots today engage in repetitive, high-volume production. The next frontier for automation, Nieves suggested, is low-volume production. ME

ASME E-Fests™

For more information on our global E-Fest events, visit
efests.asme.org

THE place to PARTY LIKE AN ENGINEER!

The latest in Innovation & Technology

Design, Advanced Manufacturing, Robotics

+

Next-gen change-makers

+

Engineering Students

A Festival

Enjoy performances, music, food and loads of fun, while meeting new people!

= E-Fests

What are ASME E-Fests?

Three-day, two-night regional events built around design, advanced manufacturing and robotics technologies. They enable engineering students to expand their knowledge, test and showcase new skills and inspire innovation.

What's part of the E-Fest Program?

- ASME Competitions
- TED-style Talks on cutting edge engineering developments
- Career briefs + mentoring
- Career development events – Professional skill development and leadership training with a practical twist
- Roundtables + networking – Students team up on fast-paced brainstorming, engineering mini-challenges, hackathons, networking events, etc.

E-Fest Asia Pacific
March 3-5, 2017
LNM Institute of Information Technology
Jaipur, India

E-Fest West
March 17-19, 2017
University of Nevada
Las Vegas, Nevada

E-Fest East
April 21-23, 2017
Tennessee Tech University
Cookeville, Tennessee

ASME SETTING THE STANDARD

The American Society of Mechanical Engineers® (ASME®)

SOUND ENGINEERING

Students build musical instruments and learn mechanical engineering.

What happens when you set a college engineering class loose to invent and build musical instruments? If a Tufts University course is any indication, you get some odd contraptions—but sure enough, they make music.

In the course last year, taught by postdoctoral fellow Aaron Johnson, students built a Rube Goldberg-esque marimba that rolls steel marbles down tracks and drops them onto wood bars with a clunk, an eerie-sounding guitar that no human plucks or picks, and a bagpipe made from PVC tubing and balloons.

Mechanical engineering, physics, and music majors in the class, titled The Science and Engineering of Music, studied the creation, characterization, and perception of musical sounds. They worked in multidisciplinary groups of three, one from each major, to create unique musical instruments. "We get peer-to-peer learning, which means we have 20 teachers in the classroom instead of one," Chris Rogers, Tufts' chair of mechanical engineering, said.

Johnson played the saxophone growing up, and most of his students played an instrument as well. In the class, he taught students the physics of music. For example, students were asked to compare the frequency spectra of different musical instruments, then answer, "How does that influence the sound of a bassoon versus a cello versus a trumpet?"

Students also applied acoustic theory in labs, where they made a monochord (a single-stringed guitar) and a PVC flute. The guitar's vibrating string closely matched its mathematical model, but the flute's air column, not so much. "The students had some difficulty with that, but I wanted them to see that we made a lot of assumptions in the theoretical model—things that actually come into play in a real flute," Johnson said.

As a final assignment, Johnson challenged the teams to make an instrument that sounds cool and was easy to play. One team built a bagpipe by stretching balloons over the end of several sets of concentrically-bonded PVC tubes. The balloons vibrate as the air flows past them to produce sound.

"The physics student was always modeling the air flows, and I was thinking about the ergonomics—how the user would play it," Matthew Mueller, the engineer on the team, said. But when theory didn't work to locate and size the finger holes on the "chanter," the pipe you play, the music student saved the day. He did it by ear, just guessing and checking.

In the end, the bagpipe's higher-pitched chanter resembled a pleasant-sounding woodwind. The bagpipe's lower-pitched drones were another story, Mueller said: "Foghorn wouldn't be far off."

