2024 **QATAR PROCESS SAFETY SYMPOSIUM**

ConocoPhillips Qatar

قطر للطاقة QatarEnergy LNG

MAKING PROCESS SAFETY **PERSONAL**

NOVEMBER 5TH, 2024

DOHA, QATAR | QPSS.QA

2024 QATAR PROCESS SAFETY SYMPOSIUM

ConocoPhillips Qatar | QatarEnergy LNG

Navigating the Intersection of Process Safety and Cybersecurity in the Age of Artificial Intelligence

Tuesday, November 5, 2024

MAKING PROCESS SAFETY **PERSONAL**

Speaker

David Moore, PE, CSP
President & CEO

AcuTech
PROCESS RISK MANAGEMENT

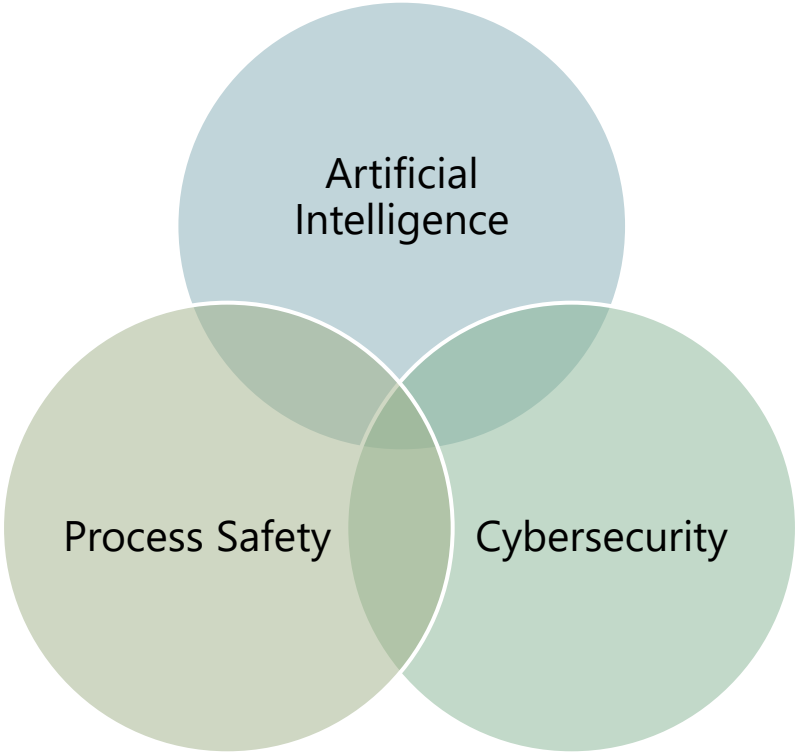
AcuTech is a full-service risk management firm providing services in process safety & risk management, physical and cyber security, and emergency preparedness across vital industries.

www.acutech-consulting.com

Introduction

- Increased digitization of critical systems and industrial controls creates an increasing risk from cybersecurity events.
- These events can be caused by digital or physical attacks against IT assets.
- AI can be an enabling technology for adversaries to cause this harm
- Technologies are integrating into our processes faster than our organizations are adapting

There is a convergence of AI, PSM, and Cybersecurity



Does AI or ML pose risks for process safety or cybersecurity?

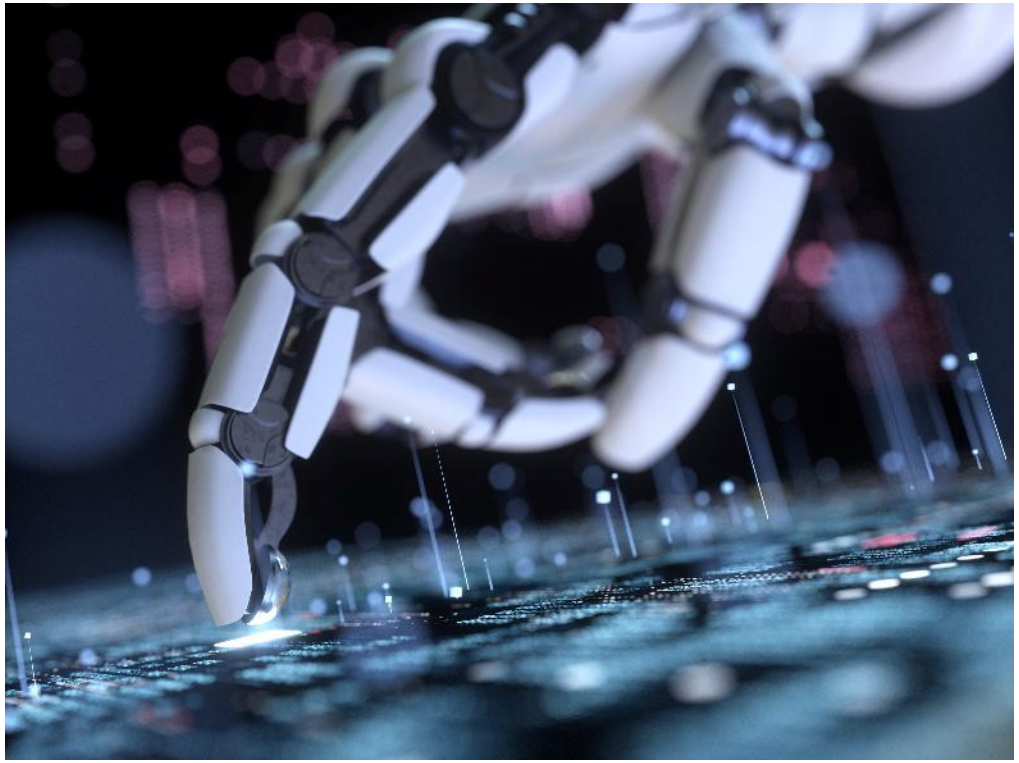
Artificial Intelligence

"The capability of computer systems or algorithms to imitate intelligent human behavior "

