NTNU

Norwegian University of
Science and Technology

Remote Access Security Recommendations for Norwegian Petroleum Companies

Peder Grundvold & Jon Smebye

Introduction

pedergrbr@gmail.com

jonsmebye@gmail.com

Responsible professor: Maria Bartnes

Supervisors: Lars Bodsberg
Roy Thomas Selbæk Myhre

- RQ: *How can new ideas and emerging technologies in remote access be applied in the development of improved remote access security recommendations for Norwegian petroleum companies?*

Introduction

Agenda

Method

Results:

Tech/solutions identified

Functional req. and user stories

Threat actors and goals

Identified focus areas

Evaluation

Final Recommendations

Q&A

Agenda

- Method
- Results
    - Technologies/solutions found in lit. study
    - Functional Requirements and User Stories
    - Threat Actors and Goals
    - Identified focus areas
    - **Final recommendations**

Feel free to ask us questions at the end of the presentation!

Introduction

Agenda

Method

Results:

Tech/solutions identified

Functional req. and user stories

Threat actors and goals

Identified focus areas

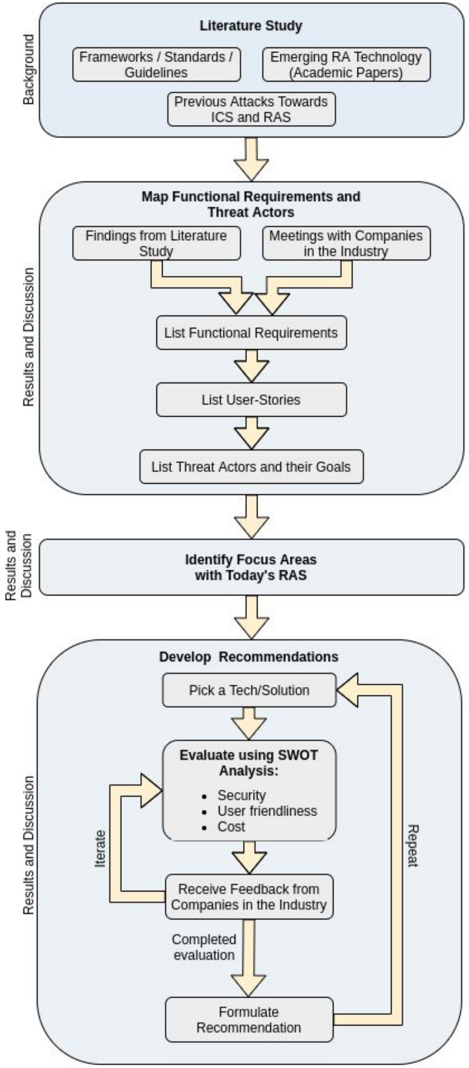
Evaluation

Final Recommendations

Q&A

Method

- Literature study
  - Existing frameworks, standards, and industry guidelines
  - Emerging RA technologies (identify different solutions)
  - Previous attacks towards ICSs
- Cooperation with the industry
  - Meetings/workshops with two petroleum companies (Alpha and Beta)
  - Insight into their remote access solutions
  - Feedback on current work
- Evaluation of identified solutions
  - SWOT-analysis
  - Meetings and feedback from Alpha and Beta
- Final result:
  - A set of concise recommendations for how new technologies could improve existing solutions



Background

Literature Study

Frameworks / Standards / Guidelines

Emerging RA Technology (Academic Papers)

Previous Attacks Towards ICS and RAS

Results and Discussion

Map Functional Requirements and Threat Actors

Findings from Literature Study

Meetings with Companies in the Industry

List Functional Requirements

List User-Stories

List Threat Actors and their Goals

Results and Discussion

Identify Focus Areas with Today's RAS

Results and Discussion

Develop Recommendations

Pick a Tech/Solution

Evaluate using SWOT Analysis:

- Security
- User friendliness
- Cost

Iterate

Receive Feedback from Companies in the Industry

Completed evaluation

Formulate Recommendation

Repeat

Introduction

Agenda

Method

Results:

