Université Grenoble Alpes

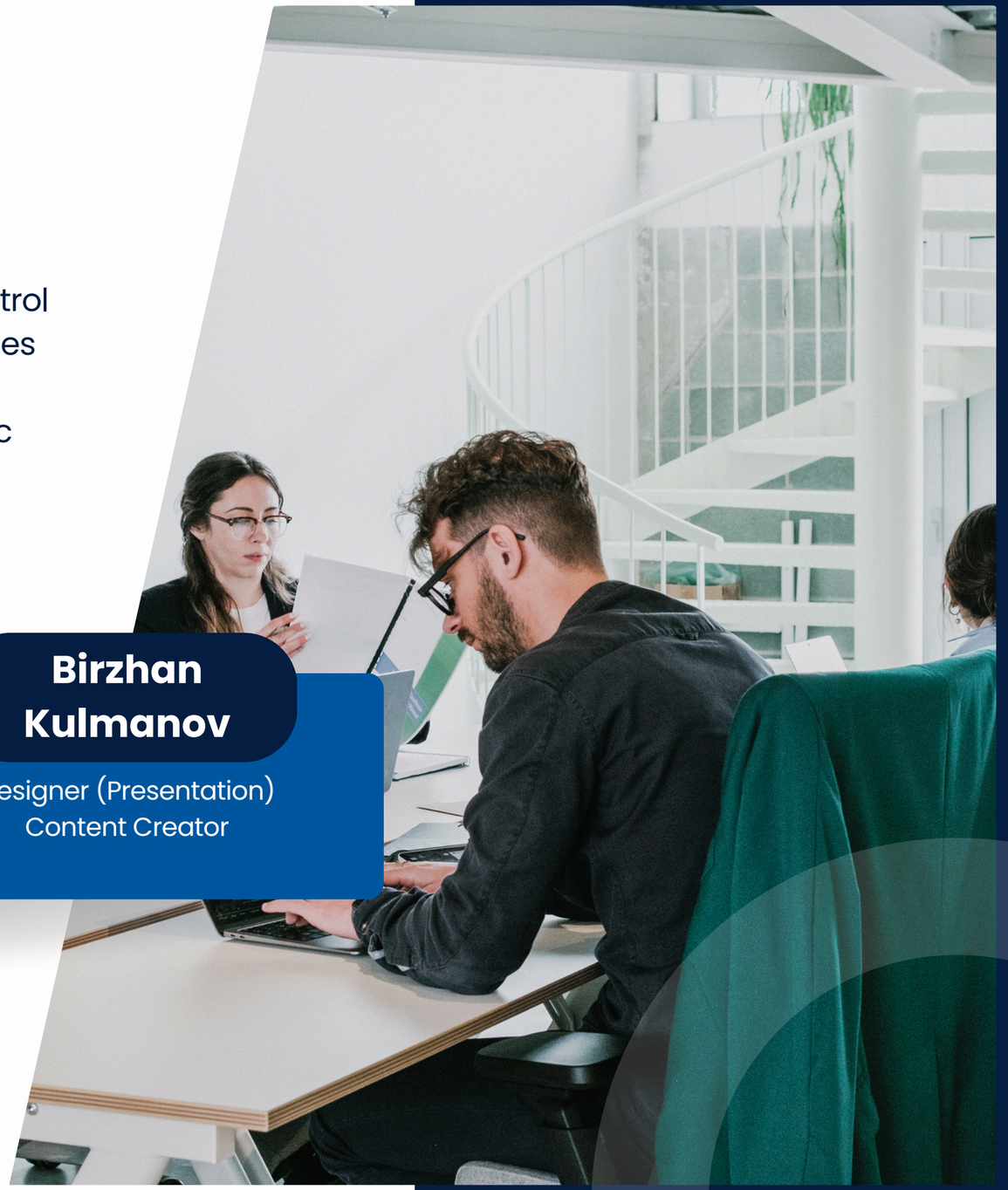
Risk Assessment ICS Cyber Threats

Instructor: Thiriet Jean Marc

Students: Birzhan Kulmanov
Umar Farooq
Bilal Sleiman

Application

ICS (Industrial Control Systems), including SCADA (Supervisory Control and Data Acquisition) systems, are the backbone of critical industries like energy, manufacturing, oil and gas, and water treatment. Any disruption to these systems can have widespread and catastrophic consequences for national security, economic stability, and public safety.



