Paul Smith

AIT Austrian Institute of Technology and a Visiting Researcher at Lancaster University, UK

KEY MESSAGE

For critical industrial systems, there is an abundance of data that can be used to provide insights about safety and security KPIs. In this talk, I will introduce the nature of this data and describe some approaches to and challenges of using machine learning to derive insights.

INTERNATIONAL CONFERENCE ON

Ensuring **Industrial Safety**

The role of government, regulations, standards and new technologies

Challenges of Monitoring Industry Safety and Security

Paul Smith, AIT Austrian Institute of Technology

UNITED NATIONS
INDUSTRIAL DEVELOPMENT ORGANIZATION

30 31 May **2019**

Vienna International Centre
Conference Room 1

Vienna, Austria

Safety and Security Monitoring

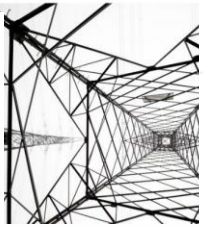
- Safety and security monitoring must be addressed as a common concern
- Cyber-attacks have targeted operational and safety-related systems

KIM ZETTER SECURITY 11.03.14 06:30 AM

AN UNPRECEDENTED LOOK AT STUXNET, THE WORLD'S FIRST DIGITAL WEAPON

KIM ZETTER SECURITY 03.03.16 07:00 AM

INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID



Hack attack causes 'massive damage' at steel works

22 December 2014 Share

The hack attack led to failures in plant equipment and forced the fast shut down of a furnace

MIT Technology Review

Computing / Cybersecurity

Triton is the world's most murderous malware, and it's spreading

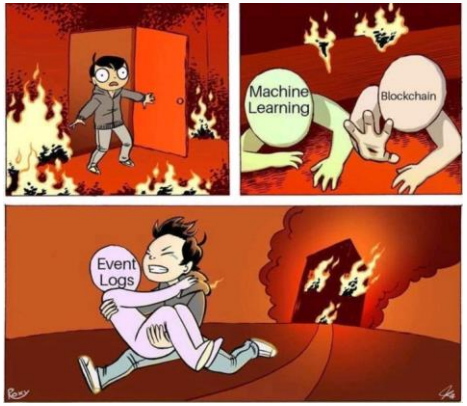
The rogue code can disable safety systems designed to prevent catastrophic industrial accidents. It was discovered in the Middle East, but the hackers behind it are now targeting companies in North America and other parts of the world, too.

Monitoring Systems

- Integration of Information and Operational Technology monitoring is still in its infancy

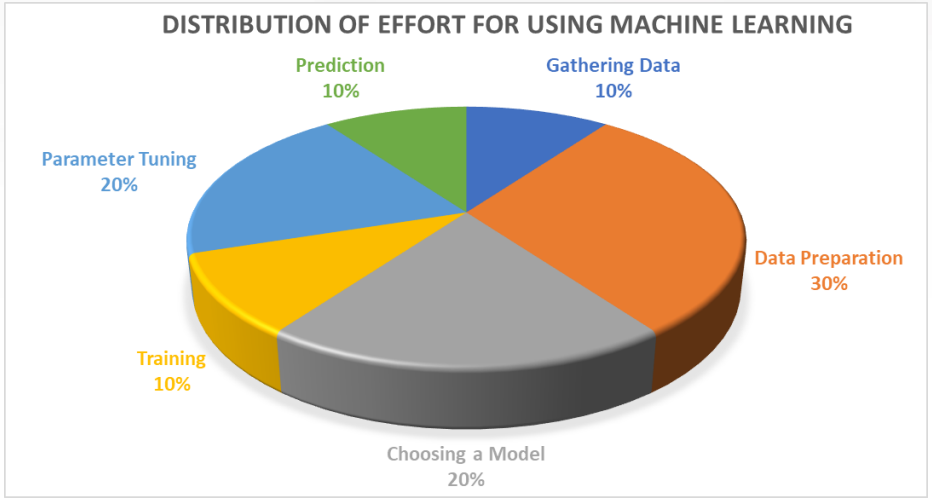
- Various data sources exist
  - IT (computer and network) systems
  - Supervisory Control and Data Acquisition (SCADA) systems
  - Process data (pressure, flow, voltage, …)

	Information Technology	Operational Technology
Security	Mature	Immature
Safety	Immature	Mature



Gaining Insights with Machine Learning

- Many different approaches exist
  - Statistical anomaly detection (e.g., KL Divergence)
  - Classical machine learning (e.g., Support Vector Machines)
  - Deep learning (e.g., neural networks)
- There is no one-size-fits-all algorithm – the 'best' approach can depend on the data (volume, dimensionality) and the questions you're trying to answer



Machine Learning Open Challenges

- *Explainability* of results from machine learning
  - Why did I get this result?
- Adversarial examples are a potential emerging threat
- Causal inference is a major open challenge – e.g., asking 'what if' questions

[1]

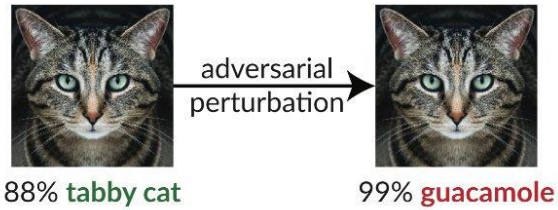


Fig. 1. A small change imperceptible to humans misleads the InceptionV3 network into classifying an image of a tabby cat as guacamole. Image taken from https://github.com/anishathalye/obfuscated-gradients.

[2]

Level	Example Questions
1. Association	What is the root cause of this event?
2. Intervention	What if I change my firewall?
3. Counterfactuals	Was it the new policy that caused the security breach?

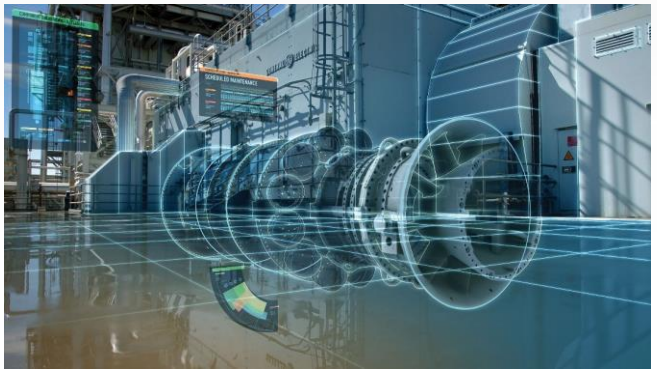
[1] A. Shamir et al., "A Simple Explanation for the Existence of Adversarial Examples with Small Hamming Distance" https://arxiv.org/pdf/1901.10861.pdf
[2] J. Pearl, "The seven tools of causal inference, with reflections on machine learning," *Commun. ACM* 62, 3 (Feb 2019), 54-60. DOI: https://doi.org/10.1145/3241036

An Emerging Technology: Digital Twins

"A digital twin is a real time digital replica of a physical device"

– Bacchiega (2017)

- Digital twins are being applied to tasks such as predictive maintenance, to reduce the likelihood of catastrophic failures
- Potential security applications of digital twins:
  - Vulnerability assessment
  - Real-time attack monitoring and detection
  - Decision support for incident response
- Many open research challenges



https://www.ge.com/research/offering/digital-twin-creation

Conclusions

- Safety and security monitoring is currently not well-integrated
  - This includes technology, people and processes
- Machine learning can be used to gain useful insights into the safety and security of a system
  - This is not straightforward … at all
  - For industry safety and security there are some open research challenges
- Digital twins are an emerging technology that has applications to both safety and security
  - This technology is still quite immature, especially for security applications