Machine Learning

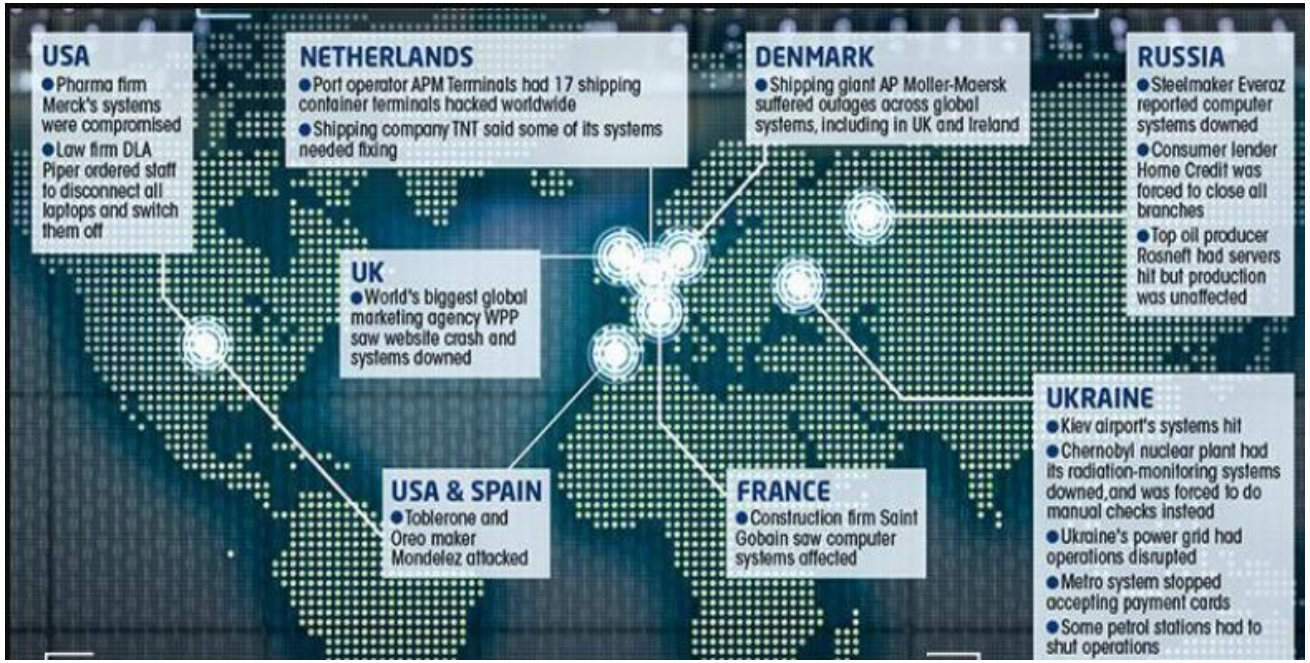
"A computational method that is a subfield of artificial intelligence and that enables a computer to learn to perform tasks by analyzing a large dataset without being explicitly programmed"

- Merriam-Webster Dictionary



Threats to the Industrial Sectors

- June 2017: a USB drop introduced a virus that rapidly proliferated through common platforms to critical infrastructure across the globe.
- 76 ports were isolated impacting 800 vessels.
- Total estimated damages exceeded 10 billion USD.

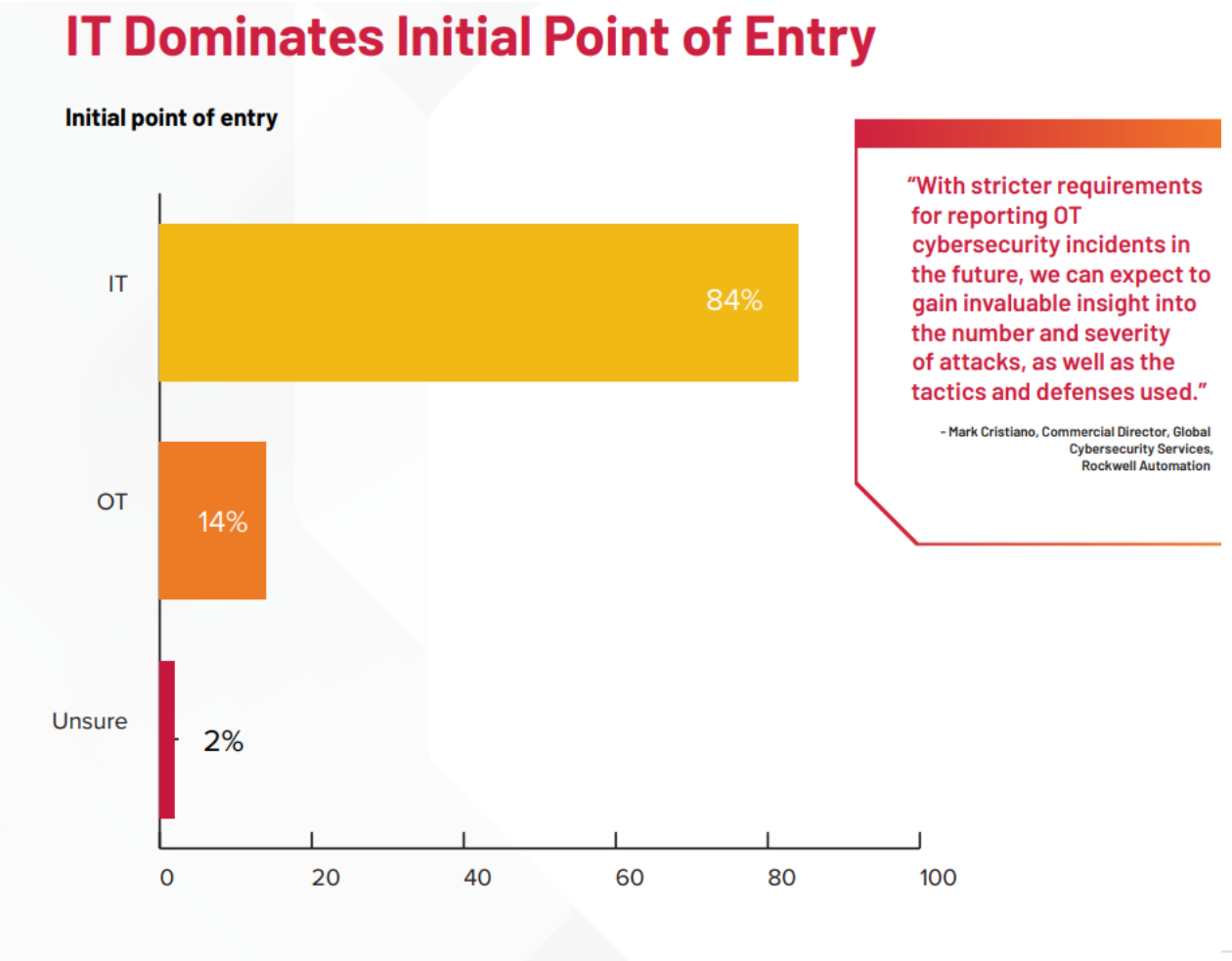


Anatomy of Industrial Cybersecurity Incidents

Anatomy of 100+ Cybersecurity Incidents in Industrial Operations: A Research Study With Recommendations For Strengthening Defenses in OT/ICS, Rockwell International

