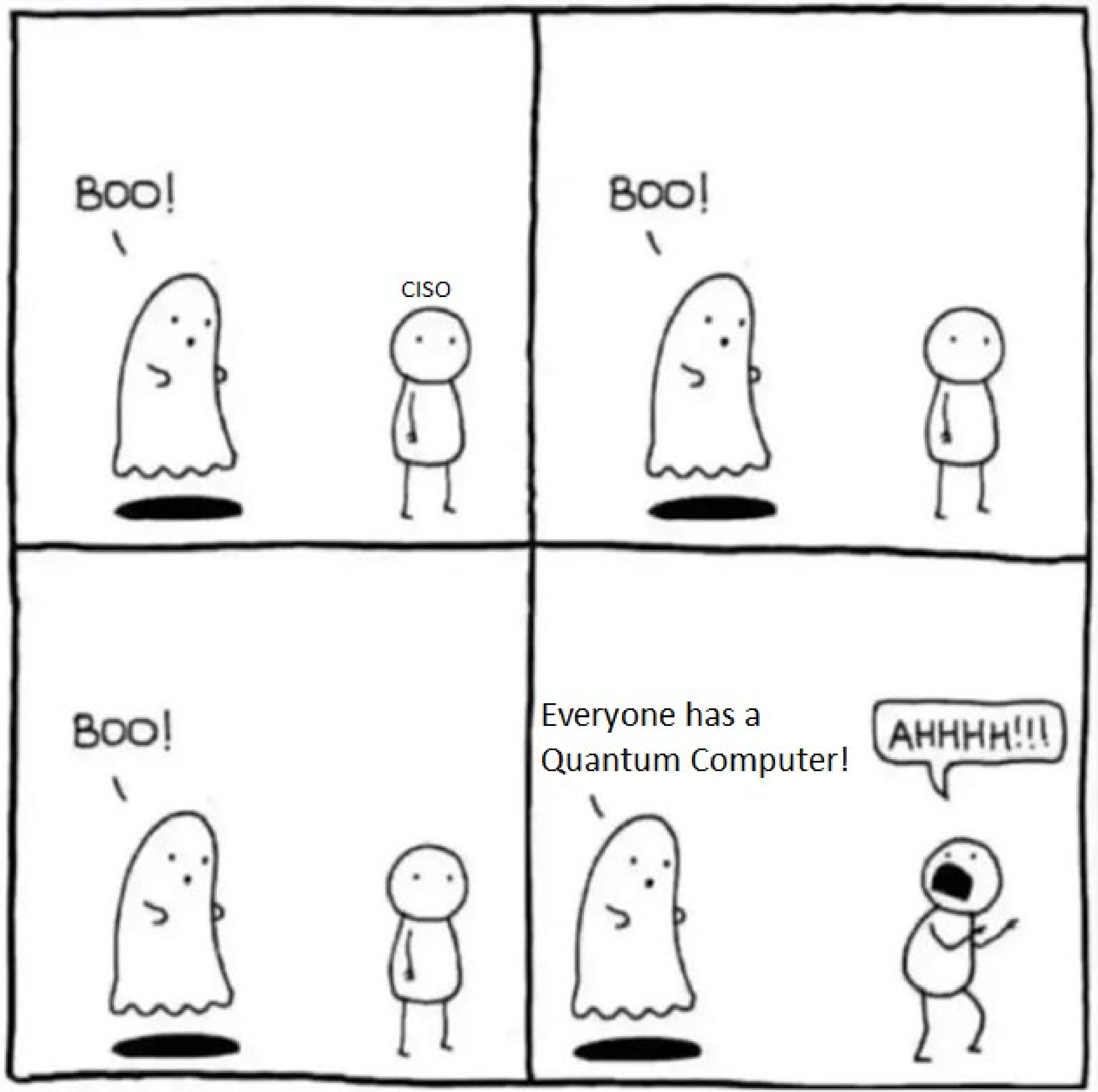
Impact of Quantum Computing on Secure Data Communication in Critical Infrastructure

