
BRIDGES TO TOMORROW
ENGINEERING, CYBERSECURITY, AND A FUTURE WORKFORCE
Denver University Bridges to Tomorrow – 2024.02.20

INTRODUCTION

- Business Owner
- Consultant
- Instructor
- Public speaker
- Community builder
- Explorer

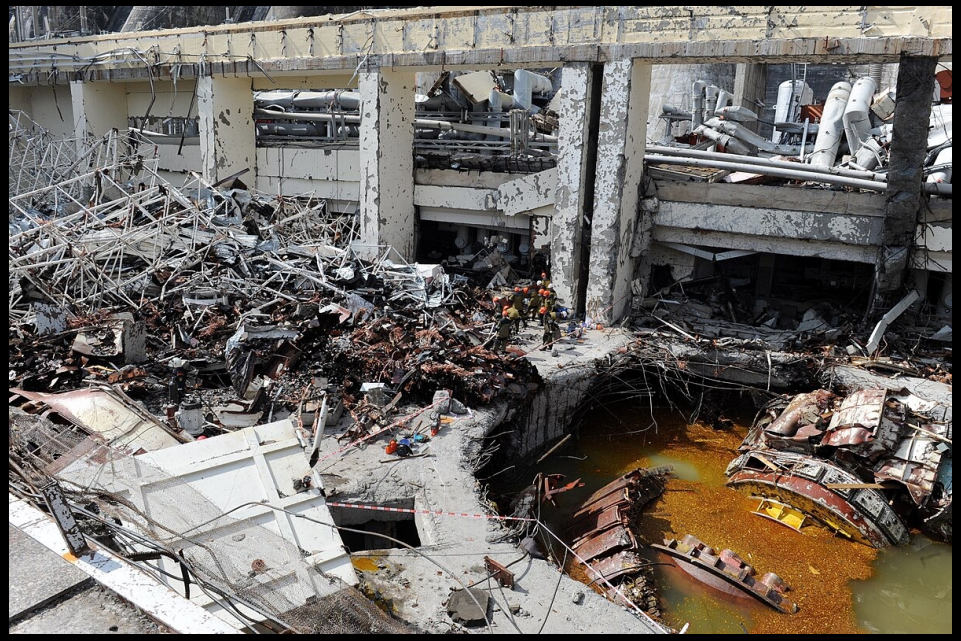
- GCIP, CISA, CRISC, CISSP-ISSAP, SSCP, NSA-IAM, CVI, TCP, SCP
- US Coordinator, Centro de Ciberseguridad Industrial (CCI)
- Former Principal Investigator, US DOE National Electric Sector Cybersecurity Organization
- EnergySec Founder, Former CEO, Director, Instructor, and President Emeritus
- Former SANS ISC456 Instructor: Essentials for NERC Critical Infrastructure Protection
- Instructor, Cyber Information Security Leader (CISL), CSA CPH
- Former utility staff (telecommunications, water & electric)
- One of the original architects of NERC CIP standards for North America
- First NERC CIP auditor in the US
- NERC CTAG, 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)
- 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