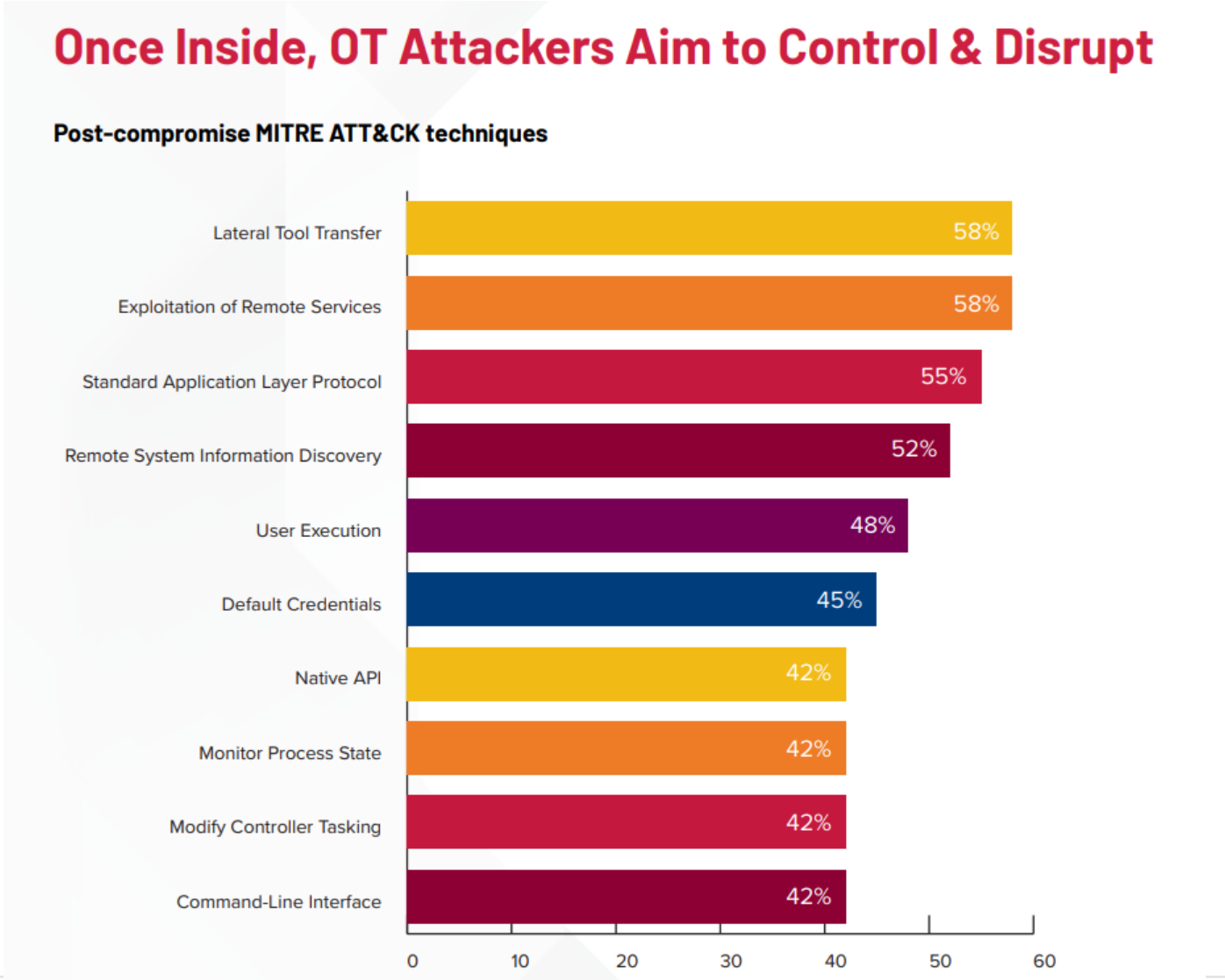
Human Element to Cybersecurity

- AI can be used to cause phishing, denial of service, IT hacks, and other forms of attacks more efficiently than human interaction alone
- Most OT incidents originate through IT systems



Anatomy of 100+ Cybersecurity Incidents in Industrial Operations: A Research Study With Recommendations For Strengthening Defenses in OT/ICS, Rockwell International

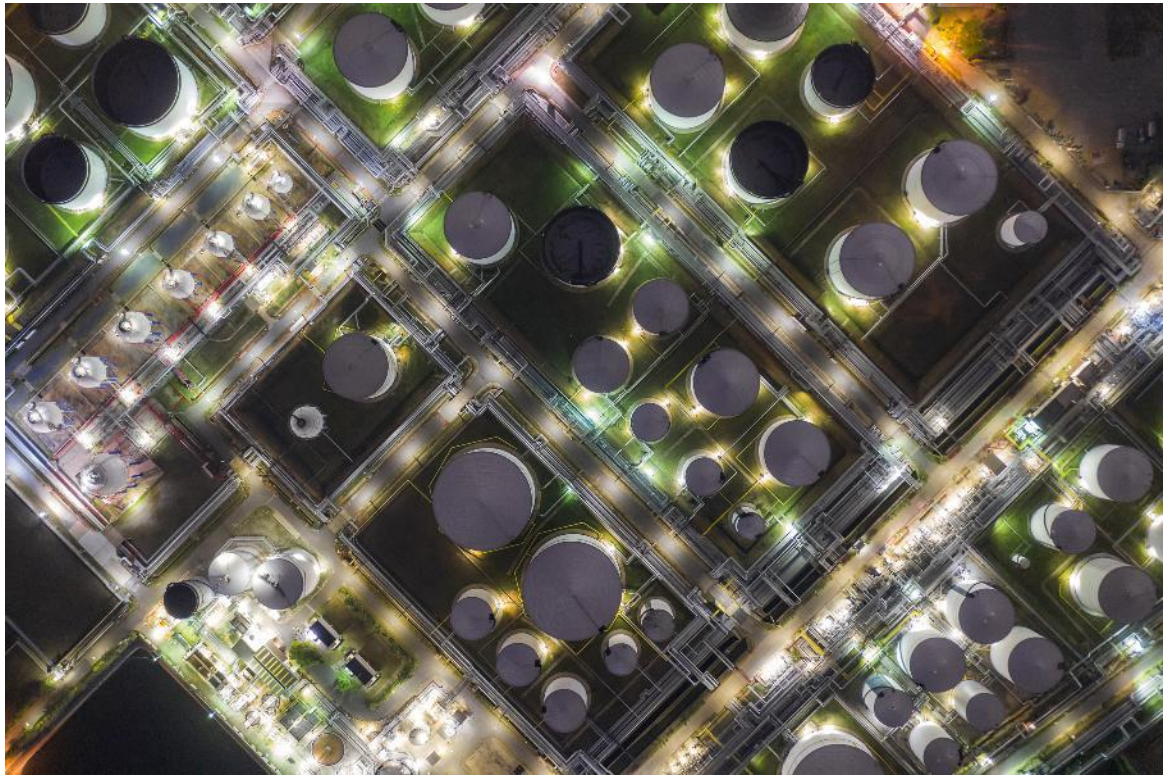
Cybersecurity Tactics



Anatomy of 100+ Cybersecurity Incidents in Industrial Operations: A Research Study With Recommendations For Strengthening Defenses in OT/ICS, Rockwell International