Niklas Mörth, CISO

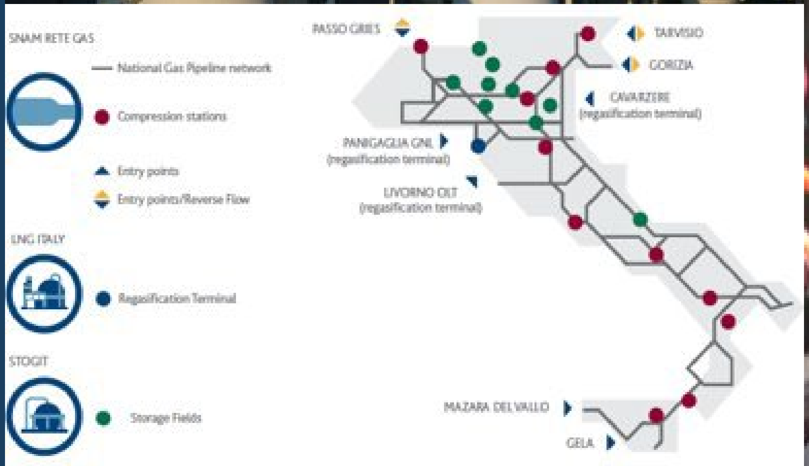
How to scare a CISO

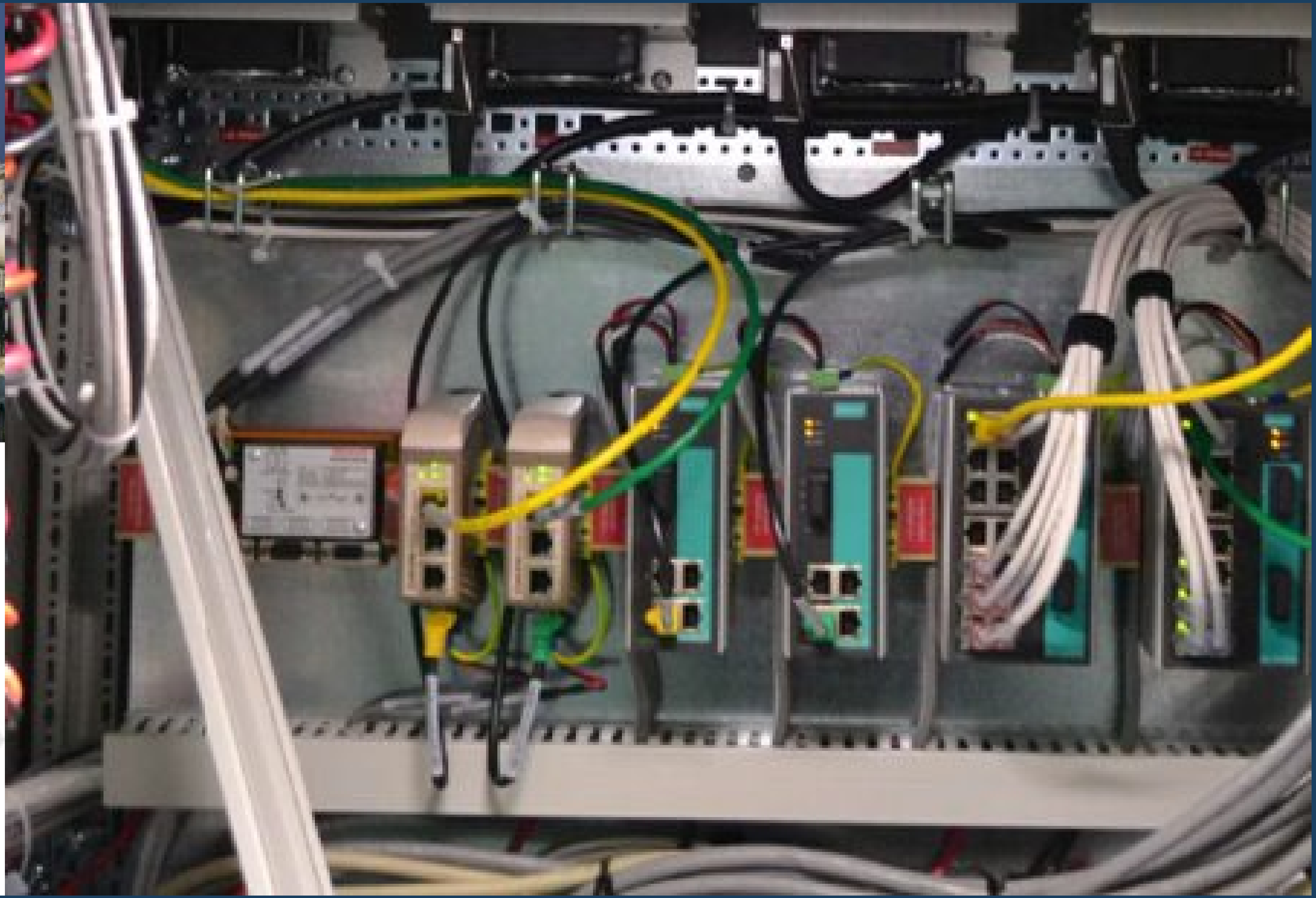


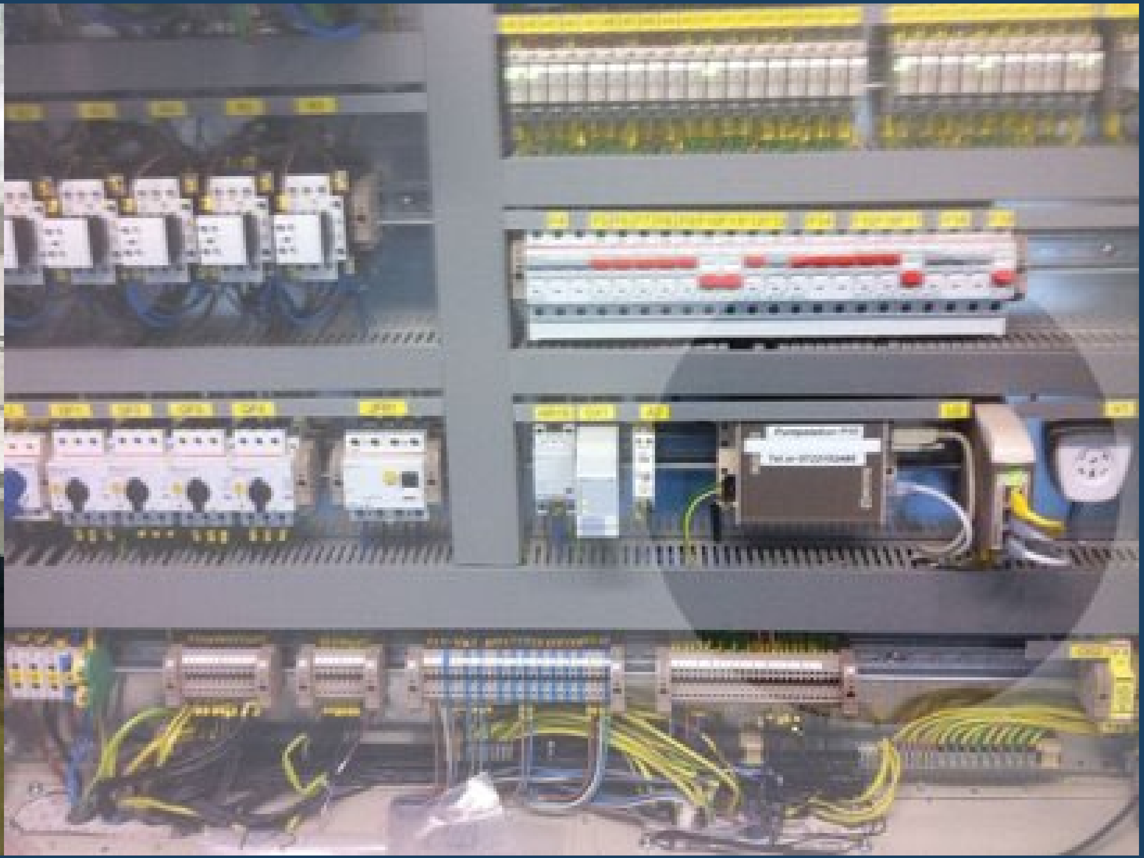
Outline

1. Critical Infrastructure
2. Quantum Computing