A DAY IN THE LIFE

FOUNDATION

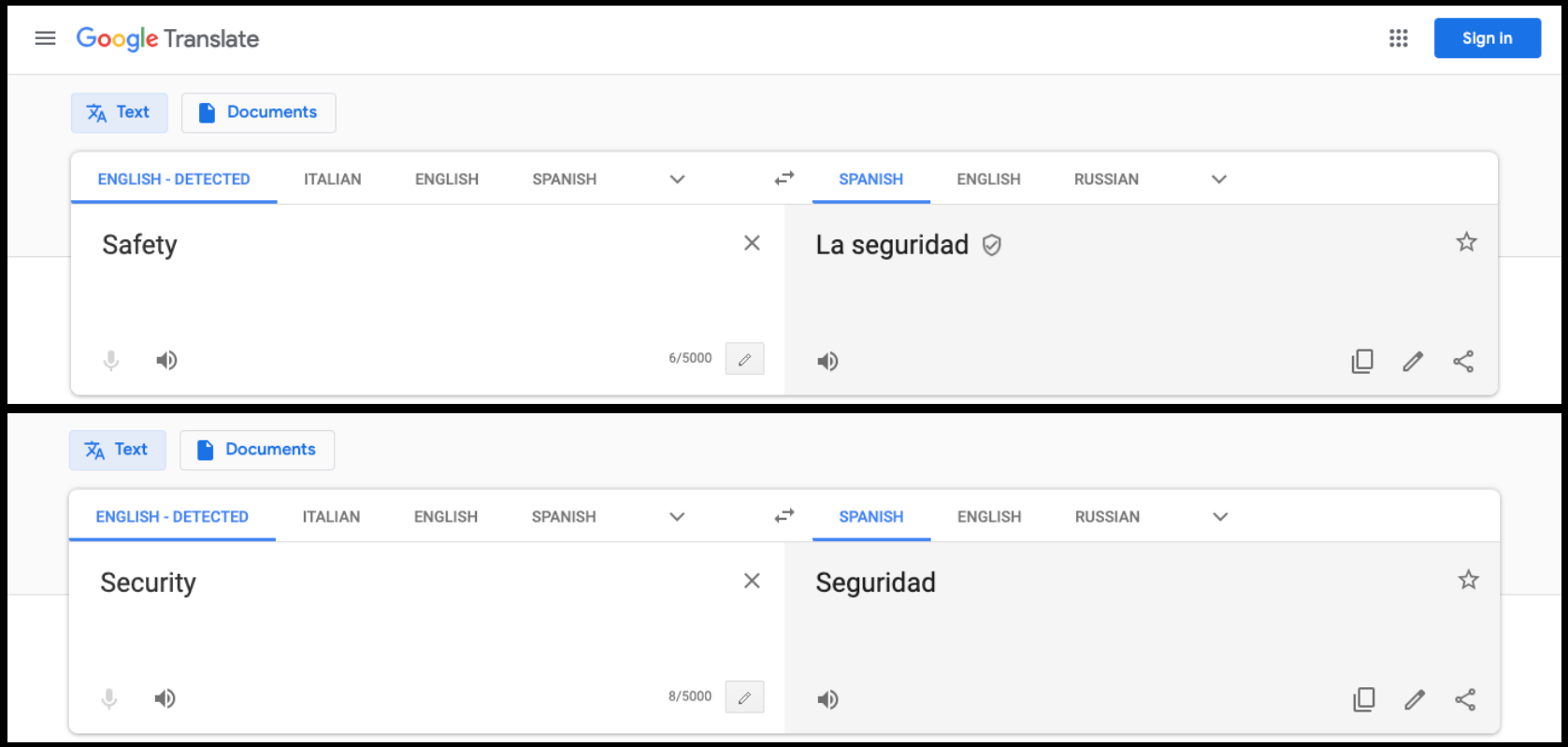
- …derived from the Latin *ingenium*, meaning "cleverness" and *ingeniare*, meaning "to contrive, devise."
- …practice of using natural science, mathematics, and the engineering design process to solve technical problems, increase efficiency and productivity, and improve systems.
- …practical way for human society to change, modify and improve the physical world around us so that humans can have a better life.
- …design or build machines, engines, or electrical equipment, or things such as roads, railroads, or bridges, using scientific principles.
- …*someone who makes things work*.

