Wavelengths

IEEE Southeastern Michigan
Electrical and Electronic Engineers Creating Our Future

Volume 64 – Issue 7

Contents

Upcoming Events

We have several events coming up this month, all are listed below, FYI.
Note: All times are EST/EDT. If any events are missed do kindly bring them to the attention of wavelengths@ieee-sem.org. Enjoy!
You can also use this bookmark to view All of the links at a single glance
http://bit.ly/sem-upcoming

Event	Date	Time
Southeastern Michigan Computer Society Chapter Monthly Admin Meeting	01 July 2024	2000 hrs
SEM Life Members Affinity Group - Admin Meeting	08 July 2024	1200 hrs
Keys to Successful Team Building	08 July 2024	1200 hrs
Distinguished Speaker Ron Arkin: "Lethal Autonomous Robots and the Plight of the Noncombatant"	08 July 2024	1700 hrs
Careers in Technology Summer Series 2024 - Amanda Alfaro - Leading Development Teams: An Agile Journey	09 July 2024	1900 hrs
Transmission Planning for Renewable Energy and Load Growth	10 July 2024	1800 hrs
Ch8: AdCom Teleconference : Southeastern Michigan Section Chapter, EMC27	11 July 2024	1100 hrs
Southeastern Michigan Section ExCom Monthly Meeting (virtual) For JULY 2024	11 July 2024	1830 hrs
Nikola Tesla: Documentary	12 July 2024	1800 hrs
Technical Activity Committee (TACom) Monthly ExCom Meeting	15 July 2024	1800 hrs
Careers in Technology Summer Series 2024 - Lou Gullo - Reliability Engineering	16 July 2024	1900 hrs
Southeastern Michigan Section Senior Member Elevation (a Virtual Event!)	20 July 2024	0900 hrs
Careers in Technology Summer Series 2024 - Arun Vishwanathan - TBD	23 July 2024	1900 hrs
Engineering Pioneer - Frank Sprague: Documentary Night	25 July 2024	1730 hrs
Careers in Technology Summer Series 2024 - Paul Carney - Unlock Your Business Potential with AI	30 July 2024	1900 hrs

Chair's Column

What to look forward to this month of July:

- Despite it being now the main summer season, we have a lot of events to look forward to. But before we plunge into those details, a look back at June. We had a total of 18 reported events (compared to 16 in May), What stood out – is how our events are attracting the keen interests of other sections and regions! I think all of our Southeastern Michigan community should be proud of this and step forward to continue raising the profile of the section and its various chapters. See the graphic charts on our YTD performance and in the TACom report.
- We recently hosted yet again 1 more Distinguished speakers – this time the topic was "Why software fails and why AI cannot help", by Dr David Fisher (retired) from Carnegie Mellon University. It was attended by over 35 persons, with lots of Q&A. Let me know if you wish for a copy.
- We co-hosted the AVS Michigan Chapter's annual symposium.
- The New Magnetics Society kicked off their events.

- ***SAVE THE DATE (2024-09-21)!*** ***The IEEE is now 140 years old.*** We have an active volunteer planning committee going. The venue has been decided – it is the Wright Museum of African American History in Detroit, Michigan. You can look up details about this at https://thewright.org . We are still open to other ideas on the celebration program. We have invited several IEEE leaders and a speaker from the IEEE History center. They will share a lot about the IEEE and our contributions to society. In addition we will have member awards and recognition, a sumptuous dinner, museum tour and memorable eclectic entertainment. Send your suggestions/ideas/emails to 140@ieee-sem.org

Volunteering:

- We, IEEE Southeastern Michigan Section, function based on the work of our volunteers. If someone has important obligations that reduce their ability to volunteer, other volunteers need to step in and carry the load. The more volunteers we have, the easier the workload on everyone. Please volunteer, you will find the experience interesting and rewarding.

What to look forward to:

- We have a ton of activities planned in JULY
- Look for the flyers in this issue, but to list a few:
- Several highly acclaimed documentaries (with a few new ones too!):
    - Nikola Tesla
    - Frank Sprague
    - Lord Kelvin and
    - Rachel Carson – Author of Silent Spring

You can find ALL the other upcoming events using the short URL link: **https://bit.ly/sem-upcoming**

Remember – every little bit helps, and the Section is here to help! If you have not taken the opportunity, do reach out to any of the Section officers (lifelong email contacts listed below). Who knows what unknown but immense value you may discover, by simply connecting with us. A possible membership annual rate discount, OR an upcoming soft skills event OR need of a professional member for a technical person resource OR opportunity to participate in a standards making process OR a chance to mentor a young graduate student in a domain badly needed in our section of the world OR network with a book publisher OR….the possibilities are limited only by your enthusiasm.

Finally, I ask you to help share news about our IEEE Section to fellow engineers. This will help us fulfill the mission and goals, which is to use technology to help society. Do help us gain more visibility – word of mouth, invitations to our tech events, skills, join as members, post our events to your social media feeds, etc.

Also of note – we take a great deal of interest in our members welfare. The ***4th senior member elevation*** event is taking place soon (July 20th). See the flyer in this issue. Note we have been timing these 3 weeks before each A&A panel meeting!

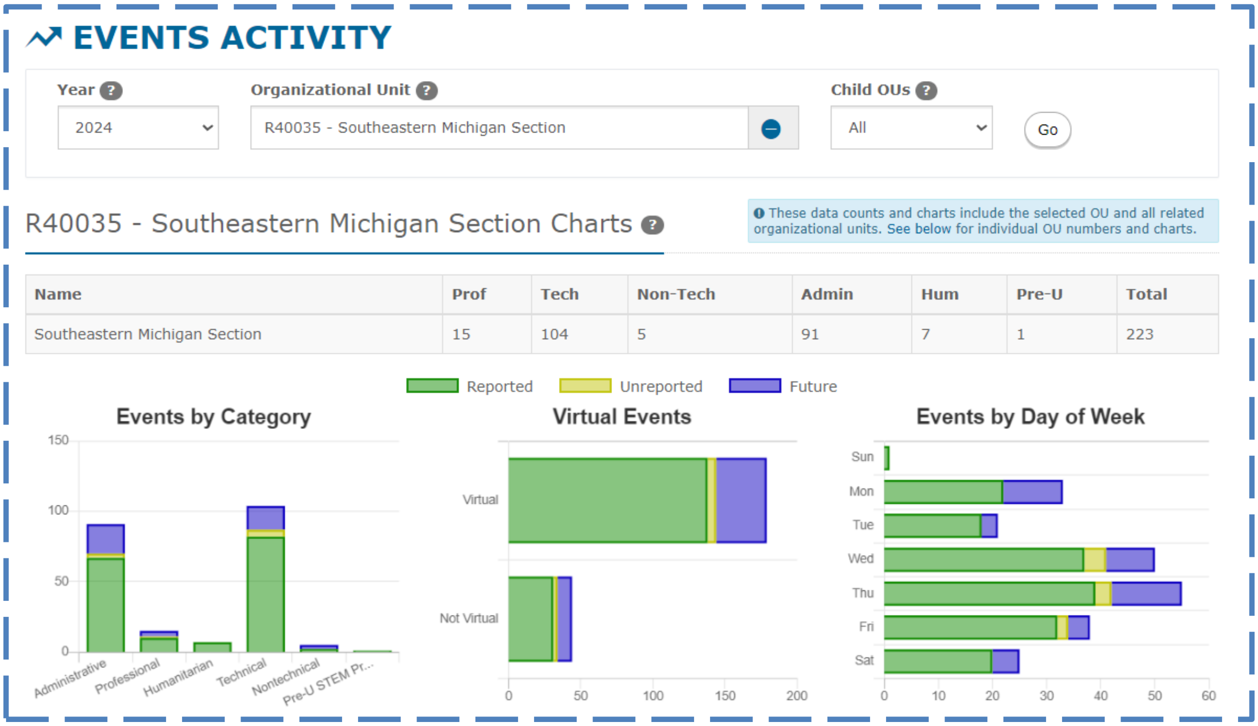
I look forward to hearing from you and seeing you at our events. As always, your ideas and suggestions are encouraged and welcome. If I don't hear back (good or bad) I will assume all is well 😊

Sharan Kalwani
Via email: chair@ieee-sem.org

Section members are encouraged to engage using ***any*** *of these online platforms:*

To reach any of our SECTION officers, for any help/assistance you seek you may try these easy to remember email addresses. The objective is to ensure business continuity, so one need not try to remember or hunt for the contact information! They can help you find your chapter officers or point you in the right direction for any query. They are:

🕮 Chair is	chair@ieee-sem.org
🕮 Vice Chair is	vicechair@ieee-sem.org
🕮 Treasurer is	treasurer@ieee-sem.org
🕮 Secretary is	secretary@ieee-sem.org
🕮 Advisor is	advisor@ieee-sem.org



EVENTS ACTIVITY

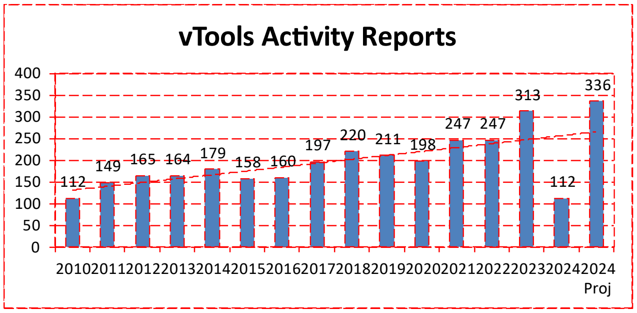
Year ? 2024 | Organizational Unit ? R40035 - Southeastern Michigan Section | Child OUs ? All | Go

R40035 - Southeastern Michigan Section Charts ?

These data counts and charts include the selected OU and all related organizational units. See below for individual OU numbers and charts.

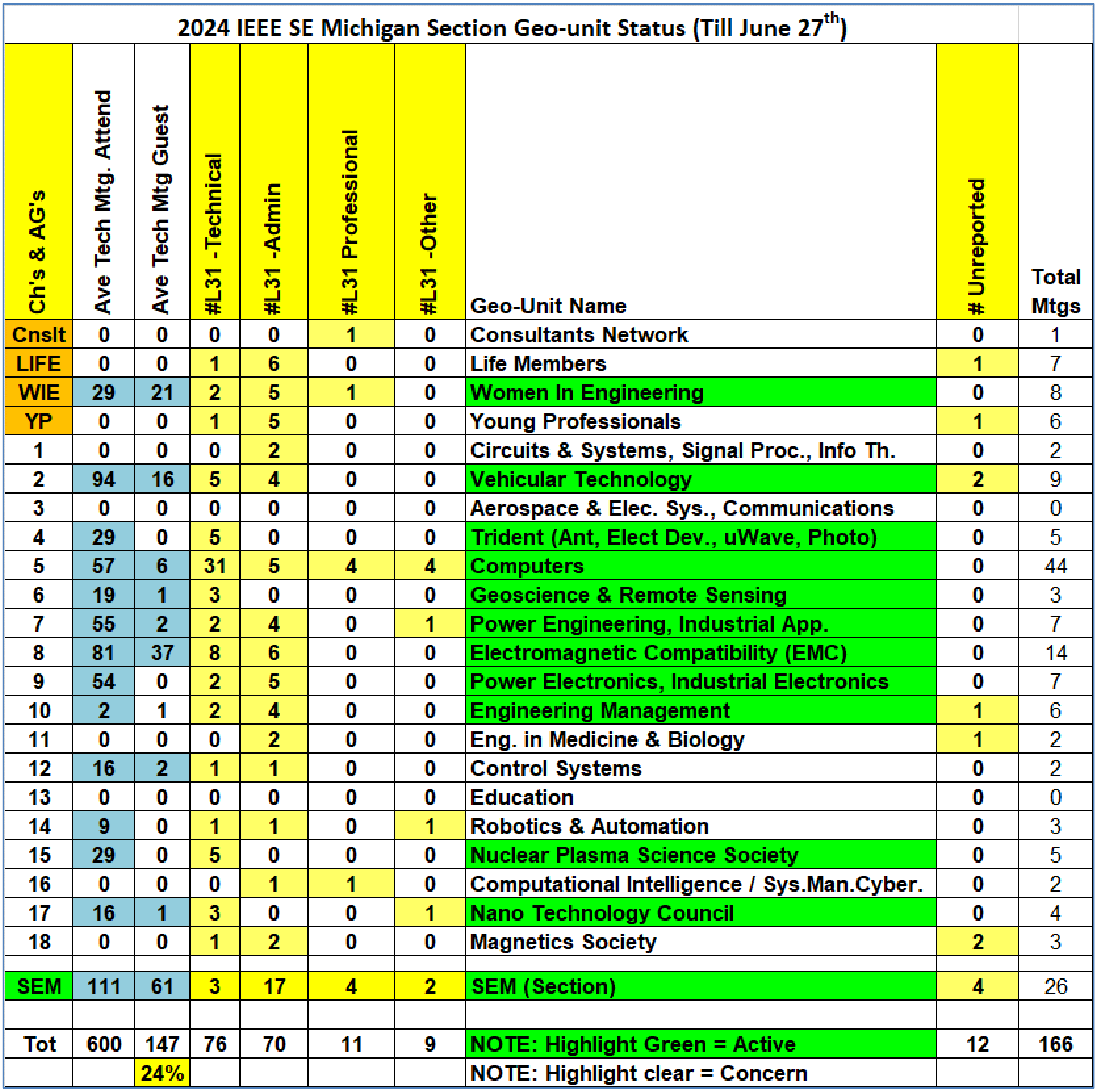
Name	Prof	Tech	Non-Tech	Admin	Hum	Pre-U	Total
Southeastern Michigan Section	15	104	5	91	7	1	223

🕮 140th event celebration team: 140@ieee-sem.org



Events tracking (YTD)

Tech Activities REPORT



2024 IEEE SE Michigan Section Geo-unit Status (Till June 27th)

Ch's & AG's	Ave Tech Mtg. Attend	Ave Tech Mtg Guest	#L31 -Technical	#L31 -Admin	#L31 Professional	#L31 -Other	Geo-Unit Name	# Unreported	Total Mtgs
Cnslt	0	0	0	0	1	0	Consultants Network	0	1
LIFE	0	0	1	6	0	0	Life Members	1	7
WIE	29	21	2	5	1	0	Women In Engineering	0	8
YP	0	0	1	5	0	0	Young Professionals	1	6
1	0	0	0	2	0	0	Circuits & Systems, Signal Proc., Info Th.	0	2
2	94	16	5	4	0	0	Vehicular Technology	2	9
3	0	0	0	0	0	0	Aerospace & Elec. Sys., Communications	0	0
4	29	0	5	0	0	0	Trident (Ant, Elect Dev., uWave, Photo)	0	5
5	57	6	31	5	4	4	Computers	0	44
6	19	1	3	0	0	0	Geoscience & Remote Sensing	0	3
7	55	2	2	4	0	1	Power Engineering, Industrial App.	0	7
8	81	37	8	6	0	0	Electromagnetic Compatibility (EMC)	0	14
9	54	0	2	5	0	0	Power Electronics, Industrial Electronics	0	7
10	2	1	2	4	0	0	Engineering Management	1	6
11	0	0	0	2	0	0	Eng. in Medicine & Biology	1	2
12	16	2	1	1	0	0	Control Systems	0	2
13	0	0	0	0	0	0	Education	0	0
14	9	0	1	1	0	1	Robotics & Automation	0	3
15	29	0	5	0	0	0	Nuclear Plasma Science Society	0	5
16	0	0	0	1	1	0	Computational Intelligence / Sys.Man.Cyber.	0	2
17	16	1	3	0	0	1	Nano Technology Council	0	4
18	0	0	1	2	0	0	Magnetics Society	2	3
SEM	111	61	3	17	4	2	SEM (Section)	4	26
Tot	600	147	76	70	11	9	NOTE: Highlight Green = Active	12	166
		24%					NOTE: Highlight clear = Concern		

SEM Section Chapter and Affinity group leaders who are not showing any technical or administrative meetings are encouraged to reach out to the TAcom for assistance. We are in a new year within the Section where we plan to exceed our projections for technical meetings hosted for our membership. Thanks to all GAs working to engage their membership.

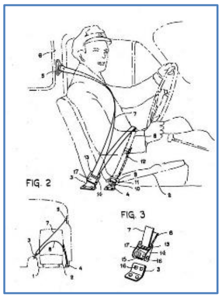
V/r Jeffery V. Mosley
Chair, Technical Activities Committee (TAcom)
jvmosley@ieee.org
Southeastern Michigan Section, IEEE Region 4

This Month in July

Or: Notable Events in Engineering & Science History, which I Did Not Know! ☺

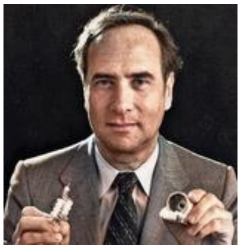
Rube Goldberg; Born 4 Jul 1883; died 7 Dec 1970 at age 87.
American cartoonist who satirized the American preoccupation with technology. His name became synonymous with any simple process made outlandishly complicated because of his series of “Invention” cartoons which use a string of outlandish tools, people, plants and steps to accomplish everyday simple tasks in the most complicated way. Goldberg applied his training as a graduate engineer and used his engineering, story-telling, and drawing skills to make sure that the “Inventions” could work, even though dozens of arms, wheels, gears, handles, cups, and rods were put in motion by balls, canary cages, pails, boots, bathtubs, paddles, and even live animals for simple tasks like squeezing an orange for juice or closing a window in case it should start to rain.

Edwin J. Houston; Born 9 Jul 1847; died 1 Mar 1914 at age 66.
Edwin James Houston was an American electrical engineer who, together with Elihu Thomson (another Philadelphia high school teacher) experimented with electricity. Houston invented, patented in 1881 and manufactured arc street-lighting. He presented the first paper, Notes on Phenomena in Incandescent Lamps, to The American Institute of Electrical Engineers when it began in 1884 (AIEE - the predecessor society of the present IEEE, The Institute of Electrical and Electronics Engineers, Inc.). The merger of Thomson-Houston and Edison General Electric companies (1892) formed General Electric. In 1894 he joined with Arthur Kennelly (who resigned from Edison's laboratory) to form a consulting company

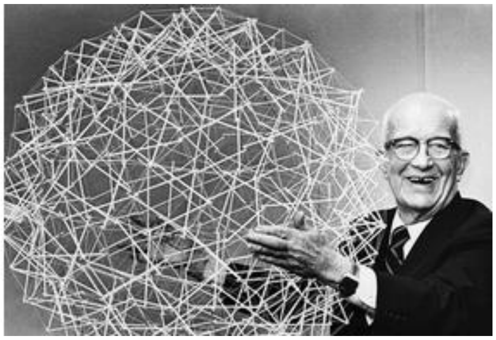


Seat-belt patent; July 1962
In 1962, a U.S. patent was issued to Swedish engineer, Nils Bohlen, for the three-point seatbelt (No. 3,043,625). His lap and shoulder design are now familiar as the passenger-restraint safety device in cars that has saved countless lives. His design replaced the earlier style of a single safety belts strapped across the body, with the buckle placed over the abdomen, which often caused severe internal injuries in high-speed crashes. Bohlin assigned the patent to Volvo, the car manufacturer for whom he worked. From Aug 1959, Volvo incorporated Bohlin's seat belt into the vehicles they manufactured. The company also made the design freely available to other car manufacturers to save more lives.

Nikola Tesla; Born 10 Jul 1856; died 7 Jan 1943 at age 86.
Serbian American inventor and researcher who designed and built the first alternating current induction motor in 1883. He immigrated to the United States in 1884. Having discovered the benefits of a rotating magnetic field, the basis of most alternating-current machinery, he expanded its use in dynamos, transformers, and motors. Because alternating current could be transmitted over much greater distances than direct current, George Westinghouse bought patents from Tesla the system when he built the power station at Niagara Falls to provide electricity power the city of Buffalo, NY. [Born in Croatia of Serbian parents. Some sources give birthdate as 9 Jul; he is said to have been born on the stroke of midnight. He celebrated his birthday as the 10th.]



