Vulnerabilities of Cyber-Physical Systems: From Football to Oil Rigs

Fred S. Roberts
Director
Command, Control, and Interoperability Center for Advanced Data Analysis (CCICADA)*
Rutgers University

*A Department of Homeland Security University Center of Excellence

Command, Control, and Interoperability Center for Advanced Data Analysis
A Department of Homeland Security Center of Excellence

Image credits: wikipedia.org

CCICADA Center

- Founded 2009 as a Dept. of Homeland Security University Center of Excellence
- Based at Rutgers University in New Brunswick/ Piscataway, NJ
- We apply methods of mathematics, computer science, statistics and operations research to problems of homeland security.
- We partner with behavioral scientists, economists, biologists, epidemiologists, physicians, sociologists, industrial engineers, etc.
- We work with public and private agencies and organizations throughout the "homeland security enterprise"

Command, Control, and Interoperability
Center for Advanced Data Analysis
A Department of Homeland Security Center of Excellence
A Department of Homeland Security Center of Excellence

Vulnerabilities of Cyber-Physical Systems: From Football to Oil Rigs

- Some of our nation's most important critical infrastructure is increasingly controlled by computer networks.
  - Power systems ("smart grid")
  - Transportation systems ("smart transportation")
  - Water supply systems
  - Air traffic control
  - Building control systems ("smart buildings")
- This infrastructure is potentially vulnerable to failures of computer systems or deliberate cyber attacks

Command, Control, and Interoperability
Center for Advanced Data Analysis
A Department of Homeland Security Center of Excellence

Cyber-Physical Systems

- ***Cyber-physical systems (CPS)***: Engineered systems that are built from and depend upon the synergy of computational and physical components.
- National Science Foundation (2013 CPS solicitation): "The CPS of tomorrow will need to far exceed the systems of today in capability, adaptability, resiliency, safety, security, and usability."

A Department of Homeland Security Center of Excellence

Super Bowl 47, New Orleans

- Was it terrorism?
- Was it cyber-terrorism?
- (Luckily just a relay device failing at Entergy Orleans)

Credit: businessinsider.com

A Department of Homeland Security Center of Excellence

Super Bowl 48, New Jersey

Credit:
new.mta.info

NJ State Police Regional Operations Intelligence Center pre-game assessment:

- ***Cyber attacks by "ideologically motivated and malicious" hackers, exploiting wireless systems, on stadium infrastructure or Super Bowl websites, is a serious possibility.***

A Department of Homeland Security Center of Excellence

CCICADA and Stadium Security

- Numerous projects on patron inspection, employee credentialing, safety and security of infrastructure, etc.
- Working with all major sports leagues (MLB, NFL, NBA, NHL, MLS, etc.) + NCAA and minor leagues

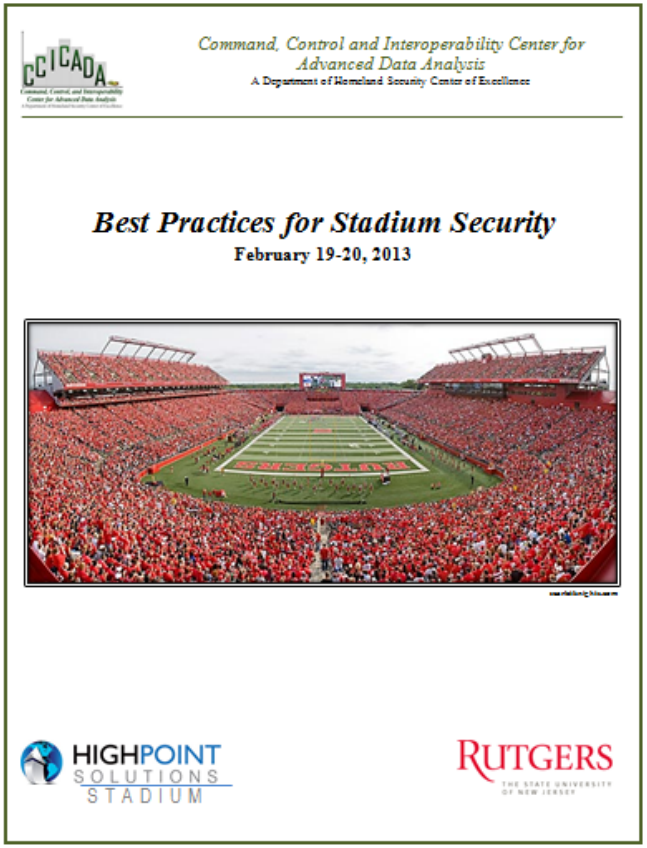
Lambeau Field – Mike Roemer/AP

CCICADA
Command, Control, and Interoperability
Center for Advanced Data Analysis
A Department of Homeland Security Center of Excellence

