ICS Breach, what to do after oh no, frameworks and issues of IM/IT

Dr. Samuel Liles

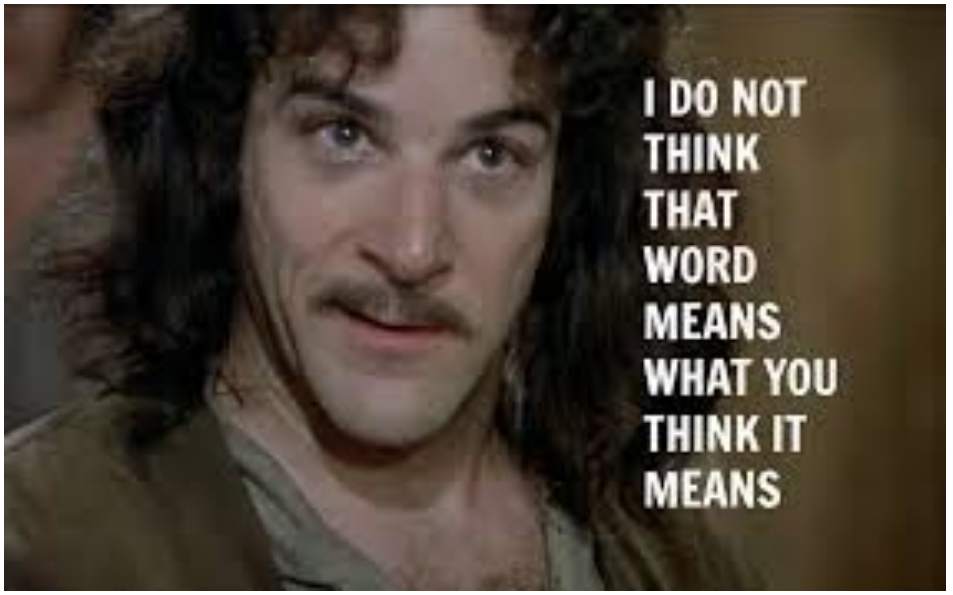
http://selil.com

Agenda

- Through the lens of risk
- Cybery thoughts
- From ICS to IoT
- Threats
- Vulnerabilities
- Frameworks

Just because…. Cyber.

- Lots of definitions
- Umbrella term for activities to increase coordination, collaboration, and understanding <break rice bowls>
- My definition: The term “cyber” itself denotes a human cognitive centric concept that deals with the disintermediation of technology centered within human activity.



