Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies

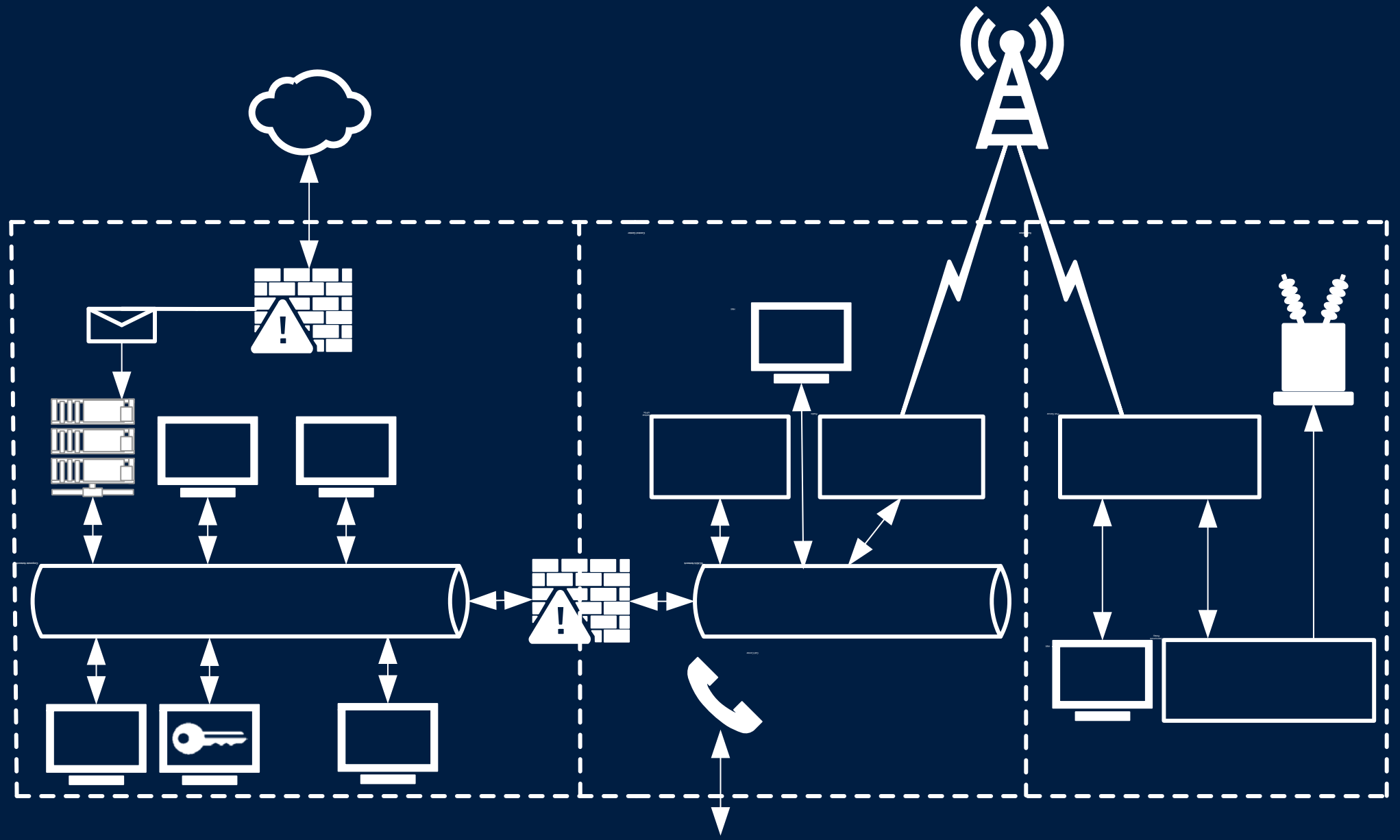
David E. Whitehead, Kevin Owens,
Dennis Gammel, and Jess Smith
Schweitzer Engineering Laboratories, Inc.