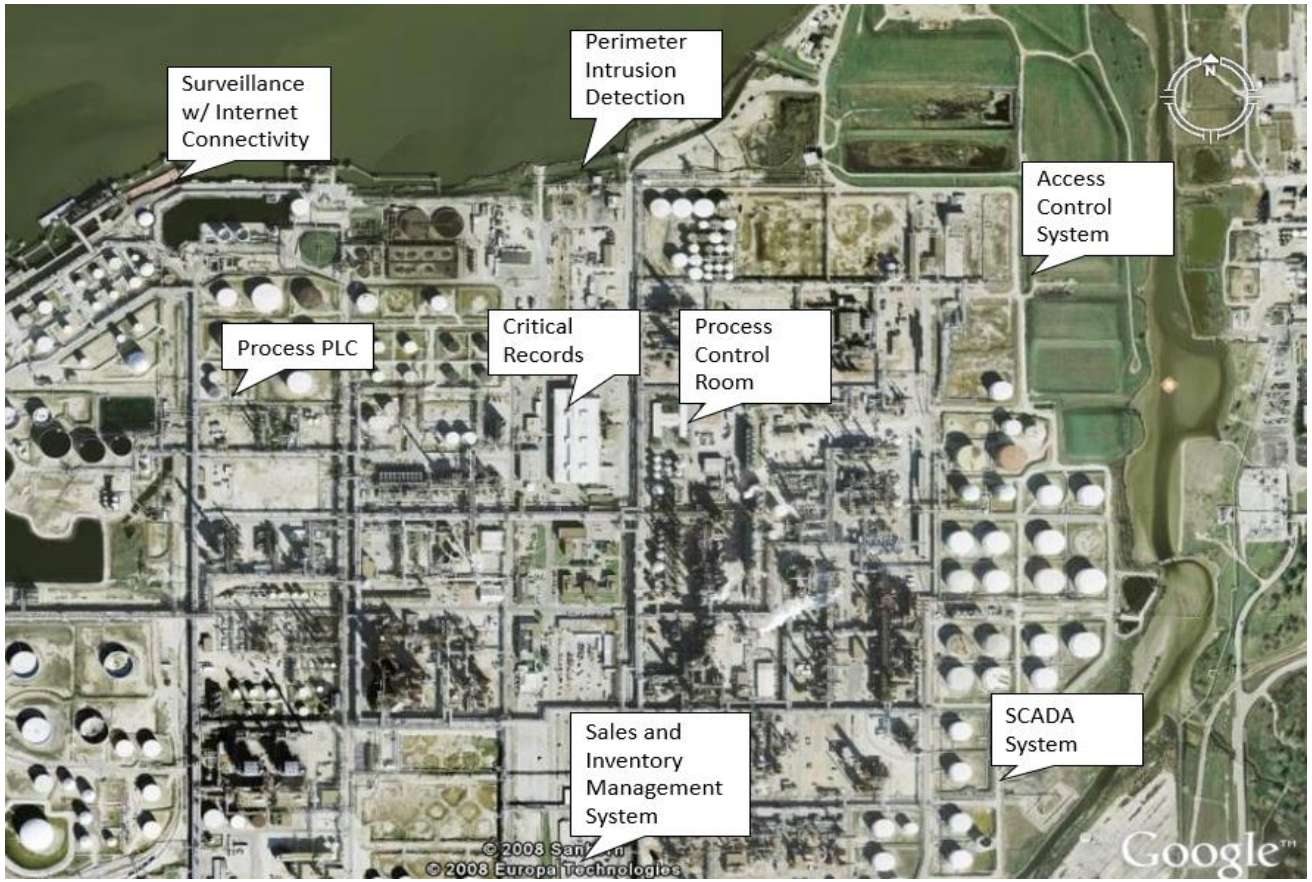
Artificial Intelligence – New Risks

- AI can make adversaries work easier or make them more effective
- Has your organization applied AI to improving the performance of a process?
- Have you evaluated the risks of using AI from a process safety and cybersecurity standpoint?
- What can every individual do to contribute to both cyber security and process safety?



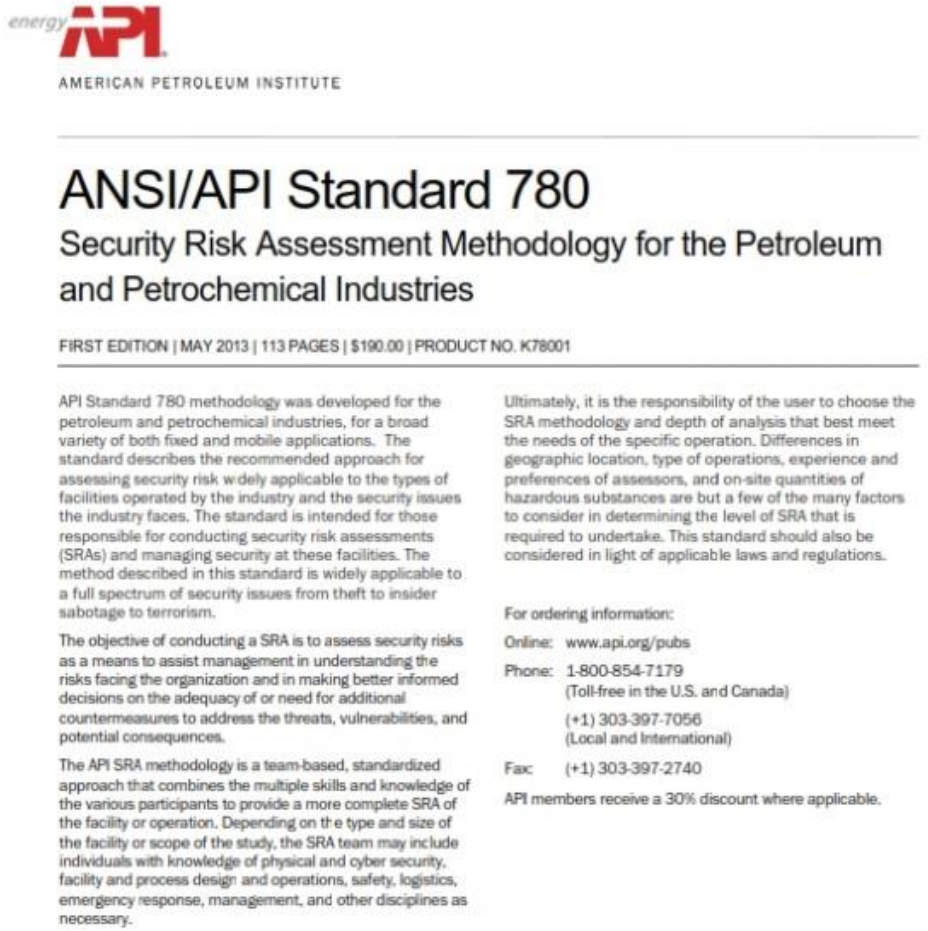
Interface of PSM and Cybersecurity

- Identify the IT/OT/Process interfaces in the SRA and PHA.
- How could a LOPC incident be caused by a cyber security incident?
- Are they protected?
- Inherently safe design?



ANSI/API Standard 780 - Security Risk Assessment Methodology

- There is a strong business case to be made to go beyond physical and cyber SRAs and employ a hybrid SRA approach that incorporates the knowledge and expertise of both cyber and physical security experts.
- Providing cybersecurity input into the ANSI/API Standard 780 SRA methodology has proven to be effective in identifying and mitigating physical cybersecurity blind spots.



energy API

AMERICAN PETROLEUM INSTITUTE

ANSI/API Standard 780

Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries

FIRST EDITION | MAY 2013 | 113 PAGES | $190.00 | PRODUCT NO. K78001

API Standard 780 methodology was developed for the petroleum and petrochemical industries, for a broad variety of both fixed and mobile applications. The standard describes the recommended approach for assessing security risk w idely applicable to the types of facilities operated by the industry and the security issues the industry faces. The standard is intended for those responsible for conducting security risk assessments (SRAs) and managing security at these facilities. The method described in this standard is widely applicable to a full spectrum of security issues from theft to insider sabotage to terrorism.

The objective of conducting a SRA is to assess security risks as a means to assist management in understanding the risks facing the organization and in making better informed decisions on the adequacy of or need for additional countermeasures to address the threats, vulnerabilities, and potential consequences.

The API SRA methodology is a team-based, standardized approach that combines the multiple skills and knowledge of the various participants to provide a more complete SRA of the facility or operation. Depending on th e type and size of the facility or scope of the study, the SRA team may include individuals with knowledge of physical and cyber security, facility and process design and operations, safety, logistics, emergency response, management, and other disciplines as necessary.