3. How to address the challenges

Critical Infrastructure

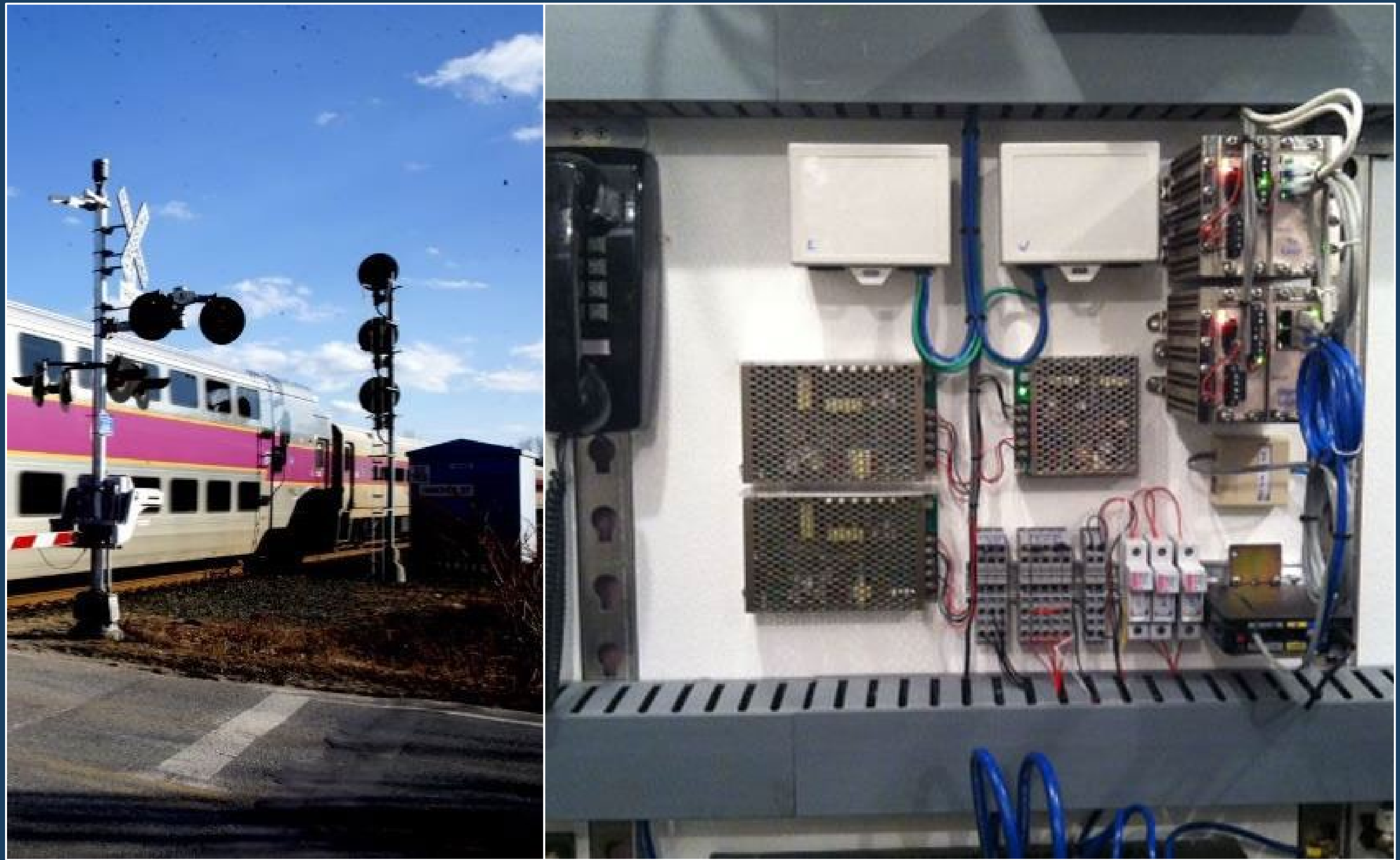

SNAM RETE GAS
National Gas Pipeline network
Compression stations
Entry points
Entry points/Reverse Flow
LNG ITALY
Regasification Terminal
STOGIT
Storage Fields
PASSO GRIES
TARVISIO
GORIZIA
CAVARZERE
(regasification terminal)
PANIGAGLIA GNL
(regasification terminal)
LIVORNO OLT
(regasification terminal)
MAZARA DEL VALLO
GELA