Random image off the teh webz

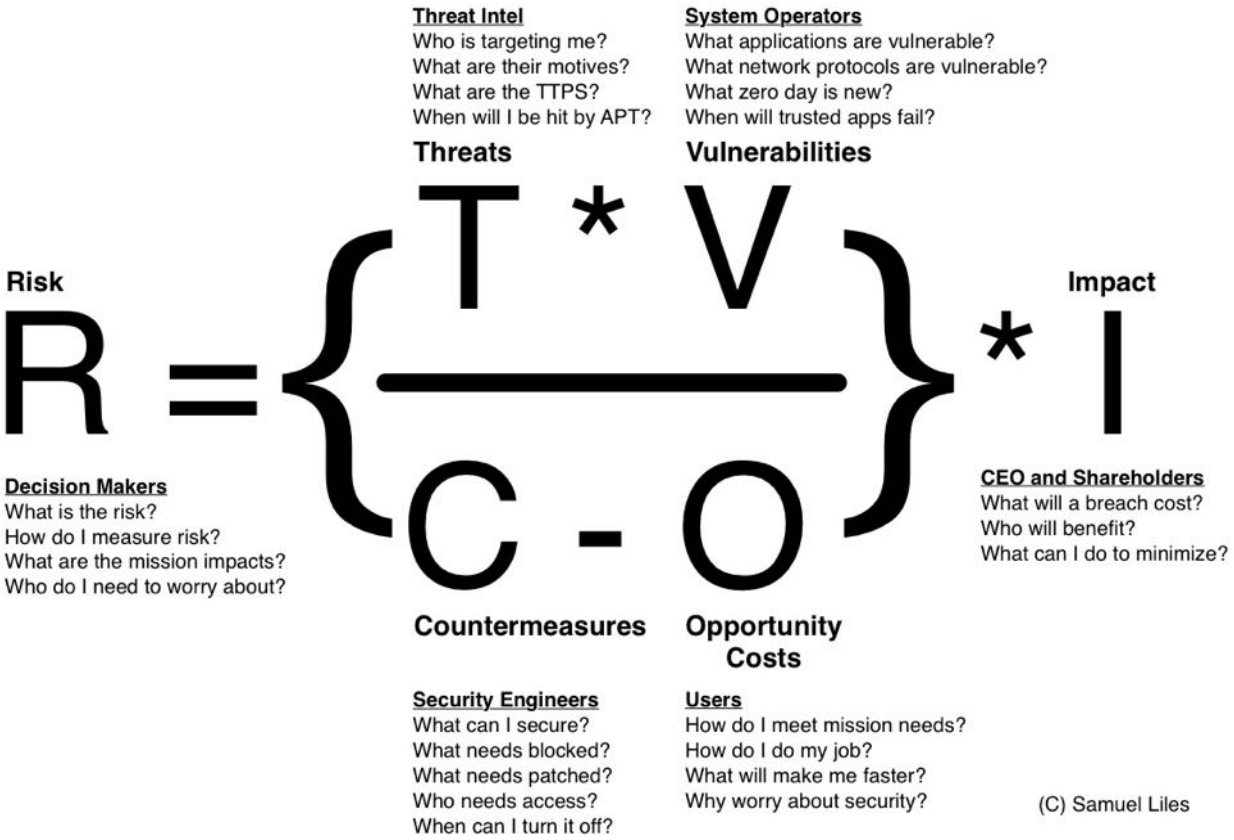
ICS/DCS/BCS/SCS/IoT/VMS

- Control systems come in a variety of favors, types, and uses
- Usually part of the academic discipline of industrial engineering or electrical engineering
- In general a product, capability, or system of systems that assist or maintain a real time process
- **Industrial control system** (ICS) is a general term that encompasses several types of **control systems** used in **industrial** production, including supervisory **control** and data acquisition (SCADA) **systems**, distributed **control systems** (DCS), and other smaller **control system** configurations such as programmable logic controllers
  https://en.wikipedia.org/wiki/Industrial_control_system oops
  http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

Industrial Control Systems

http://www.nist.gov/el/isd/images/sh_224936086_refinery_c_Christian_Lagerek_LR.jpg

Operational Technology



Threats operate on **vulnerabilities** that have inadequate **countermeasures** having some **impact**

Engineers build systems for **users** informed by **threat intelligence** that have s**ystem operators** monitored by **security teams** who respond to events through **incident response**