Theodore Maiman, Born 11 Jul 1927; died 5 May 2007 at age 79.
Theodore Harold Maiman was an American physicist who built the first working laser. He began working with electronic devices in his teens, while earning college money by repairing electrical appliances and radios. In the 1960s, he developed, demonstrated, and patented a laser using a pink ruby medium. The laser is a device that produces monochromatic coherent light (light in which the rays are all of the same wavelength and phase). The laser has since been applied in a very wide range of uses, including eye surgery, dentistry, range-finding, manufacturing, even measuring the distance between the Earth and the Moon.



R. Buckminster Fuller; Born 12 Jul 1895; died 1 Jul 1983 at age 87.

Richard Buckminster Fuller was an American inventor, educator, author, philosopher, engineer and architect who developed the geodesic dome. This large dome can be set directly on the ground as a complete structure. There is no limit to the size to which it may be built and retain sufficient structural strength. Fuller also invented a wide range of other paradigm-shifting machines and structural systems. He was especially interested in high-strength-low weight designs, with a maximum of utility for minimum of material. His designs and engineering philosophy are part of the foundation of contemporary high-tech design aesthetics. He held over 2000 patents.

U.S. Electrical units

In 1894, eight units for the measurement of electrical magnitudes were adopted in U.S. law when President Grover Cleveland signed an Act of Congress “to define and establish the units of electrical measure” for the ohm, ampere, volt, coulomb, farad, joule, watt and henry. It was specified to be “the duty of the Academy of Sciences to prescribe ... such specifications of details as shall be necessary for the practical application of the definitions.” The Act followed an International Congress held at Chicago in 1893, in connection with the World's Fair. There, a Chamber of Delegates from various nations deliberated on the definitions. The International Congress was largely due to the Institute of Electrical Engineers and to local societies in the city of Chicago.

Jay W. Forrester; Born 14 Jul 1918.

Jay Wright Forrester is an American electrical engineer and management expert. In 1944-51 he supervised the building of the Whirlwind computer at the Massachusetts Institute of Technology, for which he invented the random-access magnetic core memory, the information-storage device employed in most digital computers. He also studied the application of computers to management problems, developing methods for computer simulation.

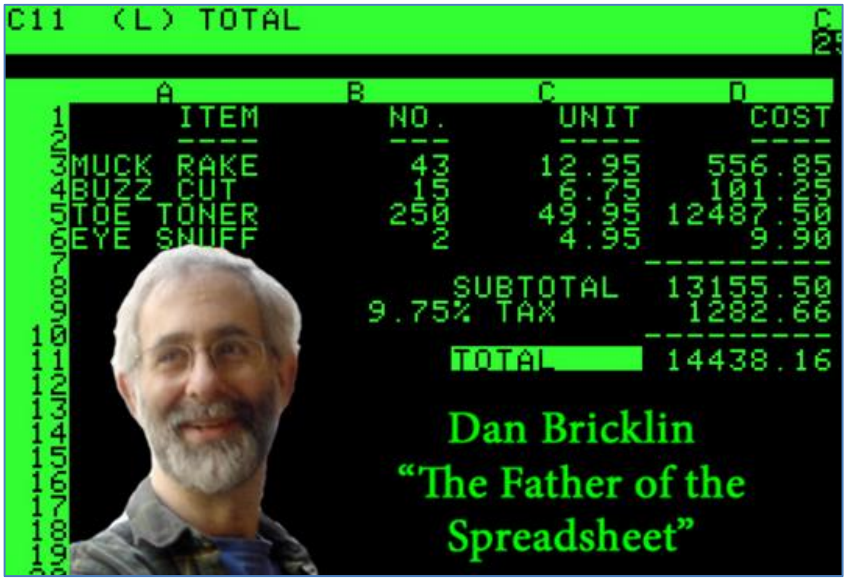
July 14th 2013, Last telegram in India

In 2013, the world's last telegram was sent in India. It was the last major country to shut down telegram service. India's 159-year-old telegram service was no longer needed, as e-mail and texting had replaced bicycle telegram messengers. In Great Britain, telegram delivery ceased in 2008, while the U.S., Western Union's dwindling service was terminated 27 Jan 2006. The first formal telegram was sent by Samuel Morse in Washington to his business partner Alfred Vail in Baltimore, on 24 May 1844. Seeking funding, he demonstrated to Congress the power of telegraphy through wires connecting cities with the message, “What hath God wrought.” In time, wires were strung across the U.S. and other countries, which eventually were connected by a Transatlantic cable under the ocean and more submarine cables.

In 1854

First telegram was sent between Mumbai and Pune.

Dan Bricklin; Born 16 Jul 1951.

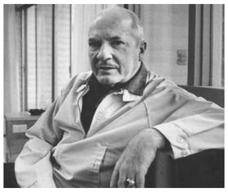


```
C11  (L) TOTAL
         A            B           C          D
 1    ITEM          NO.        UNIT       COST
 2    ----          ---        ----       ----
 3MUCK RAKE          43       12.95     556.85
 4BUZZ CUT           15        6.75     101.25
 5TOE TONER         250       49.95   12487.50
 6EYE SNUFF           2        4.95       9.90
 7                                   ---------
 8                   SUBTOTAL         13155.50
 9                 9.75% TAX           1282.66
10                                   ---------
11                      TOTAL         14438.16
```

Dan Bricklin
"The Father of the Spreadsheet"

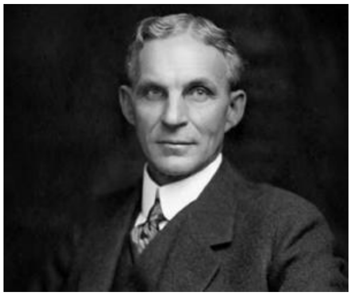
American computer scientist who with Bob Frankston created VisiCalc, the first spreadsheet computer program (1979) which created a market beyond hobbyists for the emerging personal computers. Businesses found the program very useful because of the speed and accuracy of its calculations. Originally written in 6502 assembly language to run on a 32K-byte Apple II, it was soon ported to virtually all major 6502- and Z80-based personal computers then available. They did not reap huge financial profits from the spreadsheet program, despite eventually selling over a half-million copies by 1983, because at the time, copyright protection was not generally sought for software, and it was subsequently surpassed by Lotus 1-2-3, later Microsoft Excel. It is anticipated that soon open source offerings such as LibreOffice may overtake Excel due to the extremely low (or zero cost) of entry.

Robert A. Heinlein; Born July 7, 1907



Robert A. Heinlein was an American author, naval officer, and aeronautical engineer. Heinlein is credited with pioneering a literary subgenre called hard science fiction as he was among the first to stress the importance of scientific accuracy in fiction. Robert A. Heinlein is one of the most influential science-fiction writers of all time.

Henry Ford; Born July 30, 1863; Died April 7, 1947

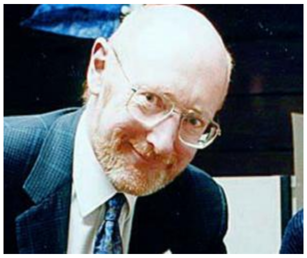


Business magnate and founder of the Ford Motor Company, Henry Ford is credited to have made the automobile an accessible conveyance for Americans in the 20th century. Following the success of his company, he became one of the richest and best-known people in the world. He also became known for his pacifism during the first years of World War I.

Marc Andreessen; Born July 9, 1971

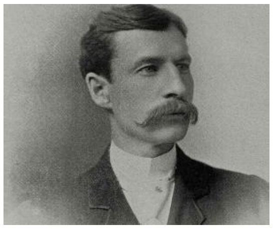
Marc Andreessen is an American entrepreneur, software engineer, and investor. He is credited with co-founding the independent computer services company Netscape as well as the private venture capital firm Andreessen Horowitz. Marc Andreessen is also credited with co-authoring one of the first web browsers, NCSA Mosaic. In 1994, he was inducted into the World Wide Web Hall of Fame.

Clive Sinclair; Born July 30, 1940



A consumer electronics pioneer, entrepreneur Clive Sinclair began his business venture selling radio and amplifier kits. He went on to launch the word's first pocket calculator and later also worked on products such as digital watches and pocket TV. He is a fan of poker and is a **Mensa** member.

Frank J Sprague; Born July 25, 1857; Died October 25, 1934



Frank Julian Sprague (July 25, 1857 – October 25, 1934) was an American inventor who contributed to the development of the electric motor, electric railways, and electric elevators. His contributions were especially important in promoting urban development by increasing the size cities could reasonably attain (through better transportation) and by allowing greater concentration of business in commercial sections (through use of electric elevators in skyscrapers).[1] He became known as the "father of electric traction". Demonstrating an aptitude for science and mathematics, Sprague secured an appointment to the U.S. Naval Academy in 1874 and, after graduation in 1878 and 2 years at sea, resigned to pursue his career in electrical engineering

This continues the yearlong feature of interesting ***engineering*** events or milestones that occurred in a specific month. Readers are invited to share their views and opinions (or suggestions) at the accompanying link. Submissions can also be made using direct email to the editors at: wavelengths@ieee-sem.org.

Past readers have asked to feature one or more of these events in more detail. So, starting in January 2024, we have been featuring both documentaries and black & white movies, that will help shed more light on these luminaries and also explore the hidden side of their life stories. We will also endeavor to republish an article from various publications in the same month of Wavelengths.

Here is a link which lists all of the documentaries featuring several of the folks mentioned in past *"This month…."* series. Enjoy!

Sharan Kalwani
2022-2024 Chair, Southeastern Michigan Section,
Passionate Engineering History Buff/Aficionado

Elections 2024

We send an eNotice, and an article in the newsletter, to all our Section members in advance of our yearly elections. IEEE MGA requires us to notify all eligible voters 6 months before an election is planned, and this announcement was designed to satisfy that requirement.

This year's schedule is planned as follows:

- **Call for nominations: September 9 - 30**
- **Completion of Ballots: October 15**
- **Ballots out for vote: October 17 - 31.**
- **Compile and reconcile results: November 15**
- **Report results to the ExCom at the December ExCom meeting.**

This year we will elect our 2025 set of officers for all Geo-units (Affinity Groups & Technical Chapters). Those officers include the Chair / Vice-Chair / Secretary / Treasurer.

Links to most Job Descriptions may be found on the Volunteer Portal at: **https://r4.ieee.org/sem/aboutsem/volunteer-portal/**.
Links to the Affinity Groups and to the Chapters may be found at: **https://r4.ieee.org/sem/aboutsem/sem-chapters/**

Note: Student Branches and HKN Chapters elect their officers on their individual schedules independently on their own.

Direct questions to: K.williams@ieee.org

Officer Training
We encourage members who are considering running for an officer position to take advantage of the 'Training Materials' available on the IEEE SEM Website at: **https://r4.ieee.org/sem/aboutsem/training/**

FREE Voice over Power Point Training: On-line virtual training modules are available through the SEM Website Training page. These videos will play directly and immediately from Google Chrome browser. They may not work well using Internet Explorer.

Turn OFF your pop up blocker if you don't see it load or download.
Blank Titles (Links) are in development.
(If you wish to rewind sections and play again, we suggest you download the module to your computer and play it using your systems 'media player'.)

Note: If you are beginning training, we recommend starting with Module # 46: Virtual Training Plan, and follow its recommendations for the training sequence. Send Questions about these Training Modules to:
Virtual_Training_QA_Forum@googlegroups.com

Please also see the notice detailing ongoing Officer Training on the next page.

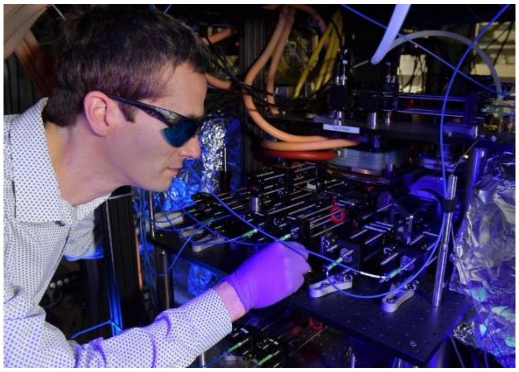
30

Lord Kelvin

Somehow, I missed listing in my monthly notable icons of science, engineering and technology – Lord Kelvin. To make amends, I found this fantastic article by Stephen Eckel of NIST, which makes for enjoyable reading and learning. Reprinted by kind permission.

How Low Can Temperature Go? Lord Kelvin and the Science of Absolute Zero

June 26, 2024
By: Stephen Eckel



In Stephen Eckel's lab at NIST, he gets to work with some of the coldest stuff in the universe.

When I wake up in the morning, the first thing I usually check is the time (to see if I should go back to sleep), but the second thing I check is the temperature outside (so that I know how to dress).

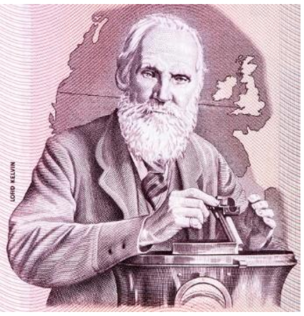
Temperature is such a common measurement that we sometimes forget how important it is. From dairy farming to rocketry, from climate science to weather prediction, so many things require an accurate knowledge of temperature.

The metric (SI) unit for temperature is called the kelvin, after Lord Kelvin, whose 200th birthday we celebrate today.

Lord Kelvin and the Early Science of Temperature

Lord Kelvin, or William Thomson, worked in what was then the emerging field of thermodynamics — transforming heat into dynamical motion. He did this both as a student at the University of Cambridge and as a young professor at the University of Glasgow. Together with his close collaborator, James Joule, he researched all sorts of problems in thermodynamics, including temperature scales.

At the time, the scientifically accepted scale for temperature was the Celsius scale, with zero temperature being the freezing point of water and 100 degrees being the boiling point of water. But after studying how gases changed volume and pressure in response to changing temperature, Thomson, Joule and other scientists realized that there was an absolute coldest temperature that could be reached.



On his 200th birthday today, we remember Lord Kelvin's many contributions to science, including calculating the coldest possible temperature — known as absolute zero.

To understand how they reached this conclusion, consider a gas in a balloon. If you cooled the balloon, the gas inside would exert less pressure against the balloon itself and against the atmosphere outside it, causing the balloon's volume to shrink.

Don't believe me? Inflate a balloon and stick it in your freezer. When you pull it out, you can feel the balloon expand. Now extrapolate: How cold would you have to make the balloon to make its volume go to zero (ignoring the fact that the gas inside will eventually condense into a liquid)? That must be the coldest possible temperature because the balloon cannot have a negative volume.

In 1848, Lord Kelvin used similar reasoning to accurately calculate the absolute coldest temperature as negative 273.15 Celsius (or negative 459.67 degrees Fahrenheit). It would be roughly another decade before scientists like Lord Kelvin and Ludwig Boltzmann understood that at absolute zero, the molecules in the gas stop moving.

Since 2019, all three of these scientists have been immortalized in the SI. The kelvin is our SI unit of temperature, defined through the Boltzmann constant, which relates temperature to energy, the SI unit of which is the joule.

Today, atomic physicists like myself use a technique partly pioneered at NIST called laser cooling, which uses lasers to cool clouds of between 100,000 and 1 billion atoms to temperatures of about 100 microkelvin. This temperature is 1/10,000th of a degree Celsius above absolute zero.

And we measure these ultracold temperatures in a way that would not be surprising to Lord Kelvin (although making such cold gases might be!).

We measure the average speed of the atoms in the gas. Researchers at NIST use such laser-cooled atoms for all sorts of applications, from atomic clocks to vacuum standards.

Vacuum Standard

Laser cooling atoms to near absolute zero only works inside a chamber where almost all the air has been removed by a pump to isolate the atoms from the surrounding environment. Such vacuum chambers are common and are used in industries such as semiconductor manufacturing.

Most of the components in your cellphone have been in and out of at least one vacuum chamber. The core components, like the central processing unit, have probably been through a chamber that has produced some of the best vacuums on Earth. For every trillion gas molecules that started in the chamber, all were removed but one. Such exquisite vacuums are required because leftover gas molecules can both contaminate the chip and scatter the ultraviolet light that is used to imprint the designed circuit. This can cause the chip to be ruined.

Amazingly, the current best way to measure such pure vacuums is by using what is effectively a vacuum tube. But now, the laser-cooled atoms in my lab may be the best sensor of ultralow vacuum pressures on Earth.

After the sensor atoms are cooled to near absolute zero, we hold the sensor atoms in a "trap" that is made entirely of magnetic fields. This trap is very weak, only able to hold onto the ultracold sensor atoms. The vacuum sensor works because if a cold sensor atom is struck by a leftover gas molecule, it will almost always be ejected from the weak trap. The rate at which this process occurs depends on the number of gas molecules the pump has left behind. Thus, determining the number of leftover gas molecules just involves counting the number of sensor atoms that remain after some time.

This "cold-atom vacuum standard (CAVS)" is a new way of measuring vacuum pressure, which NIST has played a crucial role in developing. We anticipate it being used to measure ultrapure vacuums in semiconductor manufacturing, quantum computers and other big science experiments, such as an experiment detecting collisions of extremely distant black holes, known as the Laser Interferometer Gravitational Wave Observatory (LIGO).

Having a standard like the CAVS that always gives the correct vacuum pressure reading will help these applications build better vacuum chambers, diagnose problems and increase both reliability and productivity.

The CAVS is the only experiment that I am aware of that needs to measure two very different temperatures at the same time: the sensor atom temperature of around 100 microkelvin (very cold!) and the temperature of the leftover gas in the vacuum chamber, near room temperature at 300 kelvin.

I think Lord Kelvin would be amazed to learn that two very different temperatures could exist at the same time, and both need to be measured for a single experiment to work.

This statue of Lord Kelvin in Glasgow, Scotland, was adorned with a traffic cone, as other statues have been. It's believed to be a nod to the Scottish sense of humor.

Thermometers

Another interesting research pursuit here at NIST is trying to use atoms or molecules to build a thermometer that actually measures temperature. You may be wondering what I mean.

After all, you probably have multiple thermometers in and around your home, and they all give you some number in either Fahrenheit or Celsius. But the truth is they all measure some *other* physical quantity — like the resistance of a platinum wire or the voltage generated between two dissimilar metals — that depends on temperature.

For these devices to read out a temperature in Fahrenheit or Celsius, they must be calibrated. NIST does such calibrations, and it's more likely than not that the calibration for the thermometer in your home's thermostat can be traced through a complicated set of steps all the way back to NIST.

But we may be able to make this whole calibration process simpler by making thermometers that directly measure temperature, using techniques that Lord Kelvin would appreciate.

For example, my colleague Daniel Barker and I are working on using lasers to measure the distribution of velocities of a gas of rubidium atoms at room temperature and above. This technique, called Doppler thermometry, gets at the very heart of how Lord Kelvin understood temperature.

Together with my colleague Eric Norrgard, I am also working on two projects trying to create a new type of infrared thermometer using atoms and molecules. If these efforts are successful, calibrating our thermometers could get much easier, and it may further other scientific advancements as well.

Keeping It (Very) Cool in the Lab

I came to NIST as a postdoctoral researcher in 2012 after finishing my graduate work at Yale University.

As a postdoc, I worked with some of the coldest stuff in the universe: Bose-Einstein condensates (BECs). Like the CAVS, BECs are also made of laser-cooled atoms, but they have been cooled even further to less than 100 billionths (!) of a degree above absolute zero.

After my postdoc, I decided to stay at NIST and try to use my experience with ultracold atoms and lasers to realize practical and useful standards, like the CAVS.

I gain a great sense of pride when I see what appear to be glowing balls of ultracold atoms — which are certainly fun to play with — used to solve real-world measurement problems. I suspect that Lord Kelvin may have felt the same sense of pride to see his measurements and theories regarding thermodynamics (which were probably also fun to work on) be applied to make more efficient steam engines.