DAYS SINCE LAST ACCIDENT

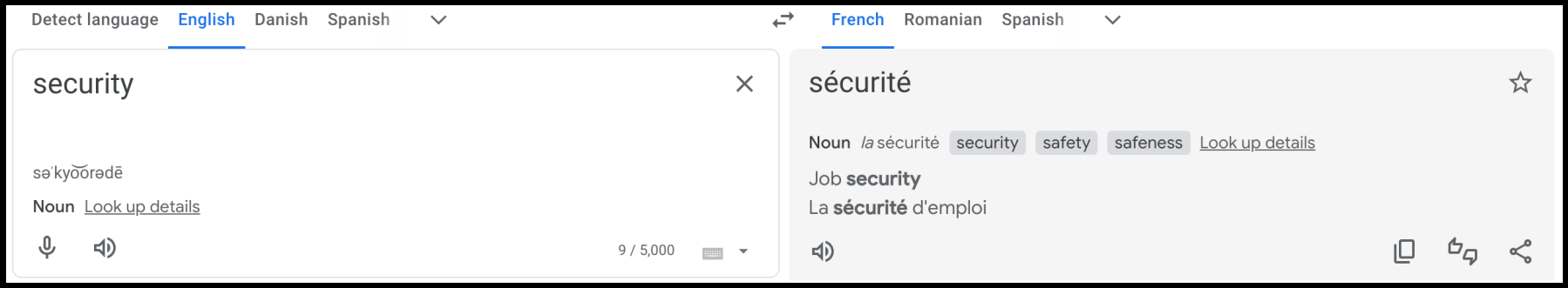



Safety
Security

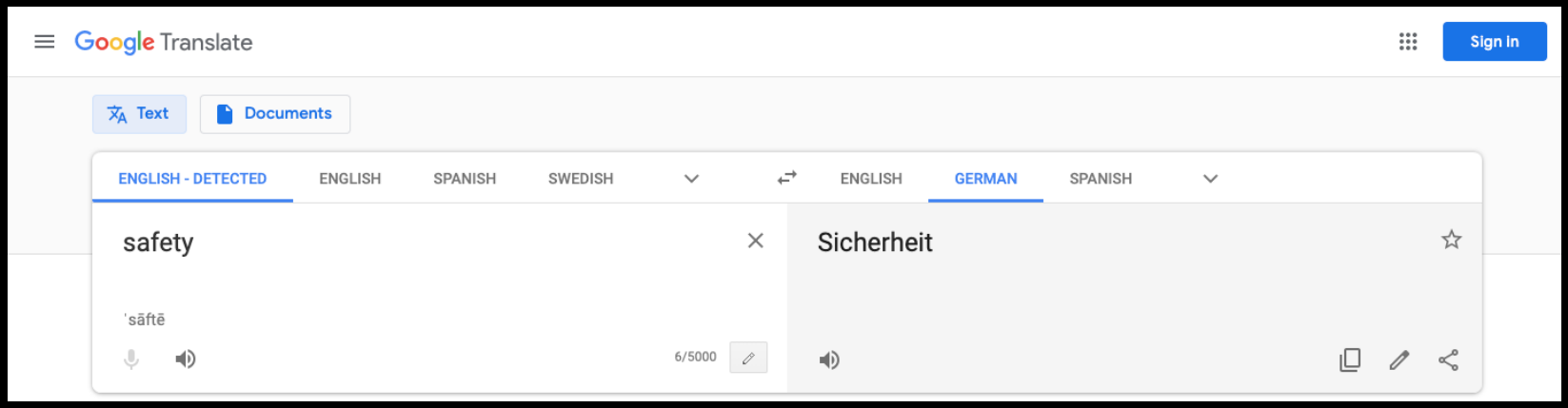
SEGURIDAD

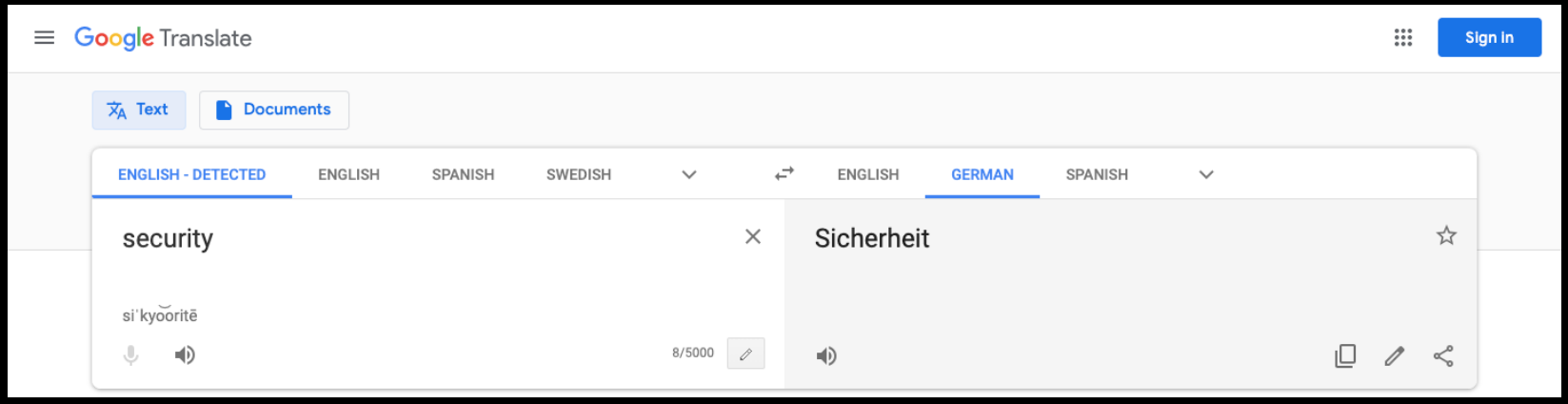

Google Translate
Sign In
Text
Documents
ENGLISH - DETECTED
ITALIAN
ENGLISH
SPANISH
SPANISH
ENGLISH
RUSSIAN
Safety
La seguridad
6/5000
Text
Documents
ENGLISH - DETECTED
ITALIAN
ENGLISH
SPANISH
SPANISH
ENGLISH
RUSSIAN
Security
Seguridad
