SUL ROSS
THE FRONTIER UNIVERSITY of Texas

Midstream Critical Manufacturing Industry Cybersecurity Hub

Oguzhan Basibuyuk (Technical contact) (Tentative)

Eric Funasaki (Business Contact)

Sul Ross State University

September …, 2024

DE-CR0000037 Project Kickoff Meeting

FAR FROM ORDINARY.

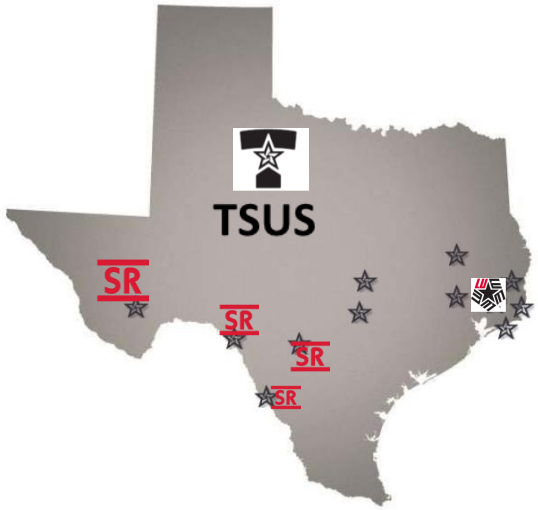
MEMBER THE TEXAS STATE UNIVERSITY SYSTEM™

YOUR Moment IS HERE

Project Contributors

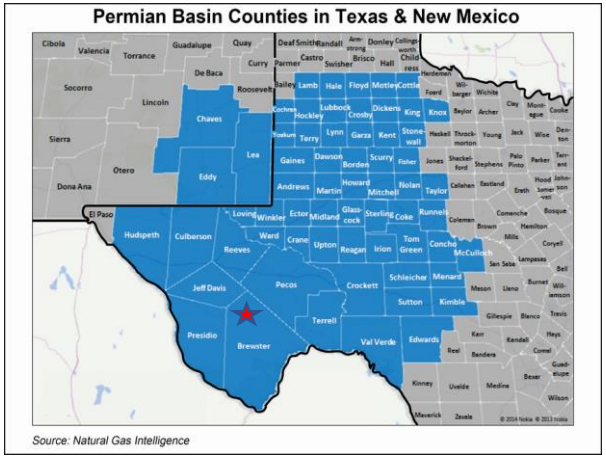
SUL ROSS
THE FRONTIER UNIVERSITY of Texas

- Est. 1917, located in Alpine, TX
- Branch campuses, branded as Rio Grande College, are located in Del Rio, Uvalde, and Eagle Pass
- 30 undergraduate, 24 master's and 1 doctoral academic program
- As of Fall 2024, the total enrolment is more than 2500 students
- SRSU is a Hispanic Serving Institution
- MS Homeland Security program was ranked as one of the top online graduate programs in 2022 and 2023



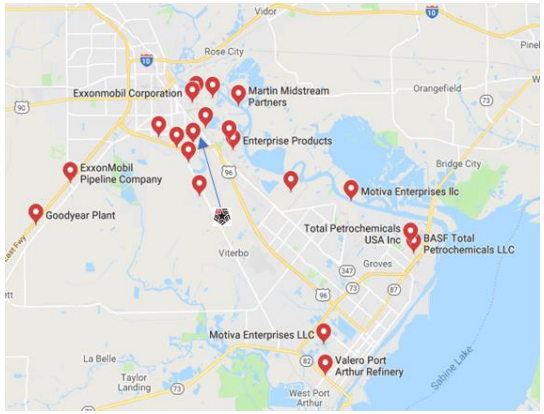
- Est. 1923; Located in Beaumont, TX.
- 76 undergraduate, 54 masters and 5 doctoral academic programs
- Home to more than 17,000 students; 48% first generation
- Emerging Hispanic Serving Institution
- A leader in online learning with offerings across the curriculum

Energy Companies in the Permian Basin and Southeast Texas Regions



- The Permian Basin is one of the oldest and most well-known hydrocarbon-producing areas.
- Almost 10% of the TX Statewide pipelines are in the region
- 21% of the TX Midstream Gas Plants are in the region
- Permian Basin represents over half of the all active rigs in the US (52%) *
- It is estimated to make up 50% of US oil production by 2030 **
- I-10, I-20 Interstate access