Happy Birthday, Lord Kelvin

Lord Kelvin didn't just calculate absolute zero. After his early work in establishing absolute temperature scales, he was instrumental in laying the first telegraph cables across the Atlantic Ocean. Lord Kelvin also invented a machine that predicted tides and a compass that helped the Royal Navy navigate the seas. While my research is not quite that varied, one of the ways I mix up my work is by working at both room temperature and temperatures near absolute zero.

One of the key things I have learned is that measuring temperature, as Lord Kelvin understood it, is almost always harder than you might think. While the ideas are straightforward, making them work in practice is the real challenge.

And this fact makes it even more impressive that Lord Kelvin accurately predicted the temperature of absolute zero … in 1848.

On his 200th birthday, I'll take a moment to appreciate that.

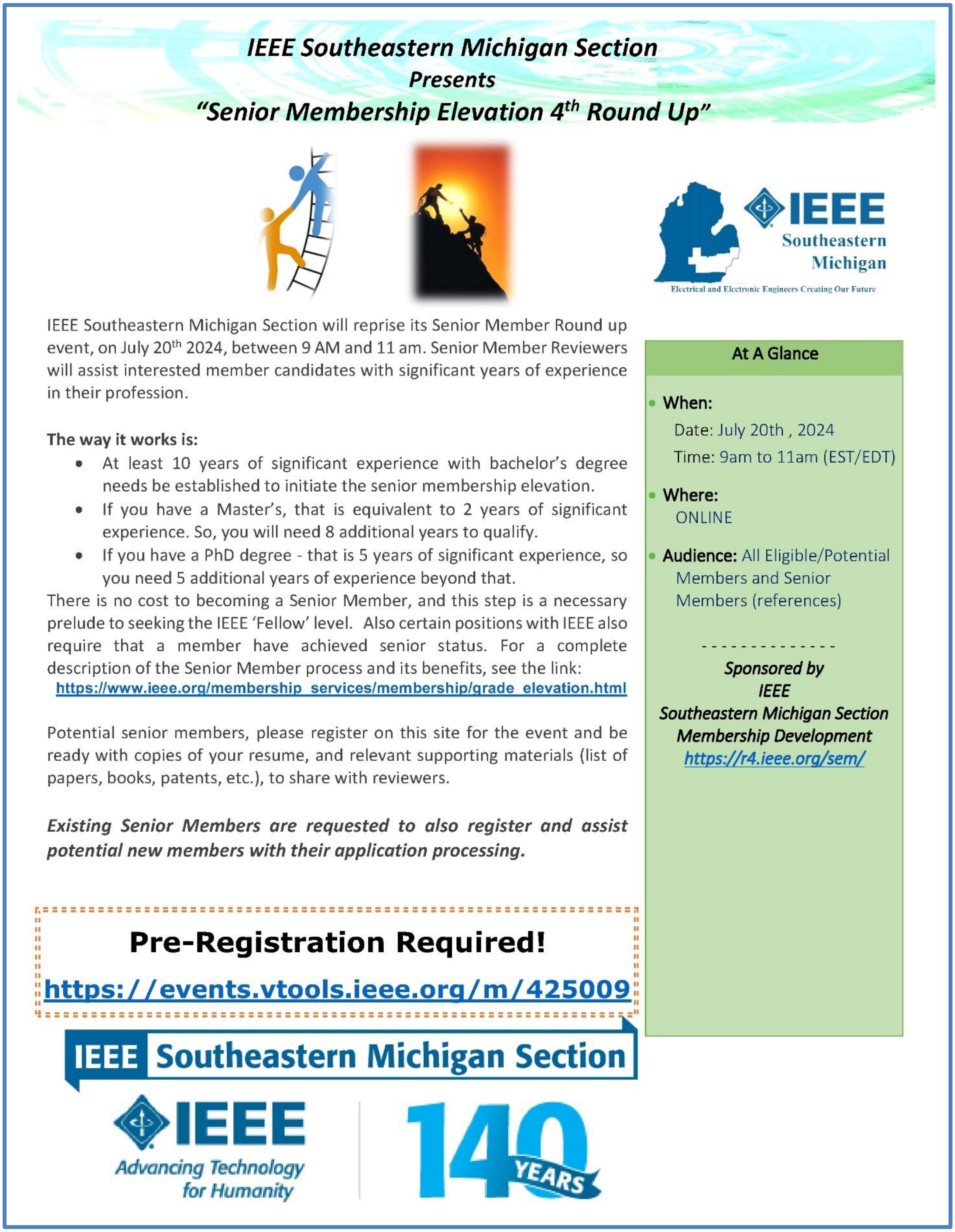
ABOUT THE AUTHOR

Stephen Eckel

Stephen Eckel is a physicist in the Sensor Science Division. His research focuses on using atoms, both at room temperature and ultracold, to probe thermodynamic quantities like pressure and temperature in calibration-free ways. He earned his Ph.D. at Yale University in 2012 and came to NIST as a postdoctoral researcher working with Bose-Einstein condensates. When not in the lab working with atoms and lasers, you will most likely find him tending to his garden or driving antique Stanley Steam cars.

Reprinted from https://www.nist.gov/blogs/taking-measure/how-low-can-temperature-go-lord-kelvin-and-science-absolute-zero

Senior Elevation July



IEEE Southeastern Michigan Section
Presents
"Senior Membership Elevation 4th Round Up"

IEEE
Southeastern
Michigan
Electrical and Electronic Engineers Creating Our Future

IEEE Southeastern Michigan Section will reprise its Senior Member Round up event, on July 20th 2024, between 9 AM and 11 am. Senior Member Reviewers will assist interested member candidates with significant years of experience in their profession.

The way it works is:

- At least 10 years of significant experience with bachelor's degree needs be established to initiate the senior membership elevation.
- If you have a Master's, that is equivalent to 2 years of significant experience. So, you will need 8 additional years to qualify.
- If you have a PhD degree - that is 5 years of significant experience, so you need 5 additional years of experience beyond that.

There is no cost to becoming a Senior Member, and this step is a necessary prelude to seeking the IEEE 'Fellow' level. Also certain positions with IEEE also require that a member have achieved senior status. For a complete description of the Senior Member process and its benefits, see the link:
https://www.ieee.org/membership_services/membership/grade_elevation.html

Potential senior members, please register on this site for the event and be ready with copies of your resume, and relevant supporting materials (list of papers, books, patents, etc.), to share with reviewers.

Existing Senior Members are requested to also register and assist potential new members with their application processing.

Pre-Registration Required!

https://events.vtools.ieee.org/m/425009

At A Glance

- **When:**
  Date: July 20th , 2024
  Time: 9am to 11am (EST/EDT)
- **Where:**
  ONLINE
- **Audience:** All Eligible/Potential Members and Senior Members (references)

- - - - - - - - - - - - - -

Sponsored by
IEEE
Southeastern Michigan Section
Membership Development
https://r4.ieee.org/sem/

IEEE Southeastern Michigan Section
IEEE
Advancing Technology for Humanity
140 YEARS

Senior Member News

The IEEE southeastern Michigan Section is extremely proud and happy to welcome members, who recently got upgraded to senior status. It is all part of our Membership Development on-going initiative to play a role in the professional lives of our members and support them in every which way possible.

Mohamad Berri & Sharan Kalwani.
Membership Development committee

Next Senior Elevation

IEEE HQ Admission and Advancement (A&A) Review Panel Meeting Schedule

The Admission & Advancement (A&A) Review Panels meet six times annually to review applications and/or nominations for election or elevation to Senior Member (SM) or Life Senior Member (LSM) grade.

- The review panel meetings are held in various locations throughout the world.
- A panel of reviewers is recruited among Senior members, Life Senior members, and Fellows in the section where the meeting is to be held. This full-day session is presided over by the Admission and Advancement Chair and/or Vice Chair, as well as a representative of the Member and Geographic Activities staff.
- **In order for an application to be reviewed at the next Panel meeting, the application, resume, and required reference forms have to be submitted and received at least Seven days prior to the meeting date. [hence †] We have scheduled ours to be on July 20th – giving us enough time to fix any gaps, etc.**
- About two weeks following a review panel meeting, an update report with the names of the newly elevated Senior members is published and available for those who hold a volunteer position.

Review panel dates and locations (note: Dates and locations are subject to change without notice.)

Please see Meeting Deadlines (Eastern Standard Time) below for more details.

2024 Meeting Dates	Meeting Deadlines (Eastern Standard Time)
3 August 2024	11:59 p.m. on 27 July 2024
28 September 2024	11:59 p.m. on 21 September 2024
23 November 2024	11:59 p.m. on 16 November 2024

2024 IEEE HQ Panel Meeting Dates

†See our own Section organized event at: https://events.vtools.ieee.org/m/425009 **OR** check the Section web site **OR** see page **14**

2024 SEM Officers

The IEEE SEM Organizational Roster is Located in the IEEE Southeastern Michigan website at: **http://sites.ieee.org/sem/**

Under the TAB titled "About SEM" use the button:
"Organization Roster" to download the PDF version of the current Roster.

(Note: It is also a good idea to download the Organization Org Chart as well in order to get the complete 'big picture' of the Section.)

(Note: To protect the members from getting spam email, the roster is password protected. Request access by sending email to our web master – Scott Lytle.)

Years ago, we used to publish the complete Chart and Roster in the Newsletter. But that was when we had only 5 committees and 9 chapters.

Today we have 16 committees and sub-committees, 18 Technical Chapters, 4 Affinity Groups and 8 Student Branches. The total roster divides into 12 pages with 247 identified officer positions.

That seems like a large organization, and it is, but it also presents our members with many volunteer opportunities to grow their capabilities through the experience of working with leaders who can guide and nurture engineering talent and widen the scope of volunteering through 'hands on' training in those 'soft skills' that can only be mastered by 'doing.'

We often refer to learning the non-technical side of an engineering career as similar to learning to play a musical instrument, or a sport, or how to dance. You can read all the books you want but, you only really learn by doing.

Reading the Roster

Once downloaded notice that the roster is divided into five major segments:

- Executive Committee
- Standing Committees
- Affinity Groups
- Technical Chapters
- Student Branches

Within each segment you should find, at a minimum, the e-mail account for each officer, and in many cases, a work phone and a cell phone for quicker contact.

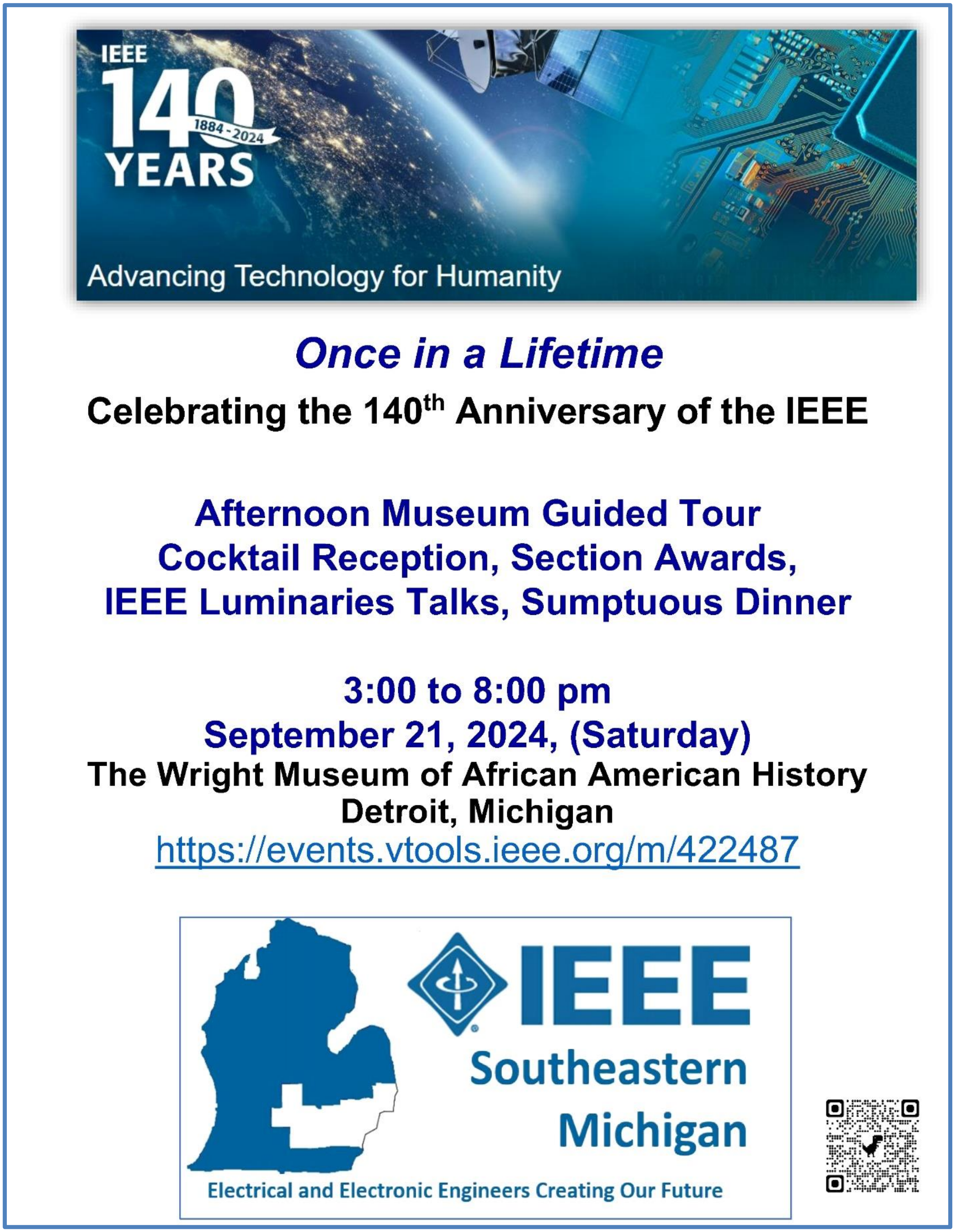
You may note a number of identified officer roles that have a blank cell (highlighted in yellow) where we would expect an officer name. These are vacant officer positions.

If you notice a vacancy where you might be interested in contributing to fill that role, please contact the relevant 'Chair' in that organization and discuss the duties of the office and consider helping out in that element.

As with all others, the road to this learning begins with the first step. That step is inquiring and finding out what skills go with each position. That information is maintained in the IEEE Center for Leadership Excellence at: **https://ieee-elearning.org/CLE/**

Good luck!

SAVE THE DATE: 140th!


IEEE
140
1884 - 2024
YEARS
Advancing Technology for Humanity
IEEE
Southeastern
Michigan
Electrical and Electronic Engineers Creating Our Future

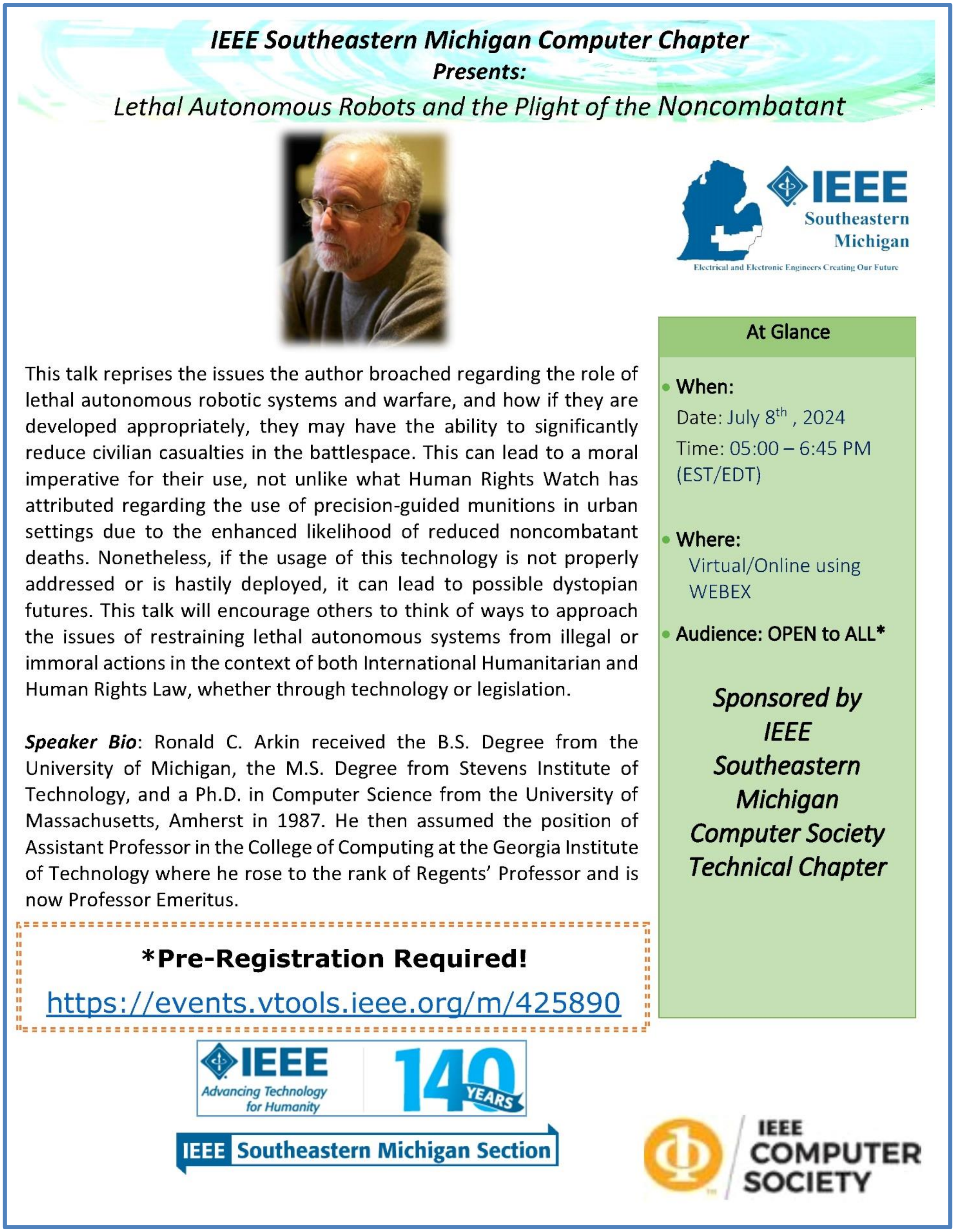
Once in a Lifetime

Celebrating the 140th Anniversary of the IEEE

Afternoon Museum Guided Tour
Cocktail Reception, Section Awards,
IEEE Luminaries Talks, Sumptuous Dinner

3:00 to 8:00 pm
September 21, 2024, (Saturday)
The Wright Museum of African American History
Detroit, Michigan
https://events.vtools.ieee.org/m/422487

Lethal Robots



IEEE Southeastern Michigan Computer Chapter

Presents:

Lethal Autonomous Robots and the Plight of the Noncombatant

IEEE
Southeastern
Michigan
Electrical and Electronic Engineers Creating Our Future

This talk reprises the issues the author broached regarding the role of lethal autonomous robotic systems and warfare, and how if they are developed appropriately, they may have the ability to significantly reduce civilian casualties in the battlespace. This can lead to a moral imperative for their use, not unlike what Human Rights Watch has attributed regarding the use of precision-guided munitions in urban settings due to the enhanced likelihood of reduced noncombatant deaths. Nonetheless, if the usage of this technology is not properly addressed or is hastily deployed, it can lead to possible dystopian futures. This talk will encourage others to think of ways to approach the issues of restraining lethal autonomous systems from illegal or immoral actions in the context of both International Humanitarian and Human Rights Law, whether through technology or legislation.

Speaker Bio: Ronald C. Arkin received the B.S. Degree from the University of Michigan, the M.S. Degree from Stevens Institute of Technology, and a Ph.D. in Computer Science from the University of Massachusetts, Amherst in 1987. He then assumed the position of Assistant Professor in the College of Computing at the Georgia Institute of Technology where he rose to the rank of Regents' Professor and is now Professor Emeritus.