Bilal Sleiman

Leader of the group
Content Creator

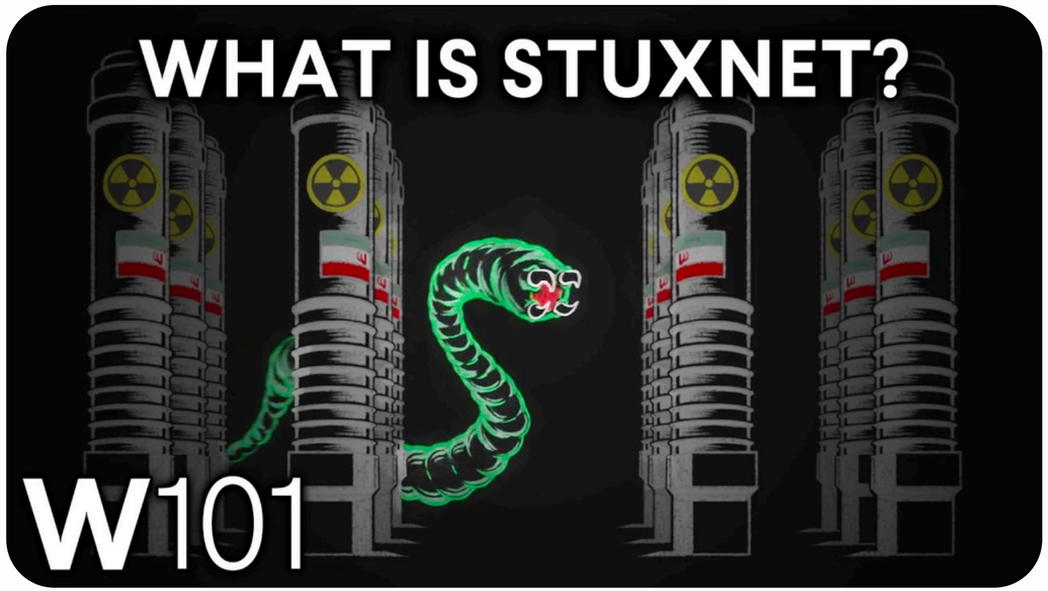
Umar Farooq

Rapporter
Content Creator

Birzhan Kulmanov

Designer (Presentation)
Content Creator

Case Studies: ICS Cyber Threats



Stuxnet Attack (2010)

The Stuxnet attack (2010) targeted Iran's nuclear facilities, specifically its SCADA systems, causing physical damage to uranium centrifuges by manipulating their speeds. It spread via USB and exploited zero-day vulnerabilities, destroying around 1,000 centrifuges and delaying Iran's nuclear program. It was the first known cyberattack to cause physical damage to industrial infrastructure.

Ukraine Power Grid Attack (2015)

The Ukraine power grid cyberattack (2015) targeted SCADA systems of energy companies, causing power outages for 230,000 people. Hackers gained access through phishing emails, remotely disabling circuit breakers. It was the first known cyberattack to successfully disrupt a power grid, highlighting vulnerabilities in critical infrastructure.

Risk Mitigation Action Plan

Cyberattacks like Stuxnet and the Ukraine power grid incident demonstrate how vulnerable ICS systems are to sophisticated threats.

01

Vulnerability Assessment and Immediate Patching

- Conduct a comprehensive security audit of all ICS and SCADA systems to identify vulnerabilities such as outdated software and weak points in network security.
- Implement immediate patching of critical systems to address known vulnerabilities and ensure all systems are updated regularly.

02

Network Segmentation and Access Control

- Isolate ICS networks from corporate IT networks to prevent malware spread. Strengthen firewalls and gateways between them.
- Enforce multi-factor authentication (MFA) and strict role-based access to ICS systems to limit unauthorized access.

03

Employee Training and Incident Response Plan

- Provide phishing awareness training and conduct simulations to improve employee response to cyber threats.
- Develop and regularly test an incident response plan to ensure quick and effective action during a cyberattack.

04

Real-Time Monitoring and System Recovery

- Implement real-time network monitoring and intrusion detection systems (IDS) to identify and address threats early.
- Maintain regular backups of critical systems and test recovery procedures to ensure swift restoration of operations after an attack.

Université Grenoble Alpes

GROUP WORK PROCESS RESPONSIBILITIES

Université Grenoble Alpes

APPLICATION DECISION
BIRZHAN KULMANOV
BILAL SLEIMAN
UMAR FAROOQ

REAL LIFE EXAMPLES
BILAL SLEIMAN

RISK EVALUATION MITIGATION PLAN
BIRZHAN KULMANOV
BILAL SLEIMAN
UMAR FAROOQ

PRESENTATION CREATION
BIRZHAN KULMANOV

CLASS PRESENTATION
UMAR FAROOQ