8/5000

SÉCURITÉ

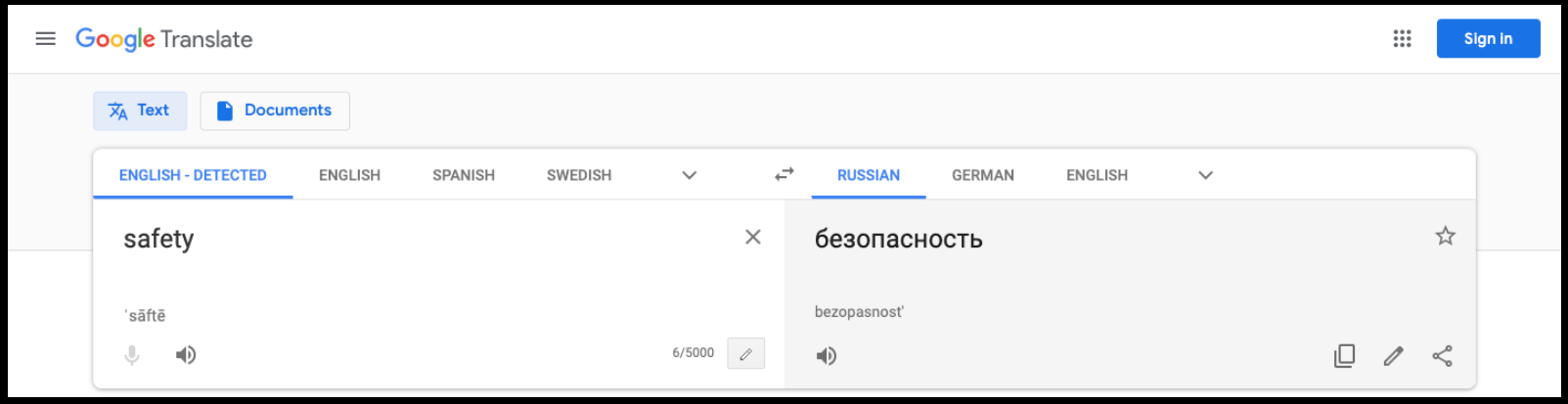

Detect language English Danish Spanish
French Romanian Spanish
security
sə'kyo͝orədē
Noun Look up details
9 / 5,000
sécurité
Noun la sécurité security safety safeness Look up details
Job security
La sécurité d'emploi
Detect language English Danish Spanish
French Romanian Spanish
safety
'sāftē
Noun Look 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