Ultimately, it is the responsibility of the user to choose the SRA methodology and depth of analysis that best meet the needs of the specific operation. Differences in geographic location, type of operations, experience and preferences of assessors, and on-site quantities of hazardous substances are but a few of the many factors to consider in determining the level of SRA that is required to undertake. This standard should also be considered in light of applicable laws and regulations.

For ordering information:

Online: www.api.org/pubs

Phone: 1-800-854-7179
(Toll-free in the U.S. and Canada)

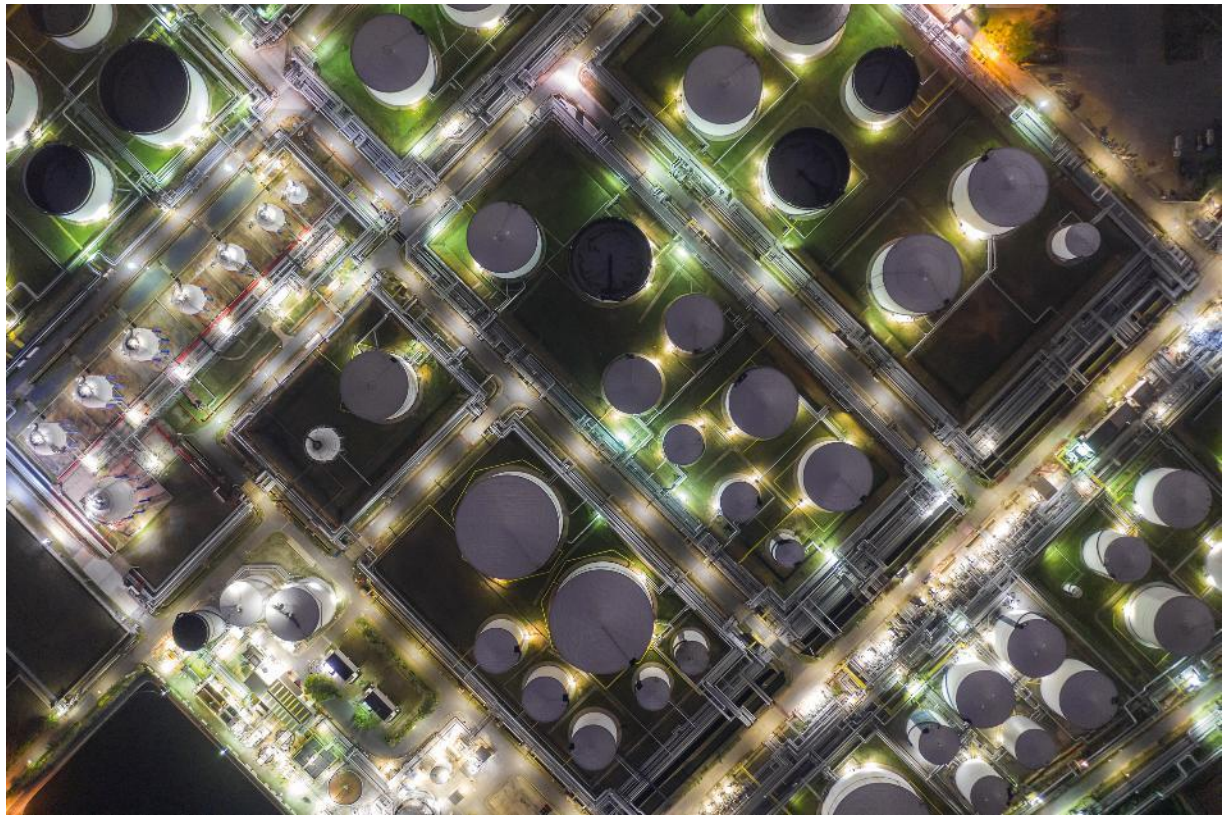
(+1) 303-397-7056
(Local and International)

Fax: (+1) 303-397-2740

API members receive a 30% discount where applicable.

Artificial Intelligence – Presence Today

- Industrial control systems (ICS) or (OT)
  - Advanced Process Control (APC) suites
  - Data historians
  - Cloud-based and edge-based data analytics tools
- Business systems (IT)
  - Data visualization software
  - Computerized Maintenance Management Systems (CMMS)
  - Industrial data analytics suites
- Risk assessment tools



Artificial Intelligence – Near Future?

- Industrial control systems (ICS) or (OT)
  - Industrial sensors and instrumentation
  - Real-time automated operating procedures
  - On-controller self-optimization tools
- Business systems (IT)
  - Dynamic employee work scheduling
  - Root Cause Failure Analysis (RCFA) and Failure Modes and Effects Analysis (FMEA)
  - Staff- and skill-augmentation

Pitfalls of Artificial Intelligence – Potential for New Unrealized Risk

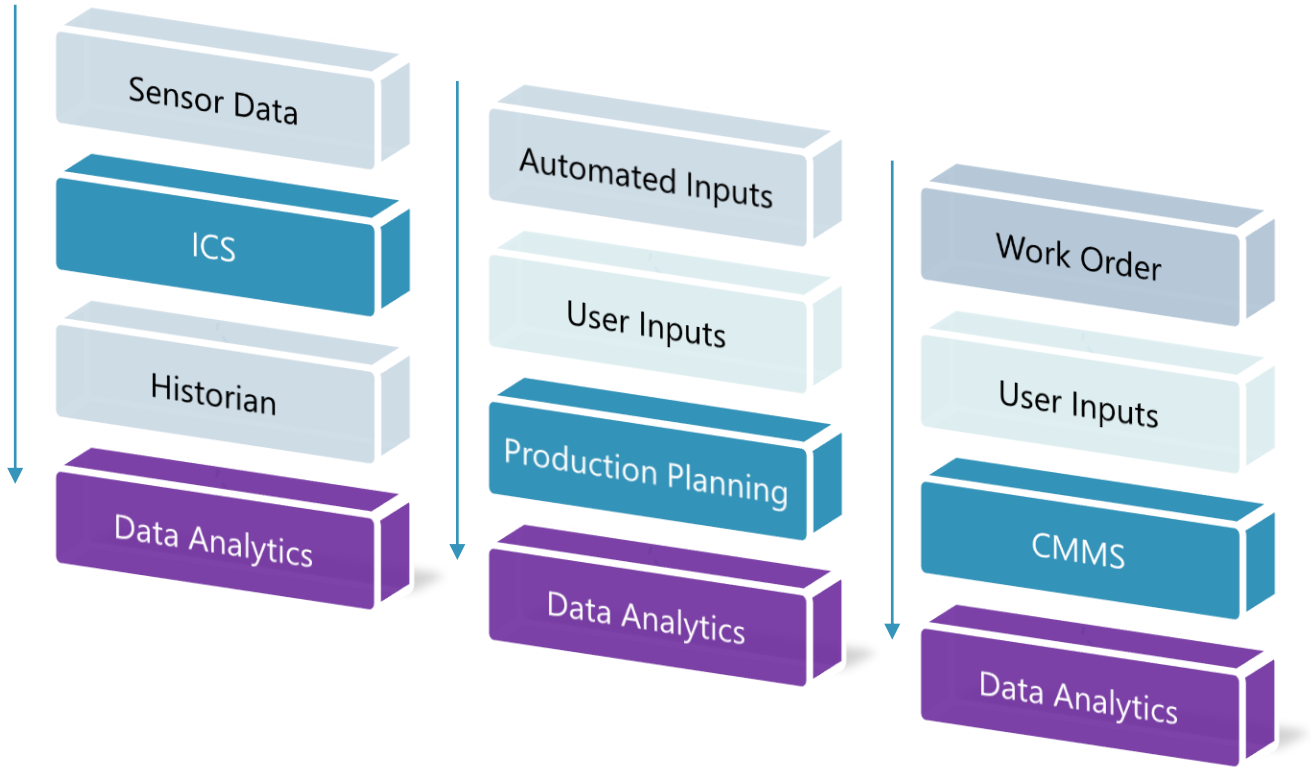
Pitfalls of Artificial Intelligence

- Large language models give what appear to be thorough, persuasive, and comprehensive answers that may also be 100% incorrect.
- Outside of the data scientists who trained those models, relatively few people can explain why those models make these mistakes.