CCICADA Project: Best Practices for Stadium Security

Supported by DHS Office of SAFETY Act Implementation (OSAI)

CCICADA's Best Practices for Stadium Security Resource Guide can be found on the OSAI website



CCICADA

Command, Control, and Interoperability Center for Advanced Data Analysis

A Department of Homeland Security Center of Excellence

It's not Just Sports Stadiums

- It's any places where large crowds gather
  - Airports
  - Train stations, bus terminals
  - Concert halls
  - Amusement parks
  - Political conventions

Port Authority Bus Terminal, NYC
Credit: nj1015.com

CCICADA
Command, Control, and Interoperability
Center for Advanced Data Analysis
A Department of Homeland Security Center of Excellence

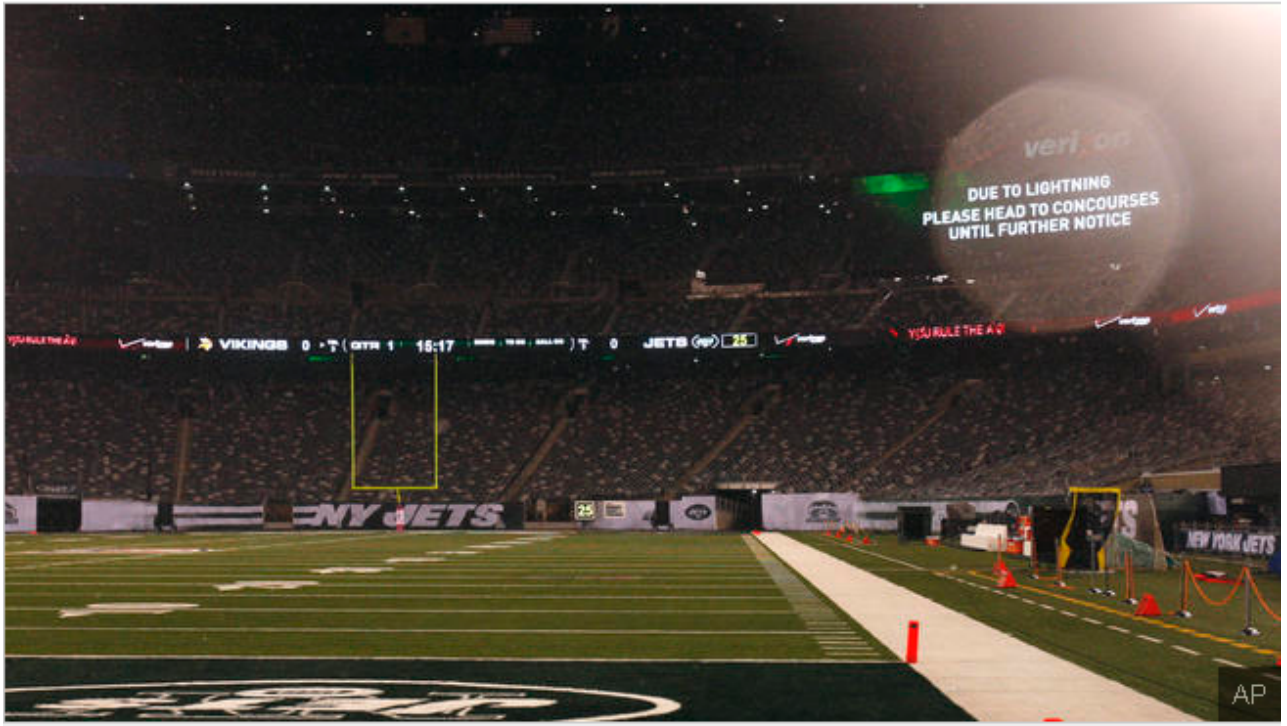
Cyber-physical Systems in Stadiums

- Access control systems
  - For patrons
  - For employees
- HVAC
- Communication systems
  - Electronic message boards
  - Public address systems
- Security cameras
- Elevators, escalators
- Lighting systems
- Power systems
- Traffic control in the parking lots

A Department of Homeland Security Center of Excellence

Example: Hacking into the Communications System

- This was a real emergency and a real message.
- But imagine what chaos a hacker could cause with a fake emergency message.