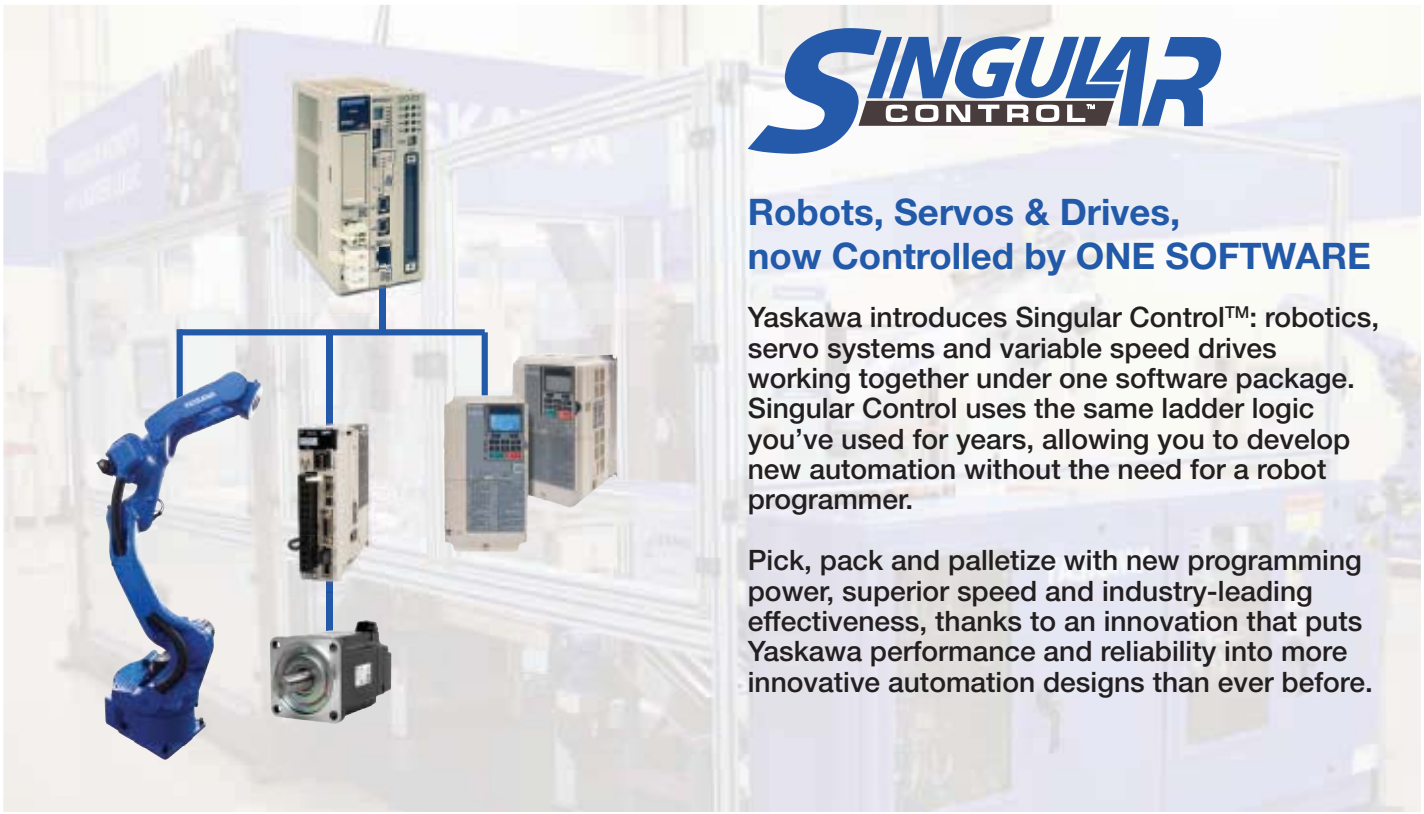
Although none of the course projects are likely to stand in for a Fender Stratocaster or Amati violin, the class did gain a new understanding and appreciation of the instruments they played growing up—and of the many ways to make music. ME

This marimba replaces mallets with steel balls. *Photo: James G. Skakoon*

JAMES G. SKAKOON is a retired mechanical design engineer and a frequent contributor.

YASKAWA

ONE FOR ALL



SINGULAR CONTROL™

Robots, Servos & Drives, now Controlled by ONE SOFTWARE

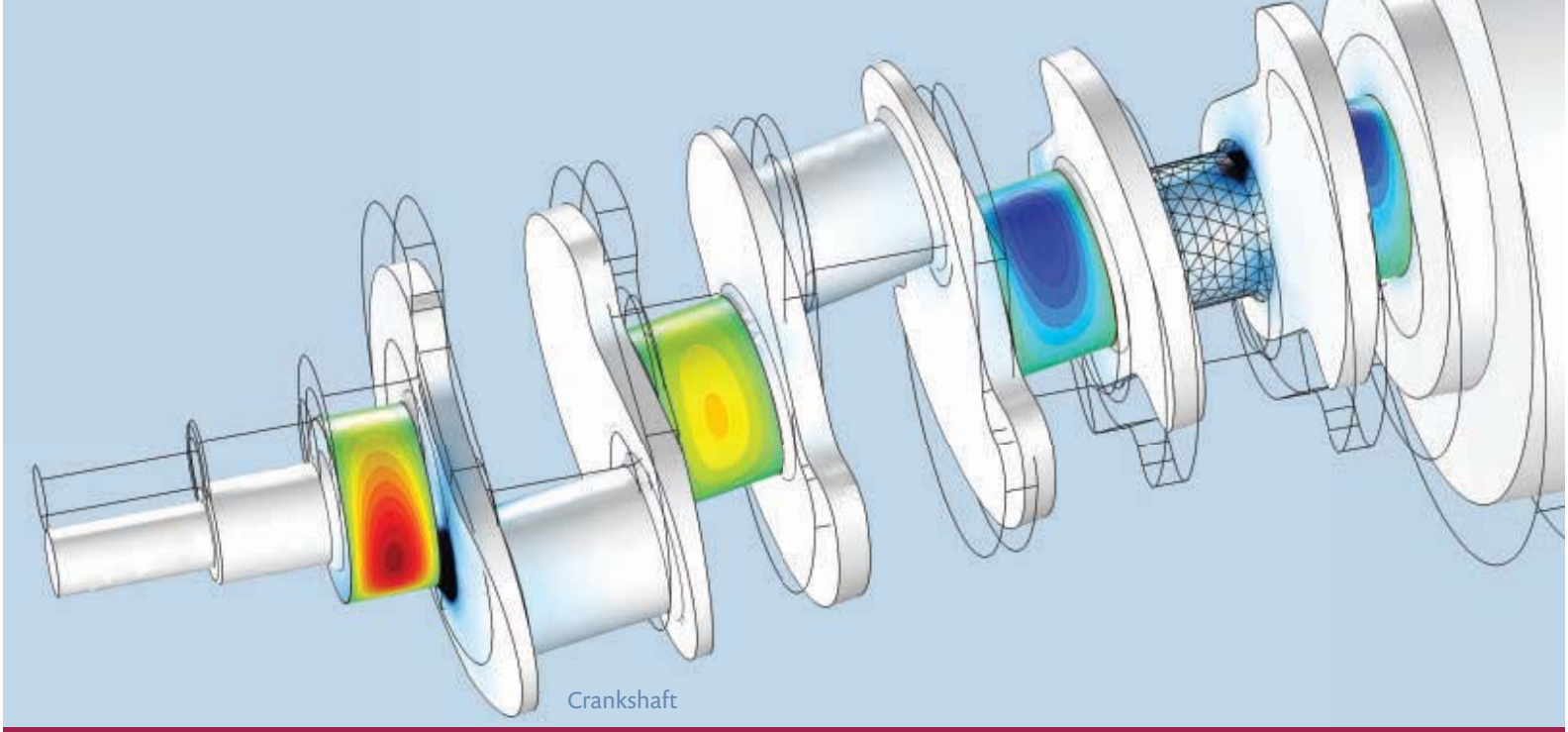
Yaskawa introduces Singular Control™: robotics, servo systems and variable speed drives working together under one software package. Singular Control uses the same ladder logic you've used for years, allowing you to develop new automation without the need for a robot programmer.