Cyber Attack on the Ukrainian Power Grid

December 23, 2015

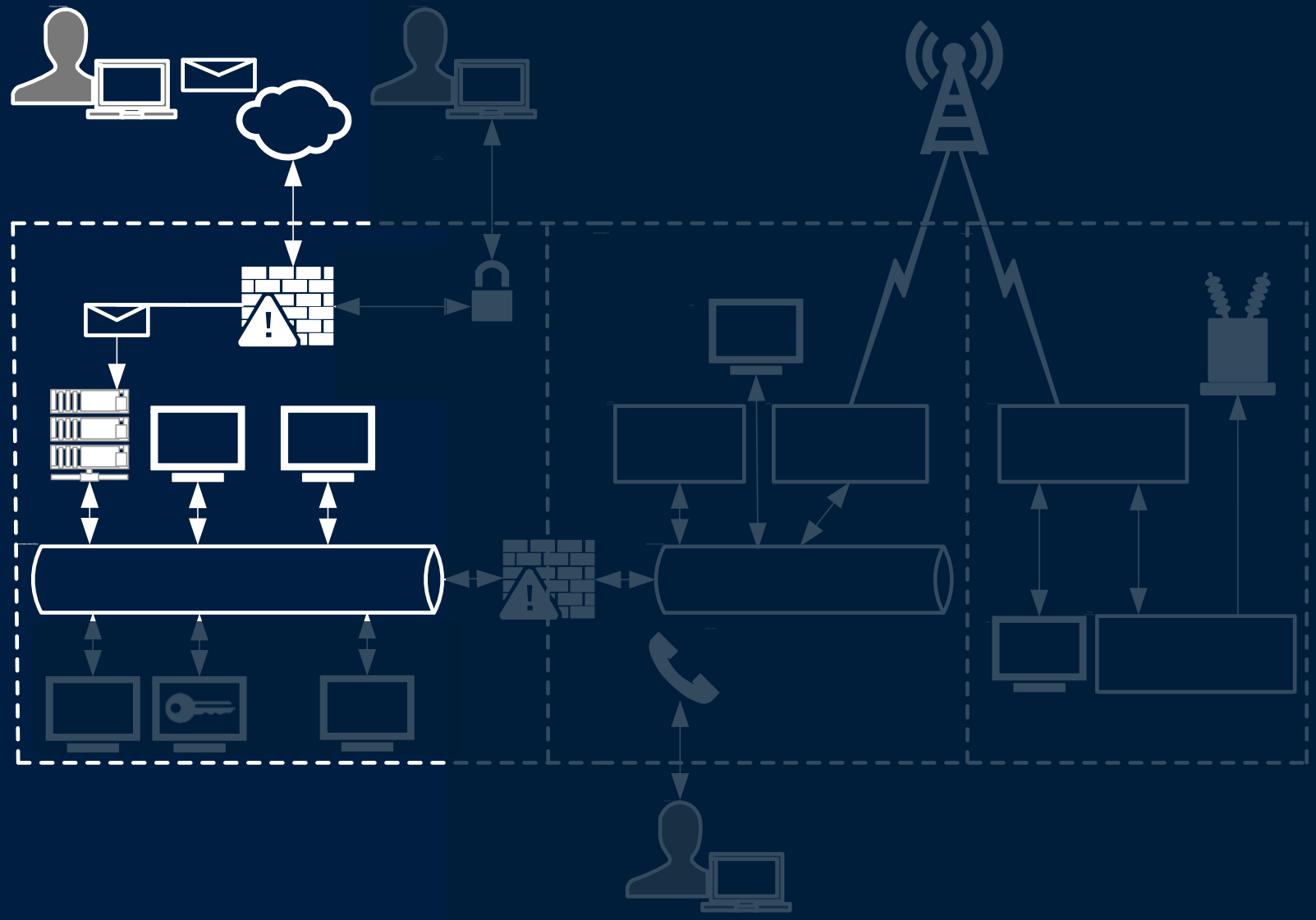
- Targeted more than 50 substations
- Left 225,000 customers without power for up to 6 hours