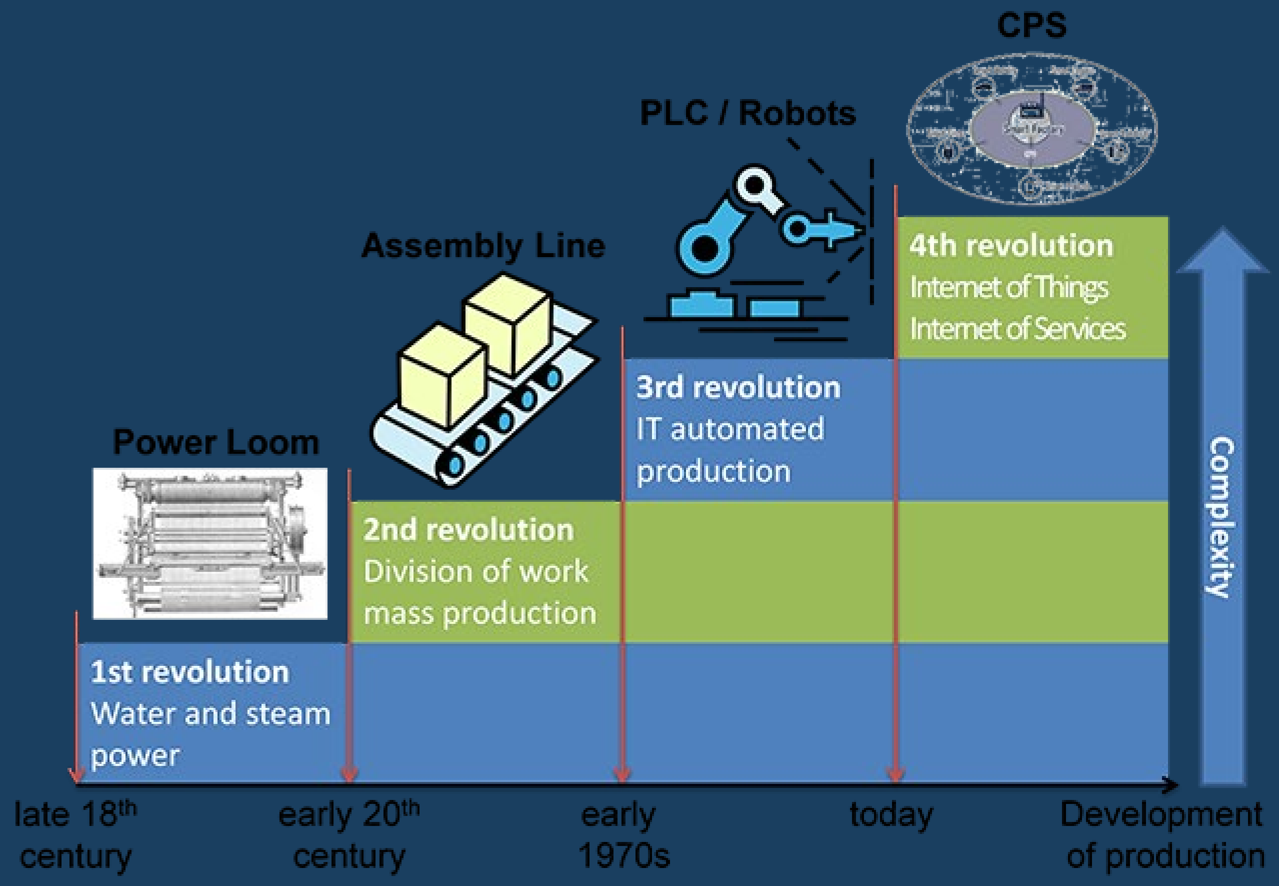
What makes them different?

- Lifetime
- Hard to access / Hard to patch
- Uptime (Availability)
- Not easily replaced



What makes them different?

- Lifetime
- Hard to access / Hard to patch
- Uptime (Availability)
- Not easily replaced