Since it was from AI data it must be true?

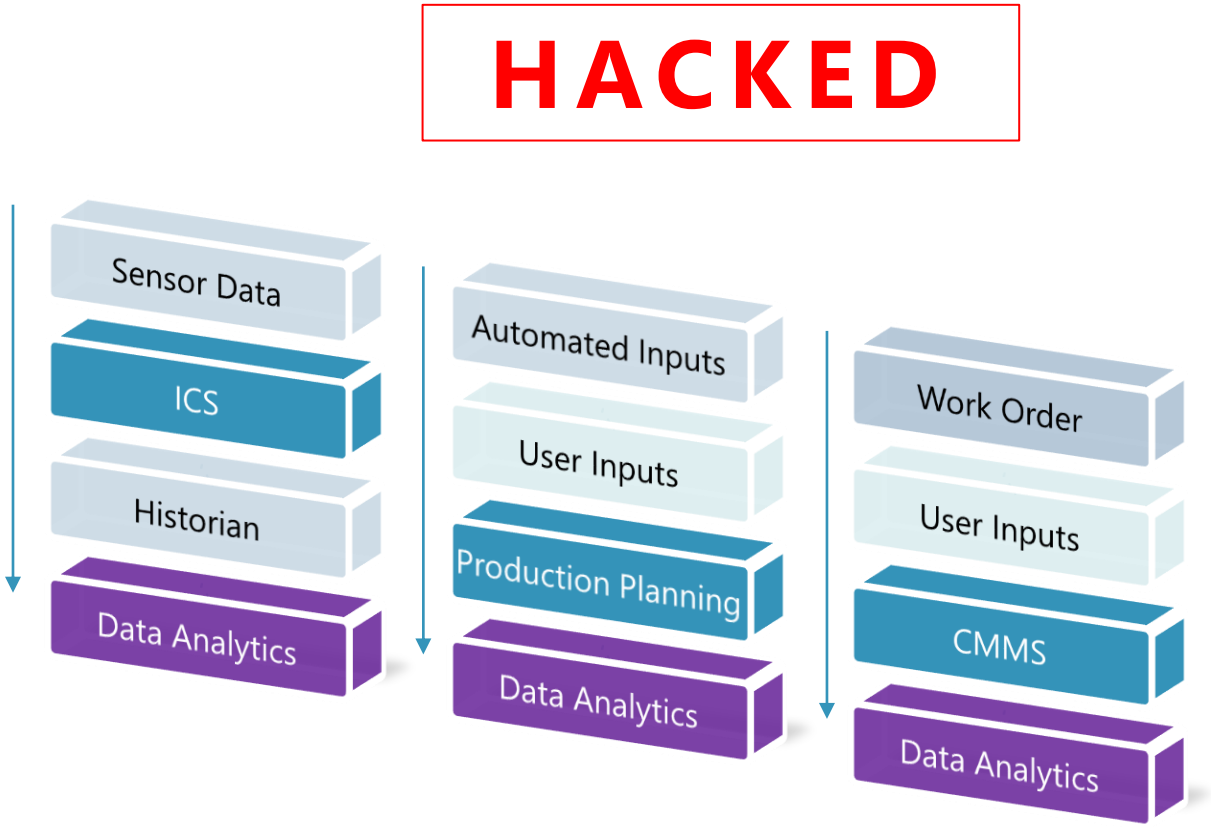
Industrial Data Analytics Suite – Potential Hazards

- Pulls in and analyzes data from multiple sources
  - Industrial Control Systems (ICS)
  - Production planning tools
  - Computerized Maintenance Management Systems (CMMS)
- A sensor could fail and starts providing bad data to a key analytics model.
- A user could input the wrong value or accidentally initiate the wrong work process and overwrite valid data with invalid data.
- The work order could be generated incorrectly, or the employee could do the wrong work, or the work order could be tracked incorrectly.