Stands are empty before an NFL football game between the Minnesota Vikings and the New York Jets on Monday, Oct. 11, 2010, in East Rutherford, N.J. The start of the game was delayed because of lightning and heavy rain; fans were cleared from the stands.

CCICADA
Command, Control, and Interoperability
Center for Advanced Data Analysis
A Department of Homeland Security Center of Excellence
A Department of Homeland Security Center of Excellence

Example: Drones over Stadiums

- A real concern of major sports leagues
- Recent NFL policy
- FAA setting rules
- Prof. Todd Humphreys of UT Austin has demonstrated how global positioning system (GPS) signals of an unmanned aerial vehicle can be commandeered by an outside source

Source: UT Austin Aerospace Engineering

A Department of Homeland Security Center of Excellence

Cyber-physical Systems in Stadiums

- Report by CNBC (Nov. 2013) names five large sports stadiums running a particular industrial control system software with known vulnerabilities.
- Include Bryant-Denny Stadium (University of Alabama) and Marlins Park (home of the Miami Marlins baseball team)
- Vulnerabilities supposedly addressed by now.

Bryant-Denny Stadium
Credit: wikipedia.org

So Why So Many Vulnerabilities?

- Building management systems have many parties involved
  - Selling
  - Implementing
  - Maintaining
- Need systems for large, complex facilities
- CPS are of great complexity and are often engineered for environments not engineered from scratch (as in the power grid)
- Cyber security neglected
- Management doesn't want to pay for cyber security (security in general)
- Public/private communication needs improvement

Another Scenario: Car Hacking in the Stadium Parking Lot

- Car hacking: criminals remotely take control of your car
- Imagine the damage a hacker could do in a stadium parking lot.

Credit: ctvnews.ca

Another Scenario: Car Hacking in the Stadium Parking Lot

- Car hacking: criminals remotely take control of your car
- A serious challenge as in-car technology becomes more sophisticated
- Already thousands of semi-autonomous cars
  - In-car computer systems
  - Electronic control units
- Coming: fully autonomous cars
  - Self-driving cars

Credit: wikipedia.org

Another Scenario: Car Hacking in the Stadium Parking Lot

- 2013: Miller (Twitter) and Valasek (IOActive) demonstrated take control of Toyota Prius and Ford Escape from a laptop.
- They were able to remotely control:
  - Smart steering
  - Braking
  - Displays
  - Acceleration
  - Engines
  - Horns
  - Lights

Credit: npr.org

Why Vulnerabilities in Cars?

- Vehicle control system depends on system components manufactured by different vendors
- Each vendor uses their own software and hardware
- Manufacturers like to develop components that will work for different kinds of vehicles (cheaper) – spreading the vulnerabilities
- Increasing complexity of components like sensors, actuators, wireless communication, multicore processors

Credit: Baheti and Gill (2011)

Why Vulnerabilities in Cars?

- Development of control system may be independent of system implementation
- Challenge of integrating various subsystems while keeping them functional
- Research missing on understanding interactions between vehicle control systems and other subsystems:
  - Engine, transmission, steering, wheel, brake, suspension

Credit: Baheti and Gill (2011)

A Department of Homeland Security Center of Excellence

From Cars to Ships

- Vulnerabilities in CPS for cars have been highly publicized.
- Much less well known: vulnerabilities in CPS of the maritime transportation system.
- CCICADA has numerous projects in collaboration with the US Coast Guard, Customs and Border Protection, and other agenicies on safety and security of the maritime transportation system.

Hacking into a Ship

- A recent demonstration by a UT Austin team showed how a potential adversary could remotely take control of a vessel by manipulating its GPS.
- The yacht "White Rose of Drachs" was successfully spoofed while sailing on the Mediterranean.
- The team's counterfeit signals slowly overpowered the authentic GPS signals until they ultimately obtained control of the ship's navigation system.
- "The ship actually turned and we could all feel it, but the chart display and the crew saw only a straight line."