Ukraine Distribution Cyber System Overview



Stage 1: Spear Phishing – March 2015

Opening an attachment with a macro installs BlackEnergy3

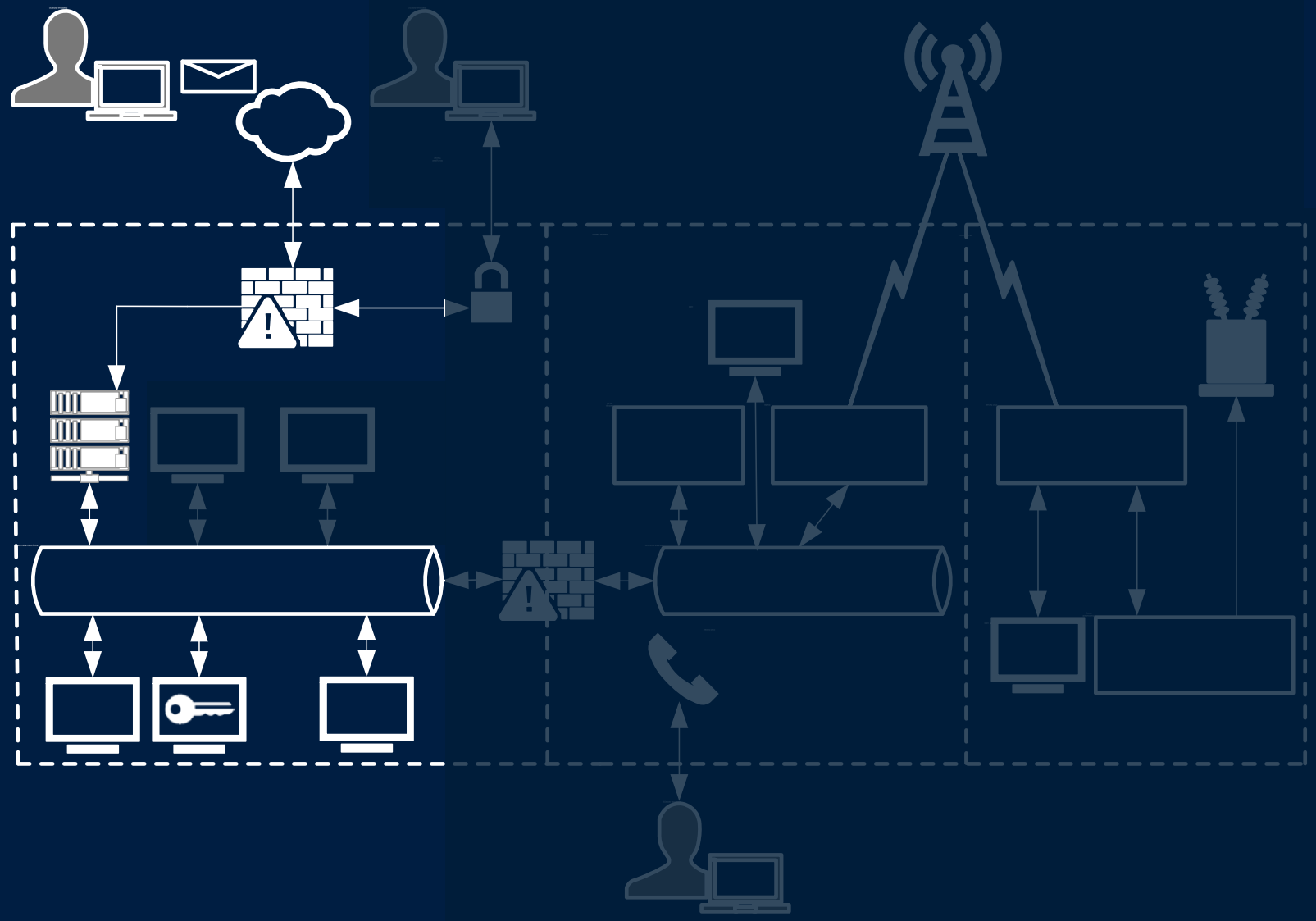


Stage 2: Access Corporate Network

Malware provides initial backdoor access

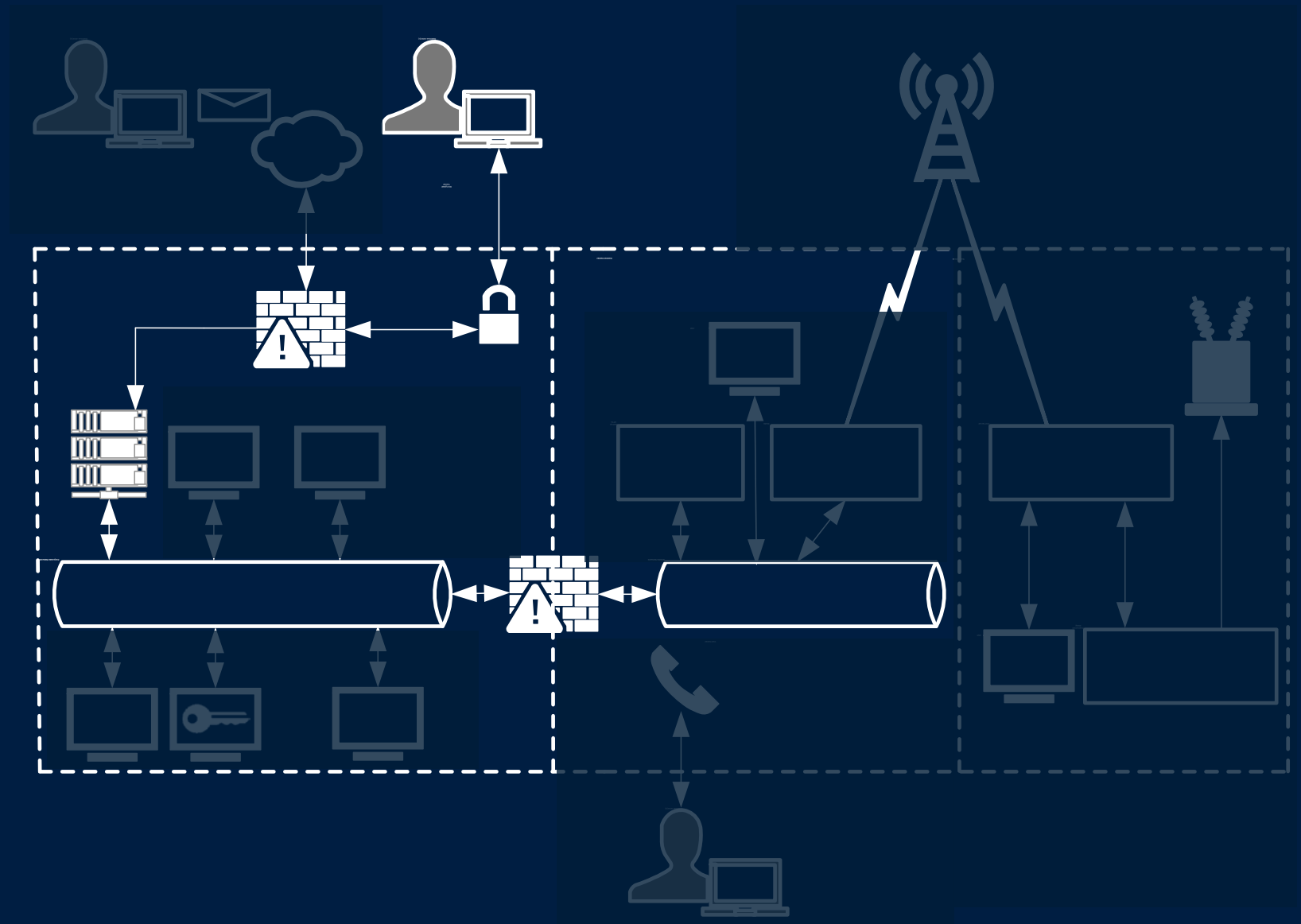