* https://rigcount.bakerhughes.com/na-rig-count
** https://permianpartnership.org/power-of-the-permian/



- 75 refineries and petrochemical facilities within 20-mile radius
- 4th largest US port by tonnage
- Nation's largest LNG hub
- Three Class-I railways
- Vast pipeline network
- Interstate access
- 85 miles east of Houston
- Part of the greater TX energy infrastructures that produce 1/3 of the Nation's transportation fuel and support 3.1 million jobs

Expected Impacts of Collaboration

- Location: The Universities are located in the regions where the Nation's major energy companies are operating
- Broader audience, more visibility and broad impact of the research
- Expertise, resource, and knowledge sharing
- Interdisciplinary research opportunity
- Operational capacity: Part of the same state university system (TSUS)

Who Does What

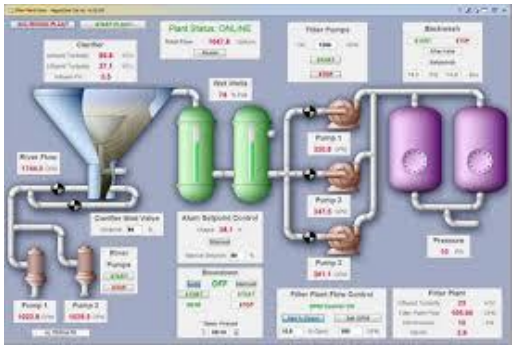
SUL ROSS
THE FRONTIER UNIVERSITY of Texas

Most of the project tasks will be performed by both universities.

- Establishing a Center of Excellence (SRSU-LU)
- Building research facilities (SRSU-LU)
- Setting up virtual and physical testbed (LU)
- Identifying cyber forensics needs (SRSU)
- Developing threat detection and response techniques for midstream industry (LU)
- Developing new course modules for undergraduate and graduate level courses (SRSU-LU)
- Developing training materials and provide training for cyber crime scene investigation and incidence response (SRSU)
- Developing training materials and provide training on industrial cybersecurity to prepare the workforce for the midstream industry (LU)
- Developing training materials and provide training to the general public, including K-12 audience(SRSU-LU)
- Evaluation, dissemination research outcomes (SRSU-LU)

Operational Technology (OT)

- OT refers to programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). Examples include Industrial Control Systems (ICS) such as :
  - Supervisory control and data acquisition systems (SCADA)
  - Distributed control systems (DCS)
  - Programmable Logic Controllers (PLC)
  - Safety Instrumented Systems (SIS)
  - Human Machine Interfaces (HMIs)
  - Sensors
- The main objective of OT technology is managing and controlling physical devices which are typically involved in the production or delivery of goods and service such as sources of energy.



Information Technology (IT)

- It refers to any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, transmission, or reception of data or information by the industry. Examples include servers, computers, software applications, databases, and other resources used for communication, data and information storage, and/or analysis.
- The main objective of IT technology is connectivity and commination of the systems for data acquisition, storage, and analysis

Current Trends/Threats: Integration of IT and OT Systems in Industry

- Traditionally, information technology (IT) and operational technology (OT) environments were designed to operate independently. OT systems were air-gapped and used closed, proprietary systems with no or very limited internet connections

- New industry conditions pushed for a new system of IT/OT integrations.

- Although the convergence of IT and OT systems have created more efficient environment and better decision making capabilities by connecting between these two previously disparate environments, it created new cybersecurity vulnerabilities.

Major Challenges

- OT and IT systems were not intended to be connected. IT systems were designed for data, OT systems were for controlling physical devices (sensors, valves etc.)
- Outdated hardware and software issues on OT systems.
- Lack of visibility for inventory and common vulnerability testing methodologies.
- Lack of experienced and skilled manpower in OT IOT technology and cybersecurity.
- Lack of cybersecurity awareness among OT operating staff.
- Structural problems such as poor network segmentation.