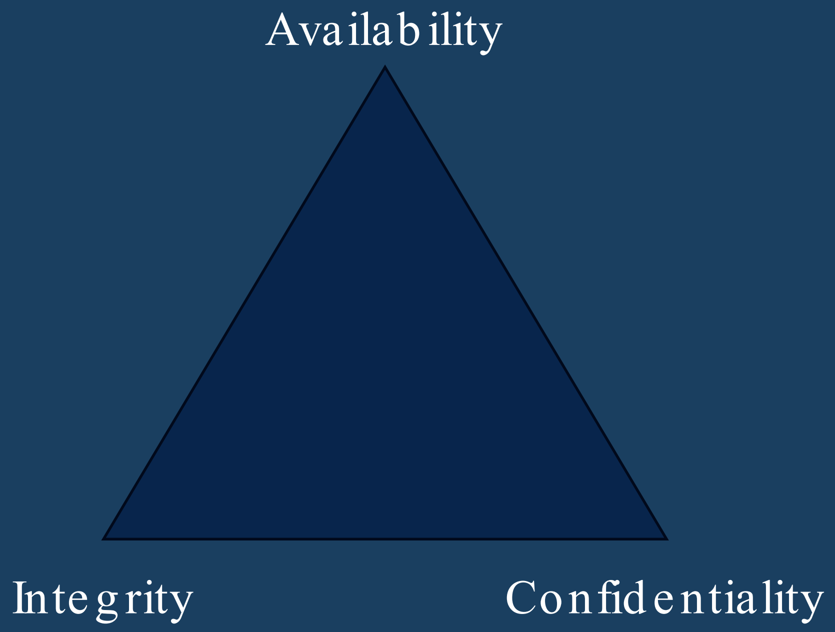


What makes them different?

- Lifetime
- Hard to access / Hard to patch
- Uptime (Availability)
- Not easily replaced

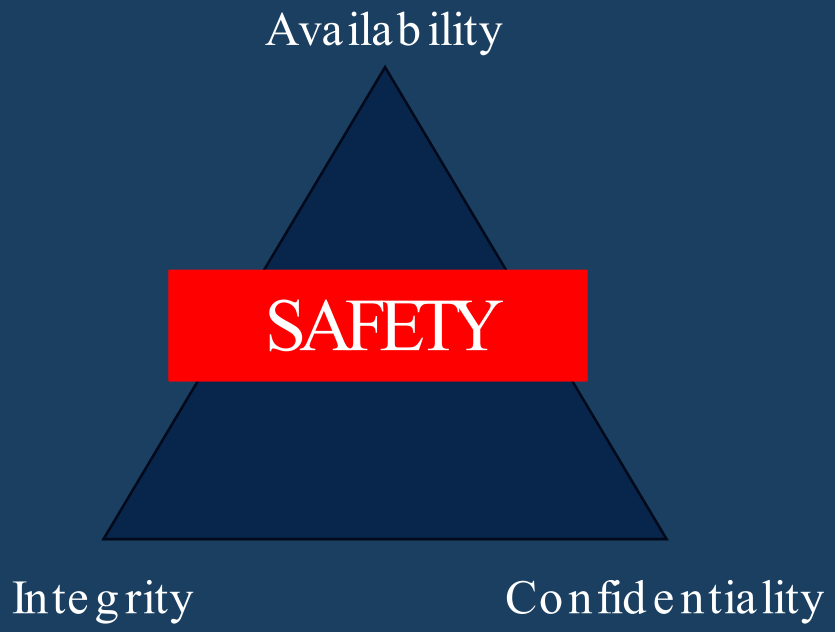
What makes them different?

- Lifetime
- Hard to access / Hard to patch
- Uptime (Availability)
- Not easily replaced



What makes them different?

- Lifetime
- Hard to access / Hard to patch
- Uptime (Availability)
- Not easily replaced



What makes them different?

- Lifetime
- Hard to access / Hard to patch
- Uptime (Availability)
- Not easily replaced

$$$

HOW'S YOUR QUANTUM COMPUTER PROTOTYPE COMING ALONG?
GREAT!
DilbertCartoonist@gmail.com
Dilbert.com
THE PROJECT EXISTS IN A SIMULTANEOUS STATE OF BEING BOTH TOTALLY SUCCESSFUL AND NOT EVEN STARTED.
4-17-12 © 2012 Scott Adams, Inc./Dist. by Universal Uclick
CAN I OBSERVE IT?
THAT'S A TRICKY QUESTION.