At Glance

- **When:**
  Date: July 8th , 2024
  Time: 05:00 – 6:45 PM (EST/EDT)
- **Where:**
  Virtual/Online using WEBEX
- **Audience: OPEN to ALL***

Sponsored by IEEE Southeastern Michigan Computer Society Technical Chapter

***Pre-Registration Required!**

https://events.vtools.ieee.org/m/425890

IEEE
Advancing Technology for Humanity
140 YEARS
IEEE Southeastern Michigan Section
IEEE COMPUTER SOCIETY

RoboFest News

Report on Robofest Summer Camps Sponsored by IEEE SEM EMC Society

The IEEE SEM EMC Society sponsored summer camps were held at LTU on two days. Robofest Day Camps offered robotics programming lessons in the morning. After lunch, students participated in mini competitions, with winning teams receiving trophies. The camp was designed for students in grades 5 through 12.

On June 26, seventeen students learned autonomous robotics programming and tested their skills in a real BottleSumo competition! See figures 1-3.

On June 27, fifteen students learned basic robotics programming skills and tested their learned skills in a real “unknown mission” competition! See figures 4-6.

Camp registration fees, lunch, participation medals, and winner trophies were provided by the Southeastern Michigan IEEE EMC Society.

Some comments from an anonymous survey after the events were:

LTU Instructors, Mentors, always do a great job. My students always love it, I Thank the sponsors for helping you with the RobFest Camp funds. It was FANTASTIC!!!!!!
It's cool and I really liked it. (From a student survey)
My son noted that the Robofest staff was very kind and encouraging. Thank you!

More photos can be accessed at: https://photos.app.goo.gl/oK8TPpBDPkD9vGvAA

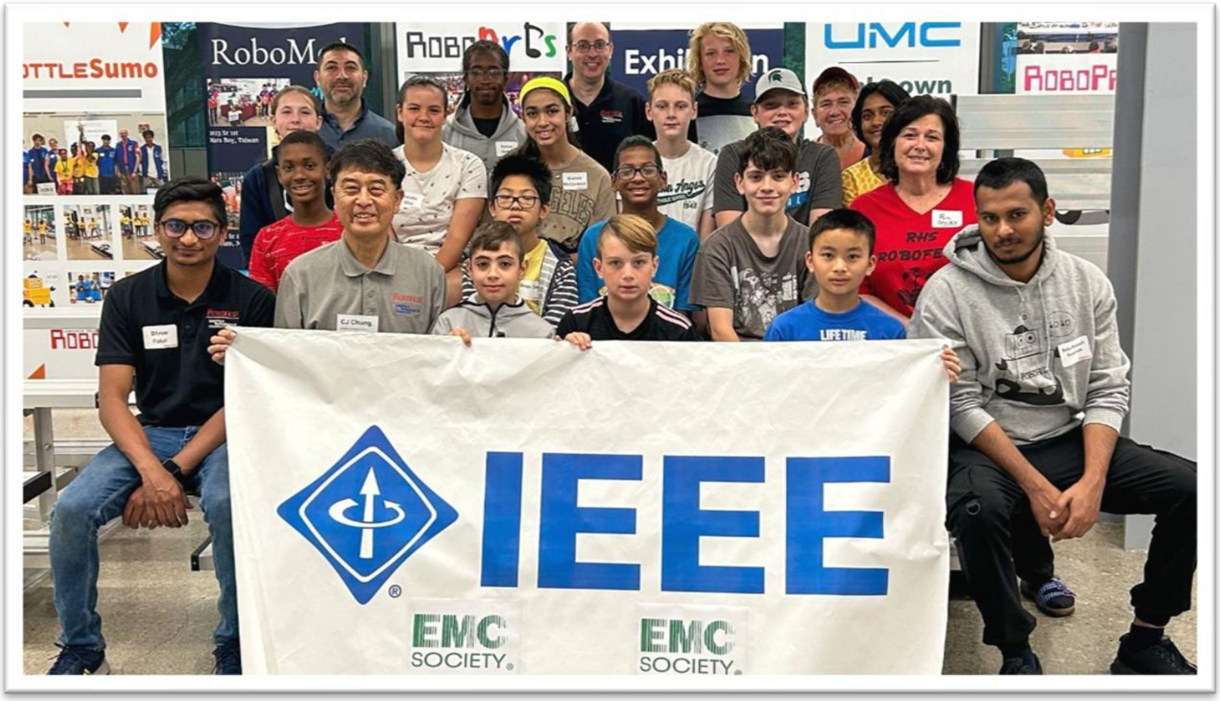


Figure 1. Day Students with a IEEE Banner

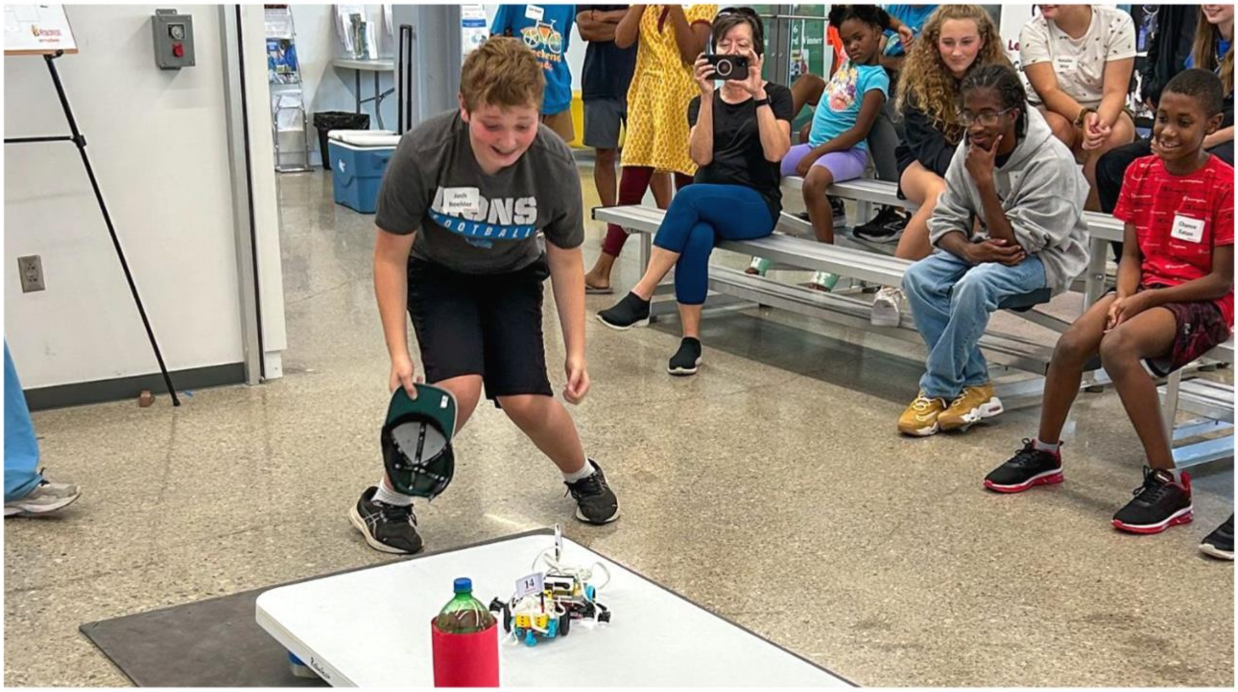


Figure 2. Excited student on Day 1

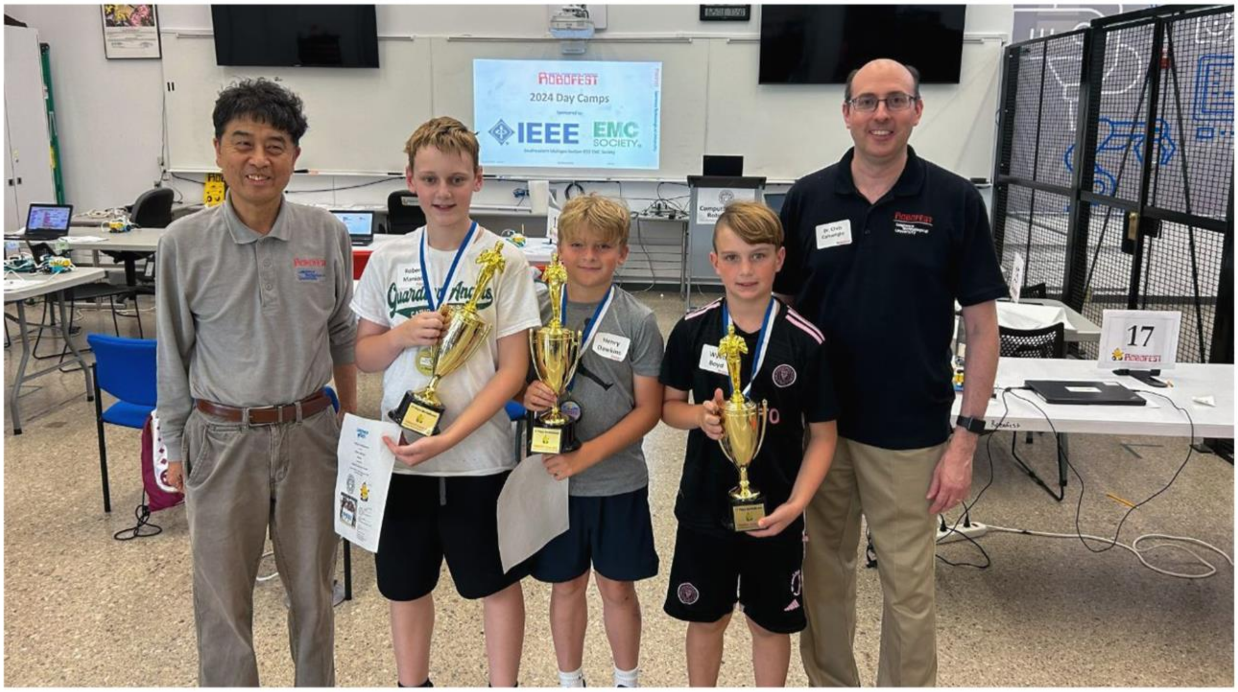


Figure 3. Day 1 BottleSumo Competition Winners with Trophies

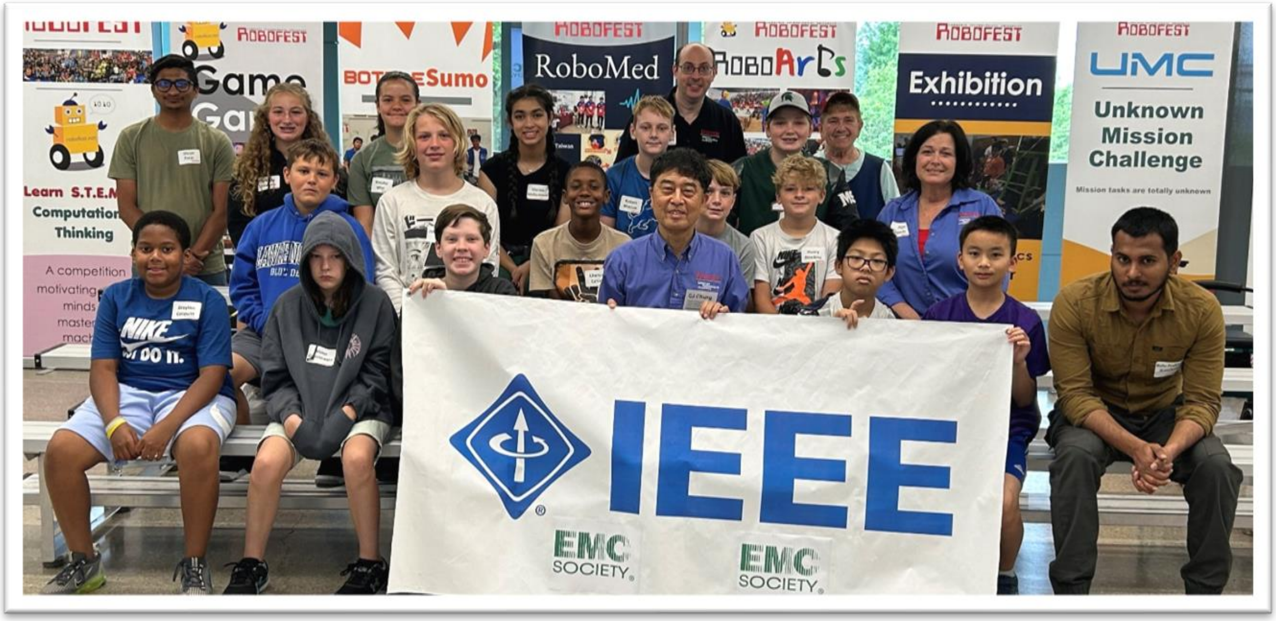


Figure 4. Day 2 students with IEEE banner

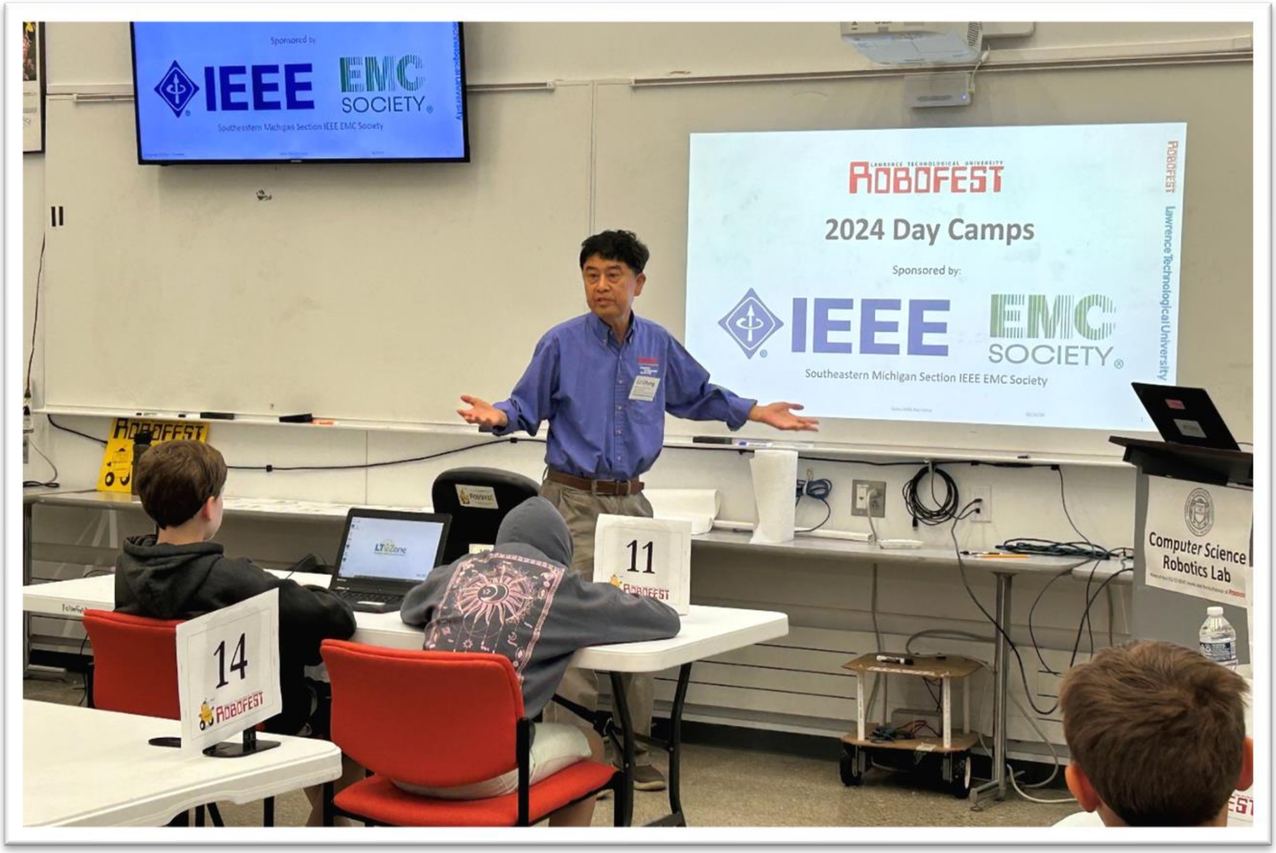

Sponsored by
IEEE
EMC SOCIETY
Southeastern Michigan Section IEEE EMC Society
LAWRENCE TECHNOLOGICAL UNIVERSITY
ROBOFEST
2024 Day Camps
Sponsored by:
IEEE
EMC SOCIETY
Southeastern Michigan Section IEEE EMC Society
Lawrence Technological University
Computer Science Robotics Lab
11
14
ROBOFEST

Figure 5. CJ Chung, Founder of Robofest and IEEE Senior Member introduced IEEE and EMC and encouraged them to join IEEE later

Figure 6. Day 2 competition winners

Lawrence Technological University / Robofest / J-233 / 21000 W. Ten Mile Rd, Southfield, MI 48075
Prof. Elmer Santos, Director, esantos@ltu.edu
Shannan Palonis, Assistant Director, spalonis@ltu.edu
Pam Sparks, Coordinator, psparks@ltu.edu
Dr. CJ Chung, Robofest Founder, Executive Council Chair, cchung@ltu.edu
Dr. Chris Cartwright, Executive Council Member
Dr. Eric Martinson, Executive Council Member

http://www.robofest.net http://facebook.com/robofest https://www.linkedin.com/company/robofest-official

ELECTIONS ALERT!

To all IEEE SEM Officers at all levels: IEEE Elections 2024 / 2045:

In years past, the Executive Committee, and its Standing Committees of Southeastern Michigan Section have conducted ALL the elections for each of our Geo-units (Chapters, Affinity Groups, and the primary Section Executive Committee officers).

This year, according to the instructions in the MGA Policy and Procedures (P&P) Manual 2024, each Geo-unit is directed to setup its own election committee, nominate its own officer candidates and conduct its own elections.

See the complete instructions in the P&P Manual at:
https://mga.ieee.org/images/files/Current_MGA_Operations_Manual_2024__22_June.pdf
In Section **9.13**. Search for "**GEOGRAPHIC UNIT ELECTIONS**" starting on Page 126.

Other information is available at:
https://mga.ieee.org/volunteer-hub/geographic-unit-operations/geographic-unit-elections

MGA On Line Election Training Sessions on July 15:

Training **Session Registration Details:**

Please click below to register for the session that best fits your schedule. The password for registration if prompted is MGAelections.