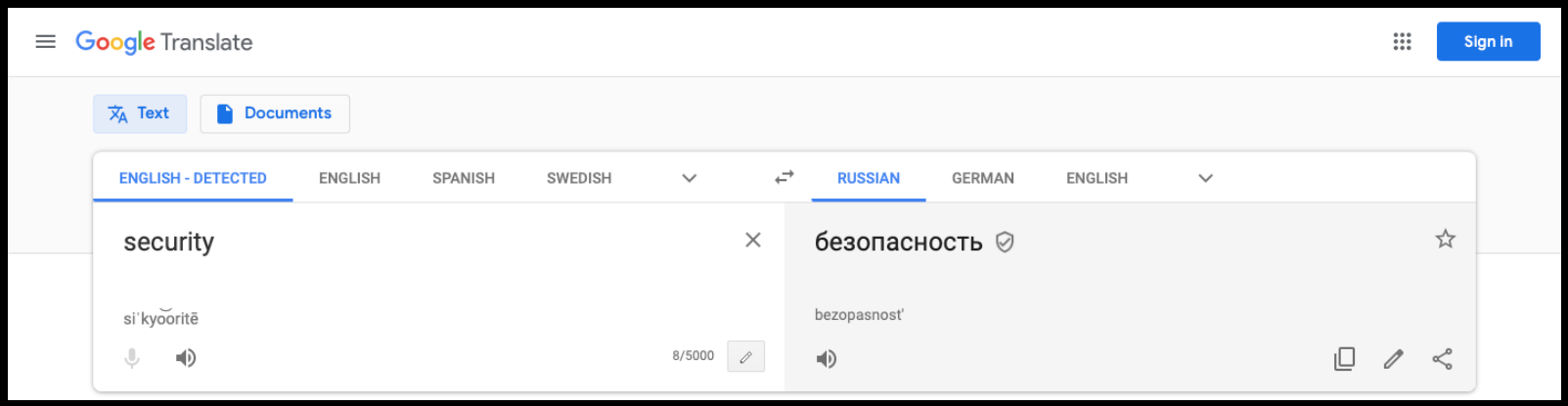
SICHERHEIT


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

БЕЗОПАСНОСТЬ





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*.

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

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

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 is very difficult to achieve

