Canadian Nuclear Safety Commission | Commission canadienne de sûreté nucléaire

CMD 21-H4.47A

File / dossier : 6.01.07
Date: 2021-05-26
Edocs: 6572823

Supplementary Information

Renseignements supplémentaires

Presentation from Louis Bertrand

Presentation de Louis Bertrand

In the Matter of the

À l'égard de

Darlington New Nuclear Project

Projet de nouvelle centrale nucléaire de Darlington

Application to renew the nuclear power reactor site preparation licence for the Darlington New Nuclear Project

Demande de renouvellement du permis de préparation de l'emplacement d'une centrale nucléaire pour le projet de nouvelle centrale nucléaire de Darlington

Commission Public Hearing

Audience publique de la Commission

June 10-11, 2021

10-11 juin 2021

Canada

Comments on Ontario Power Generation Nuclear Power Reactor Site Preparation Licence for the Darlington Site

Louis Bertrand, P.Eng.

CNSC Hearing 2021-H-04

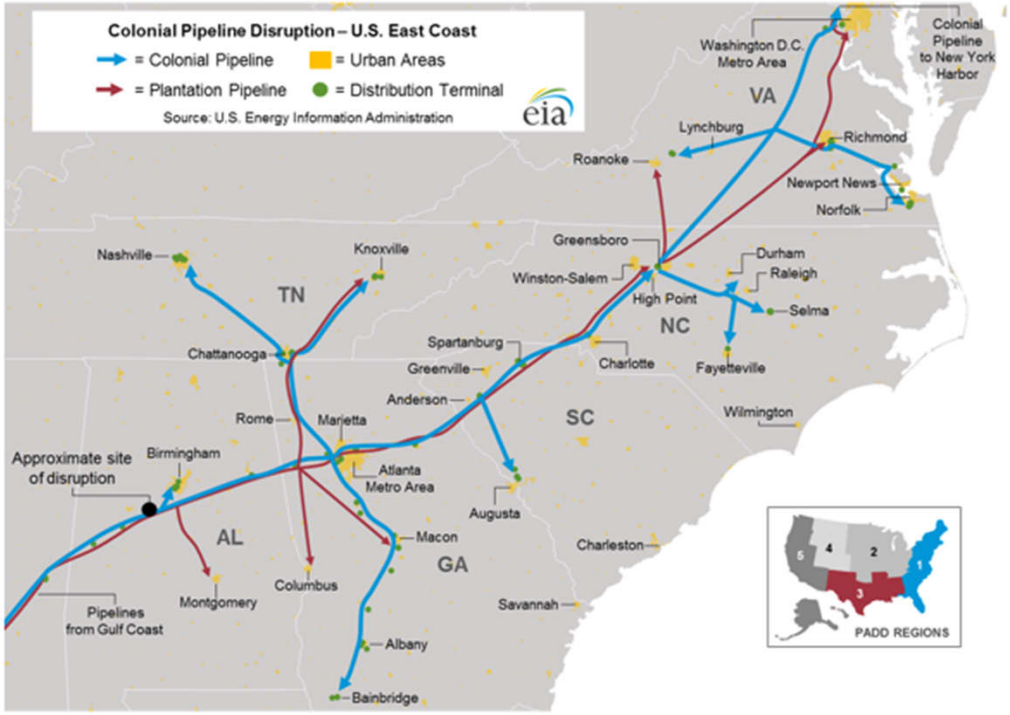
June 11, 2021

Cybersecurity & Safety: Related but distinct

- Cybersecurity of IT (software, networking) & OT (ICS) assets
  - Integrity & availability: function as intended, software & settings are intact
  - Negative proof: difficult to prove that there are no flaws, no vulnerabilities
- Safety
  - Functionality
  - Fail safe / defense in depth
  - Entire system operates as intended (not only the individual components)
  - Negative proof: difficult to prove that there are no harmful emergent system behaviours (must rely on OPEX)

Colonial Pipeline: Lessons learned

- Attack May 6, 2021; service disrupted May 7; service restored May 12
- $5M ransomware attack disrupted IT assets, not operational technology