Stage 3: Theft of User Credentials

Active Directory® credentials obtained



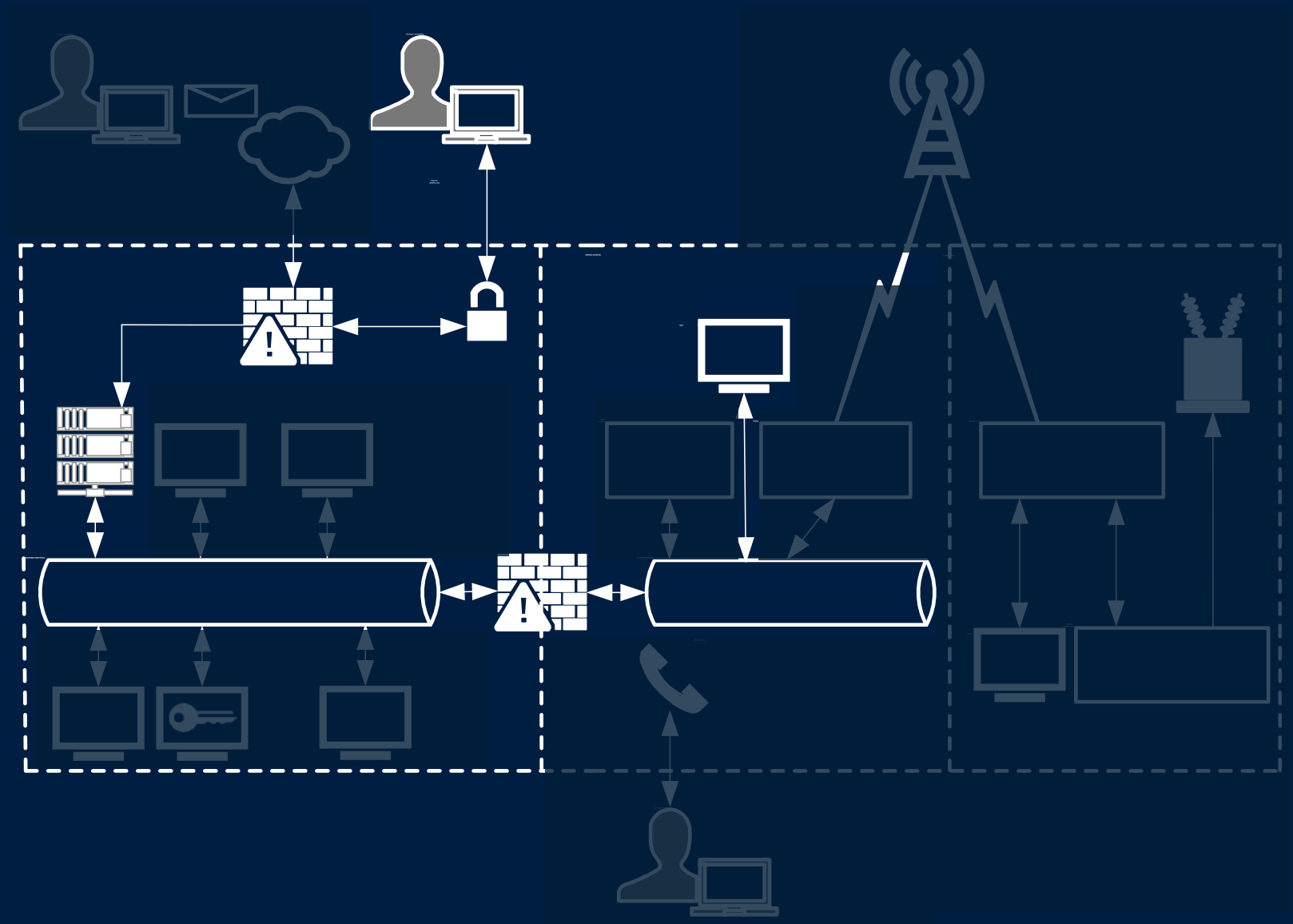
Stage 4: Create Encrypted Tunnels

