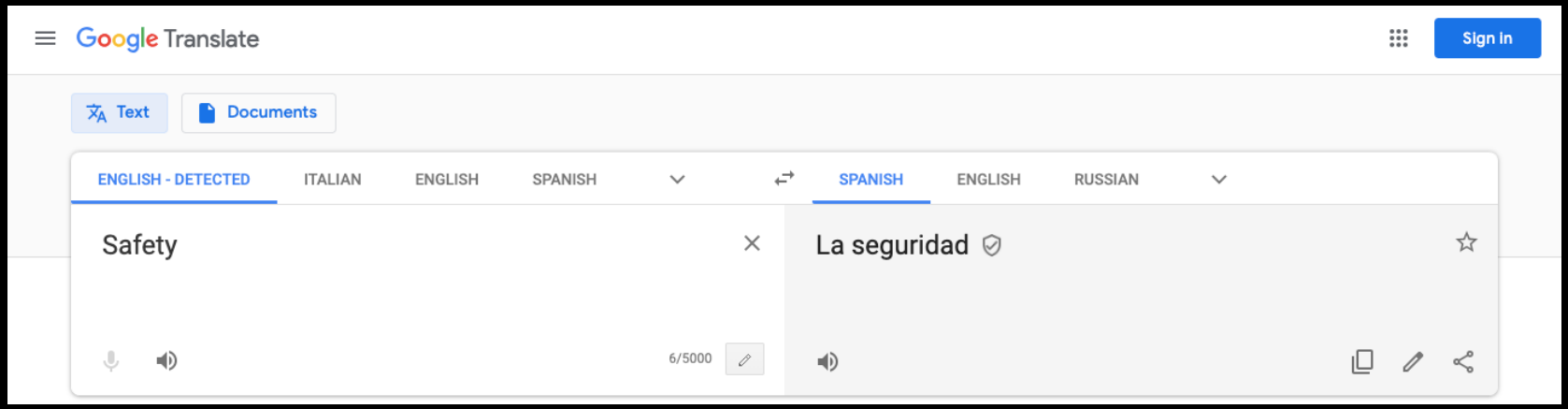

SECURITY & SAFETY
OPPOSING FORCES OR SUPPORTING PRACTICES?
RSA Conference – 2024.05.09

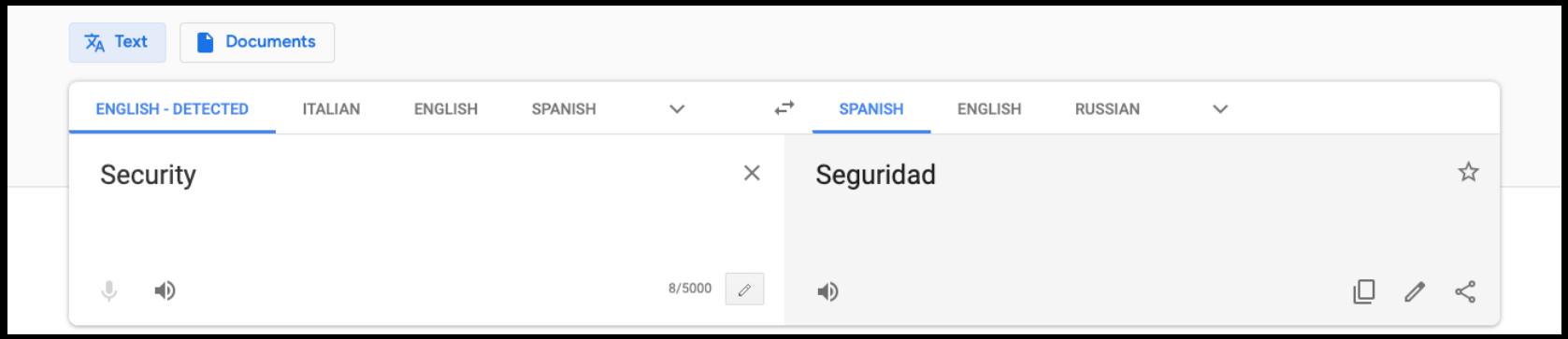
- **CEO, Ampyx Cyber – Specialized International Industrial Cybersecurity Firm (Portland, Tallinn); IICS Alliance Member**
- GCIP, CISA, CRISC, CISSP-ISSAP, SSCP, NSA-IAM, CVI, TCP, SCP
- US Coordinator and Professor, Centro de Ciberseguridad Industrial (CCI; Madrid)
- Instructor, Cyber Information Security Leader (CISL; Copenhagen)
- Former Principal Investigator, US DOE National Electric Sector Cybersecurity Organization
- EnergySec Founder, Former CEO, Director, Instructor, and President Emeritus
- Former utility staff (telecommunications, water & electric)
- Former SANS ISC456 Instructor: Essentials for NERC Critical Infrastructure Protection
- One of the original architects of NERC CIP standards for North America
- First NERC CIP auditor in the US
- NERC SCWG, SITES, and SPIDERWG contributor
- Speaker/contributor to multiple FERC Technical Committees, NOPRs and Orders
- Contributing author for DHS CISA Cross-Sector Cyber Performance Goals (CPGs)
- Contributing author for NARUC/DOE Cybersecurity Baselines for Electric Distribution
- Cybersecurity Advisory Team for State Solar, NARUC/NASEO
- National Telecommunications and Information Administration (NTIA) and Idaho National Lab (INL) Software Bill of Materials (SBOM) Energy POC Stakeholders
- DOE Solar Energy Technology Office (SETO) and National Renewable Energy Lab (NREL) Industry Advisory Board (IAB) for the Securing Solar for the Grid (S2G)
- Advisor to multiple industrial hardware and software vendors, boards of directors, government agencies around the world