- 15 July 2024: 5:00 AM ET
    - **https://ieee.webex.com/weblink/register/r29fecc9a3262302de2e19cad5557161c**
- 15 July 2024: 12:00 PM ET
    - **https://ieee.webex.com/weblink/register/r2ceb2217b6be7918d1e3f32240658f8c**
- 15 July 2024: 9:00 PM ET
    - **https://ieee.webex.com/weblink/register/r24f8b73a59718e10c80a8b6153f80a43**

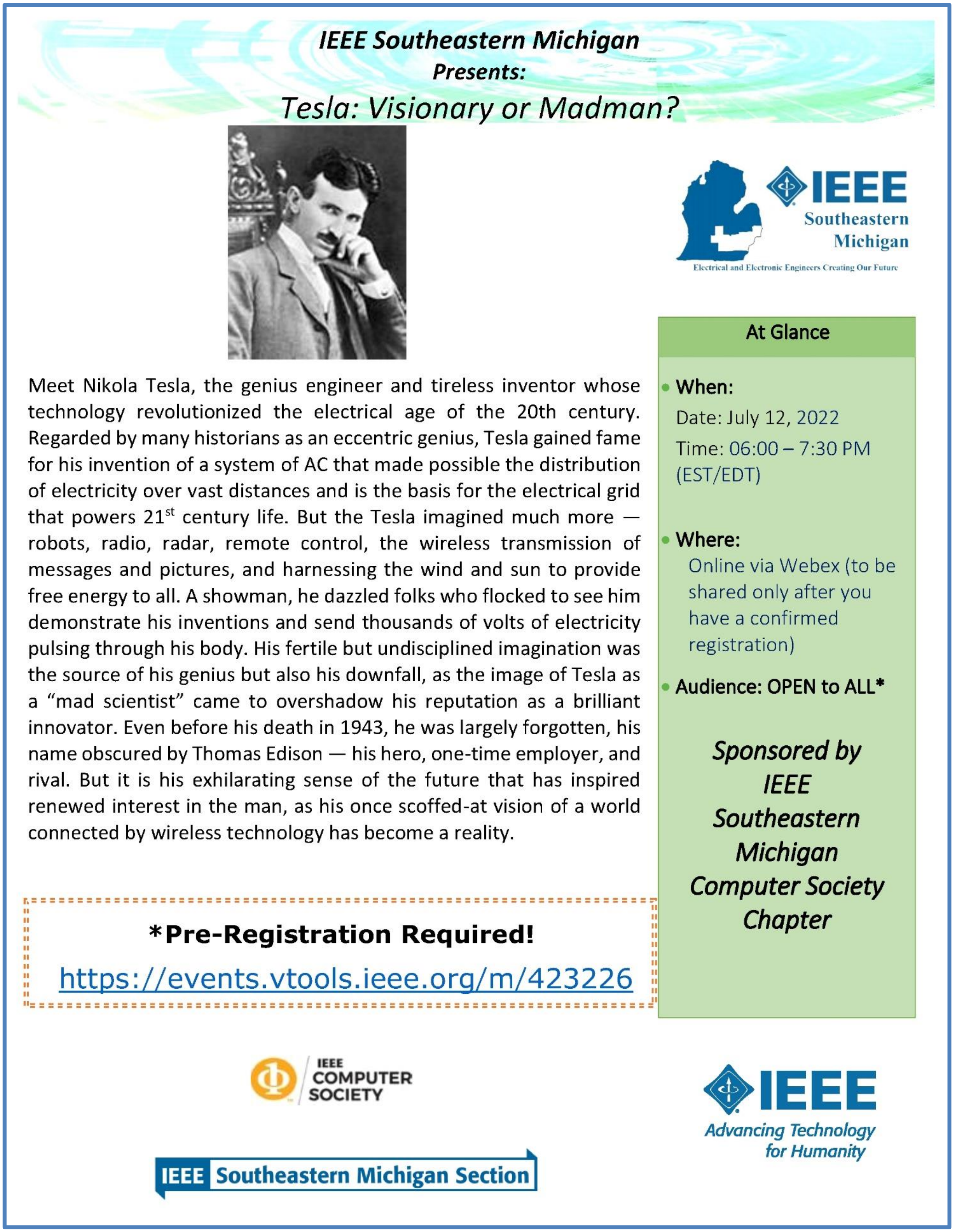
Topics Covered:

- In depth Section use of the new Nominations/Elections Tool
- Recap of first training:
    - Elections process overview
    - Highlighting available resources
    - FAQ
- Reminder: Elections to start by 15 August
- Q&A session

Who Should Attend:

These training sessions are designed for Geographic Unit Officers and Elections (previously Nominating) Committee members working on elections for their Geographic Units. Officers are asked to forward this invitation to their respective Elections (previously Nominating) Committee members.

Tesla Documentary



IEEE Southeastern Michigan

Presents:

Tesla: Visionary or Madman?

Meet Nikola Tesla, the genius engineer and tireless inventor whose technology revolutionized the electrical age of the 20th century. Regarded by many historians as an eccentric genius, Tesla gained fame for his invention of a system of AC that made possible the distribution of electricity over vast distances and is the basis for the electrical grid that powers 21st century life. But the Tesla imagined much more — robots, radio, radar, remote control, the wireless transmission of messages and pictures, and harnessing the wind and sun to provide free energy to all. A showman, he dazzled folks who flocked to see him demonstrate his inventions and send thousands of volts of electricity pulsing through his body. His fertile but undisciplined imagination was the source of his genius but also his downfall, as the image of Tesla as a “mad scientist” came to overshadow his reputation as a brilliant innovator. Even before his death in 1943, he was largely forgotten, his name obscured by Thomas Edison — his hero, one-time employer, and rival. But it is his exhilarating sense of the future that has inspired renewed interest in the man, as his once scoffed-at vision of a world connected by wireless technology has become a reality.

***Pre-Registration Required!**

https://events.vtools.ieee.org/m/423226

At Glance

- **When:**

  Date: July 12, 2022

  Time: 06:00 – 7:30 PM (EST/EDT)

- **Where:**

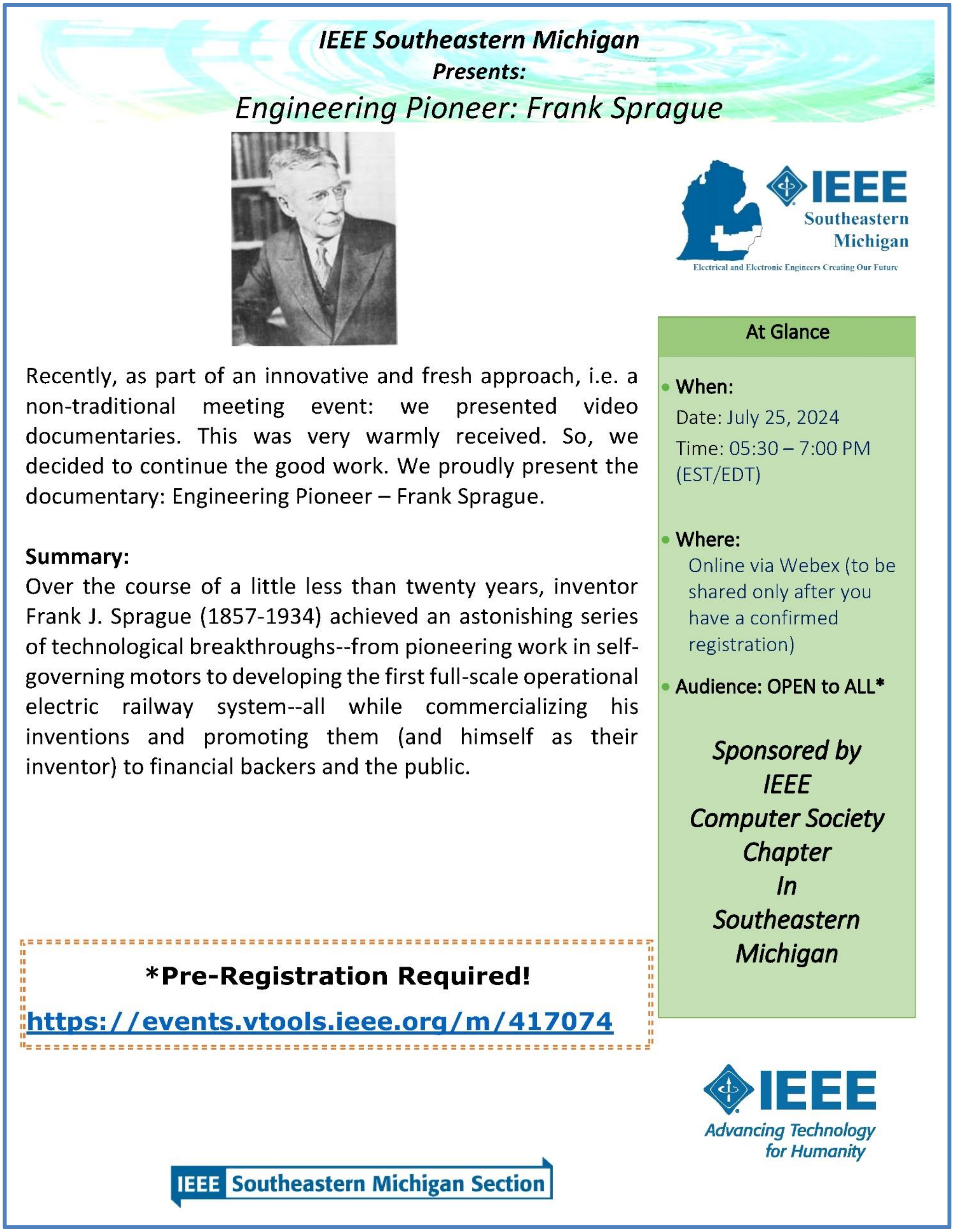
  Online via Webex (to be shared only after you have a confirmed registration)

- **Audience: OPEN to ALL***

Sponsored by IEEE Southeastern Michigan Computer Society Chapter

IEEE Southeastern Michigan
Electrical and Electronic Engineers Creating Our Future
IEEE COMPUTER SOCIETY
IEEE Southeastern Michigan Section
IEEE Advancing Technology for Humanity

Sprague Documentary



IEEE Southeastern Michigan

Presents:

Engineering Pioneer: Frank Sprague

IEEE Southeastern Michigan

Electrical and Electronic Engineers Creating Our Future

Recently, as part of an innovative and fresh approach, i.e. a non-traditional meeting event: we presented video documentaries. This was very warmly received. So, we decided to continue the good work. We proudly present the documentary: Engineering Pioneer – Frank Sprague.

Summary:

Over the course of a little less than twenty years, inventor Frank J. Sprague (1857-1934) achieved an astonishing series of technological breakthroughs--from pioneering work in self-governing motors to developing the first full-scale operational electric railway system--all while commercializing his inventions and promoting them (and himself as their inventor) to financial backers and the public.

At Glance

- **When:**
  Date: July 25, 2024
  Time: 05:30 – 7:00 PM (EST/EDT)
- **Where:**
  Online via Webex (to be shared only after you have a confirmed registration)
- **Audience: OPEN to ALL***

Sponsored by IEEE Computer Society Chapter In Southeastern Michigan

***Pre-Registration Required!**

https://events.vtools.ieee.org/m/417074

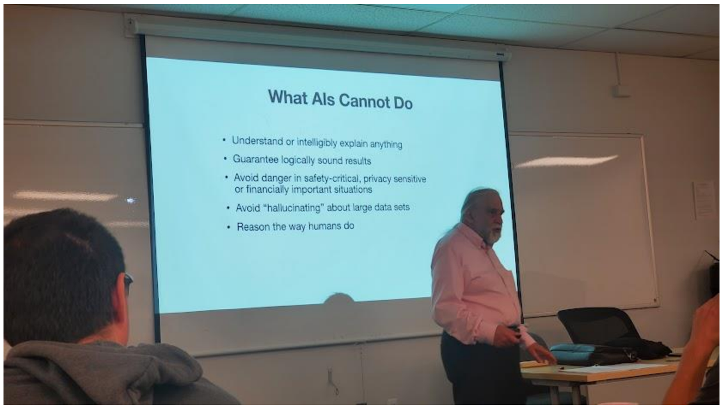
IEEE Advancing Technology for Humanity

IEEE Southeastern Michigan Section

Why Software Fails

Distinguished Speaker Series
David Fisher (retired CMU)
on
"Why Software Fails and why AI cannot help"

On June 20th, the IEEE Southeastern Michigan Computer Society Chapter and in co-operation with the IEEE Student Branch of Lawrence Technological University (LTU) of Southfield, co-hosted a distinguished speaker talk on "Why Software Fails and why AI cannot help". The speaker was Dr. David Fisher, Professor Emeritus from Carnegie Mellon University and a veteran in the field of modern computing.



What AIs Cannot Do

- Understand or intelligibly explain anything
- Guarantee logically sound results
- Avoid danger in safety-critical, privacy sensitive or financially important situations
- Avoid "hallucinating" about large data sets
- Reason the way humans do

Dr. Fisher spoke on the topic of artificial intelligence (AI); the constraints, history, and its current role in society in an hour+ long presentation. The audience was a healthy mixture of students, professors, industry professionals, and local IEEE members who all contributed to a diverse and engaging discussion. Without a doubt, Dr. Fisher's seminar generated several catalysts of thought and debate amongst attendees regarding AI's controversial claims and projections for the future. It was once widely believed that computers would enhance the speed, reliability, and applicability of human deductive reasoning in the physical and social sciences, much as motorized vehicles (e.g., cars, trains, airplanes) have enhanced the speed, reliability, and applicability of human manual abilities in transportation. Yet, 60 years later, computers can be used confidently only for paperwork tasks, analysis of regularly structured data, and simple process control applications. Complex software rarely satisfies user needs, is untrustworthy and difficult to maintain, and largely opaque to its users. Artificial intelligence (AI) methods including heuristics, machine learning, and statistical methods are in opposition to sound deductive reasoning. This presentation explained certain practical and logical impediments to computer enhancement of human deductive reasoning, the deductive limitations of modern programming languages, the role of AI, and provides some promising alternatives.

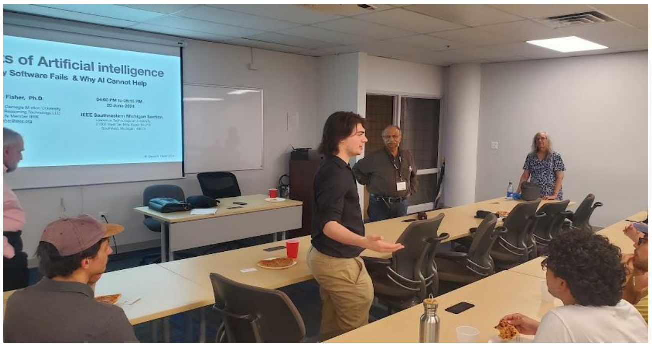
This event marked the return of IEEE's Student Branch at Lawrence Tech, the first of many more activities to come with the aid of dedicated student members. Read more about the LTU Student branch elsewhere in this issue.

This was also the second of a series of several Distinguished Speaker talks being organized and there are many more to come.

Speaker Bio:
David A Fisher is the founder and chief technologist at Reasoning Technology LLC and emeritus professor at Carnegie Mellon University (CMU). He has a Ph.D. in computer science from CMU, M.S.E from Moore School of Electrical Engineering at Univ. of Pennsylvania, and B.S. in mathematics from CMU. He was chief engineer for the CREATE high performance computing program within the Office of the Secretary of Defense, president of Incremental Systems Corporation, vice president for advanced development at Western Digital Corp (WDC), a program manager at National Institute of Standards and Technology (NIST), and a researcher at the Software Engineering Institute (SEI) . He has over 200 publications in programming language design, compiler construction, infrastructure protection and network security, bounded workspace and near linear time algorithms, embedded systems, theory of emergence, instruction set architectures, and high-performance computing. [He lectures in the U.S., Canada, and Europe.]. David can be reached at Email: dafisher@ieee.org

LTU Student Branch News

IEEE Student Branch at LTU gets new leadership!



Ben Tollis, LTU SB chair

This past June, The LTU Student branch along with the Computer Society Chapter, helped cohost the second Distinguished Speaker series talks. Assisting with the event were LTU students, Ben Tollis and Joseph Pielack; both students now hold officer positions in the IEEE student organization on campus. Ben Tollis, chair person, is currently an incoming senior pursuing bachelor's degrees in both electrical and computer engineering. He is actively involved in research projects in convolutional neural networks but also has interests in computer hardware and low-level programming. Outside of his role as a student and chairman, he serves as senior resident assistant of the freshman dormitory on LTU's campus where he leads a resident assistant team of fifteen. Ben is also involved in aiding administration in the university's departments of housing, student life, career services, and DEI. He is driven to make the school year successful and enriching for those pursuing interests in technology at LTU.

Joseph Pielack, LTU SB Treasurer

Joseph Pielack, jpielack@ltu.edu, also an incoming senior, serves as the IEEE Student Branch Treasurer and majors in audio engineering technologies at LTU. As an avid learner and musical specialist, Joseph is experienced in taking on personal engineering projects and giving them a creative twist. Recently, he has been handcrafting his own stratocaster guitar from scratch and has built several unique pedals for special effects. Joseph has developed a keen interest in the mechanics of sound and acoustics, anticipating to begin research soon. His campus involvement does not end at being a student, however, he is actively employed as an experienced resident assistant, having worked in multiple LTU housing facilities. Joseph is also a student employee of the Lawrence Tech buildLab, where he performs operations involving the following: wood cutting, laser cutting, CNC routing, and clay milling. His goal this year is to bring in new students and offer an environment that hosts excitement and action using applied engineering.

The fresh LTU IEEE student chapter is united under the concepts of teamwork, opportunity, and passion for the technological. These pillars have inspired LTU's members to develop a strong desire to accumulate new and prospective members. Great care is being taken by the branch officers to prime and prepare for the exciting new school year ahead, which will flip the script for a typical IEEE Student Branch. The weight of the term, "professional organization," will not connotate to a lack of enthusiasm, action, or equate to stiffness; the goal is for events to dispel this preconception. Plans include seminar series, research projects, lab workshops, study sessions, mixers, and more, where engaging elements will be applied to all. The team is highly optimistic about beginning these endeavors and would appreciate the support of fellow IEEE members and enthusiasts to make the LTU Student Branch experience the best it can be. Thanks to the IEEE SE Michigan Section for the opportunity and "Go Blue Devils!"

-Ben Tollis, btollis@ltu.edu
LTU IEEE Student Branch Chair

CANbus Attack Vectors

A Study of Attack Vectors on CAN Bus

Yashwanth Naidu Tikkisetty
yashwanthnaidut@oakalnd.edu
Dr. Subramaniam Ganesan
ganesan@oakland.edu

Abstract

In this study, we examine the vulnerabilities of the Controller Area Network (CAN) bus within the automotive industry, with a particular emphasis on maintaining a balance between operational efficiency and cybersecurity. The CAN bus, a cornerstone of vehicle communication systems, is increasingly subjected to a wide array of cyber threats that pose significant risks to vehicle safety and passenger privacy. Our investigation delves into various attack vectors, systematically categorizing them into direct manipulation, disruption, passive attacks, and protocol exploitation, hence giving an overview of possible attacks. Furthermore, this paper discusses the countermeasures currently in place to counter these threats, and at enhancing the security of CAN bus communications. Through a detailed analysis, including case studies, this paper aims to provide an in-depth overview of potential attacks on the CAN bus and evaluate the effectiveness of the countermeasures implemented to combat these challenges.

I. Introduction

The Controller Area Network (CAN) bus is the communication backbone connecting Electronic Control Units (ECUs) in modern automobiles, and it is essential to the coordination of intricate functions. As automobiles become more sophisticated, networked devices that ensure efficiency and security, the CAN bus plays a crucial role as a conduit for the seamless transfer and receiving of operational data between ECUs.

The operational integrity and privacy of car systems are seriously threatened by cyber threats that loom big over the automobile sector and are not immune to this crucial communication hub. This paper delves into the multifaceted cybersecurity challenges faced by the CAN bus, exploring a spectrum of attack vectors that range from direct manipulation and disruption to passive eavesdropping, protocol exploitation, and unauthorized access attacks.

The development of connected car technologies and the advent of advanced driver assistance systems (ADAS) have increased the attack surface and given hostile actors new ways to jeopardize vehicle safety. Studies such as those by Amato and Coppolino, and Kurbanov and Grebennikov, underscore the urgency of developing robust detection and mitigation strategies to shield the CAN bus from such vulnerabilities.

Through a comprehensive analysis, this paper aims to shed light on the intricate dynamics of CAN bus attacks, drawing on real-world case studies and pioneering research efforts. By examining the countermeasures currently in place, with a particular emphasis on encryption techniques, we try to chart a course towards secured automotive communication systems that can withstand the evolving area of cyber threats.
This overview aims to both clarify the critical security requirements related to the CAN bus and stimulate more academic discussion and advancement in the field of automotive cybersecurity. We open the door to improving vehicle resilience in the face of growing cyber threats by negotiating the complexity of CAN bus vulnerabilities and their implications.

Amato and Coppolino introduce a method based on deep learning to detect attacks on the CAN-bus. Their method is validated through the analysis of a real-world dataset that includes injected messages from various attack types, such as denial of service, fuzzy pattern attacks, and targeted attacks on specific components [1].

Kurbanov and Grebennikov illustrate how vehicles equipped with Advanced Driver-Assistance Systems (ADAS) can be compromised, enabling attackers to manipulate crucial vehicle modules through Acceleration/Wheel Steering Attacks [2].

Zhang and Binbin demonstrate the execution of frame injection attacks through the OBD port, enabling attackers to manipulate the vehicle's lighting, locking, and steering systems [3].