Source: UT Austin "Know"

CCICADA
Command, Control, and Interoperability
Center for Advanced Data Analysis
A Department of Homeland Security Center of Excellence

Hacking into a Ship

- The maritime transportation system is critical to the US economy.
- 95% of goods in international trade are still transported by sea.
- Disruption of global supply chain for commodities such as oil could cause dramatic problems for the world-wide economy.
- Disruption of the maritime transportation system could cause billions of dollars in damage to the economy.

Command, Control, and Interoperability
Center for Advanced Data Analysis
A Department of Homeland Security Center of Excellence

Modern Ship CPS

- For modern ships: dependence on a proliferation of sophisticated technology – that is subject to cyber attack
  - ECDIS (Electronic Chart Display and Information System)
  - AIS (Automatic Identification System)
  - Radar/ARPA (Radio Direction and Ranging) (Automatic Radar Plotting Aid)
  - Compass (Gyro, Fluxgate, GPS and others)
  - Steering (Computerized Automatic Steering System)
  - VDR (Voyage Data Recorder –"Black Box")
  - GMDSS (Global Maritime Distress and Safety System)
  - Numerous other advanced units and systems

Thanks to Capt David Moskoff, US Merchant Marine Academy, for many of the following examples

Electronic Chart Display & Info System

- Electronic Chart Display and Information System (ECDIS):
  - Computer-based navigation system
  - Can be used as an alternative to paper navigation charts
  - Integrates a variety of real-time information
  - Automated decision aid - continuously determining ship's position in relation to land, charted objects, navigation aids and unseen hazards
  - Includes electronic navigational charts and integrates position information from the Global Positioning System (GPS) and other navigational sensors, such as radar, fathometer and automatic identification systems (AIS).
  - May also display additional navigation-related information, such as sailing directions.

Electronic Chart Display & Info System

- Electronic Chart Display and Information System enables solo watchstanding

Electronic Chart Display & Info System

- World's largest container ship: Triple E Maersk under construction
  - 18,000 containers
  - 400 meters long!
  - Crew size: Can operate with 13 crew members!!
    - ➢Thanks to ECDIS & other such systems.

Credit: http://www.worldslargestship.com/

Electronic Chart Display & Info System

- ECDIS flaws might would allow an attacker to access and modify files and charts on board or on shore; could cause serious environmental and financial damage, even loss of life.
- In Jan. 2014, the NCC Group tried to penetrate an ECDIS product from a major manufacturer.
- Several security weaknesses were found: ability to read, download, replace or delete any file stored on the machine hosting ECDIS, etc.
- Once such unauthorized access is obtained, attackers could be able to interact with the shipboard network and everything to which it is connected.

Sources: templarexecs.com 2014, CyberKeel 2014

Automatic Identification System

- Automatic Identification System (AIS) transceivers on over 400,000 ships (2013 estimate).
- Estimated that the number will soon reach a million.
- Installation is mandatory for all passenger ships and commercial (non-fishing) ships over 300 metric tons.
- Tracks ships automatically by electronically exchanging data with other ships, AIS base stations, and satellites.

Source: Help Net Security

Credit: wikipedia.org

Automatic Identification System

- An attacker with a $100 VHF radio could exploit weaknesses in Automatic Identification System which transmits data (e.g. vessels' identity, type, position, heading and speed to shore stations).
- The attacker could also tamper with the data, impersonate port authorities, communicate with the ship or effectively shut down communications between ships and with ports.

Source: templarexecs.com 2014

Automatic Identification System

- In Oct. 2013 Trend Micro demonstrated how easy it is to penetrate a ship's AIS.
- Plausible scenarios (CyberKeel 2014):
  - Modification of all ship details, position, course, cargo, speed, name
  - Creation of "ghost" vessels at any global location, which would be recognized by receivers as genuine vessels
  - Trigger a false collision warning alert, resulting in a course adjustment

Dr. Marco Balduzzi of Trend Micro discussing potential scenario
Credit: Help Net Security

Automatic Identification System

- In Oct. 2013 Trend Micro demonstrated how easy it is to penetrate a ship's AIS.
- Plausible scenarios continued (CyberKeel 2014):
  - Send false weather information to a vessel to have them divert around a non-existent storm
  - The ability to impersonate marine authorities to trick the vessel crew into disabling their AIS transmitter, rendering them invisible to anyone but the attackers themselves
  - Cause vessels to increase the frequency with which they transmit AIS data, resulting in all vessels and marine authorities being flooded by data. Essentially a denial-of-service attack