The Cybercrime Picture

- **According to several surveys* , Ransomware attacks impacting OT environments are on the rise and remain costly.**
- **In 2023, 69% of targeted organizations paid the ransom, over half of the organizations that paid the ransom suffered financial ramifications of $100,000 USD or more.**
- **In the new threat environment cyber attacks not only target the IT system but also OT systems together.**
- **Generative AI is on the rise and causing security concerns.**

- **https://web-assets.claroty.com/claroty-industrial-survey-report-dec-2023.pdf**
- https://www.fortinet.com/content/dam/fortinet/assets/reports/report-state-ot-cybersecurity.pdf

Impacts of IT/OT Cybersecurity

- Safety
  - Personal safety
  - Process safety
  - Product safety
- Environmental
- Financial
- Lost of revenue
- National Security

Recent Cyber Attacks on Critical Industrial Facilities

- The Bowman Avenue Dam (2013)
- NotPetya (2017)
- Triton (2017)
- EDP (2020)
- NTPC (2020)
- LookBack Attack (2020)
- Colonial Pipeline (2021)
- Florida Oldsmar Water Plant (2021)
- Aliquippa Water Authority (2024)
- Rising geopolitical tensions and financial opportunity continue to spur actors to target industrial environments – including hacktivists, nation-state actors and criminal gangs.

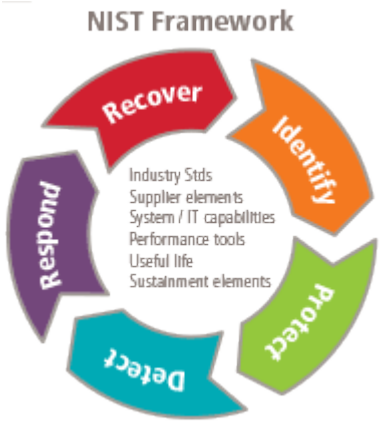
Project Objectives

- Build cybersecurity and cyber-forensics capabilities in the TSUS.
- Develop threat detection and response techniques for ICS (Industrial Control Systems) and CPS (Cyber-Physical Systems) using machine learning and data analytics.
- Create formal and continuing education materials in cybersecurity, computer science, and pipeline operations.
- Develop a specialized workforce for midstream cybersecurity.
- Disseminate results to enhance cybersecurity awareness.

Features

- Integrated research, education, and outreach activities

- Project team expertise:
  - Cybersecurity
  - Cybercrime Investigation
  - Digital Forensics
  - Engineering, Process Safety
  - Data analytics



Tasks

SOPO Task/ Subtask Title
Project Management and Planning
Developing the center's infrastructure, resources, and capabilities
Knowledge creation and research
Education
Training
Dissemination

Activities

- ***Research***: Case studies on cyberattacks and development of simulations.
- ***Education and Outreach***: Curriculum development, training workshops, and symposia for midstream professionals and the general public.
- ***Training***: Development of materials for industrial and K-12 audiences.

Research Approach

- Identify cyber forensics needs for the midstream industry.
- Develop threat detection and response strategies using machine learning.
- Create knowledge through simulation testbeds of ICS and CPS systems.

Educational Development & Educational Innovation

- Develop new course modules in cybersecurity, computer science, and engineering.
- Collaborate across disciplines to implement new programs.
- Conduct annual assessments of educational outcomes.

Workforce Training & Development

- Train professionals in cybersecurity and cyber-forensics.
- Engage with K-12 audiences to promote cybersecurity awareness.
- Provide cyber crime scene investigation training.

Dissemination and Outreach Strategy

- Host annual symposiums, workshops, and seminars.
- Publish newsletters, e-pamphlets, and research articles in peer-reviewed journals.
- Develop and maintain a public website for cybersecurity resources and materials.

Key Deliverables

- Two testbeds for cybersecurity research, education, and training
- Four case studies of representative, diverse cyber risks
- Four case studies to identify the needs and create knowledge in cyber forensics for the midstream industry.
- Education: 500 students, 150 k-12 students
- Training: 150 professionals or people seeking career change
- 1 online learning hub, 6 newsletters
- 2 symposiums, 6 seminars/workshops
- One special session in a national conference for two years
- One informal education event to K-12 students per year
- Multiple journal publications and conference presentations

Related Units

SRSU

Department of Homeland Security and Criminal Justice

Department of Computer, Mathematical, and Physical Sciences

Office of Information Technologies

LAMAR University

College of Engineering

Department of Computer Science

Southeast Texas Regional Center of Texas Manufacturing Assistance Center (TMAC)

Key Personnel

Eric Funasaki
SRSU Dean of Research & Sponsored Programs

Helen Lou
LAMAR Chemical Engineering

Ismail Gunes
SRSU Department of HS/CJ

Oguzhan Basibuyuk
SRSU Department of HS/CJ

SUL ROSS
THE FRONTIER UNIVERSITY of Texas

THANK YOU FOR YOUR ATTENTION

QUESTIONS ?