AMPYX CYBER

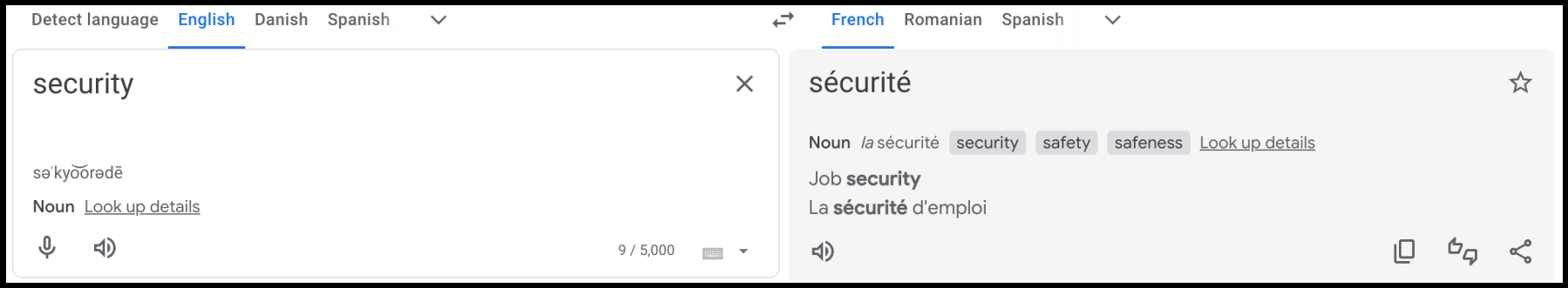
- Boutique international industrial cybersecurity firm
  - Cyber and physical security services
  - Regulation, standards, frameworks
  - Architecture, integration, orchestration
  - Program development
  - Solver of hard security/regulatory problems
- Offices:
  - Portland, USA
  - Tallinn, Estonia
- IICS Alliance member
- We keep you ahead of your adversaries – *and your auditors*