U.S. Energy Information Administration - Colonial Pipeline Disruption U.S. East Coast

- Not directly applicable here? Pipelines span long distances, have multiple substations and physical attack points, reactors are local. <u>But</u> IT operations closely tied to OT, had to shut down operations

SolarWinds supply chain attack (2021)

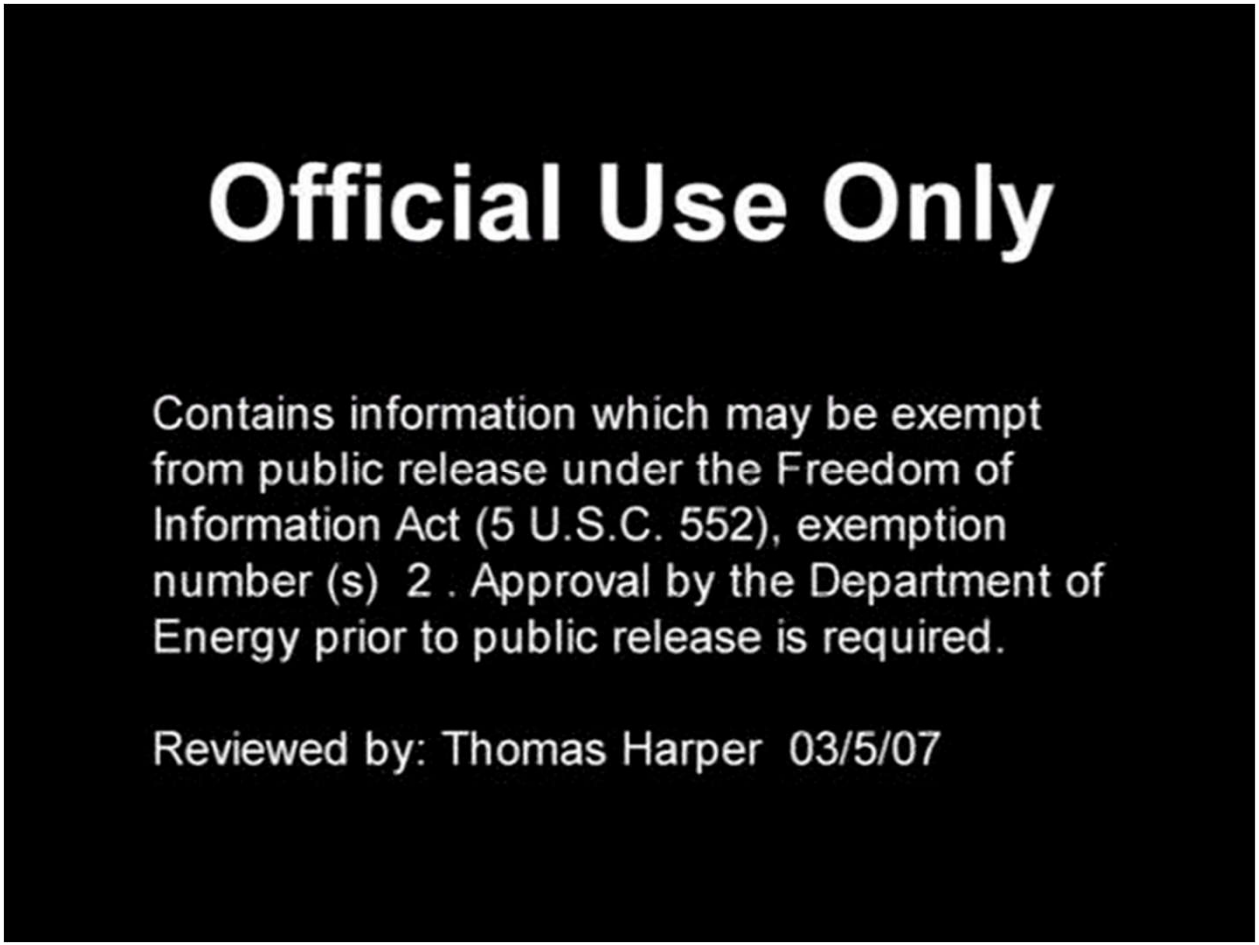
- SolarWinds Orion network monitoring platform compromised
  - Compromised component was digitally signed by vendor, downloaded by private and public sector customers
  - Discovered by FireEye after theft of security testing software tools
- Attack likely by nation state actors
  - Well resourced, highly skilled, patient
- Selective targeting: compromised component widely distributed (18,000+ customers) but selective follow-up breaches of US government agencies, research labs and cybersecurity firms