Encrypted tunnel to the control center networks



Stage 5: Gain Access to HMIs

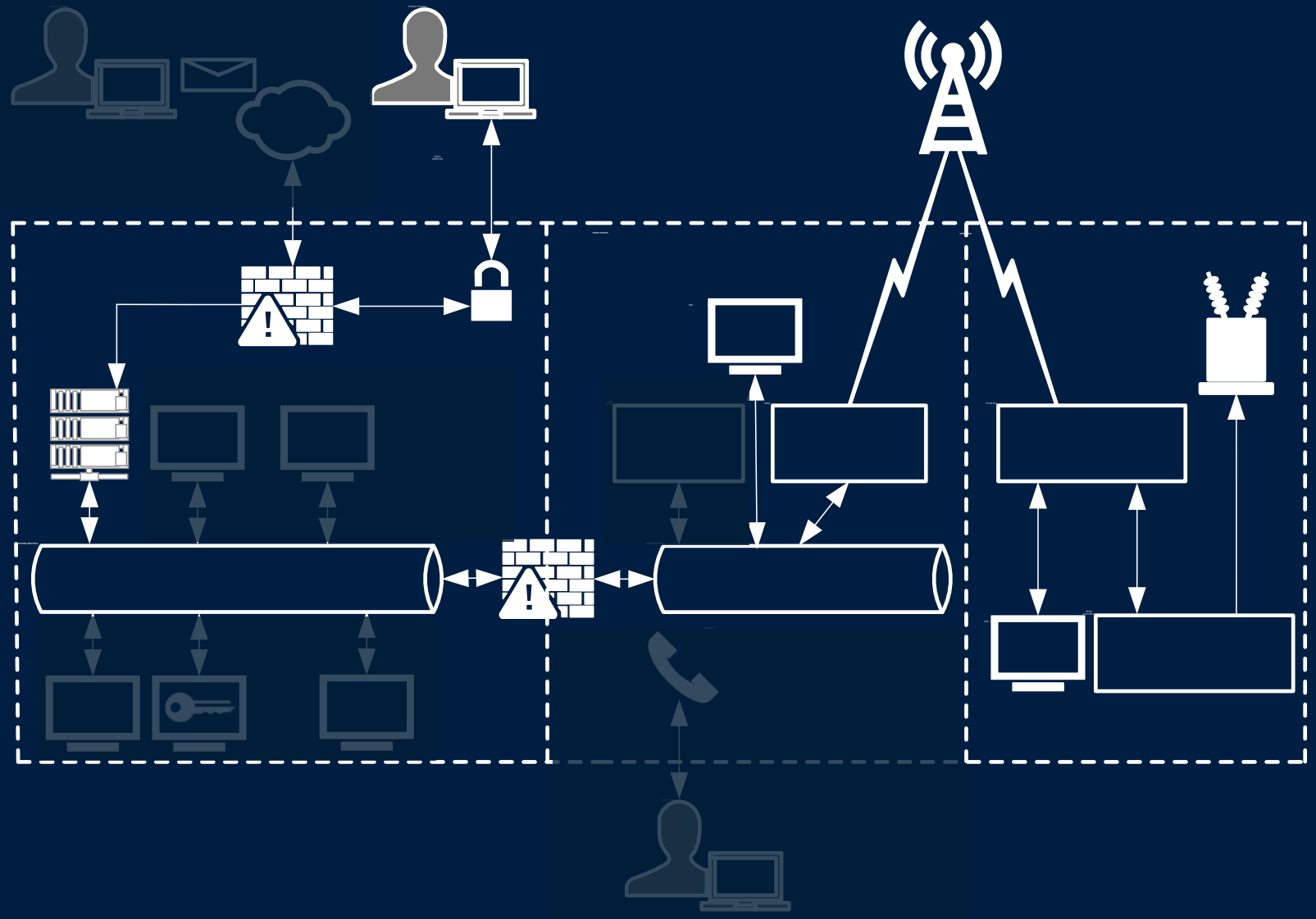
Accessed HMI computers in control center