Tech/solutions identified

Functional req. and user stories

Threat actors and goals

Identified focus areas

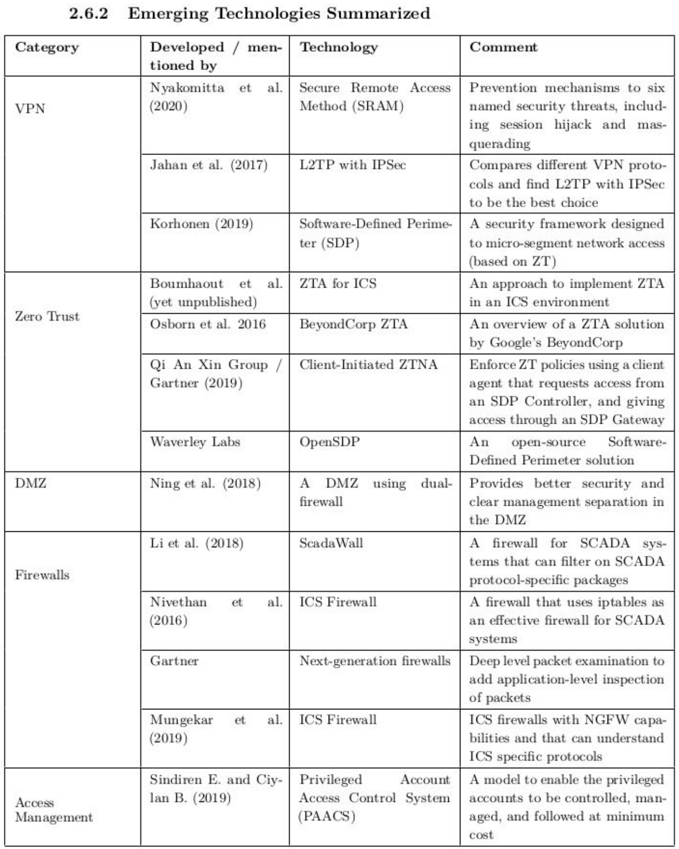
Evaluation

Final Recommendations

Q&A

Remote Access Solutions and Technologies Identified

- VPN
- Zero Trust Security
- DMZ
- Firewalls
- Access management
- Network Access Control
- Sandboxing security
- Sheep dipping
- Intrusion and Anomaly Detection Systems
- Unidirectional Security Gateways



2.6.2 Emerging Technologies Summarized

Category	Developed / mentioned by	Technology	Comment
VPN	Nyakomitta et al. (2020)	Secure Remote Access Method (SRAM)	Prevention mechanisms to six named security threats, including session hijack and masquerading
	Jahan et al. (2017)	L2TP with IPSec	Compares different VPN protocols and find L2TP with IPSec to be the best choice
	Korhonen (2019)	Software-Defined Perimeter (SDP)	A security framework designed to micro-segment network access (based on ZT)
Zero Trust	Boumhaout et al. (yet unpublished)	ZTA for ICS	An approach to implement ZTA in an ICS environment
	Osborn et al. 2016	BeyondCorp ZTA	An overview of a ZTA solution by Google's BeyondCorp
	Qi An Xin Group / Gartner (2019)	Client-Initiated ZTNA	Enforce ZT policies using a client agent that requests access from an SDP Controller, and giving access through an SDP Gateway
	Waverley Labs	OpenSDP	An open-source Software-Defined Perimeter solution
DMZ	Ning et al. (2018)	A DMZ using dual-firewall	Provides better security and clear management separation in the DMZ
Firewalls	Li et al. (2018)	ScadaWall	A firewall for SCADA systems that can filter on SCADA protocol-specific packages
	Nivethan et al. (2016)	ICS Firewall	A firewall that uses iptables as an effective firewall for SCADA systems
	Gartner	Next-generation firewalls	Deep level packet examination to add application-level inspection of packets
	Mungekar et al. (2019)	ICS Firewall	ICS firewalls with NGFW capabilities and that can understand ICS specific protocols
Access Management	Sindiren E. and Ciylan B. (2019)	Privileged Account Access Control System (PAACS)	A model to enable the privileged accounts to be controlled, managed, and followed at minimum cost

Part of a table taken from the master thesis

Introduction

Agenda

Method

Results:

Tech/solutions identified

Functional req. and user stories

Threat actors and goals

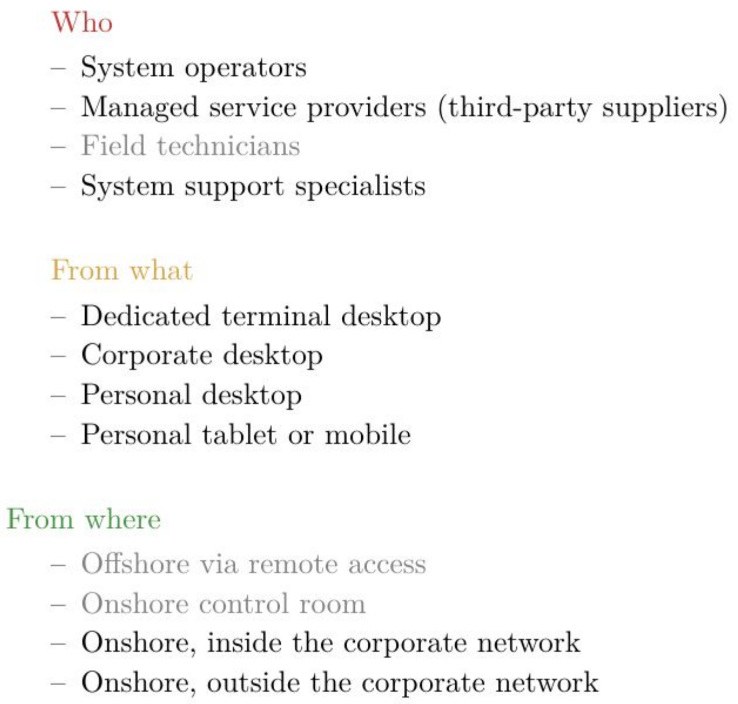
Identified focus areas

Evaluation

Final Recommendations

Q&A

Functional Requirements & User Stories



Who

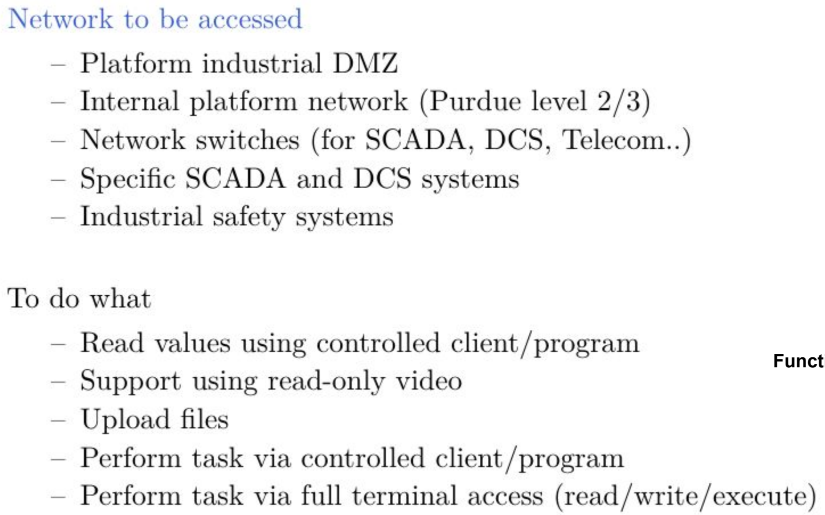
- System operators
- Managed service providers (third-party suppliers)
- Field technicians
- System support specialists

From what

- Dedicated terminal desktop
- Corporate desktop
- Personal desktop
- Personal tablet or mobile

From where

- Offshore via remote access
- Onshore control room
- Onshore, inside the corporate network
- Onshore, outside the corporate network



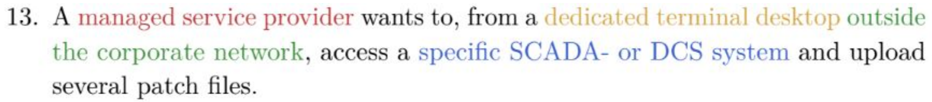
Network to be accessed

- Platform industrial DMZ
- Internal platform network (Purdue level 2/3)
- Network switches (for SCADA, DCS, Telecom..)
- Specific SCADA and DCS systems
- Industrial safety systems

To do what

- Read values using controlled client/program
- Support using read-only video
- Upload files
- Perform task via controlled client/program
- Perform task via full terminal access (read/write/execute)

An example of a user story:



13. A managed service provider wants to, from a dedicated terminal desktop outside the corporate network, access a specific SCADA- or DCS system and upload several patch files.