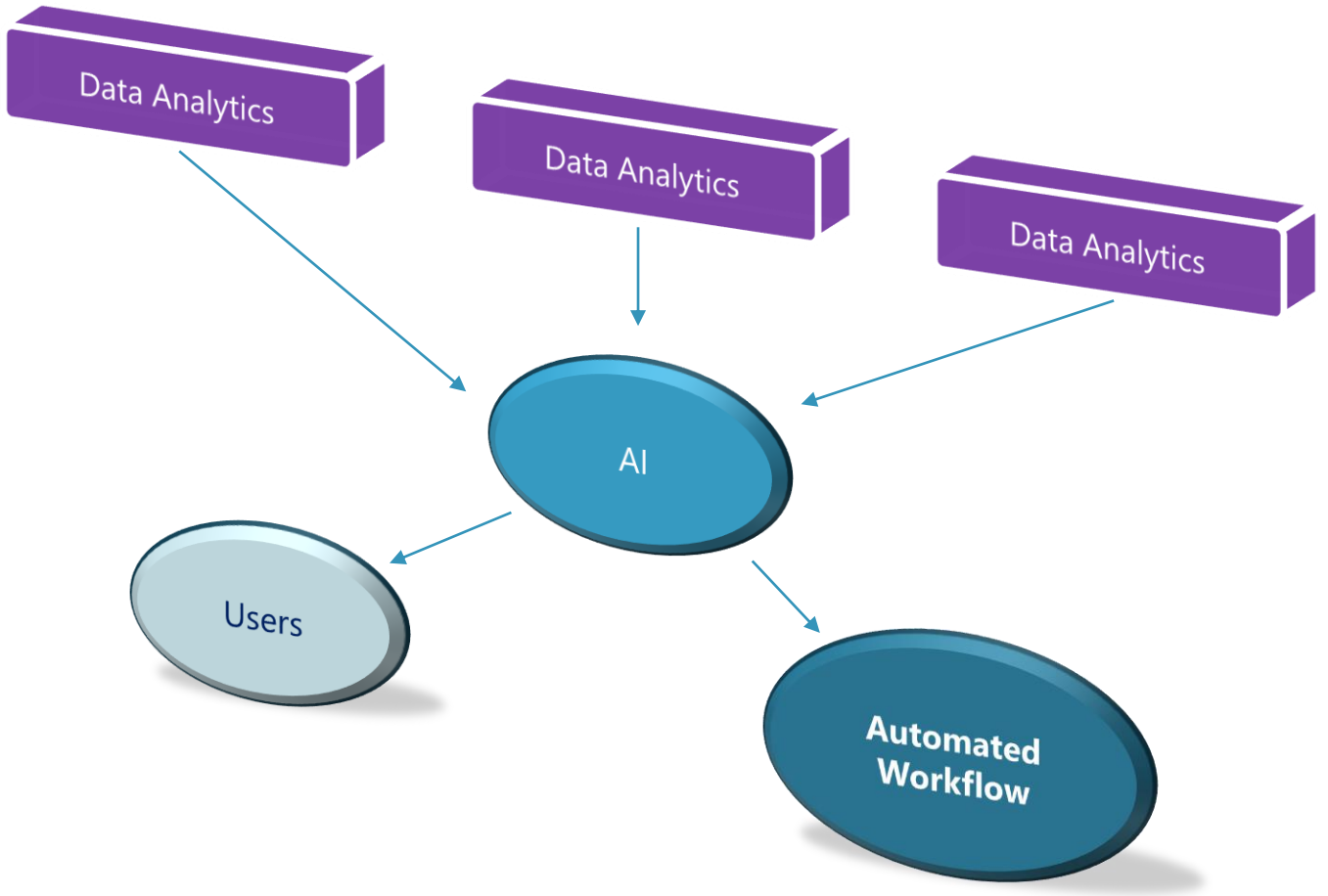
Industrial Data Analytics Suite

- A facility could experience a cybersecurity event.
- Systems would be compromised, providing bad data to the data analytics platform, but in this event the source of the bad data may not be as easily discoverable.
- A malicious actor may be able to substitute controller firmware that alters the sensor values being processed while presenting valid values to the operator.
- A hacker could alter or disable specific automated inputs into the production planning suite, thereby impacting long-term forecasting but going unnoticed in the short-term.
- The computerized maintenance management system if cloud-based, could receive a Denial-of-Service attack, rendering it inoperable.



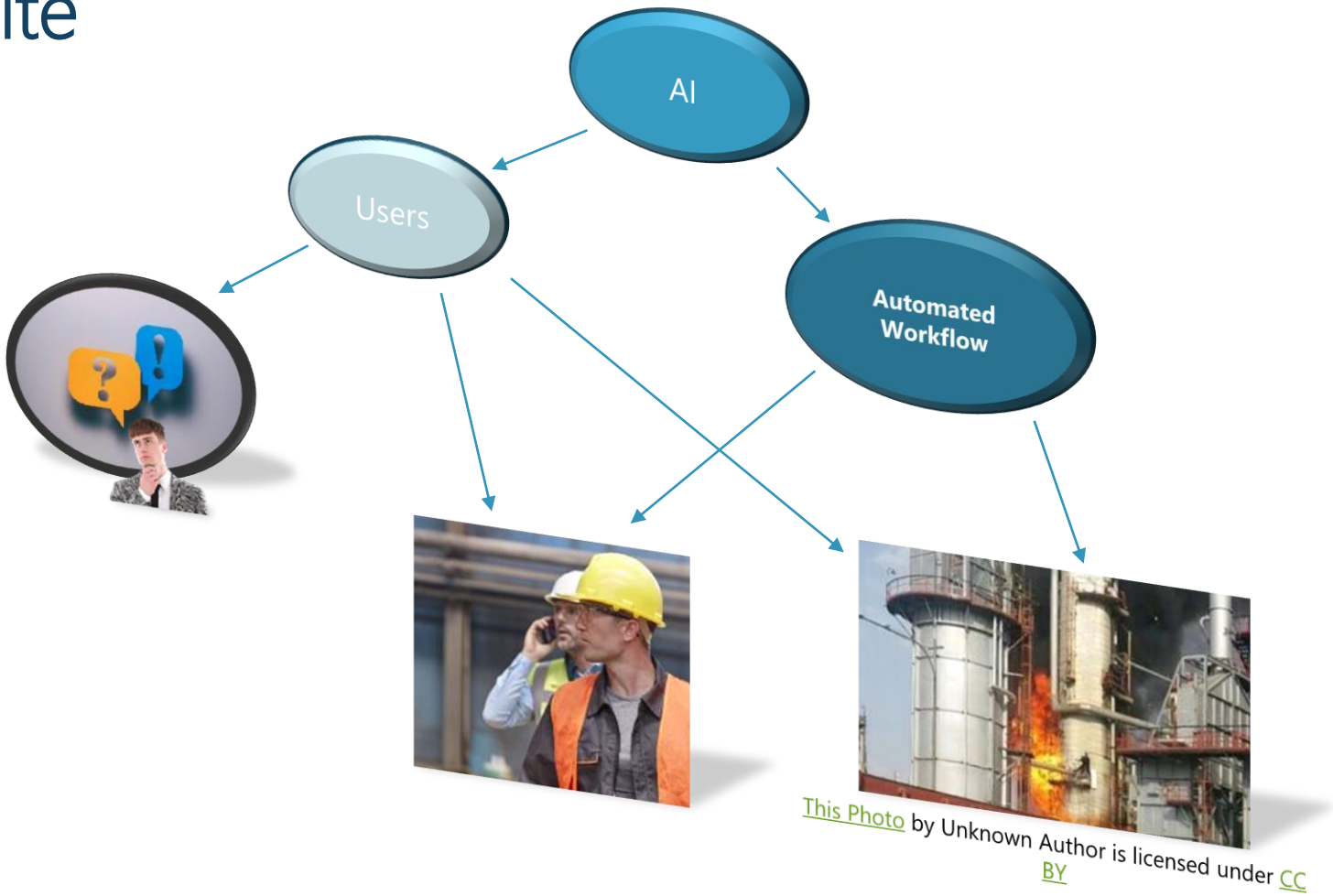
Industrial Data Analytics Suite

- Multiple data sources, some of which may or may not be compromised, providing data that may or may not be compromised.
  - Will the AI models recognize those data errors?
  - Can they recognize good data from bad, quality data from intentionally erroneous data?
  - How will they respond to the bad data?
  - Will the AI models respond exactly as expected, or do something completely unexpected?
  - Can a human user recognize a problem and intervene before erroneous analysis and results occur?
  - What if the analysis results are automatically fed into other systems and there is no human in the loop to recognize there is a problem until the problem presents in more noticeable ways?