Ning and Wang devise two specific attacks, Spoofing and Bus-Off, on an actual vehicle, along with detection mechanisms for each, showcasing their practical applicability [4].

Farivar and Haghighi delve into the security aspects of smart cars' Adaptive Cruise Control Systems by executing two covert attacks on the speed regulator. They also introduce a novel intrusion detection and compensation method, validated through Matlab simulations, to counter such threats effectively [5].

Yun Yang, Zongtao Duan and Mark Tehranipoor demonstrate Injection of malicious code into an existing ECU and addition of malicious ECU to the network [6].

An attacker can gain access to an ECU by adding a malicious code to an existing ECU that performs the attack, or by introducing a malicious ECU to the network. Between these two paths of attacks, the path of adding a malicious code to an existing ECU is more dangerous because it can be performed remotely without the need for physical access to the vehicle, and it can be scaled to other vehicles that contain the same vulnerability. [7]

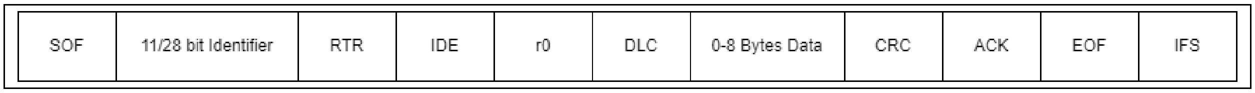
There is plenty more to be explored. However, we will have an overview of these attacks in the following sections.

II. Overview of CAN

CAN is a message-based protocol designed to allow microcontrollers and devices to communicate with each other within a vehicle without a central host computer. Introduced by Bosch in the mid-1980s, CAN was developed to meet the growing complexity of vehicle systems, aiming to reduce wiring harness sizes, improve reliability, and enhance performance.

CAN operates on a multi-master bus configuration, allowing each node (or ECU) on the network to transmit data and control messages independently. CAN employs a non-destructive bitwise arbitration process, ensuring that in cases of simultaneous transmission attempts, messages with higher priority (lower identifier values) are given precedence without data corruption.

The physical layer of CAN typically employs a differential signaling system over two wires, CAN High and CAN Low, enhancing resistance to electrical noise. The logical states, dominant (logical 0) and recessive (logical 1), are determined by the differential voltage between these wires, ensuring robust signal integrity even in the electrically noisy environments of vehicles.



SOF	11/28 bit Identifier	RTR	IDE	r0	DLC	0-8 Bytes Data	CRC	ACK	EOF	IFS

Fig -1: CAN Bus Frame

Data transmission in CAN is executed through frames, with the standard format encompassing several fields:

- Start of Frame (SOF): A single dominant bit marking the beginning of a frame. Send a dominant bit, bit '0'.
- Arbitration Field: Contains the identifier that determines the priority of the message and its type (data or remote). A standard CAN frame (CAN 2.0A) has 11-bit ID while extended CAN (CAN2.0B) frame has 29-bit ID.
- Remote Transmission Request(RTR): Allows the ECU to request messages from other ECUs by sending the recessive, '1' bit.
- IDE: Indicate the base format frame. (Standard CAN frame/Extended CAN frame).
- r0: Reserved bit/ Flexible Data Format (FDF) bit. Indicated whether the frame is Standard CAN or CAN FD.
- Data Length Code (DLC): Contains the length of the data in bytes (0-8 bytes).
- Data: The actual data to be transmitted. (0 to 8 bytes).
- CRC: Cyclic Redundancy Check, delimiter bit. Should be recessive bit, '1'.
- Acknowledgement Bit (ACK): Confirms the CRC bit.
- EOF: This end-of-frame (EOF), 7-bit field marks the end of a CAN frame (message) and disables bit stuffing, indicating a stuffing error when dominant.
- IFS–This 7-bit interframe space (IFS) contains the time required by the controller to move a correctly received frame to its proper position in a message buffer area.[8]

CAN's data transmission protocol ensures real-time communication, vital for the synchronous operation of vehicle systems, with mechanisms like bit stuffing and frame error checking to maintain data integrity.

The CAN protocol has some built in security features such as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), Collision Detection and Arbitration on Message Priority(CD+AMP) and 5 error checking methods; Start of Frame(SOF) single dominant bit for synchronization, Cyclic Redundancy Check(CRC) checksum for data integrity, Acknowledgement(ACK) bit for successful data transmission and End of Frame(EOF) bit for stuffing error and frame finalization. In addition to these, there are 2 other security features which are in form of Error Confinement Mechanism; Receiver Error Counter(REC) and Transmitted Error Counter(TEC).

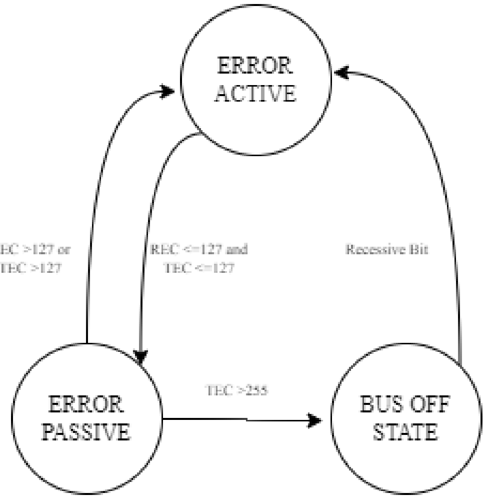


Fig 2: CAN Bus States

Each node has two counts that track errors: one for errors when receiving data (REC) and another for errors when sending data (TEC). If there's a mistake while sending, the TEC goes up by eight, and if the mistake is while receiving, the REC just goes up by one. If a node sends or receives a message without any problems, the count that went up goes down by one. All nodes start with zero counts and are in a normal working state. If a node's count goes over 127 because of too many errors, it goes into a quiet state where it doesn't interrupt the network. If the TEC count goes over 255, that node stops participating in the network altogether.

III. Categorization of Attacks

In this section, we delve into the classification of cyber-attacks targeting automotive systems, complemented by relevant case studies. We will explore the various types of attacks, examining their methodologies and impact. This comparative analysis aims to shed light on the diverse attack vectors and the mechanisms by which they compromise vehicle security.

A. Direct Manipulation Attacks

These attacks in the automotive industry would include injecting malicious data into the vehicle communication network targeting the CAN bus system. These attacks directly interfere with the normal operation of ECU by manipulating the messages exchanged between them.

i) Injection Attack

There was a demonstration of security vulnerabilities by Tobias Hoppe, Stefan Kiltz and Jana Dittmann which is outlined in their paper [9]. One of the core vulnerabilities exploited in theirs tests is the lack of inherent security measures in the CAN protocol; the absence of encryption and authentication mechanism. The authors focus on the electric window lift system of a vehicle. They introduce malicious code into an ECU connected to the CAN network, which is designed to activate under specific conditions, such as when the vehicle exceeds a certain speed. Once triggered, the malicious code sends unauthorized CAN messages that command the electric widow to open. This practical experiment showcases the feasibility of injection attacks on real automotive systems but also highlights the potential safety risks associated with such vulnerabilities.

An injection attack or a code reprogramming attack on a single ECU can affect all ECUs connected to the CAN. The attack is facilitated by the CAN protocols open nature, where messages broadcasted on the network lack encryption, making them readable and modifiable by any node within the network. The absence of authentication allows the injected malicious messages to appear legitimate to other ECUs, leading to unauthorized actions such as opening the electric window. This type of attack demonstrates a direct manipulation attack where the attacker actively alters the system's operation by injecting malicious data into the network.

ii) Fuzzing Attack

This attack involves deliberately introducing malformed or random data into the vehicles network to elicit unpredictable responses, errors, or system crashes. This attack can be seen demonstrated in [10], where they manipulated the CAN to seize control over vital modules including the brake and engine control units through the On-Board Diagnostics II (OBD-II) port. The attack was executed by persistently employing the continuous fuzzing method, which led to the deactivation of the brake system while the vehicle was in motion at 40mph, alongside tampering with the instrument cluster with false data, altering engine parameters and disabling the engine altogether.

iii) Frame Falsifying Attack

Frame Falsifying Attacks involve altering legitimate CAN message frames to include false data, misleading the receiving ECUs and potential leading to incorrect operations or system states. This attack could be leveraged to falsify critical data such as sensor readings, vehicle speed or system status indicators, leading to unsafe driving conditions or enabling further exploitations of the vehicles systems. Executing a Frame Falsifying Attack requires the attackers to have some level of access to the CAN network, which could be achieved through direct physical conditions like OBD-II port or remotely via vulnerabilities in the vehicle's wireless communication interfaces such as Bluetooth or cellular connections.

iv) Spoofing Attack/ ECU Impersonation

A Spoofing attack involves an attacker sending fraudulent messages that mimic those of a legitimate ECU. This type of attack exploits the lack of authentication mechanisms in the CAN protocol, allowing malicious entities to inject or alter messages within the network without detection.

One such attack was demonstrated by researchers [6]. The study introduces an approach utilizing a Recurrent Neural Network with long Short-Term Memory (RNN-LSTM) units. This advanced machine learning model is trained to recognize the unique fingerprint signals emitted by each ECU during normal operation. By analyzing these signals, the RNN-LSTM classifier can discern between legitimate messages and those modified by the attackers aiming to spoof the system. The researchers detail the process of generating these ECUU fingerprint signals for model training, emphasizing the need for diverse dataset that accurately is demonstrated through its ability to accurately authenticate ECU in real-time.

B. Disruption Attacks

Disruption attacks are designed to interrupt or degrade the normal operation of the vehicle's network communication. These attacks can take various forms but generally aim to overwhelm the system with traffic or exploit specific vulnerabilities to prevent the normal flow of communication between ECUs.

i) Denial Of Service (DoS) Attack/ Bus-Off Attack

Zixiang Bi and Guoai Xu discuss the DoS attack in their research article [11]. This Attack leverages the shared bus resources of the CAN system. In a DoS attack scenario, a malicious ECU can increase bus occupancy by sending high-priority messages without adherence to the bus protocol, causing delays or complete suspension of other messages. They describe on how attackers can execute DoS attacks by injecting high-priority messages into the CAN bus, preventing the delivery of other critical messages. This attack can paralyze the vehicles functionality or lead to abnormal ECU reactions rather than merely disrupting regular message delivery.

ii) Flood Attack

The flood attack involves overwhelming the network with excessive traffic, thereby saturating the communication channel, and preventing legitimate messages from being transmitted effectively. This can lead to degradation in vehicle performance, potentially compromising critical functionalities such as braking, steering or engine control.

In normal scenario, the CAN bus adheres to a priority-based arbitration scheme, where messages with lower identifier values are given precedence. In a flood attack case, the attacker exploits this mechanism by continuously transmitting high-priority messages, effectively monopolizing the bus. This sustained flood of messages creates a bottleneck, leading to significant delays or complete blocking of legitimate lower-priority messages critical for the vehicle's operational safety and efficiency. [12] talks about the subtilities of detecting attacks such as flood attacks and highlights the need for sophisticated Intrusion Detection System (IDS) that are adept at discerning between actual high-frequency traffic and malicious flooding.

C. Passive Attacks

Passive attacks involve stealthy monitoring and interception of data without directly interfacing with the network's operation. Unlike active attacks that disrupt or manipulate data flow, in passive attacks, the attackers eavesdrop on the communication between ECU undetected.

i) Sniffing Attack

Sniffing attacks are primarily categorized as passive, where the attackers covertly eavesdrop on the traffic without altering or interrupting the flow data. This passive characteristic makes sniffing insidious as it can be challenging to detect the presence of a sniffer on the network. Attackers leverage sniffing to gather sensitive information such as user credentials, account details and other critical data that can be transmitted in clear text over the network. Sniffing attacks can lead to more sever cybersecurity incidents, such as Distributed Denial of Service (DDoS) attacks, Man-In-The-Middle attacks, and data theft.

There are various methodologies that attackers use in sniffing attacks to gain access to data. Once such form of sniffing attack is highlighted by the author B. Prabadevi and N. Jeyanthi. They [12] talk about MAC flooding attack which is a variation of Denial of Service (DoS) attack. The method mentioned involves flooding a network switch with an excessive number of MAC address requests. The sheer volume of these requests forces the switch into a fail-open mode, effectively transforming it into a hub that broadcasts all incoming requests across the network, rather than directing them to the appropriate port. This state of the switch enables the attacker's sniffers to capture sensitive information that would typically be restricted. As a counter measure for this attack, a 'switch port-security' feature is offered by Cisco, which limits the input from unauthorized hosts by scrutinizing the MAC addresses. This security feature along with others like IPv6 adoption and encrypted sessions, plays a crucial role in safeguarding against sniffing attacks by imposing strict controls on network access and data transmission.

ii) Man in The Middle Attack

Unlike passive eavesdropping, MITM attacks are active, involving the interception, alteration or fabrication of messages exchanged between the victims. This allows attackers not only to stealthily listen in on the conversation but also to manipulate the information being transmitted. The execution of MITM attack begins with the attacker establishing independent connections with the victims, tricking both into believing they are directly communicating with each other. Once this deceptive setup is established, the attacker gains the ability to intercept and alter the data flowing between the two parties. This breach can lead to sever consequences, including the theft of sensitive information such as login credentials, personal data, financial information, and corporate secrets.

A MITM was demonstrated in the context of monitoring nodes. The paper [14] delves into this attack vector with focus on monitoring node's vulnerability to MITM attacks. In the demonstrated scenario, the adversary could access message bodies for eavesdropping purposes, but their attempts at injecting forgeries were thwarted by the presence of a Message Authentication Code (MAC). The monitor node, crucial for removing malicious frames by replacing them with error frames after MAC verification, had to be directly connected to the monitoring CAN bus to function effectively. To counteract potential MITM attacks, it was suggested that a pivotal node, such as an engine control unit or a central gateway, assume the monitor node's responsibilities.

D. Protocol Exploitation

Protocol Exploitation attacks target the inherent vulnerabilities and limitations within the CAN protocol itself, leveraging its standard operations to carry out malicious activities. These attacks exploit the protocol's design to introduce unauthorized actions or behaviors within the vehicle's network without necessarily injecting new messages.

i) Replay Attack

Replay attacks involves attacker recording actual messages from the network and then playing them back later. This type of attack can cause unintended behaviors in the vehicle's systems by replaying previous real actions at inappropriate times. The researchers from Beijing University have simulated a replay attack on test vehicles by injecting a set of CAN messages that were previously recorded and ordered into the CAN bus [11] . They generated Replay Attack datasets by randomly inserting segments of these prerecorded CAN messages into regular traffic traces. The experiment demonstrated that the Replay attack could cause the test vehicle to repeat some of its previous operations, such as adjusting air conditioning settings, switching gears, and moving windows. They found that the Replay attack was challenging to identify due to its nature of using legitimate messages.

ii) Double Receive Attack

This refers to an attack scenario where the attackers force a network node like ECU, to receive the same message twice. This could be problematic to the system as the timing, or the uniqueness of a message is critical for operation. For example, receiving a command to apply brakes twice in quick succession could have unintended consequences. A hypothetical scenario was devised [6], where an attacker compromises an ECU to send fraudulent messages. These messages could mimic those from a legitimate source, effectively confusing the receiving units. The scenario depicted involves three ECUs on a CAN bus, with one being malicious. The malicious ECU sends a spoofed message pretending to be from a trusted ECU, exploiting the CAN protocol's lack of authentication to make the receiving ECU accept the fraudulent message. This kind of attack could lead to unauthorized actions or disrupt the vehicle's normal operation.

To counteract such threats, the researchers proposed an intrusion detection system using a Recurrent Neural Network (RNN) with Long Short-Term Memory (LSTM) units. This advanced machine learning model was trained to distinguish between legitimate and modified messages by recognizing the unique 'fingerprints' of ECU signals during normal operations. The researchers simulated ECU signals to generate a sufficient dataset for training the RNN-LSTM model. They then adjusted the model parameters to capture the unique ECU fingerprint signals, producing a significant number of sample fingerprints for a diverse set of ECUs.

The simulation results showed that the RNN-LSTM model could effectively identify spoofed messages by analyzing the unique signal characteristics of each ECU. The model's performance was measured against traditional classifiers like Bagged Decision Trees, Neural Networks, and Support Vector Machines, demonstrating superior accuracy in detecting spoofing attacks.

IV. Counter Measures for CAN Bus Attacks

Although there are possible attack scenarios on CAN bus, there are several counter measures implemented with improvements throughout the years for these attacks. CAN is essential for the seamless operation of numerous vehicle functions but also has become a focal point for potential cybersecurity threats. As vehicles become increasingly connected and reliant on digital systems, the security of the CAN bus is paramount to ensuring the safety and privacy of passengers. Recognizing the inherent vulnerabilities within the CAN protocol, which lacks built-in security features such as encryption and authentication, researchers and cybersecurity professionals have dedicated substantial efforts to devising robust countermeasures. These strategies are designed to fortify the CAN bus against a spectrum of attacks, ranging from message injection and spoofing to more sophisticated man-in-the-middle and replay attacks. The following discussion delves into the multifaceted approaches developed to shield the CAN bus from such threats, encompassing advanced cryptographic techniques, intrusion detection systems, secure boot schemes, and other security measures.

a. Cryptographic Algorithms: The use of cryptographic encryption ensures the confidentiality of CAN messages, while cryptographic MACs (Message Authentication Codes) and digital signatures authenticate the sender, thereby preventing a range of attacks including sniffing, injection, ECU impersonation, and frame falsifying. However, this approach requires changes to all CAN nodes, increases communication latency, may alter CAN bus behavior, and relies on the secrecy and strength of the used keys [7].

b. Intrusion Detection Systems (IDS): These systems employ machine learning and deep learning algorithms to detect anomalies in CAN messages, effectively identifying various attacks such as fuzzing, injection, ECU impersonation, DoS (Denial of Service), and frame falsifying attacks. Despite their capabilities, IDS systems may lack mitigating actions, fail to detect all attacks, especially minor deviations, introduce communication latency, and depend heavily on data training [7].

c. Secure Boot Scheme: This scheme uses cryptographic integrity algorithms at the ECU level to detect the presence of malicious code and take necessary actions to prevent it from affecting the CAN bus. This approach helps prevent attacks originating from malicious code injections, offering the added benefit of mitigating risks associated with executing malicious code that does not directly affect the CAN bus. While effective, the secure boot scheme necessitates changes to all CAN nodes and cannot detect attacks involving added malicious ECUs [7].

d. Physical and Network Layer Protections: Countermeasures include filter methods to avoid undesired signals, spatiotemporal challenge-response methods for detecting spoofing, and signal encryption to prevent GPS spoofing. Also, physical challenge-response authentication and anonymity encryption techniques are suggested to secure subsystems like TPMS (Tire Pressure Monitoring Systems) and WSS (Wheel Speed Sensors) [15].

e. Advanced Protocols and Firewalls: Proposals include the use of AES (Advanced Encryption Standard) encryption with MAC for securing CAN bus communications, as well as secure gateways and firewalls to protect against unauthorized access and ensure only authorized ECUs can communicate [15].

f. Diverse Data Security Techniques: Approaches such as multifactor authentication and stronger cryptographic algorithms are suggested to enhance the security of passwords, keys, and overall network communications [15].
These countermeasures highlight the multifaceted approach required to protect the CAN bus from a wide range of security threats, emphasizing the need for encryption, authentication, intrusion detection, and secure communication protocols to safeguard vehicular networks.

V. Conclusion

Within the complex network of car communications, the Controller Area Network (CAN) bus is a critical, but weak, link in the field of automotive cybersecurity. Upon examining the many aspects of CAN bus vulnerabilities, attack vectors, and countermeasures, it is clear that striking a balance between operational efficiency and cybersecurity is not only desirable but also essential for protecting vehicle passengers' privacy and safety.

The numerous cyberthreats that threaten the CAN bus have been methodically examined in this study. These dangers range from direct manipulation and protocol exploitation to disruptive assaults and passive eavesdropping. Every type of attack highlights the creativity of bad actors as well as the CAN protocol's built-in weaknesses, which are the absence of encryption and authentication procedures.