Introduction

Agenda

Method

Results:

Tech/solutions identified

Functional req. and user stories

Threat actors and goals

Identified focus areas

Evaluation

Final Recommendations

Q&A

Threat Actors and Goals

Who

- Nation-state (APT)
- Script kiddie
- Cybercriminal
- Unintentional insider
- Intentional insider
- Competitors
- Cyber terrorist
- Cyber activist

Goal

- Financial gain
- Hinder production
- Intelligence or intellectual theft
- Terrorism
- Publicity

Introduction

Agenda

Method

Results:

Tech/solutions identified

Functional req. and user stories

Threat actors and goals

Identified focus areas

Evaluation

Final Recommendations

Q&A

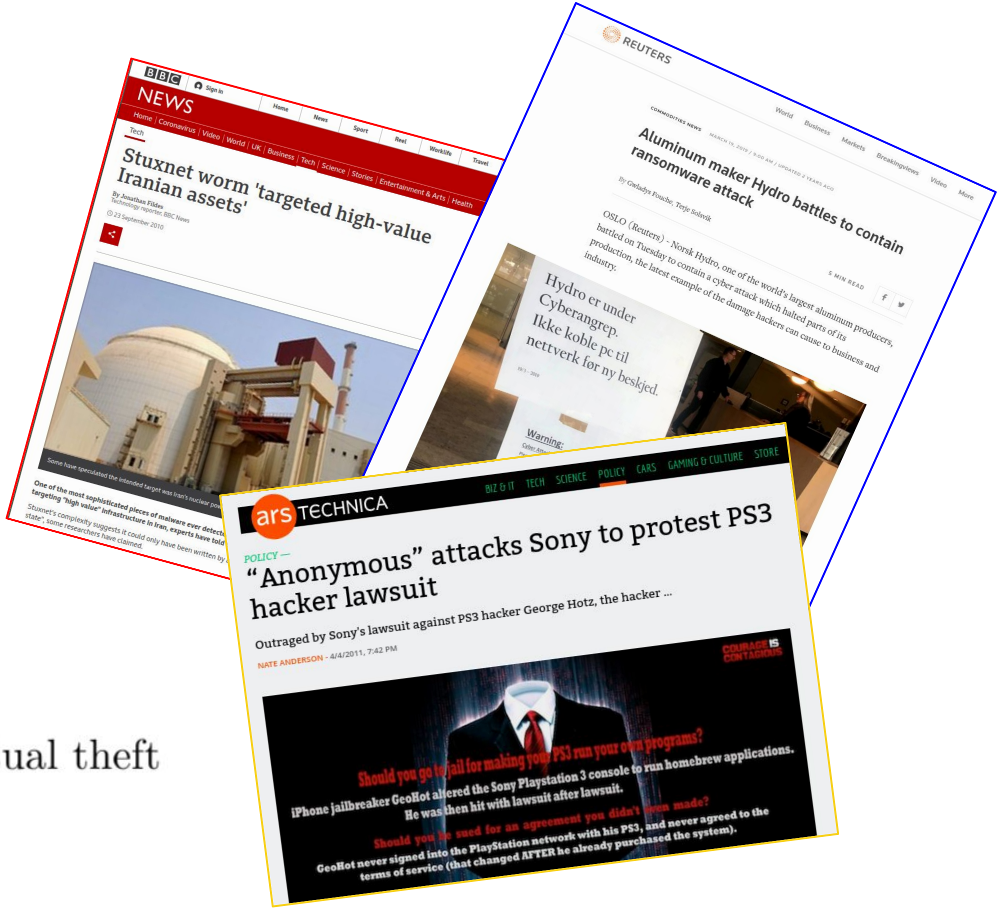
Threat Actors and Goals

Who

- Nation-state (APT)
- Script kiddie
- Cybercriminal
- Unintentional insider
- Intentional insider
- Competitors
- Cyber terrorist
- Cyber activist

Goal

- Financial gain
- Hinder production
- Intelligence or intellectual theft
- Terrorism
- Publicity



BBC NEWS Sign in Home News Sport Reel Worklife Travel

Home | Coronavirus | Video | World | UK | Business | Tech | Science | Stories | Entertainment & Arts | Health

Tech

Stuxnet worm 'targeted high-value Iranian assets'

By Jonathan Fildes
Technology reporter, BBC News

23 September 2010

Some have speculated the intended target was Iran's nuclear pow

One of the most sophisticated pieces of malware ever detect targeting "high value" infrastructure in Iran, experts have told

Stuxnet's complexity suggests it could only have been written by state", some researchers have claimed.