ENGINEERING VS. SECURITY

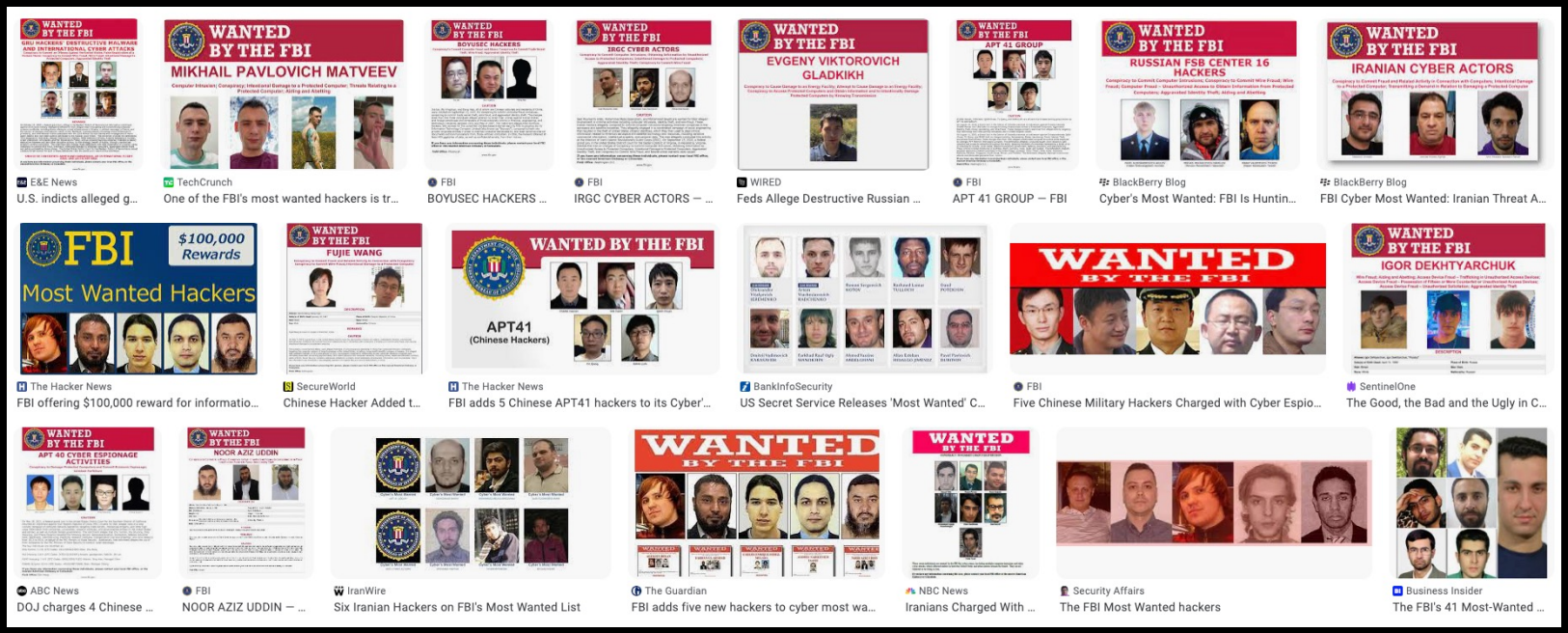
Engineering

- Focuses on designing, building, and maintaining physical systems
- Applies principles from physics, mathematics, and material science
- Concerned with functionality, efficiency, and safety of structures and machines
- Involves problem-solving to meet human needs
- Tangible, physical outcomes

OT/ICS Security

- Prioritizes system availability and physical safety over integrity and confidentiality
- Involves understanding threats specific to industrial environments and processes
- Deep integration with engineering disciplines to understand operational context and potential impacts
- Resilience and rapid recovery to maintain critical operations and minimize downtime

ENGINEERING VS. SECURITY



"Mother nature may be harsh, but she's not malicious…"

ENGINEERING VS. ENGINEERING

- Terminology & jargon
- Project focus & perspectives
- Professional identity
- Problem solving approach
- Scale and precision
- Regulatory & safety standards
- Technology adoption & innovation
- Interdisciplinary projects
- Resource allocation & budgeting
- Regional & geographic
- Demographics
- Language
- Understanding & respecting different expertise

ENGINEERING AND ENGINEERING

The importance of interdisciplinary collaboration

- Better, more holistic project outcomes
- Innovation comes from intersections
- Clear, jargon-free communication, without judgement
- Balance project priorities
- Minimize resource competition; look for opportunities
- Use project management techniques with this focus
- Take the opportunity to learn from other discipline
- Use collaborative technologies

ENGINEERING AND ENGINEERING

- Interdisciplinary collaboration can present challenges
- Creates unique opportunities for innovation and improvement

- SEEK
  - Effective communication
  - Mutual respect
  - Focus on shared goals

ENGINEERING AND SECURITY

- Engineering and security have merged in an approach called Cyber-Informed Engineering (CIE)
- Extends the “secure by design” principle
- Introduces cybersecurity considerations at the earliest stages of system design, long before the incorporation of software and security controls
- Secure the system using the physics and mechanics of engineering controls—not just digital monitoring and controls

ENGINEERING AND SECURITY

- Engineers make some of the best OT/ICS cybersecurity professionals
- Very dynamic environment
- Rewarding sense of purpose and fulfillment
- Higher degree of diversity
- High demand, often with rapid advancement
- High pay scales

SUMMARY

- Interdisciplinary and diverse engineering teams can make the best teams and achieve the most innovative outcomes
- This doesn't come easy, but it is worth it
- Enhancing interdisciplinary and diverse engineering knowledge with security can provide an even better result

RESOURCES

- Cyber-Informed Engineering (CIE) - https://inl.gov/cie/
- CISA ICS/OT security training - https://www.cisa.gov/resources-tools/training/ics-virtual-learning-portal
- Getting started in OT security - https://www.amperesec.com/podcast/breaking-into-ot-security

OPEN QUESTIONS

Patrick C. Miller – CEO, Ampere Industrial Security

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