SEGURIDAD

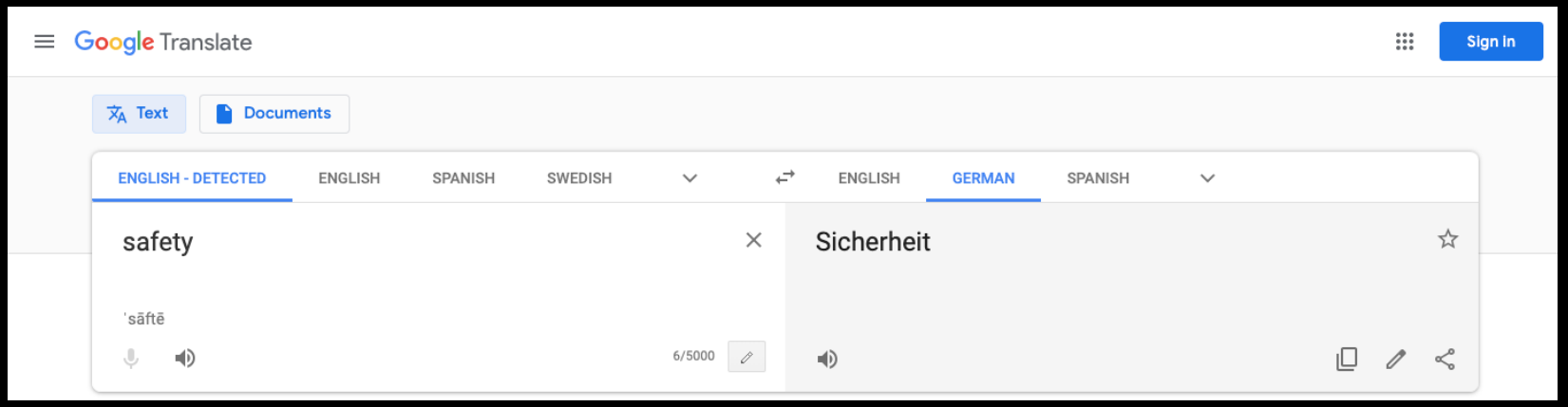

Google Translate
Sign In
Text
Documents
ENGLISH - DETECTED
ITALIAN
ENGLISH
SPANISH
SPANISH
ENGLISH
RUSSIAN
Safety
La seguridad
6/5000

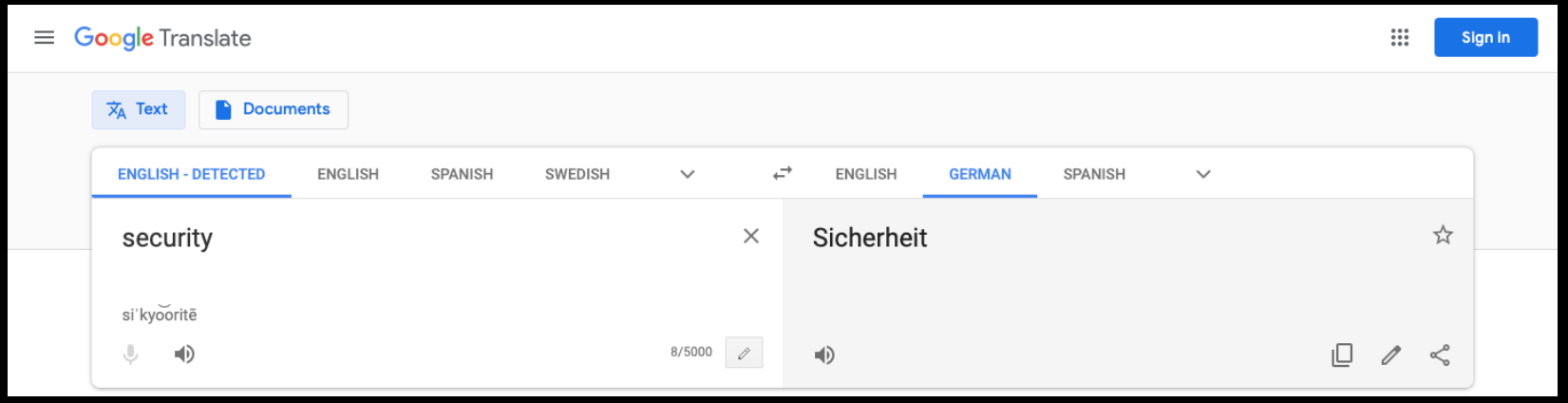

Text
Documents
ENGLISH - DETECTED
ITALIAN
ENGLISH
SPANISH
SPANISH
ENGLISH
RUSSIAN
Security
Seguridad
8/5000