Quantum Computing

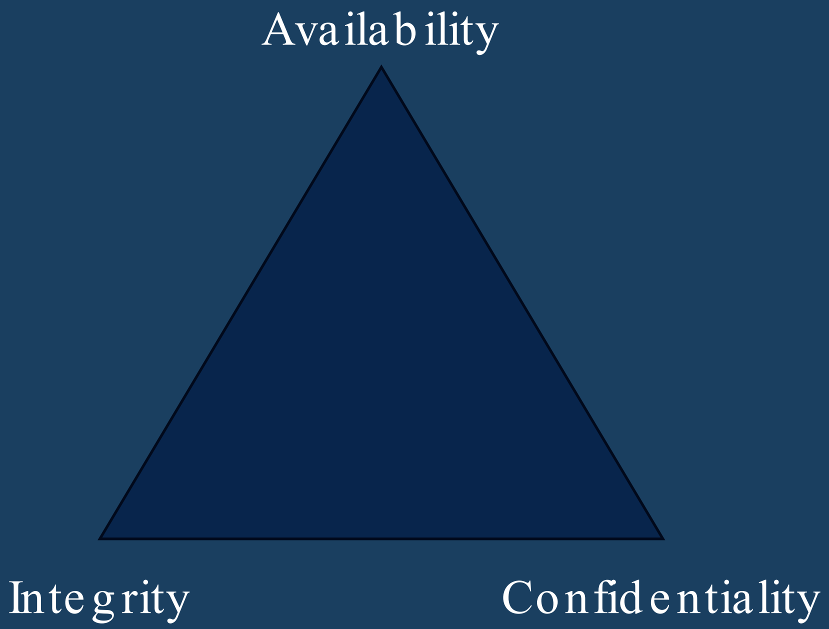
What is the fuzz about

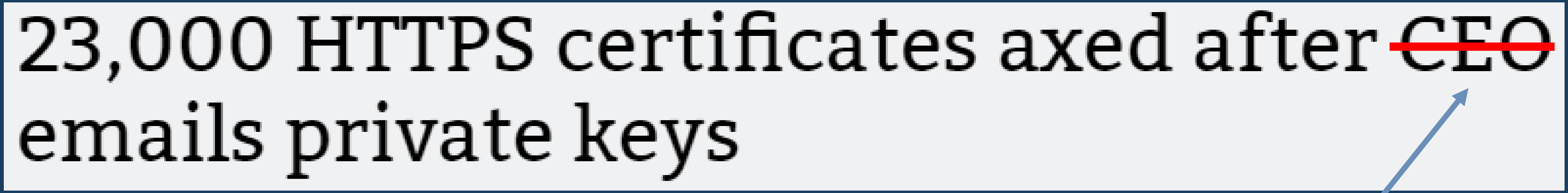
Quantum computers make hard mathematical problems easy (easier)

- But this is not about Shor's or Grover's algorithms
- Neither about NIST short list of quantum secure algorithms

- BIG threat to RSA, ECC etc..
- Some threat to Hash and symmetric algorithms
- SNDL (Store Now, Decrypt Later)

- Mainly threats to Confidentiality!





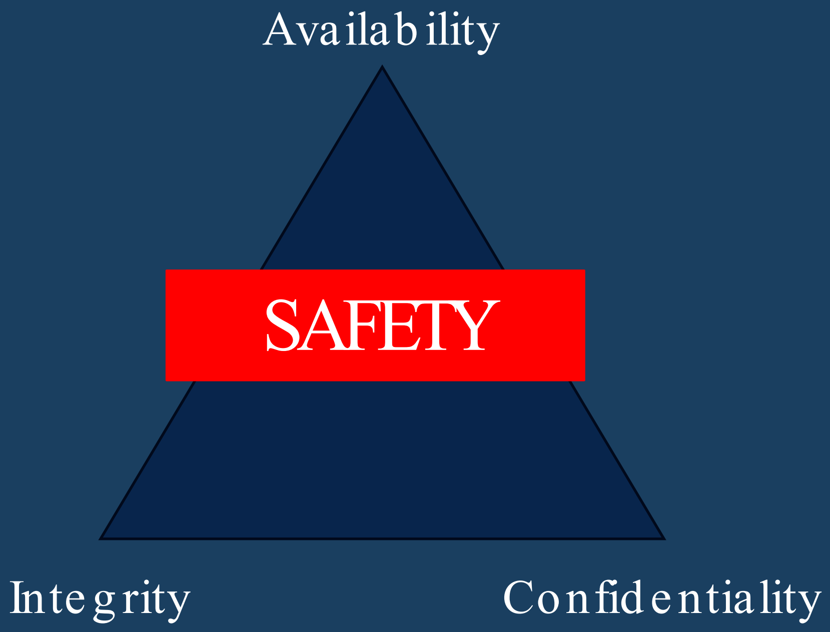
23,000 HTTPS certificates axed after ~~CEO~~ emails private keys

Quantum Computer

Threats in Critical Infrastructure

- DoS – Denial of Service
- MitM – Man in the Middle
- Topology and Config (SNDL?)

- Anywhere asymmetric cryptography is used!



Summary and The Future

What should you do?

- Gather knowledge (Especially your own assets)
- Follow what happens (NIST, etc.)
- Become Agile!

westermo

Your partner for mission critical industrial networks