Industrial Data Analytics Suite

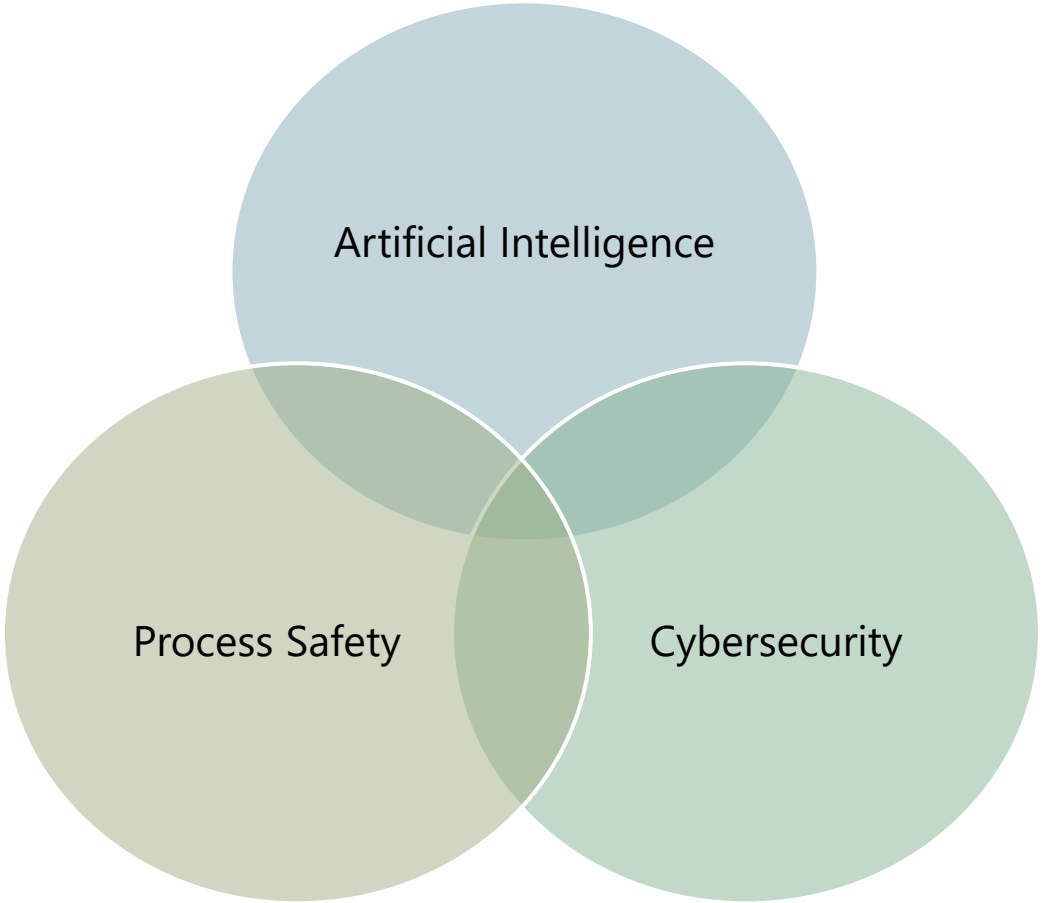
- Multiple users
- Multiple potential results
  - They could be benign
  - They could be disruptive
  - They could be catastrophic



Organizations Considering AI

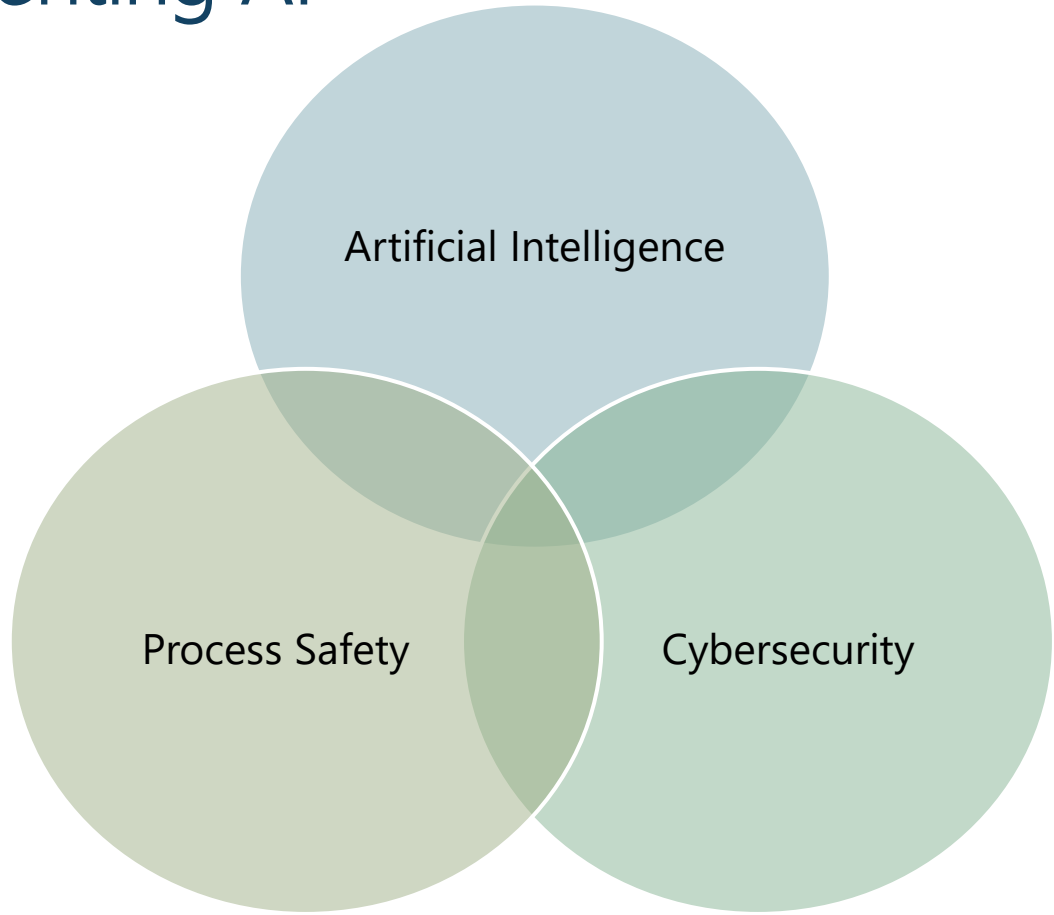
Thoroughly understand:

- How AI functions
- How AI needs to be maintained
- How AI fits into your operational structure
- How to put safeguards around AI's functionality



As the Organization Starts Implementing AI

- Include cybersecurity and AI in process safety reviews
  - Capture potential touchpoints where a system could be affected by AI or a cyber attack and impact process safety
  - Capture overlap between programs to understand program requirements, work processes, and personnel responsibilities
- Conduct process safety assessments
- Properly train all personnel
- Make sure to include Operational Technology (OT) and ICS



What are solutions?

- Cybersecurity Assessments
  - Develop a robust, functional, enterprise-wide cybersecurity program
  - Conduct cybersecurity risk assessments: the Cyber PHA
  - Conduct routine cybersecurity program audits
  - Conduct cyber vulnerability assessments

- Process Safety Assessments
  - Consider the process safety risks of AI/ML applications during PHAs, Operating Procedures and other PSM frameworks
  - Conduct PHAs focused on risks of AI/ML applications
  - Conduct routine audits & assessments

Conclusions – Collaborate on Process Safety and Cybersecurity

- Cybersecurity and process safety professionals must coordinate their efforts to counter potential threats:
- Process safety impacts understood
- Ensuring that measures applied to critical assets are effectively integrated with security systems and align with safety and operational requirements.

Conclusions - Embrace Convergence

- Organizations with converged cybersecurity and process safety functions are more resilient and better prepared to identify, prevent, mitigate, and respond to threats.

2024 QATAR PROCESS SAFETY SYMPOSIUM

ConocoPhillips Qatar | QatarEnergy LNG

DAVID MOORE, PE, CSP
President & CEO
AcuTech Group, Inc.

NAWAYD SHAIKH
Group Leader, Qatar
AcuTech Consulting LLC

HEADQUARTERS
1750 Tysons Blvd, Suite 200
McLean, VA 22102
USA

QATAR OFFICE
Office No. 1415
Al Fardan Office Tower, 14th Floor
61 Al Funduq St., West Bay
Doha, Qatar, P.O Box 31316

EMAIL ADDRESS
contact@acutech-consulting.com

WEBSITE
www.acutech-consulting.com

CONTACT US