REUTERS

World Business Markets Breakingviews Video More

COMMODITIES NEWS MARCH 19, 2019 / 9:00 AM / UPDATED 2 YEARS AGO

Aluminum maker Hydro battles to contain ransomware attack

By Gwladys Fouche, Terje Solsvik

5 MIN READ

OSLO (Reuters) - Norsk Hydro, one of the world's largest aluminum producers, battled on Tuesday to contain a cyber attack which halted parts of its production, the latest example of the damage hackers can cause to business and industry.

Hydro er under Cyberangrep. Ikke koble pc til nettverk før ny beskjed.
19/3 – 2019
Warning:
Cyber Atta

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE

POLICY —

“Anonymous” attacks Sony to protest PS3 hacker lawsuit

Outraged by Sony's lawsuit against PS3 hacker George Hotz, the hacker ...

NATE ANDERSON - 4/4/2011, 7:42 PM

COURAGE IS CONTAGIOUS
Should you go to jail for making your PS3 run your own programs?
iPhone jailbreaker GeoHot altered the Sony Playstation 3 console to run homebrew applications.
He was then hit with lawsuit after lawsuit.
Should you be sued for an agreement you didn't even made?
GeoHot never signed into the PlayStation network with his PS3, and never agreed to the terms of service (that changed AFTER he already purchased the system).

Introduction

Agenda

Method

Results:

Tech/solutions identified

Functional req. and user stories

Threat actors and goals

Identified focus areas

Evaluation

Final Recommendations

Q&A

Identified Focus Areas with Today’s Solution

1. The **access management** used by our collaborating companies in their RAS could be improved.
   - Work permit systems are cumbersome and manually managed, meaning that users have to be manually added and deleted. This leads to high costs because of wasted time and frequent use of technical support.

2. According to companies Alpha and Beta **file transfer** is an important feature in the RAS.
   - While current solutions work, as this poses a major attack surface, there is room for improvement.

Introduction

Agenda

Method

Results:

Tech/solutions identified

Functional req. and user stories

Threat actors and goals

Identified focus areas

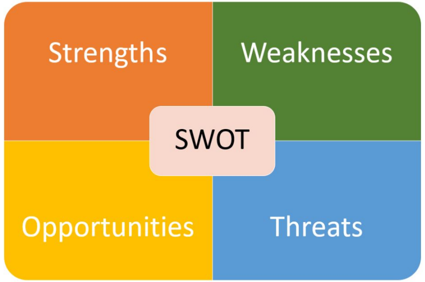
Evaluation

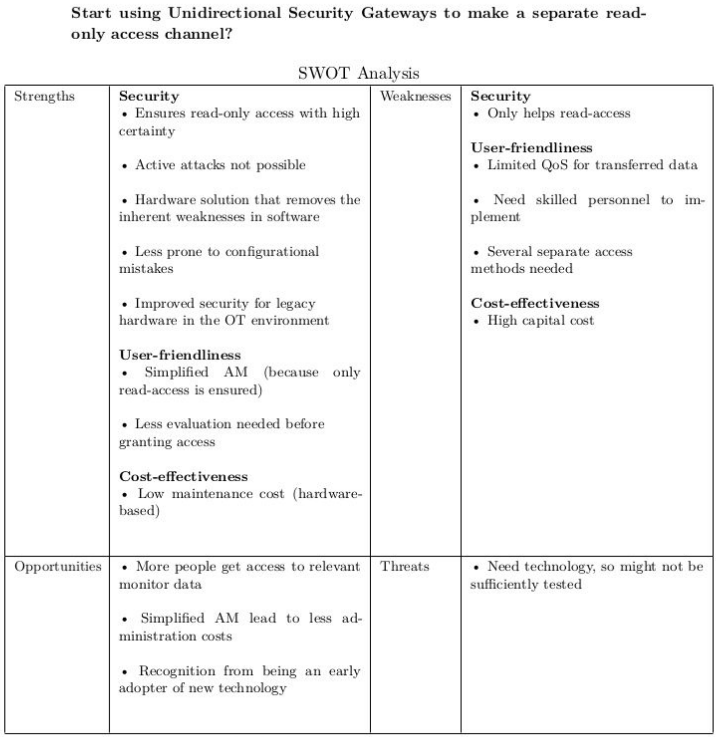
Final Recommendations

Q&A

Evaluation

- Seven solutions and/or technologies were evaluated using SWOT analysis
- **Criteria used:**
  - Security
  - User-friendliness
  - Cost-effectiveness
- Five resulted in new recommendations, two were rejected





Start using Unidirectional Security Gateways to make a separate read-only access channel?