SÉCURITÉ

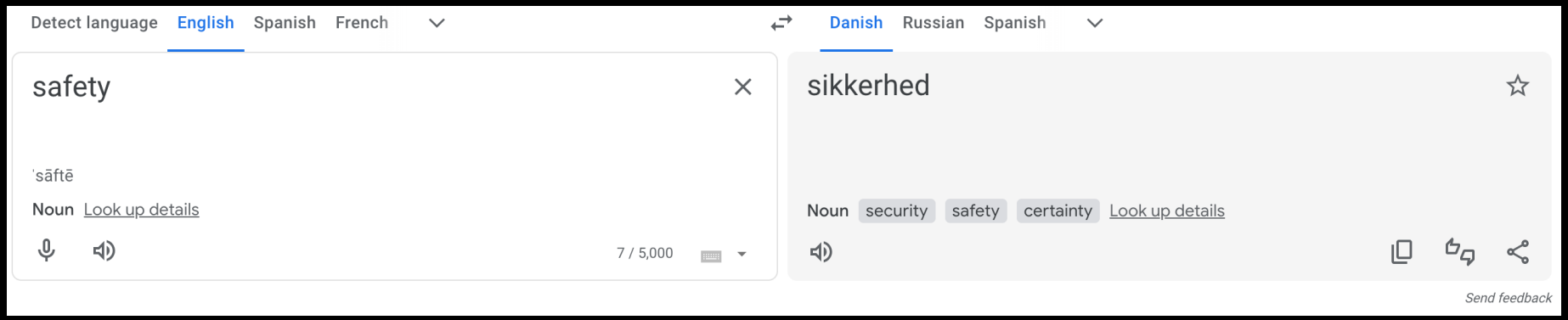

Detect language English Danish Spanish
French Romanian Spanish
security
sə'kyo͝orədē
Noun Look up details
9 / 5,000
sécurité
Noun la sécurité security safety safeness Look up details
Job security
La sécurité d'emploi
Detect language English Danish Spanish
French Romanian Spanish
safety
'sāftē
Noun Look up details
7 / 5,000
sécurité
Noun la sécurité security safety safeness Look up details
They should leave for their own safety
Ils devraient partir pour leur propre sécurité

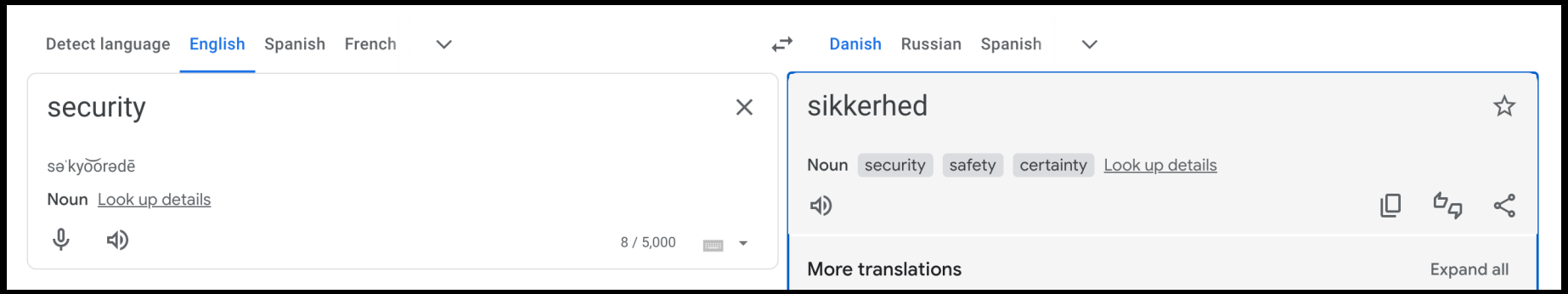
SICHERHEIT


Google Translate
Sign In
Text
Documents
ENGLISH - DETECTED
ENGLISH
SPANISH
SWEDISH
ENGLISH
GERMAN
SPANISH
safety
'sāftē
6/5000
Sicherheit