Aurora Generator Test (2007)

- DHS & INL (DoE)
  - Details released through FOI request
- Required deep knowledge of electric utility operations
- This knowledge is within reach of nation state enabled actors

Aurora Generator Test (2007)

Audio for ambient noise only, no narration.

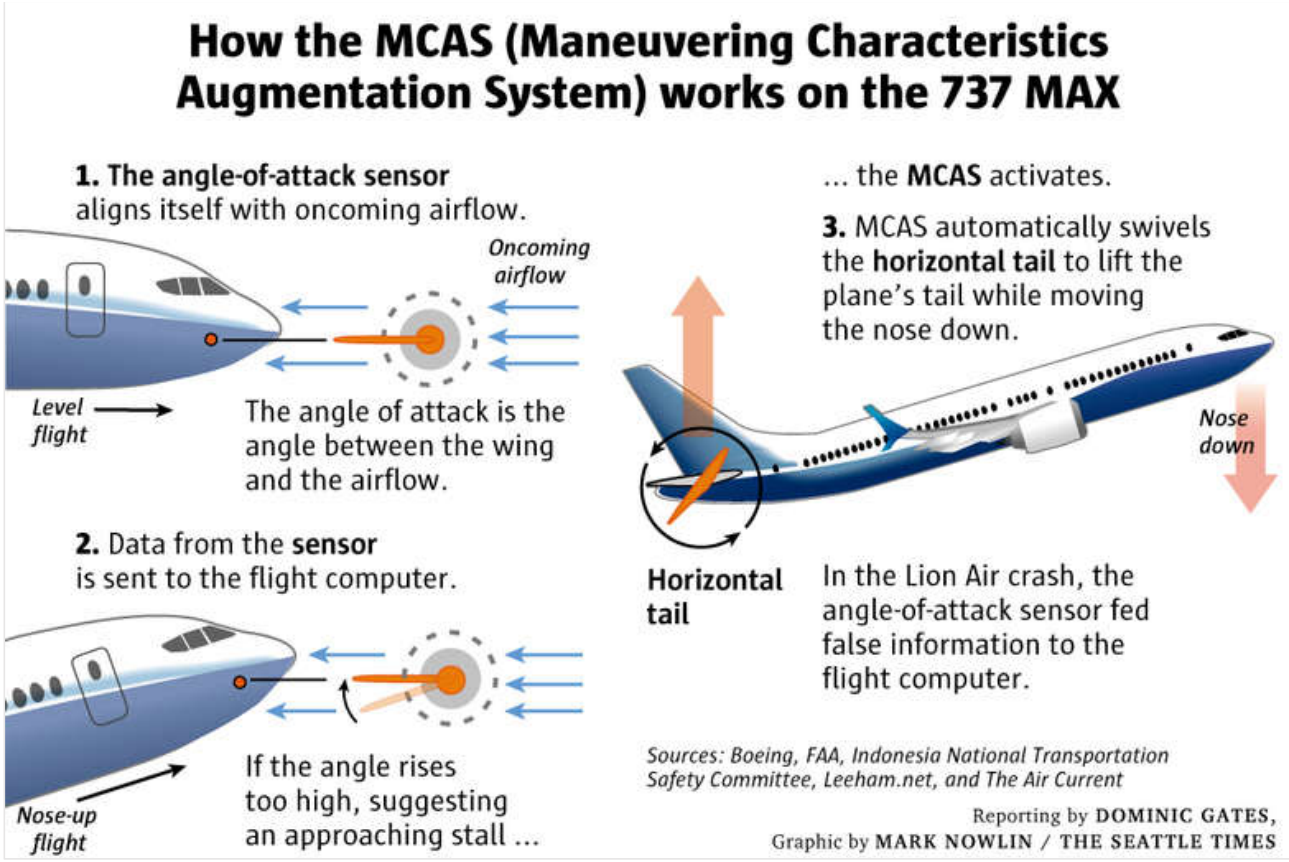


Ukraine power utilities (2015, 2016)