SWOT Analysis

Strengths	**Security** • Ensures read-only access with high certainty • Active attacks not possible • Hardware solution that removes the inherent weaknesses in software • Less prone to configurational mistakes • Improved security for legacy hardware in the OT environment **User-friendliness** • Simplified AM (because only read-access is ensured) • Less evaluation needed before granting access **Cost-effectiveness** • Low maintenance cost (hardware-based)	Weaknesses	**Security** • Only helps read-access **User-friendliness** • Limited QoS for transferred data • Need skilled personnel to implement • Several separate access methods needed **Cost-effectiveness** • High capital cost
Opportunities	• More people get access to relevant monitor data • Simplified AM lead to less administration costs • Recognition from being an early adopter of new technology	Threats	• Need technology, so might not be sufficiently tested

Table taken from the master thesis

Introduction

Agenda

Method

Results:

Tech/solutions identified

Functional req. and user stories

Threat actors and goals

Identified focus areas

Evaluation

Final Recommendations

Q&A

Conclusion - Final Recommendations

1. *Use a hybrid approach between perimeter-based security and Zero Trust Architecture, where they continually add security barriers based on* ***Zero Trust*** *principles. Barriers to add could be:*

    a. *Enforce system-wide continuous network monitoring in combination with machine learning-based anomaly detection. This includes support for monitoring OT-specific protocols.*

    b. *Integrate a risk- and identity-based access management architecture as described above in order to remove workload from the work permit system.*

    c. *Upgrade the existing NAC mechanism to include user/device behavior and environmental factors such as client use patterns and IP geolocation.*

Introduction

Agenda

Method

Results:

Tech/solutions identified

Functional req. and user stories

Threat actors and goals

Identified focus areas

Evaluation

Final Recommendations

Q&A

Conclusion - Final Recommendations

2. *Use a **Next-Generation Firewall** with deep packet inspection and intrusion prevention systems at the network perimeter (Purdue level 3.5).*

3. *Add an **ICS firewall** with NGFW capabilities at the industrial perimeter (Purdue level 1.5) that can operate on OT-specific protocol messages.*

Conclusion - Final Recommendations

4. *Implement a **Sandboxing** solution to use with file transfers, either locally, cloud-based, or in a hybrid solution.*

Introduction

Agenda

Method

Results:

Tech/solutions identified

Functional req. and user stories

Threat actors and goals

Identified focus areas

Evaluation

Final Recommendations

Q&A

Conclusion - Final Recommendations

5. *Implement **Unidirectional Security Gateways** to enforce read-only access to critical systems.*

Introduction

Agenda

Method

Results:

Tech/solutions identified

Functional req. and user stories

Threat actors and goals

Identified focus areas

Evaluation

Final Recommendations

Q&A

Conclusion - Final Recommendations

1. *Use a hybrid approach between perimeter-based security and Zero Trust Architecture, where they continually add security barriers based on* ***Zero Trust*** *principles. Barriers to add could be:*

    a. *Enforce system-wide continuous network monitoring in combination with machine learning-based anomaly detection. This includes support for monitoring OT-specific protocols.*

    b. *Integrate a risk- and identity-based access management architecture as described above in order to remove workload from the work permit system.*

    c. *Upgrade the existing NAC mechanism to include user/device behavior and environmental factors such as client use patterns and IP geolocation.*

2. *Use a* ***Next-Generation Firewall*** *with deep packet inspection and intrusion prevention systems at the network perimeter (Purdue level 3.5).*

3. *Add an* ***ICS firewall*** *with NGFW capabilities at the industrial perimeter (Purdue level 1.5) that can operate on OT-specific protocol messages.*

4. *Implement a* ***Sandboxing*** *solution to use with file uploads, either locally, cloud-based, or in a hybrid solution.*

5. *Implement* ***Unidirectional Security Gateways*** *to enforce read-only access to critical systems.*

Q&A

pedergrbr@gmail.com

jonsmebye@gmail.com