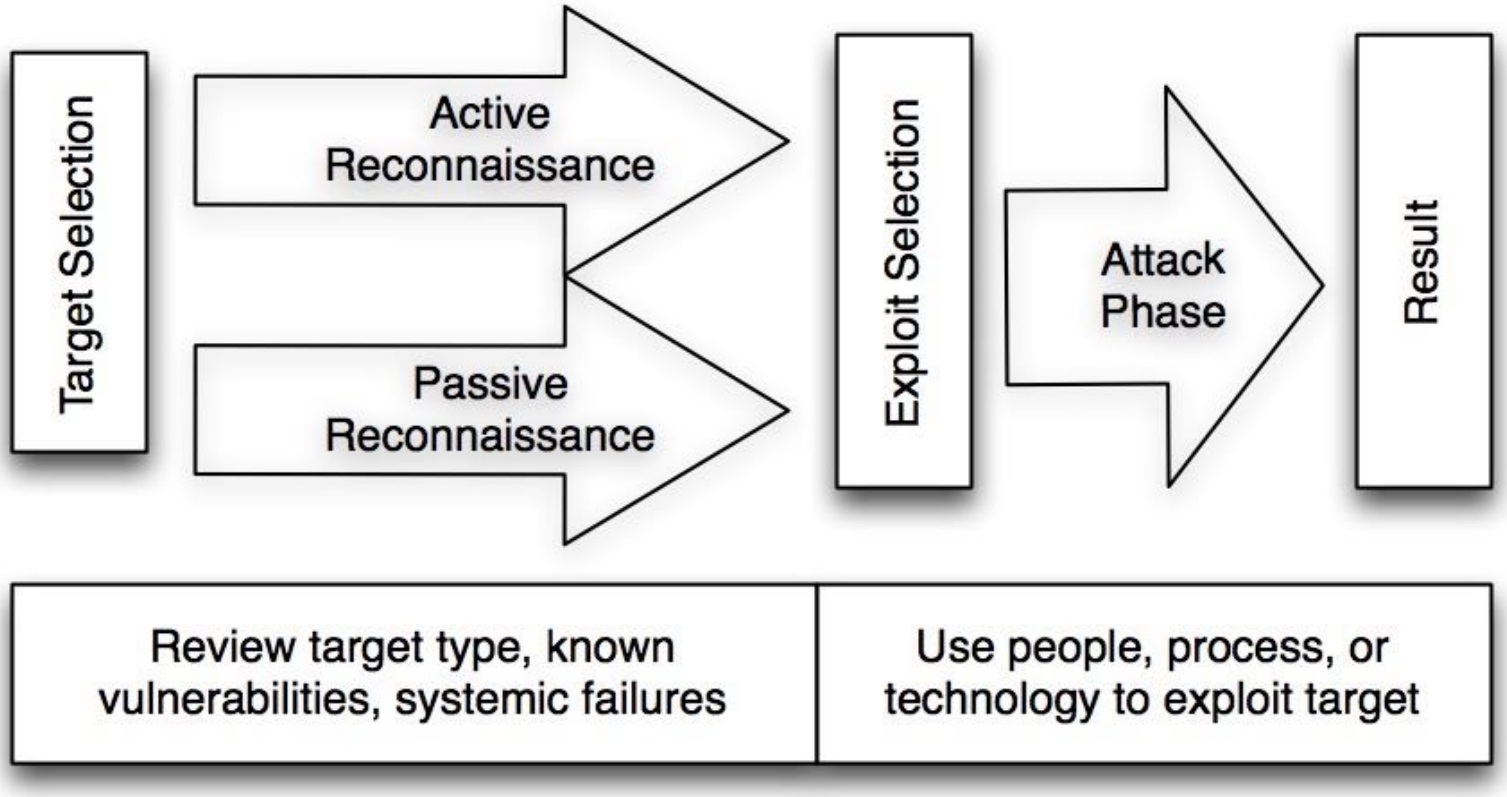
Opportunity costs of **users** are often ignored creating increased organization wide **risk**