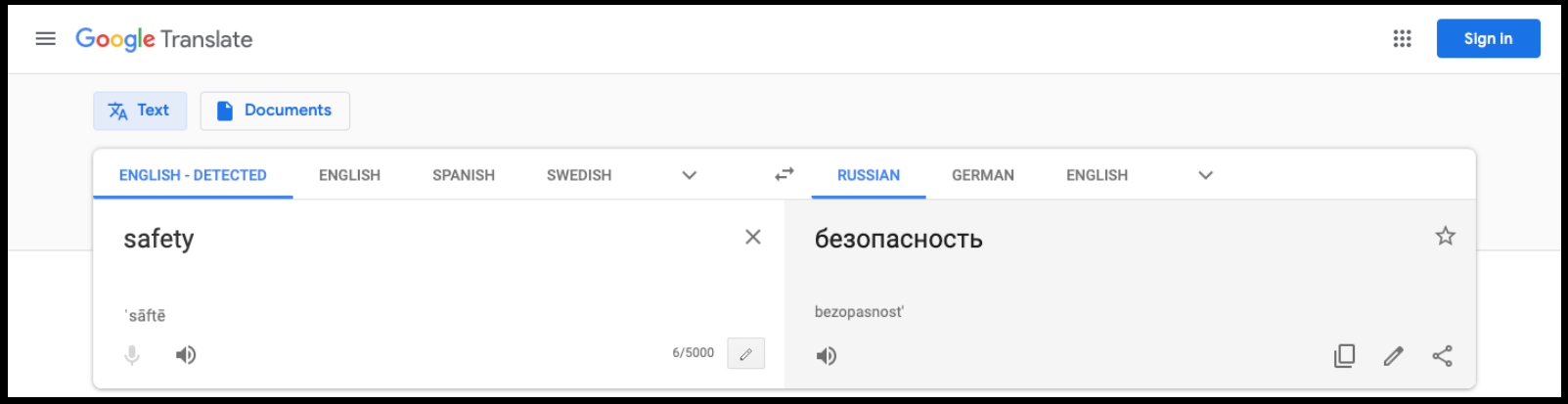

Google Translate
Sign In
Text
Documents
ENGLISH - DETECTED
ENGLISH
SPANISH
SWEDISH
ENGLISH
GERMAN
SPANISH
security
si'kyo͝oritē
8/5000
Sicherheit