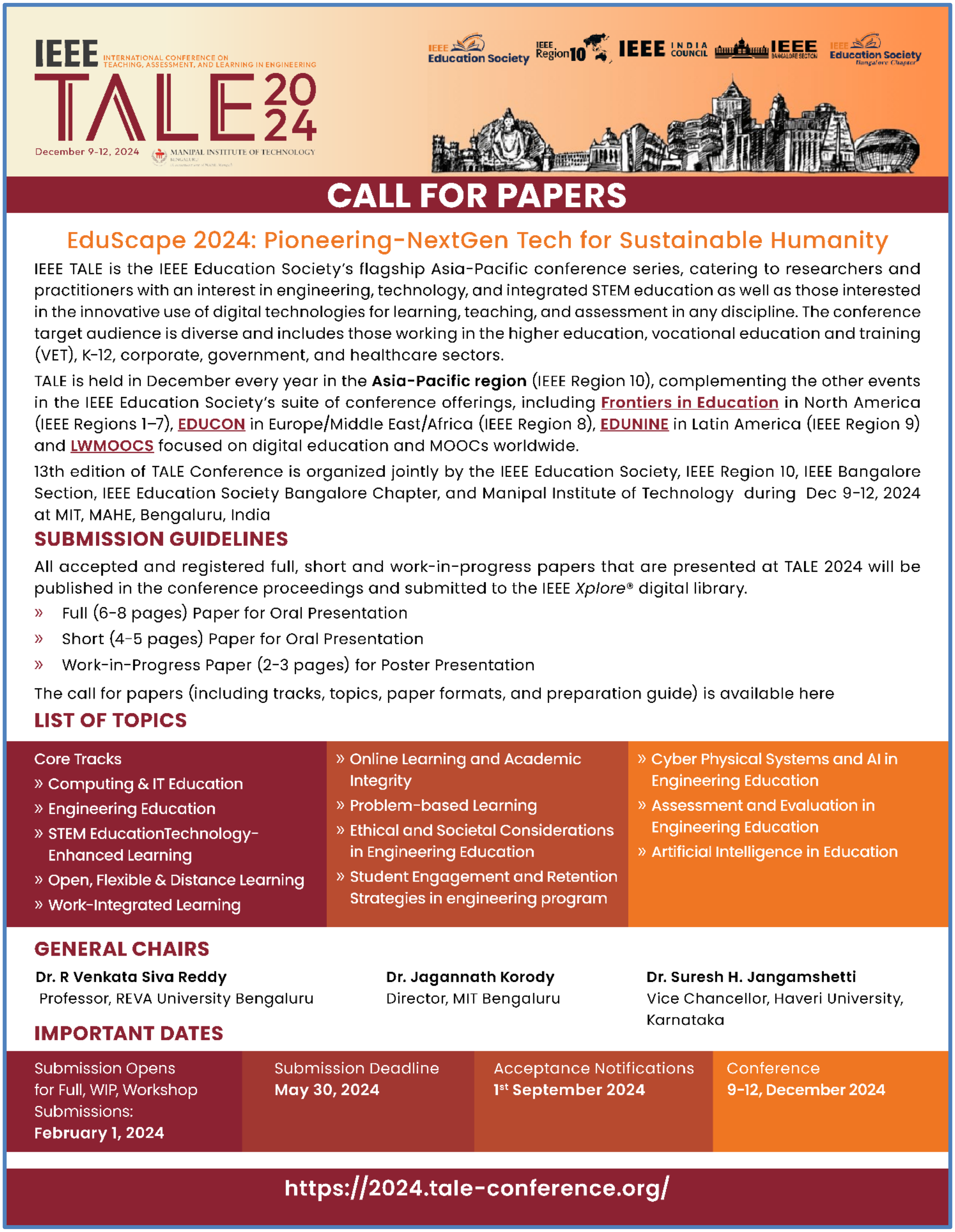
We have investigated how these vulnerabilities might be used to undermine vehicle safety through innovative research and real-world case studies. These vulnerabilities range from sophisticated spoofing attacks that imitate authentic ECUs to injection attacks that modify ECU communications. These scenarios provide a clear picture of the possible outcomes of unresolved security flaws, ranging from the interruption of vital safety systems to illegal control of vehicle activities.
In light of this, the countermeasures covered in this article—which range from sophisticated network protocols and secure boot methods to cryptographic algorithms and intrusion detection systems—act as the CAN bus's first line of defense against cyberattacks. These tactics set the stage for a more secure automotive future in addition to improving the secrecy, integrity, and availability of CAN communications.

In conclusion, protecting the CAN bus in contemporary cars necessitates a complex fusion of cutting-edge cryptography methods, live intrusion detection systems, and durable hardware security modules—all of which must be incorporated inside a strong security-by-design framework. Adoption of these diverse technical countermeasures is critical as cars develop into highly networked and autonomous systems, protecting vehicular communications availability, integrity, and secrecy from an ever-growing array of cyberthreats. The future automotive infrastructure depends on this all-encompassing approach to cybersecurity, which is supported by constant innovation and strict validation. It also strengthens user privacy and safety in the digital era of transportation.

VI. References

[1] Amato, F., Coppolino, L., Mercaldo, F., Moscato, F., Nardone, R., Santone, A.: CAN-bus Attack Detection with Deep Learning. IEEE https://doi.org/10.1109/TITS.2020.3046974
[2] Kurbanov, A., Grebennikov, S., Gafurov, S., Klimchik, A.: Vulnerabilities in the vehicle's electronic network equipped with ADAS system. https://doi.org/10.1109/DCNAIR.2019.8875529
[3] Zhang, Y., Ge, B., Li, X., Shi, B., Li, B.: Controlling a car through OBD injection. https://doi.org/10.1109/CSCloud.2016.42
[4] Ning, J., Wang, J., Liu, J., Kato, N.: Attacker identification and intrusion detection for in-vehicle networks. https://doi.org/10.1109/LCOMM.2019.2937097
[5] Farivar, F., Sayad Haghighi, M., Jolfaei, A., Wen, S.: On the security of networked control systems in smart vehicle and its adaptive cruise control. https://doi.org/10.1109/TITS.2021.3053406
[6] Yun Yang, Zongtao Duan, Mark Tehranipoor,: Identify a Spoofing Attack on an In-Vehicle CAN Bus Based on the Deep Features of an ECU Fingerprint Signal. https://www.mdpi.com/2624-6511/3/1/2
[7] Adly, S., Moro, A., Hammad, S., Maged, S.A.: Prevention of Controller Area Network (CAN) Attacks on Electric Autonomous Vehicles. https://doi.org/10.3390/app13169374
[8] Introduction to Controller Area Network (CAN), Texas Instruments Application Report.
[9] Tobias Hoppe, Stefan Kiltz and Jana Dittmann.: Security Threats to Automotive CAN Networks- Practical Examples and Selected Short-Term Countermeasures. https://link.springer.com/chapter/10.1007/978-3-540-87698-4_21
[10] Mehmet Bozdal, Mohammad Samie, Sohaib Aslam and Ian Jennions.: Evaluation of CAN Bus Security Challenges. https://www.mdpi.com/1424-8220/20/8/2364
[11] Zixiang Bi, Guoai Xu, Guosheng Xu, Miaoqing Tian, Ruobing Jiang and Suato Zhang.: Intrusion Detection Method for In-Vehicle CAN Bus Based on Message and Time Transfer Matrix. https://www.hindawi.com/journals/scn/2022/2554280/
[12] Siti-Farhana Lokman, Abu Talib Othman and Muhammad-Husaini Abu-Bakar.: Intrusion detection system for automotive Controller Area Network (CAN) bus systems: a review. https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-019-1484-3
[13] B. Prabadevi, N. Jeyanthi.: A Review of Various Sniffing Attacks and its Mitigation Techniques. https://www.researchgate.net/publication/329467167_A_Review_on_Various_Sniffing_Attacks_and_its_Mitigation_Techniques
[14] Ryo Kurachi, Yutaka Matsubara, Hiroaki Takada.: CaCAN- Centralized Authentication System in CAN. https://www.researchgate.net/publication/320083914_CaCAN_-_Centralized_Authentication_System_in_CAN
[15] Bhavesh Raju.M, Prabhat Thakur and Ghanshyam Singh.: Aspects of Cyber Security in Autonomous and Connected Vehicles. https://doi.org/10.3390/app13053014

TALE 2024


IEEE Education Society
IEEE Region 10
IEEE INDIA COUNCIL
IEEE BANGALORE SECTION
IEEE Education Society Bangalore Chapter
MANIPAL INSTITUTE OF TECHNOLOGY BENGALURU

IEEE INTERNATIONAL CONFERENCE ON TEACHING, ASSESSMENT, AND LEARNING IN ENGINEERING

TALE 2024

December 9-12, 2024

CALL FOR PAPERS

EduScape 2024: Pioneering-NextGen Tech for Sustainable Humanity

IEEE TALE is the IEEE Education Society's flagship Asia-Pacific conference series, catering to researchers and practitioners with an interest in engineering, technology, and integrated STEM education as well as those interested in the innovative use of digital technologies for learning, teaching, and assessment in any discipline. The conference target audience is diverse and includes those working in the higher education, vocational education and training (VET), K-12, corporate, government, and healthcare sectors.

TALE is held in December every year in the **Asia-Pacific region** (IEEE Region 10), complementing the other events in the IEEE Education Society's suite of conference offerings, including **Frontiers in Education** in North America (IEEE Regions 1–7), **EDUCON** in Europe/Middle East/Africa (IEEE Region 8), **EDUNINE** in Latin America (IEEE Region 9) and **LWMOOCS** focused on digital education and MOOCs worldwide.

13th edition of TALE Conference is organized jointly by the IEEE Education Society, IEEE Region 10, IEEE Bangalore Section, IEEE Education Society Bangalore Chapter, and Manipal Institute of Technology during Dec 9-12, 2024 at MIT, MAHE, Bengaluru, India

SUBMISSION GUIDELINES

All accepted and registered full, short and work-in-progress papers that are presented at TALE 2024 will be published in the conference proceedings and submitted to the IEEE *Xplore*® digital library.

» Full (6-8 pages) Paper for Oral Presentation

» Short (4-5 pages) Paper for Oral Presentation

» Work-in-Progress Paper (2-3 pages) for Poster Presentation

The call for papers (including tracks, topics, paper formats, and preparation guide) is available here

LIST OF TOPICS

Core Tracks

» Computing & IT Education

» Engineering Education

» STEM EducationTechnology-Enhanced Learning

» Open, Flexible & Distance Learning

» Work-Integrated Learning

» Online Learning and Academic Integrity

» Problem-based Learning

» Ethical and Societal Considerations in Engineering Education

» Student Engagement and Retention Strategies in engineering program

» Cyber Physical Systems and AI in Engineering Education

» Assessment and Evaluation in Engineering Education

» Artificial Intelligence in Education

GENERAL CHAIRS

Dr. R Venkata Siva Reddy
Professor, REVA University Bengaluru

Dr. Jagannath Korody
Director, MIT Bengaluru

Dr. Suresh H. Jangamshetti
Vice Chancellor, Haveri University, Karnataka

IMPORTANT DATES

Submission Opens for Full, WIP, Workshop Submissions:
February 1, 2024

Submission Deadline
May 30, 2024

Acceptance Notifications
1st September 2024

Conference
9-12, December 2024

https://2024.tale-conference.org/

ORG UNITS cheat sheet

Section Unit Name or Affinity Group or Chapter Name (Organizational Unit code is in parentheses)
Consultants Network Affinity Group: (CN40035)
Life Members: (LM40035)
Young Professionals: (YP40035)
Women in Engineering: (WE40035)
Chapter: 01 (CH04049) (SP01) Signal Processing Society, (CAS04) Circuits and Systems Society and (IT12) Information Theory Society
Chapter: 02 (CH04051) (VT06) Vehicular Technology Society
Chapter: 03 (CH04053) (AES10) Aerospace and Electronic Systems Society and (COM19) Communications Society
Chapter: 04 (CH04050) (AP03) Antennas and Propagation Society, (ED15) Electron Devices Society, (MTT17) Microwave Theory and Techniques Society,
Chapter: 05 (CH04055) (C16) Computer Society
Chapter: 06 (CH04056) (GRS29) Geosciences and Remote Sensing Society
Chapter: 07 (CH04057) (PE31) Power Engineering Society, (IA34) Industrial Applications Society
Chapter: 08 (CH04088) (EMC27) Electromagnetic Compatibility Society
Chapter: 09 (CH04087) (IE13) Industrial Electronics Society, (PEL35) Power Electronics Society
Chapter: 10 (CH04142) (TEM14) Technology and Engineering Management Society
Chapter: 11 (CH04099) (EMB18) Engineering in Medicine & Biology
Chapter: 12 (CH04103) (CS23) Control Systems Society
Chapter: 13 (CH04113) (E25) Education Society
Chapter: 14 (CH04115) (RA24) Robotics And Automation Society
Chapter: 15 (CH04144) (NPS05) Nuclear Plasma Sciences Society
Chapter: 16 (CH04125) (CIS11) Computational Intelligence Society, (SMC28) Systems, Man and Cybernetics Society
Chapter: 17 (CH04128) (NANO42) Nanotechnology Council
Chapter: 18 (CH04162) (MAG33) Magnetics Society
Section Unit Name or Affinity Group or Chapter Name (Organizational Unit code is in parentheses)
University Of Detroit-Mercy: (STB00531)
Michigan State University: (STB01111)
University Of Michigan-Ann Arbor: (STB01121)
Wayne State University: (STB02251)
Lawrence Technological University: (STB03921)
Oakland University: (STB06741)
Eastern Michigan University: (STB11091)
University of Michigan-Dearborn: (STB94911)

Use the Geo-unit ‘Code’ for faster access in the vTools system applications.

HKN Code	HKN Name (Student IEEE Honor Society)
HKN029	University of Michigan-Ann Arbor, Beta Epsilon
HKN042	University of Detroit-Mercy, Beta Sigma
HKN054	Michigan State University, Gamma Zeta
HKN073	Wayne State University, Delta Alpha
HKN163	University of Michigan-Dearborn, Theta Tau
HKN164	Lawrence Institute of Technology, Theta Upsilon
HKN190	Oakland University, Iota Chi
HKN244	Southeastern Michigan Alumni

Organization Unit IEEE Code	Student Technical Chapter name
SBC00531	University of Detroit-Mercy, Computer Society Chapter
SBC02251	Wayne State University, Computer Society Chapter
SBC03921	Lawrence Tech University, Computer Society Chapter
SBC06741	Oakland University, Engineering in Medicine & Biology

Why do we publish this? Well, this is most useful when searching the vTools page for entering L31s or creating new events or searching for existing events!

Curated & Maintained By
Sharan Kalwani,
Chair, IEEE Southeastern Michigan Section (2022-2024)
Editor, Wavelengths (*Serving you as an active newsletter contributor since 2018)*
Enthusiastic IEEE volunteer since 2011

Use the Geo-unit ‘Code’ for faster access in the vTools system applications.

Activities & Events

We try to publish IEEE events in several places to ensure that everyone who may want to attend has all the available relevant information. **NOTE: The IEEE SE Michigan section website is located at http://r4.ieee.org/sem/**

SEM Wavelengths:
https://r4.ieee.org/sem/about-sem/sem-history/wavelengths-magazine-archive/

SEM Calendar of events:
https://r4.ieee.org/sem/sem-calendar/
Select “SEM Calendar” button in the top row of the website. This is our ‘Active’ event listing site where everyone should look first to see what events are scheduled for our Section in the near future.

SEM Collabratec Workspace:
https://ieee-collabratec.ieee.org/app/workspaces/5979/IEEE-Southeastern-Michigan-Section/activities
An IEEE supported space for online chat, discussions, connecting with other global IEEE entities, besides our local Michigan folks.

vTools Meetings:
http://sites.ieee.org/vtools/
Select “Schedule a Meeting” button in the left-hand column of buttons.

Other Happenings

Here are some of the non-IEEE functions that may be of interest to you or someone you know. Let us know if you have a special interest in a field that encourages technical study and learning and wish to share opportunities for participation with members of the section. NOTE: Copy the URL and paste it into your browser address bar.
These websites were checked in June 2022 and found viable.
Send details to: wavelengths@ieee-sem.org OR letters@ieee-sem.org

Michigan Institute for Plasma Science and Engineering: Seminars for the academic year:
https://mipse.umich.edu/seminars.php

Model RC Aircraft
http://www.skymasters.org

Model Rocketry
https://www.nar.org/find-a-local-club/nar-club-locator/

Astronomy
http://www.go-astronomy.com/astro-clubs-state.php?State=MI

Experimental Aircraft Association
https://www.eaa.org/en/eaa/eaa-chapters/find-an-eaa-chapter

Robots
https://www.robofest.net/index.php/about/contact-us

Science Fiction Conventions
https://2022.penguicon.org/

http://www.confusionsf.org/

Mad Science
http://www.madscience.org/

ESD PE Review Class
https://www.esd.org/programs/pe/

Maker Faire:
https://swm.makerfaire.com/

It appears that the SouthWest Michigan Maker Faire was a casualty of the Global Pandemic, as were many of our friends and several organizations.

However, we retain this link for anyone wishing to make contact and consider pumping life back into what was a wonderful experience.

Executive Committee

The Executive Committee is the primary coordination unit for Southeastern Michigan (SEM) IEEE operations. The basic organization chart below shows the 2023 arrangement of communications links designed to provide inter-unit coordination and collaboration.

The SEM Executive Committee meets in a teleconference each month on usually on a Thursday at 6:30 pm. The specific meeting days, times, phone or WebEx numbers and log in codes are published on the IEEE SEM Website calendar: **http://r4.ieee.org/sem/** Click on the "Calendar" button in the top banner on the first page of the web site.

If you wish to attend, or just monitor the discussions, please contact **Christopher Johnson**, the section secretary at secretary@ieee-sem.org and request to be placed on the distribution list for a monthly copy of the agenda and minutes. More meeting details are available on the next page of this newsletter.

Other Meetings:
About half of our members maintain memberships in one or more of the IEEE technical societies, which automatically makes them members of the local chapter which is affiliated with that society. As a result, they should receive notices of the local chapter meetings each month.