Automatic Identification System

- Somali pirates help choose their targets by viewing navigational data online, prompting ships to either turn off their navigational devices, or fake the data so it looks like they're somewhere else. (Reuters 4/23/14)

Credit: wikipedia.org

Automatic Identification System

- How it could work: “Frequency Hopping Attack” (Balduzzi & Pasta)
  - Every vessel is tuned in on a range of frequencies where they can interact with port authorities, as well as other vessels.
  - There is a specific set of instructions that only port authorities can issue that make the vessel's automatic information system transponder work on a specific frequency.
  - A malicious attacker can spoof this type of "command" and practically switch the target's frequency to another one which will be blank. This will cause the vessel to stop transmitting and receiving messages on the right frequency, effectively making it "disappear" and unable to communicate.

Automatic Identification System

- In Oct. 2013 Trend Micro demonstrated how easy it is to penetrate a ship's AIS.
- Why? (CyberKeel 2014):
  - The key problem with AIS is that it has no built-in security. All information is automatically assumed as being genuine and hence treated as correct piece of information.
  - Additionally, AIS messages are not encrypted and therefore very easy for outsiders to tap into and manipulate.

Automatic Identification System

- Potential Countermeasures to AIS Vulnerability:
  - Addition of authentication in order to ensure that the transmitter is the owner of the vessel
  - Creating a way to check AIS messages for tampering
  - Making it impossible to enact replay attacks by adding time checking
  - Adding a validity check for the data contained in the messages (e.g. geographical information)

Source: Help Net Security

GPS Jamming

- GPS Jamming can wreak havoc with modern ships.
- The UK & Irish General Lighthouse Authority directed GPS jamming equipment at a specific patch of ocean.
- On a vessel entering the jamming zone, a range of services failed: the AIS transponder, the dynamic positioning system, the ship's gyro calibration system and the digital selective calling system.
- The crew was able to cope with multiple alarms as they had been expecting this.
- However, on a modern vessel the bridge might in some cases be single-manned at night, causing significant problems should such a situation occur.

Source: CyberKeel 2014

GPS Jamming

- GPS jamming is possible with low cost jammers available over the Internet (though illegal).
- Many devices are battery-operated or can be plugged into a cigarette lighter and cost as little as $20.

Credit: CAPT David Moskoff

Oil Rigs

- Not just ships – ***vulnerabilities extend to the entire maritime transportation system.***
- Hackers recently shut down a floating oil rig by tilting it. (Reuters 4/23/14)
- Another rig was so riddled with computer malware that it took 19 days to make it seaworthy again. (Reuters 4/23/14)

Credit: www.peakoil.net

Cargo

- Cargo is also affected.
- 2011-2013: Hackers infiltrated computers connected to the Port of Antwerp, located specific containers, made off with their smuggled drugs and deleted the records.
- Attackers obtained remote access to the terminal systems; released containers to their own truckers without knowledge of the port or the shipping line.
- Access to port systems was used to delete information as to the existence of the container after the fact.

Source: Reuters 4/23/14, CyberKeel

Credit: wikipedia.org

Cargo

- In 2012 it was revealed that crime syndicates had penetrated the cargo systems operated by the Australian Customs and Border protection.
- The penetration of the systems allowed the criminals to check whether their shipping containers were regarded as suspicious by the police or customs authorities.
- The consequence was that containers with contraband were abandoned whenever such attention was identified by the criminals.

Credit: CyberKeel

Credit: commons.wikipedia.org

Cargo

- The Iranian shipping line IRISL suffered from a successful cyber attack in 2011.
- The attacks damaged all the data related to rates, loading, cargo number, date and place.
- This meant that no one knew where containers were, whether they had been loaded or not, which boxes were onboard the ships or onshore.
- Even though the data was eventually recovered, it led to significant disruptions in operations and resulted in sending cargo to wrong destinations causing severe financial losses.
- Additionally, a considerable amount of cargo was lost.

Credit: CyberKeel

Ports

- Today, ports rely as much on computer networks as on human stevedores.
- Complex networked logistics management systems track maritime cargo from overseas until reaching a U.S. retailer.
- Networked control systems are also often involved in the loading and unloading of these goods.
- Modern gantry cranes and other systems use optical recognition and other technologies to locate, scan, and manage all facets of port terminal operations.
- Automated container terminal systems use GPS to facilitate the automatic placement and movement of containers.