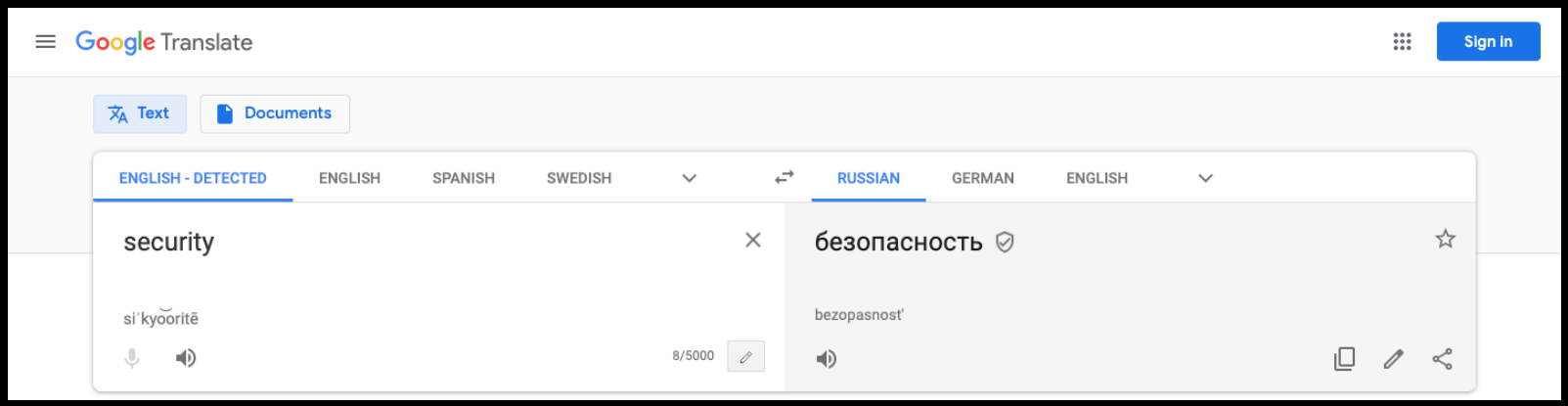
SIKKERHED


Detect language English Spanish French
Danish Russian Spanish
safety
ˈsāftē
Noun Look up details
7 / 5,000
sikkerhed
Noun security safety certainty Look up details
Send feedback


Detect language English Spanish French
Danish Russian Spanish
security
səˈkyo͝orədē
Noun Look up details
8 / 5,000
sikkerhed
Noun security safety certainty Look up details
More translations
Expand all

БЕЗОПАСНОСТЬ





contact@ampyxcyber.com | www.ampyxcyber.com | +1.503.272.1414 | @ampyxcyber

DEFINITIONS

- **Safety**: Relative freedom from danger, risk, or threat of harm, injury, or loss to personnel and/or property, whether caused deliberately or by accident. *See also security*.

- **Security**: The prevention of and protection against assault, damage, fire, fraud, invasion of privacy, theft, unlawful entry, and other such occurrences caused by deliberate action. *See also safety*.


Safety
Security

WHAT DOES AI THINK?

- Q: “What is the difference between safety and security?”

- A: “Safety is about preventing accidents and harm that might occur naturally or through carelessness, while security is about defending against deliberate threats or attacks.”

– ChatGPT4

DIFFERENCES - SIMPLIFIED

Safety

- “Accident avoidance”
- Focus on loss or damage to life or property
- Can be the result of a security failure
- Easy to use is often safer to use
- Keeping the product from affecting the environment
- Protecting people from the machines

Security

- “Crime prevention”
- Focus on availability, integrity and confidentiality
- Can escalate into a safety issue
- Easy to use is often exploitable
- Keeping the environment from affecting the product
- Protecting the machines from people

DIFFERENCES - EXAMPLES

- Safety requires emergency exits
- Must be easy to exit by anyone

- Security would prefer a wall instead of an access point
- Should be locked and only authorized personnel with access can enter or exit

BOTH ARE COMPONENTS OF RISK

Risk Management: Risk = Probability x Severity

- Probability for Safety Risk Management is a function of design – material selection, tolerances, design margin, and a function of manufacturing (things that are easily estimated)
- Probability for Security Risk Management is a function of motivation – financial gain, mayhem, and a function of opportunity, open vulnerabilities (things are not easily estimated or even known)

- Probability for Safety Risk Management largely stays the same over time, and only change as the design or manufacturing changes
- Probability for Security Risk Management can immediately change from "Low" to "Frequent" once an exploit is known/available

SAFETY VS. SECURITY

- Goals can be contradictory
  - Control system access control: group or individual?
  - System complexity: segmentation and more technology
- Does one have more importance than the other?
  - Can take over security interface to disable safety measures
  - Point-to-point connection for safety exploited through security vulnerability to cause harm
- Security must be functional to support safety
- Security is the process for ensuring or enabling safety
- Balancing both should be the objective, but this can be very difficult to achieve