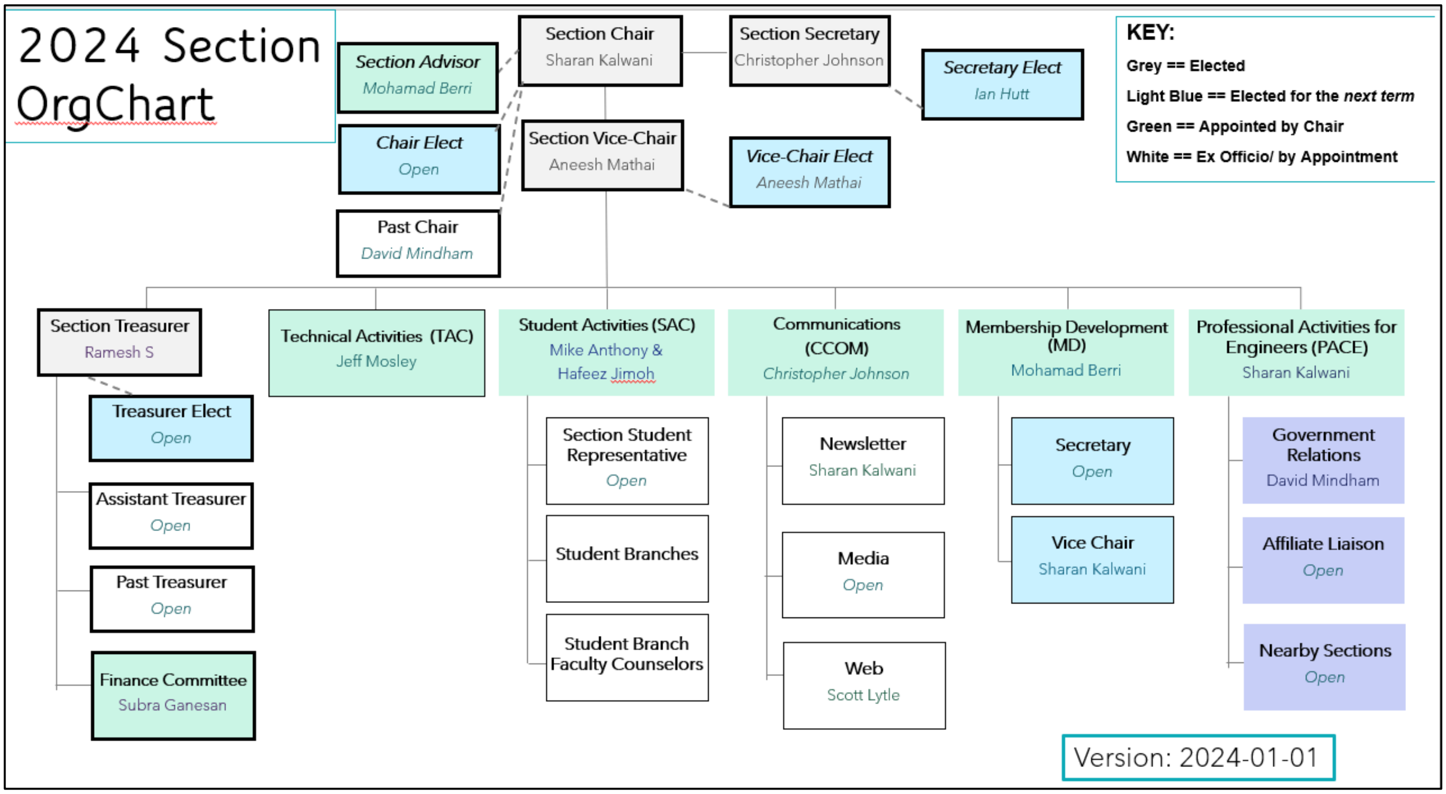
However, members of the section may have multiple technical interests and would like to have meeting information of other chapters. In order to communicate the meeting dates of all the chapters, affinity groups etc., to our members to facilitate their attendance, leaders of the groups are requested to send meeting information to our webmasters for posting on section's calendar.

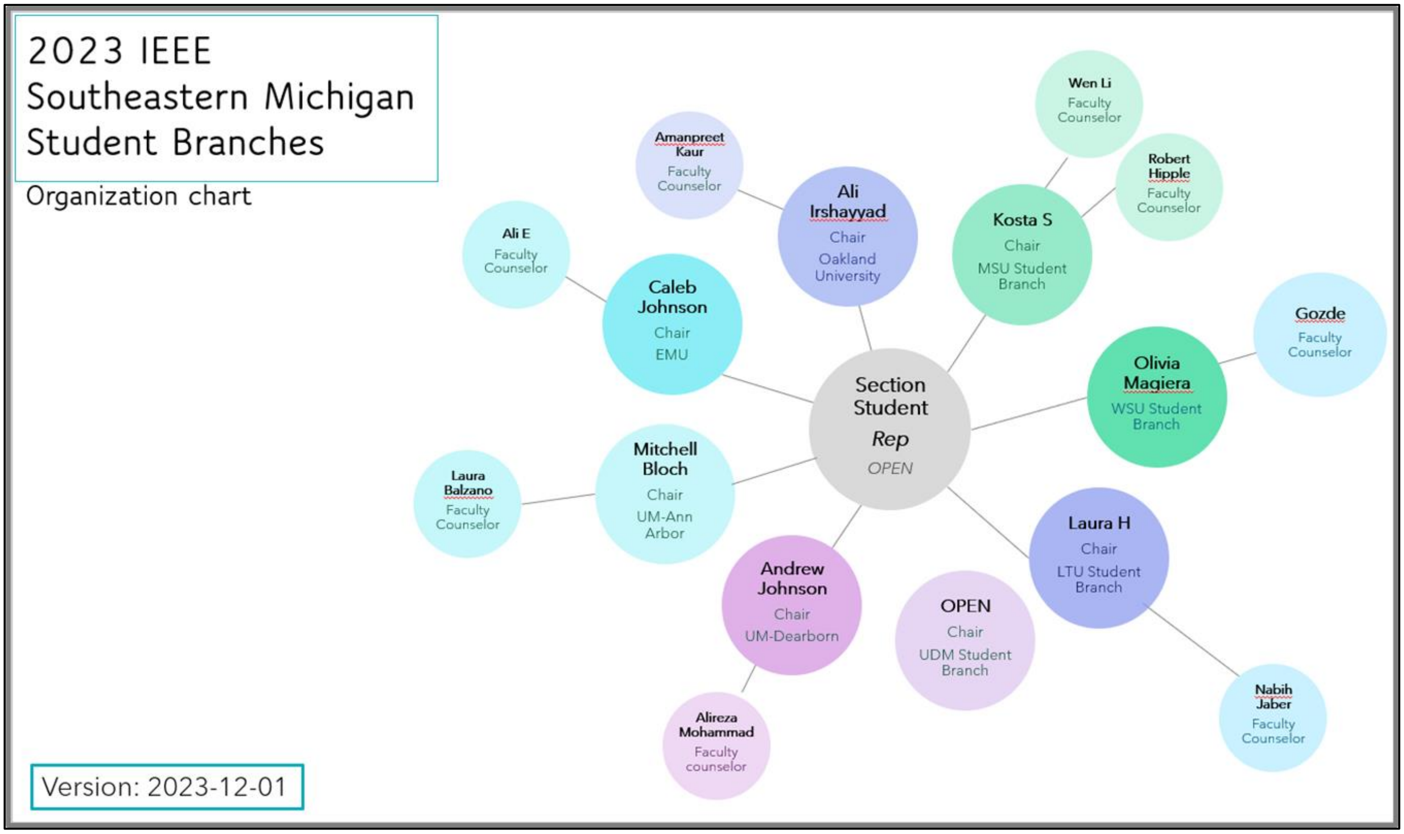
More detailed information on meetings may be found through the IEEE SEM Website: **http://r4.ieee.org/sem/** and clicking on the **SEM meetings list** button near the bottom of the left-hand banner.

Automatic e-mail notification of web updates may be received using the "**Email Notifications**" button at the top of the **SEM Tools/Links** side banner.

Christopher Johnson (Secretary)
Email: secretary@ieee-sem.org

If you wish to download the complete SEM Organization Chart, in PDF format, it will be made available soon at http://r4.ieee.org/sem/ . In the meantime, you may use the diagram below (recently refreshed!)





ExCom Meeting Schedule

NOTE: All SEM members are invited to attend ALL ExCom (Executive Committee) meetings:

Below is the 2024schedule for the Section ExCom meetings with links to add the events to your calendar. It is important that ***at least one person*** from each Chapter/Affinity Group attends each scheduled ExCom meeting. Please mark your calendars for the 2024 meetings. Or link your personal calendar to the SEM Web calendar.

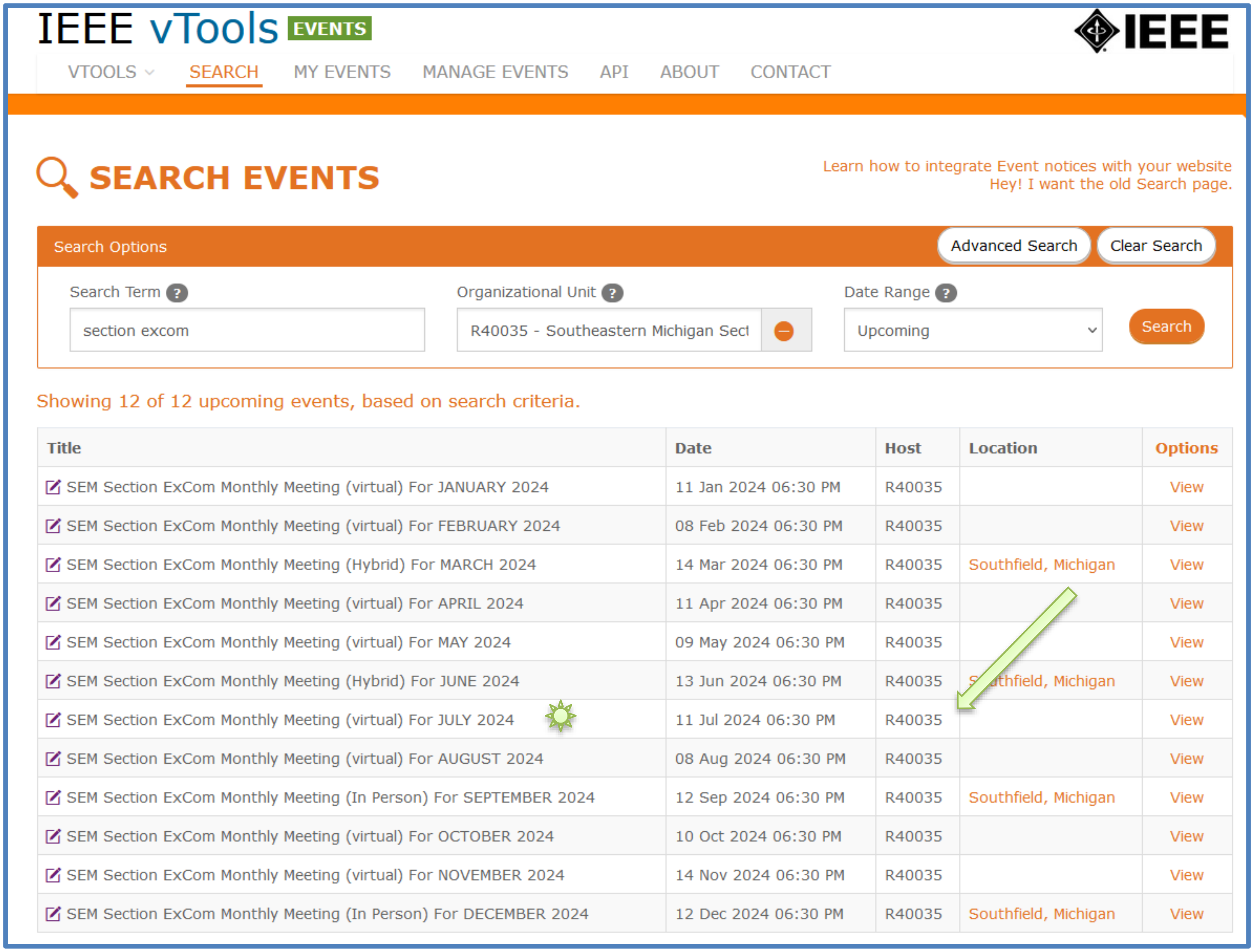
Section Administrative Committee (ExCom) Meeting Schedule for 2024: (clickable links)

Note: All IEEE Members are welcome at any IEEE meeting, at any time but please register so we can be sure to accommodate you. This month's meeting is highlighted in **Bold**.

ExCom Meeting (all clickable links)	***Date & Start Time, Duration***
Section ExCom Monthly Meeting (virtual) For JULY	11 Jul 6:30 PM, 1 hour
Section ExCom Monthly Meeting (virtual) For AUGUST	08 Aug 6:30 PM, 1 hour
Section ExCom Monthly Meeting (Hybrid) For SEPTEMBER	12 Sep 6:30 PM, 2 hours
Section ExCom Monthly Meeting (virtual) For OCTOBER	10 Oct 6:30 PM, 1 hour
Section ExCom Monthly Meeting (virtual) For NOVEMBER	14 Nov 6:30 PM, 1 hour
Section ExCom Monthly Meeting (In Person) For DECEMBER	12 Dec 6:30 PM, 2 hours

Christopher Johnson (Secretary)
Email: secretary@ieee-sem.org

Section Administrative Committee (ExCom) Meeting Schedule for 2024: (screen snapshot)



SEARCH EVENTS

Learn how to integrate Event notices with your website
Hey! I want the old Search page.

Search Options

Search Term: section excom

Organizational Unit: R40035 - Southeastern Michigan Sect

Date Range: Upcoming

Showing 12 of 12 upcoming events, based on search criteria.

Title	Date	Host	Location	Options
SEM Section ExCom Monthly Meeting (virtual) For JANUARY 2024	11 Jan 2024 06:30 PM	R40035		View
SEM Section ExCom Monthly Meeting (virtual) For FEBRUARY 2024	08 Feb 2024 06:30 PM	R40035		View
SEM Section ExCom Monthly Meeting (Hybrid) For MARCH 2024	14 Mar 2024 06:30 PM	R40035	Southfield, Michigan	View
SEM Section ExCom Monthly Meeting (virtual) For APRIL 2024	11 Apr 2024 06:30 PM	R40035		View
SEM Section ExCom Monthly Meeting (virtual) For MAY 2024	09 May 2024 06:30 PM	R40035		View
SEM Section ExCom Monthly Meeting (Hybrid) For JUNE 2024	13 Jun 2024 06:30 PM	R40035	Southfield, Michigan	View
SEM Section ExCom Monthly Meeting (virtual) For JULY 2024	11 Jul 2024 06:30 PM	R40035		View
SEM Section ExCom Monthly Meeting (virtual) For AUGUST 2024	08 Aug 2024 06:30 PM	R40035		View
SEM Section ExCom Monthly Meeting (In Person) For SEPTEMBER 2024	12 Sep 2024 06:30 PM	R40035	Southfield, Michigan	View
SEM Section ExCom Monthly Meeting (virtual) For OCTOBER 2024	10 Oct 2024 06:30 PM	R40035		View
SEM Section ExCom Monthly Meeting (virtual) For NOVEMBER 2024	14 Nov 2024 06:30 PM	R40035		View
SEM Section ExCom Monthly Meeting (In Person) For DECEMBER 2024	12 Dec 2024 06:30 PM	R40035	Southfield, Michigan	View

Editorial Corner

Previous editions in this series may be found on the IEEE SEM website at: http://r4.ieee.org/sem/. Click on the "Wavelengths" button in the top row of selections.

Comments and suggestions may be sent to the editorial team at wavelengths@ieee-sem.org
OR
sharan.kalwani@ieee.org
nilesh.dudhaia@ieee.org
k.williams@ieee.org
cgjohnson@ieee.org
akio@emcsociety.org

We rely on our officers and members to provide the 'copy' that we finally present to readers of the newsletter.
The **Wavelengths Focus Plan and Personal Profiles** plan shown in the matrix below is presented to ensure coverage of section activities and events.

We try to complete the newsletter layout a week before the first of the month to allow time for review and corrections. If you have an article or notice, please submit it two weeks before the first of the month or earlier if possible.

The plan below relies on the contributions of our members and officers, so please do not be shy. If you have something that should be shared with the rest of the section, we want to give you that opportunity.

We always encourage all chapters and student branches to share news of activities (both past and future) in their arenas. Please feel free to share any and all information so your peers, colleagues can hear about all the good work you do.

Quote*:*
"If a tree falls in a forest and no one hears it, how do you know it actually fell??"

So, publicize your work, one never knows when it can pay off!

Editors:

We are always looking for members interested in helping to edit the newsletter. The process is always more fun with more people to share the duties. Having more participants and contributors also helps us keep the newsletter interesting.

Join the Team:

If you feel you might like to join the team, or would like to train with us, please contact one of us at:
wavelengths@ieee-sem.org

Sharan Kalwani,
Chair, IEEE SE Michigan Education Society Chapter
Vice-Chair, IEEE SE Michigan Computer Society Chapter
Co-Editor, Wavelengths,
2018~2019~2020~2021~2022-2023-2024

Wavelengths Annual Publication Plan for Articles

Month	AG's	Ch's	Ch's	SB's	Special Notice	Reporting Events	Monthly Focus	Awards
Jan		1		OU	New Year Officers	Officer's Welcome	The Year Ahead	
Feb	Cons	2		MSU	Science Fair Judges	National Engrs Wk.	Surviving Winter	
Mar		3	13	EMU	Elections - Prep			
Apr		4		U/M-D		ESD Gold Awards	Chapter Focus	
May	Life	5	14			Science Fair		
Jun		6					Leadership Skills	
Jul		7	15				Students Issues	
Aug	WIE	8			Nominations Call		Womens Issues	
Sep		9	16	LTU	Ballots	Engineers Day?	Professional Skills	
Oct		10		U/M-AA	Elections!	IEEE Day		
Nov	YP	11	17	WSU	Election Results	New Fellows		
Dec		12		U/D-M	IEEE-Com Apmts.		Happy Holidays	R4 Nom

Wavelengths Annual Publication Plan for Personal Profiles

Month	Profiles	Profiles	Committees
Jan	Chair	New Officers	ExCom
Feb	Treasurer		Communications
Mar	Secretary		Conference
Apr	Stud-Rep		Education
May	V-Chair		Executive
Jun	Sect-Adviser		Finance
Jul	Sr Officers		Membership
Aug			Nominations
Sep			PACE
Oct			Student Activiies
Nov			Technical Activiies
Dec	Editor-WL		

IEEE
Southeastern
Michigan
Electrical and Electronic Engineers Creating Our Future

Web & Social Sites

Southeastern Michigan Section Website
http://r4.ieee.org/sem/

Each of the sites below may be accessed through the Website:

Section Website Event Calendar
(Select the "SEM Calendar" button - top row)

SEM Facebook Page
(Select the "f" button under the top row)
https://www.facebook.com/groups/ieeesemich

SEM LinkedIn Page
(Select the "in" button under the top row)
https://www.linkedin.com/groups/1766687/

SEM Twitter Account (new)
(Select the "🐦" button under the top row)
https://www.twitter.com/ieeesemich

SEM Collabratec *Community* Page
https://ieee-collabratec.ieee.org/app/section/R40035/IEEE-Southeastern-Michigan-Section

SEM Collabratec *Workspace* Page
https://ieee-collabratec.ieee.org/app/workspaces/5979/IEEE-Southeastern-Michigan-Section/activities

SEM Instagram (new)
https://www.instagram.com/ieeesemich/

SEM Officers:
For a complete listing of all - Section - Standing Committee - Affinity Group - Chapter and Student Branch SEM Officers Roster on the web page (top banner)

Section Officers

Section Chair
Sharan Kalwani

Section Vice-Chair
Aneesh Mathai

Section Secretary
Christopher Johnson

Section Treasurer
Ramesh Sethu

Standing Committees:

Section Adviser
Mohamad Berri

Wavelengths Editor
Sharan Kalwani

Educational Committee
Anthony Will (Chair)

Finance Committee
Subra Ganesan (Chair)

Membership Development
Mohamad Berri (Chair)

Awards & Nominations
Jerry Song (Chair)

PACE
Sharan Kalwani (Chair)

Student Activities
Michael Anthony & Hafeez Jimoh (Co-Chairs)

Student Mentors
OPEN

SECTION Student Rep
OPEN

Technical Activities
Jeffery Mosley

Information Management

IEEE Southeastern Michigan

Electrical and Electronic Engineers Creating Our Future

IEEE Southeastern Michigan

Visit Us on the Web at:
http://r4.ieee.org/sem

I had to travel 400 miles over mountains in torrential rain to buy a spare computer part.

It was a hard drive.

Advertising Rates

SEM Website & Newsletter

Leadership Meetings

SEM Executive Committee Monthly Teleconferences:

- 2nd Thursday of Each Month @ 6:30 PM
- Check the Section Web Calendar at:
  http://r4.ieee.org/sem/sem-calendar/
  (Select the "SEM Calendar" button in the top row.)

OR

SEM Executive Committee Meetings:

- Find the location, and Registration at:
  http://bit.ly/sem-ieee

SEM Standing Committee Meetings:
SEM Affinity Group Meetings:
SEM Technical Society/Chapter Meetings:
SEM University Student Branch Meetings:

- Meeting schedules are announced on SEM Calendar
  http://r4.ieee.org/sem/
  (Select the "SEM Calendar" button in the top row.)
- Registration for all at:
  http://bit.ly/sem-upcoming