Pick, pack and palletize with new programming power, superior speed and industry-leading effectiveness, thanks to an innovation that puts Yaskawa performance and reliability into more innovative automation designs than ever before.

For more info:
http://budurl.me/YAI1005

IT'S PERSONAL
YASKAWA

YASKAWA AMERICA DRIVES & MOTION DIVISION YASKAWA.COM **1-800-YASKAWA**



Crankshaft

MULTIPHYSICS FOR EVERYONE

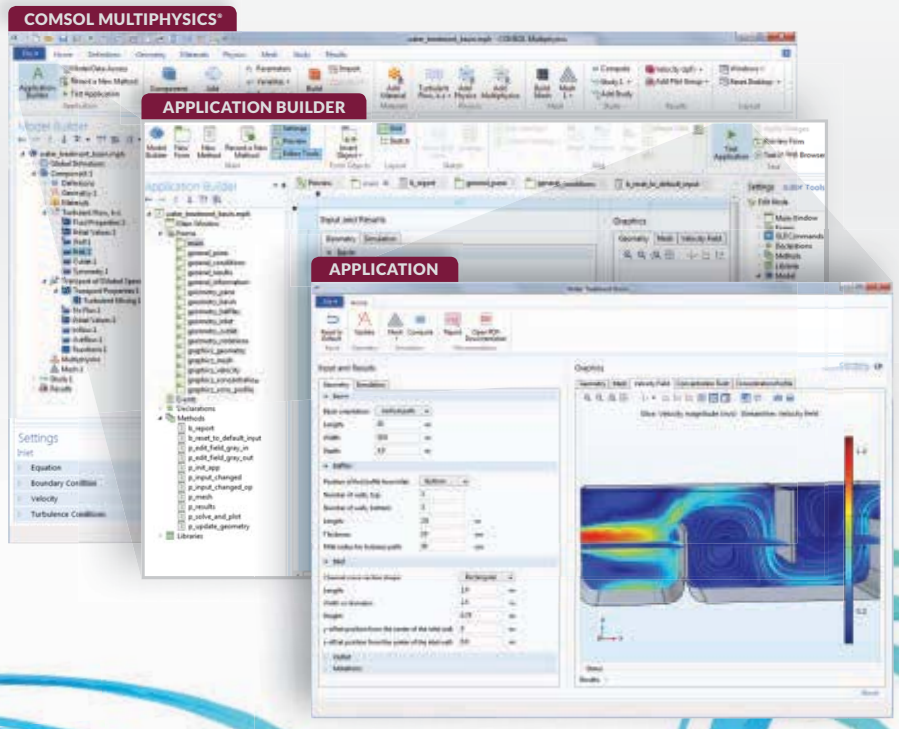
The evolution of computational tools for numerical simulation of physics-based systems has reached a major milestone.

Custom applications are now being developed by simulation specialists using the Application Builder in COMSOL Multiphysics®.

With a local installation of COMSOL Server™, applications can be deployed within an entire organization and accessed worldwide.

Make your organization truly benefit from the power of analysis.

comsol.com/application-builder



Water treatment basin

COMSOL