TECHNOLOGY PATH

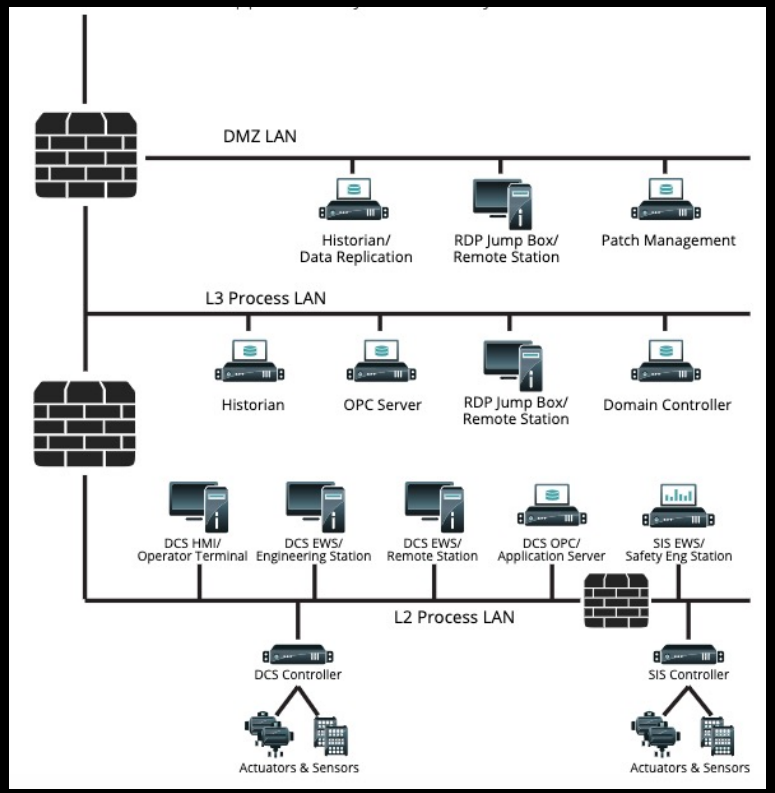
- Safety and security technologies are increasing in use
- Most future technologies will be digital and connected
  - Cyber Informed Engineering (CIE)

- Digital systems bring new risks
  - More attack surface area
  - Access and availability
  - Data integrity: sensor, aggregator, annunciator/alarming
  - Data storage, reconnaissance and inference

EXAMPLE: TRITON/TRISIS

SEPARATION VS. ISOLATION

- Logical separation of security systems and safety systems is required – *if not already isolated physically (air gapped)*
- Safety and security manual/physical processes still matter
  - Cyber Informed Engineering (CIE)



SAFETY AWARENESS

- Everyone knows that safety is everyone's job
- How many days since last incident?
- How many hours of required training to perform job?
- Safety marking, paint, signs, posters, tailboard sessions
- "Safety minute"
- Culture of reporting and improvement
- KPI(s) for management
- Can reflect poorly on insurance, stock, etc.

SECURITY AWARENESS

- Emails that everyone ignores
- Intranet messages that everyone ignores
- Videos that everyone ignores
- Phishing tests that everyone fails
- Training that everyone hates and puts off until last minute
- KPI(s) that are meaningless (especially to the board)
- Culture of ”do not talk” about security incidents
- Can reflect poorly on insurance, stock, etc. (but it depends…)

BORROW WHAT WORKS

- Separation and isolation are not optional
- Highly restricted access and very strong controls
- Use same/similar approach for security awareness that is used for safety awareness
- Use operational content and messaging staff will recognize and understand (identify with)
- Foster culture of reporting and transparency
- Develop meaningful metrics and drive continuous improvement
- Consider Cyber Informed Engineering (CIE)
- Give both the same degree of visibility and responsibility at executive level

IT'S ALL RISK MANAGEMENT

- What is your risk tolerance for safety?
- What is your risk tolerance for security?
- Are they different? Why?
- Measure, message and manage both programs similarly


CAUTION
THIS MACHINE
HAS NO BRAIN
USE YOUR OWN


DANGER
DO NOT TOUCH
Not only will this kill you,
it will hurt the whole time
you're dying.


SAFETY FIRST
PLEASE KEEP YOUR LEGS &
ARMS INSIDE THE CAR
UNTIL THE CAR STOPS.
LIMBS ARE DIFFICULT TO REPLACE

CONTACT ME

Patrick C. Miller – CEO, Ampyx Cyber

- Email pmiller@ampyxcyber.com
- LinkedIn https://www.linkedin.com/in/millerpatrickc/
- Mastodon @patrickcmiller@infosec.exchange
- Threads, BlueSky, Twitter @patrickcmiller
- Phone +15032721414