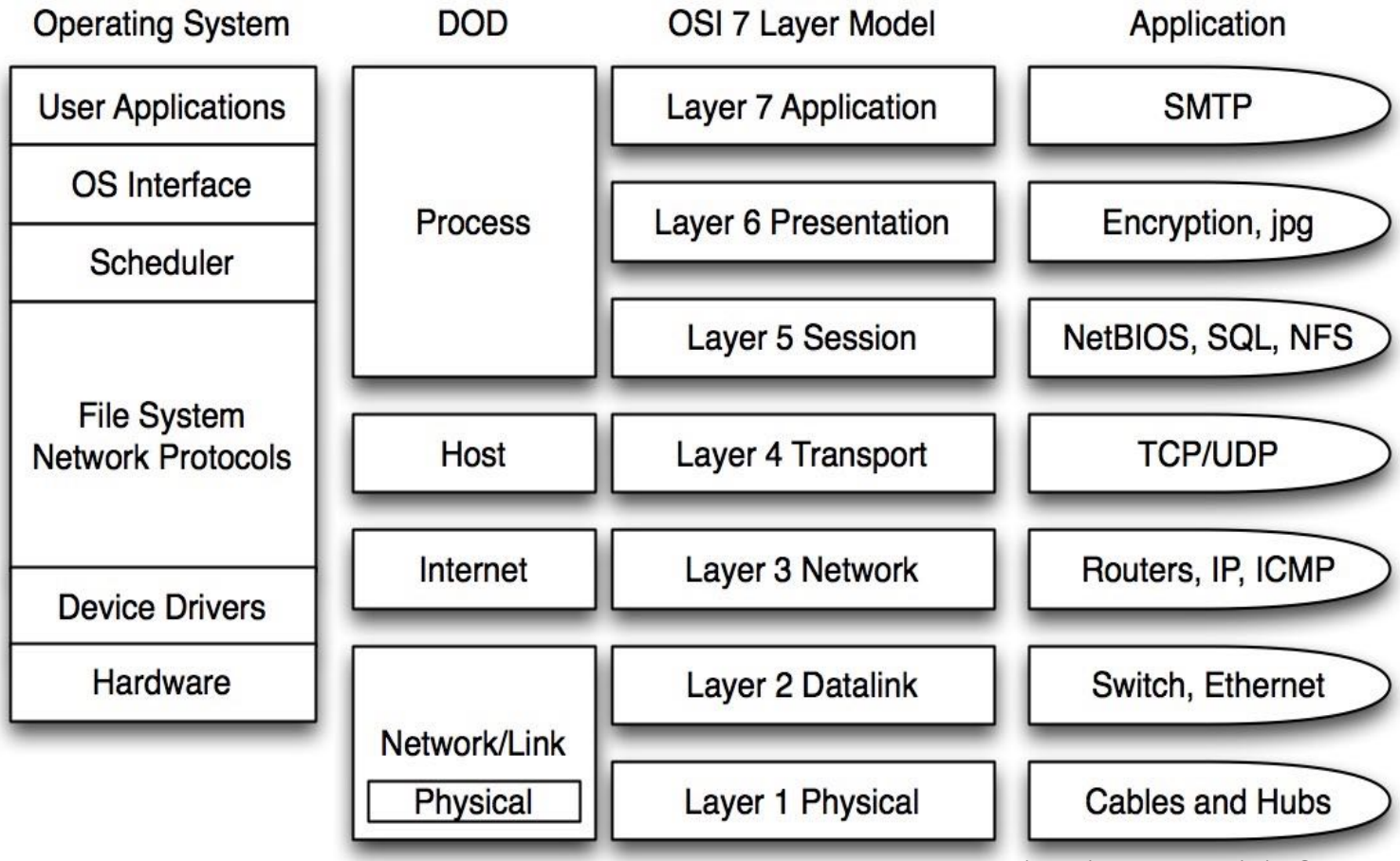
Vulnerabilities

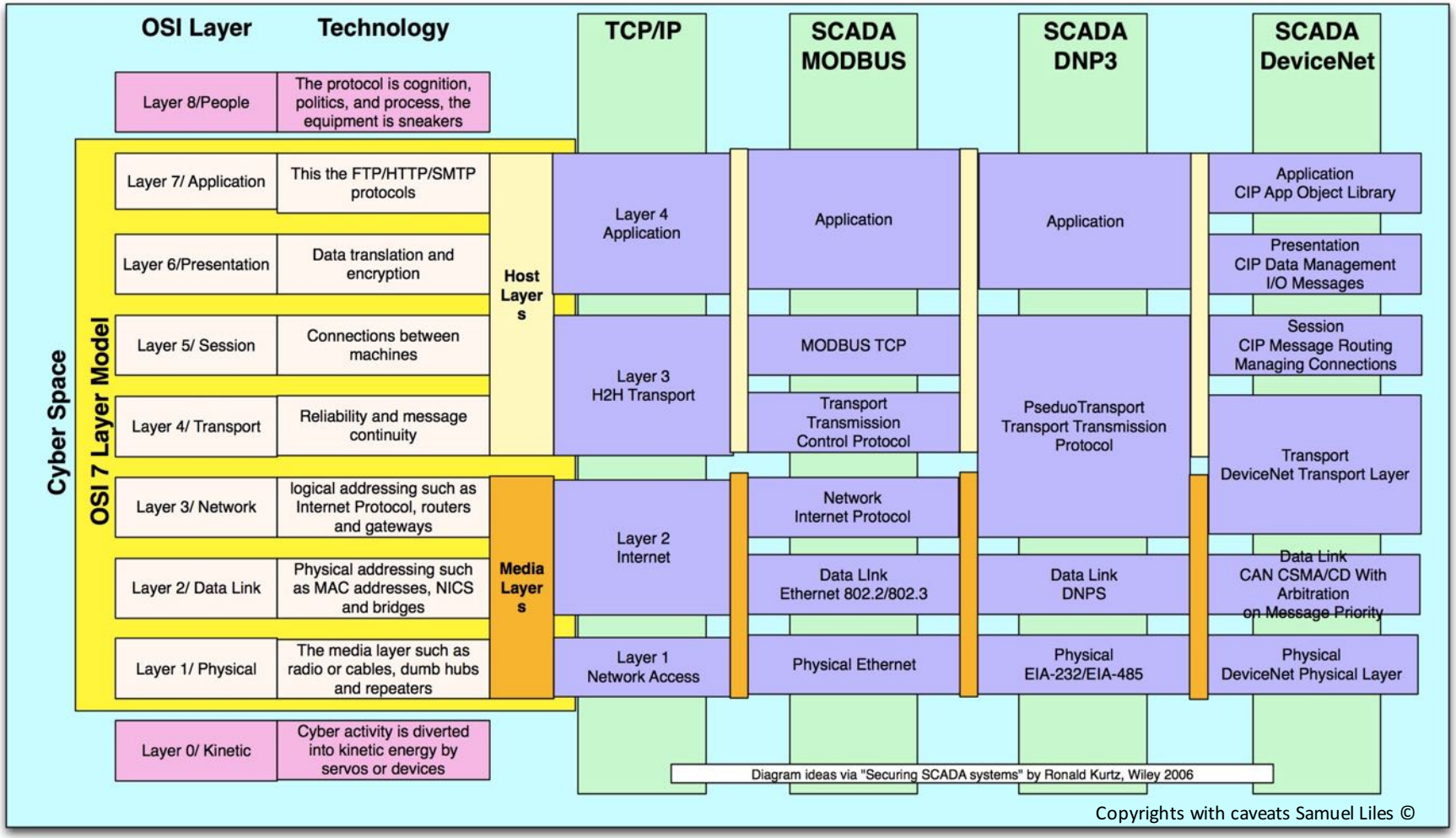
- Policy and procedures vulnerabilities
  - Passwords, design, guidelines, administrative mechanisms
- Platform vulnerabilities
  - Configuration, hardware, software, supply chain, malware
- Network vulnerabilities
  - Configuration, hardware, perimeter, monitoring & logging, communication, wireless

Threats

- Attackers
- Bot-Network Operators
- Criminals
- Foreign Intelligence Services
- Insiders
- Phishers
- Spammers
- Spyware/malware authors
- Terrorists
- Industrial spies







That moment when millions of voices scream “Not the cyber!”

- **Maroochy Shire Sewage Spill**[5]**.** In the spring of 2000, a former employee of an Australian organization that develops manufacturing software applied for a job with the local government, but was rejected. Over a two-month period, the disgruntled rejected employee reportedly used a radio transmitter on as many as 46 occasions to remotely break into the controls of a sewage treatment system. He altered electronic data for particular sewerage pumping stations and caused malfunctions in their operations, ultimately releasing about 264,000 gallons of raw sewage into nearby rivers and parks.

  http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/

- **Taum Sauk Water Storage Dam Failure**[11]. In December 2005, the Taum Sauk Water Storage Dam suffered a catastrophic failure releasing a billion gallons of water. The failure of the reservoir occurred as the reservoir was being filled to capacity or may have possibly been overtopped. The current working theory is that the reservoir's berm was overtopped when the routine nightly pump-back operation failed to cease when the reservoir was filled. According to AmerenUE, the gauges at the dam read differently than the gauges at the Osage plant at the Lake of the Ozarks, which monitors and operates the Taum Sauk plant remotely. The stations are linked together using a network of microwave towers, and there are no operators on-site at Taum Sauk.

  http://en.wikipedia.org/wiki/Taum_Sauk_Dam_Failure

Frameworks

ISO/IEC 27035:2011 provides a structured and planned approach to:
1. detect, report and assess information security incidents;
2. respond to and manage information security incidents;
3. detect, assess and manage information security vulnerabilities; and
4. continuously improve information security and incident management as a result of managing information security incidents and vulnerabilities.