Source: CDR Joe Kramek, Brookings Report 2013

Ports

- The entire port is vulnerable – from cargo handling to truck and crane movement.
- Easily available jammers could close down a port at cost of more than $1B per day.

Command, Control, and Interoperability
Center for Advanced Data Analysis
A Department of Homeland Security Center of Excellence

Maritime Cyber Security

- The cyber threats to the maritime domain are serious.
- These threats not well known.
- In November 2011, the European Network and Information Security Agency reported that, "[t]he awareness on cybersecurity needs in the maritime sector is currently low to non-existent."
- 2013 Brookings Report found that of the six ports studied, only one had conducted a cyber security vulnerability assessment and not a single one had a cyber incident response plan

Command, Control, and Interoperability
Center for Advanced Data Analysis
A Department of Homeland Security Center of Excellence

Maritime Cyber Security

- The cyber threats to the maritime domain are serious.
- These threats not well known.
- Recent GAO report found that DHS needs to better address maritime cyber security (in particular port cyber security)
- GAO recommended that:
  - USCG assess cyber-related risks & use the assessment to inform maritime security guidance;
  - FEMA use the cyber risk assessment to inform its grant guidance

Maritime Cyber Security

- The cyber threats to the maritime domain are serious.
- These threats not well known.
- Is the maritime transportation system "special" in its cyber threats?
- In some ways.
- But mostly the issues involve lack of awareness by management, lack of information about attacks and vulnerabilities, emphasis on physical security, lack of cyber security training of personnel – similar to many other sectors.
- The industry can and should learn from other industries.
- We need to spread awareness of the maritime cyber threat.

Maritime Cyber Security

- CCICADA will hold the first-ever tutorial and symposium on Maritime Cyber Security
- March 2-3, 2015 at Rutgers University, Piscataway, NJ
- Keynote by Admiral Chuck Michel, US Coast Guard
- Registration is limited
- Register at ccicada.org

CCICADA
Command, Control, and Interoperability Center for Advanced Data Analysis
A Department of Homeland Security Center of Excellence

Research Issues in Security of Cyber-Physical Systems

NSF CPS solicitation 2013:

- Develop the fundamental science needed to engineer systems of the complexity of cyber-physical systems that you can have high confidence in.
- Find ways to conceptualize and design for the deep interdependencies among engineered systems and the natural world.

A Department of Homeland Security Center of Excellence

Research Issues in Security of Cyber-Physical Systems

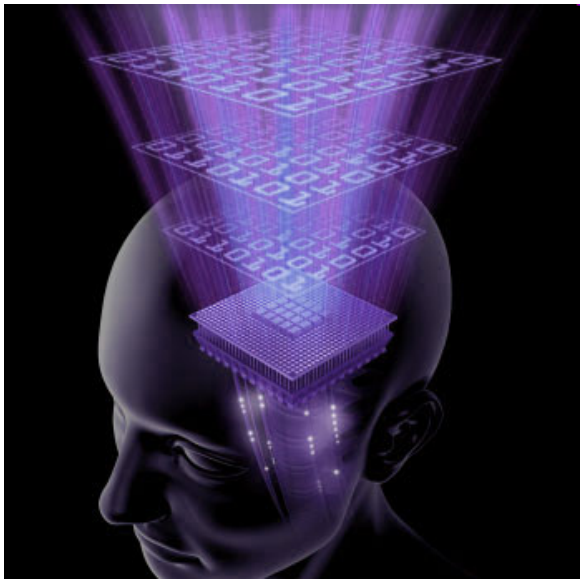
- Need methods of verification and validation.
- How can you certify performance of such highly complex systems?
- Right now, overdesign may be only route to system certification.

Credit: collegepals.org

Command, Control, and Interoperability Center for Advanced Data Analysis
A Department of Homeland Security Center of Excellence

Research Issues in Security of Cyber-Physical Systems: Data

- Huge amounts of data available to describe CPS.
- Challenge: Find ways to utilize data to enhance safety and security of CPS.
- Data about state of the system can come to us so fast humans can't process it.
- Need tools for rapid system understanding.
- Need tools for rapid anomaly detection.



Vulnerabilities of Cyber-Physical Systems: From Football to Oil Rigs

For More Information:

Dr. Fred Roberts
froberts@dimacs.rutgers.edu

CCICADA Center
www.ccicada.org