- December 2015 blackout of three Ukrainian power utilities
  - Small scale attack December 2016
- Multiple coordinated vectors
  - Substations shut down, remote operations disrupted
  - Backup power supplies incapacitated
  - Customer call centre DoS, flooded with nuisance calls
- Attackers were operating within networks for over 6 months, able to move within networks & identify vulnerabilities
- Political motive: erode public trust in state agencies

Boeing 737-MAX MCAS failure

- Commercial pressure and conflicting goals contributed to poor design decisions: catch up to Airbus, or ensure safety?
- Software was merely the proximate cause



OPG and SM(N)R contractor are commercial operators, subject to commercial pressures – deadlines, performance guarantees, budget…

A lot has changed since the 2009 EIS: the threats are new and very real

- Successful attackers can be
  - Sophisticated
  - Knowledgeable
  - Well resourced
  - Patient
  - Nation state actors
- Motives can be strategic
  - Eroding confidence in public institutions
  - Espionage
- Targets are more diverse
  - Supply chain
  - Operational technology
  - Device firmware
  - Portable devices
- Integration of IT and OT
  - What used to run a 4-20mA current loop or RS-422 now has an IP stack

Challenges to safety and security culture

- Commercial pressures on the SMR vendor/operator/owner are of concern for the safe operation of new nuclear power plants
- Tensions between cybersecurity and operational engineering
  - Emerging threats require prompt remediation
  - Safety culture requires careful planning and execution
  - Commercial pressure demands continuous production
- Information sharing is the *de facto* standard in information security and software development, but not in the nuclear industry
- By definition, hackers are “beyond design basis”

Hacker challenge

- Brainstorming exercise proposed by Dr. Bruce Schneier
- Goal: **Eat pancakes**
- One rule: **Don’t pay**
- There are no other rules. Go.

The Simpsons - 20th Century Fox

- Can your accident modelling pass the ”Eat Pancakes” challenge?
  - Must include malicious tampering in assessing initiating events and responses
  - Software doesn’t “break” predictably like a motor or a valve

Site preparation or new reactors?

- The application to renew the site preparation licence does not match the proponent's public statements about building an experimental small modular nuclear reactor on the site
  - The original application (2011) specifically mentioned three possible technologies: next gen CANDU or PWR (GE AP1000, Areva et al. EPR)
  - The current application doesn't mention any specific technology, therefore there is no way to understand the challenges and risks
- Clearly, what is being proposed is much more than knocking down a few trees, shoring up the shoreline and building a road

What is at stake?

Experimental reactor in a heavily populated area

- Two of the suggested reactors are dug into the ground (GE Hitachi BWRX-300 and Terrestrial Energy IMSR)
  - Did 2009 EIS discuss underground geology?
  - Impossible to inspect outer shell when buried
- Two of the suggested reactors operate at extremes of temperature and pressure (Terrestrial Energy IMSR and X-Energy XE-100)
  - Theoretically safe and workable, but in practice?
- Unknown type, level of activity and chemical composition of wastes
  - How are they to be stored? For how long?

Did we (the public) agree to this?

The licence application should be rejected

- The environmental and risk landscape studied in the 2009 EIS has changed considerably
  - Cybersecurity threats escalated
  - Software complexity increased
  - Operations rely on networking
- The site preparation licence application does not match the proponent's stated intentions
  - There is still one year left in the licence period for the proponent to present firm and detailed plans for public review
  - At most, grant a one-year extension to prepare a new application

Thank you / Merci

Questions?

Overlooking Lake Ontario from Darlington Park

https://flickr.com/photos/trance12/210933539/