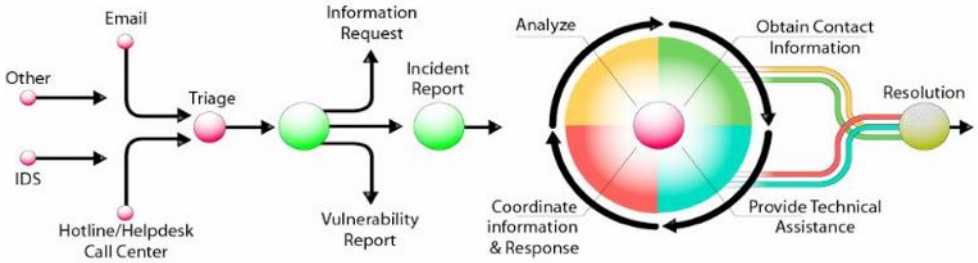
[ISO/IEC 27035:2011: Information Security Incident Management]

Preparation, identification, containment, eradication, recovery, and lessons learned.

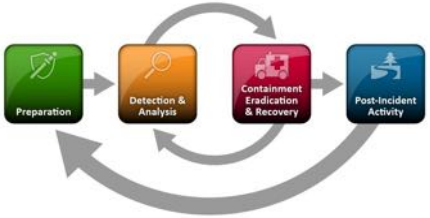
[SANS: Creating and Managing an Incident Response Team]

Incident triage, incident coordination, incident resolution

[RFC 2350: Expectations for Computer Security Incident Response]



[CERT: Handbook for Computer Security Incident Response Teams (CSIRTs)]



[NIST 800-61: Computer Security Incident Handling Guide]

Securing all the things

- Restrict logical access to the ICS network and network activity
- Restrict physical access to the ICS network and devices
- Protect individual ICS components from exploitation
- Maintain functionality during adverse conditions
- Plan on restoration of system after an incident

http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

Some sources not cited but referred

- Byres, E., & Lowe, J. (2004, October). The myths and facts behind cyber security risks for industrial control systems. In *Proceedings of the VDE Kongress* (Vol. 116, pp. 213-218). http://web-post.www.controlglobal.com/assets/Media/MediaManager/The_Myths_and_Facts_behind_Cyber_Security_Risks.pdf
- Jaatun, M. G., Albrechtsen, E., Line, M. B., Tøndel, I. A., & Longva, O. H. (2009). A framework for incident response management in the petroleum industry. *International Journal of Critical Infrastructure Protection*, *2*(1), 26-37. https://www.researchgate.net/publication/245478708_A_framework_for_incident_response_management_in_the_petroleum_industry
- Stouffer, K., Falco, J. and Scarfone, K., 2011. Guide to industrial control systems (ICS) security. *NIST special publication*, *800*(82), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
- Ten, C. W., Liu, C. C., & Manimaran, G. (2008). Vulnerability assessment of cybersecurity for SCADA systems. *Power Systems, IEEE Transactions on*, *23*(4), 1836-1846. http://feihu.eng.ua.edu/NSF_CPS/year1/w13_3.pdf

Other Resources

- ICS-CERT https://ics-cert.us-cert.gov/
- Industrial Control Systems Working Group https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG
- SANS-ICS http://ics.sans.org/
- USACE Control Systems Cybersecurity Technical Center of Expertise http://www.hnc.usace.army.mil/Media/FactSheets/FactSheetArticleView/tabid/10784/Article/608766/industrial-control-systems-cybersecurity-technical-center-of-expertise.aspx
- Installation Support and Programs Management http://www.hnc.usace.army.mil/Missions/InstallationSupportandProgramsManagement.aspx

Questions?