Stage 6: Manipulate Circuit Breakers

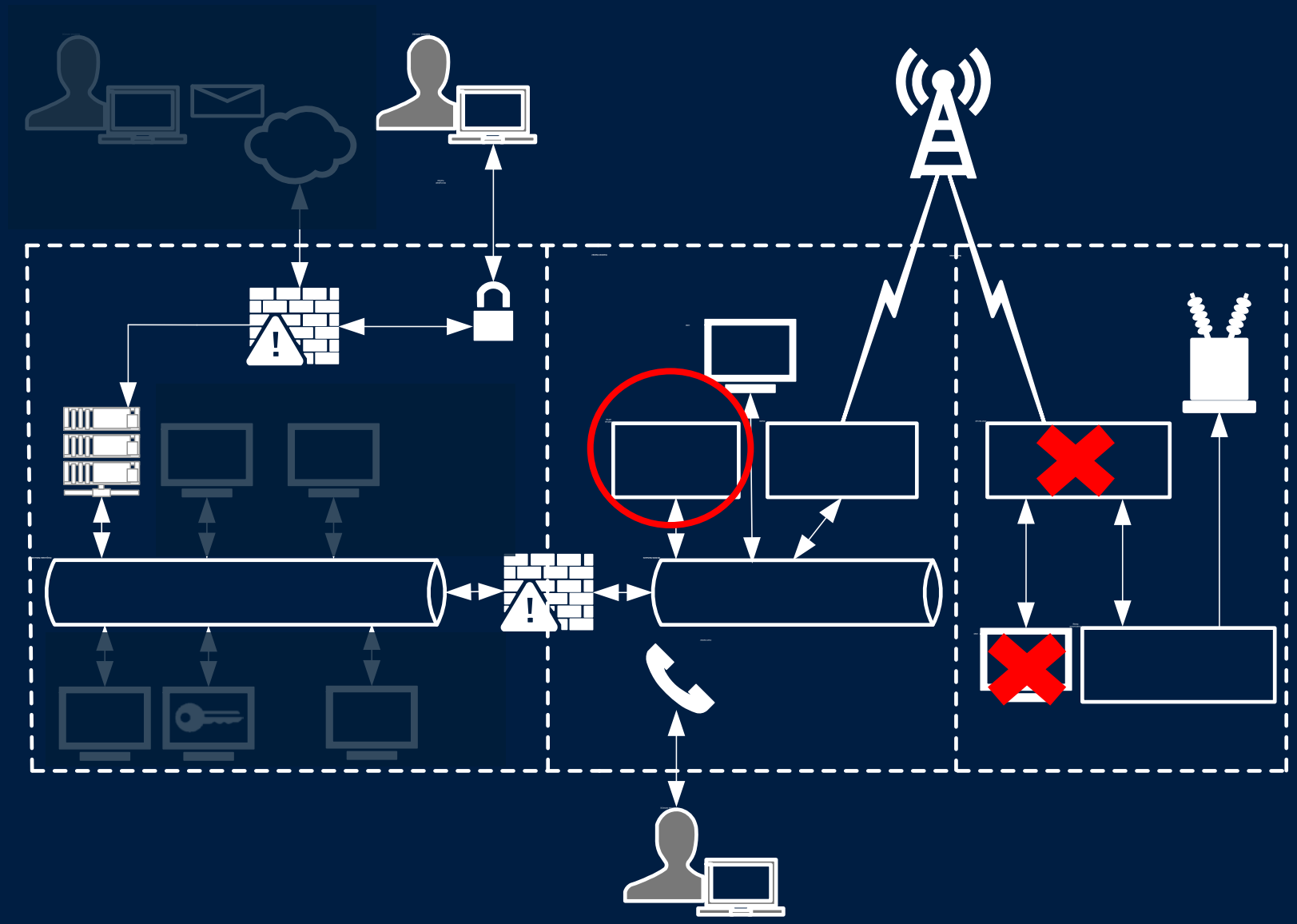
Attack Occurs on Dec 23 2015 @ 3:30 PM

HMI used to manually open breakers



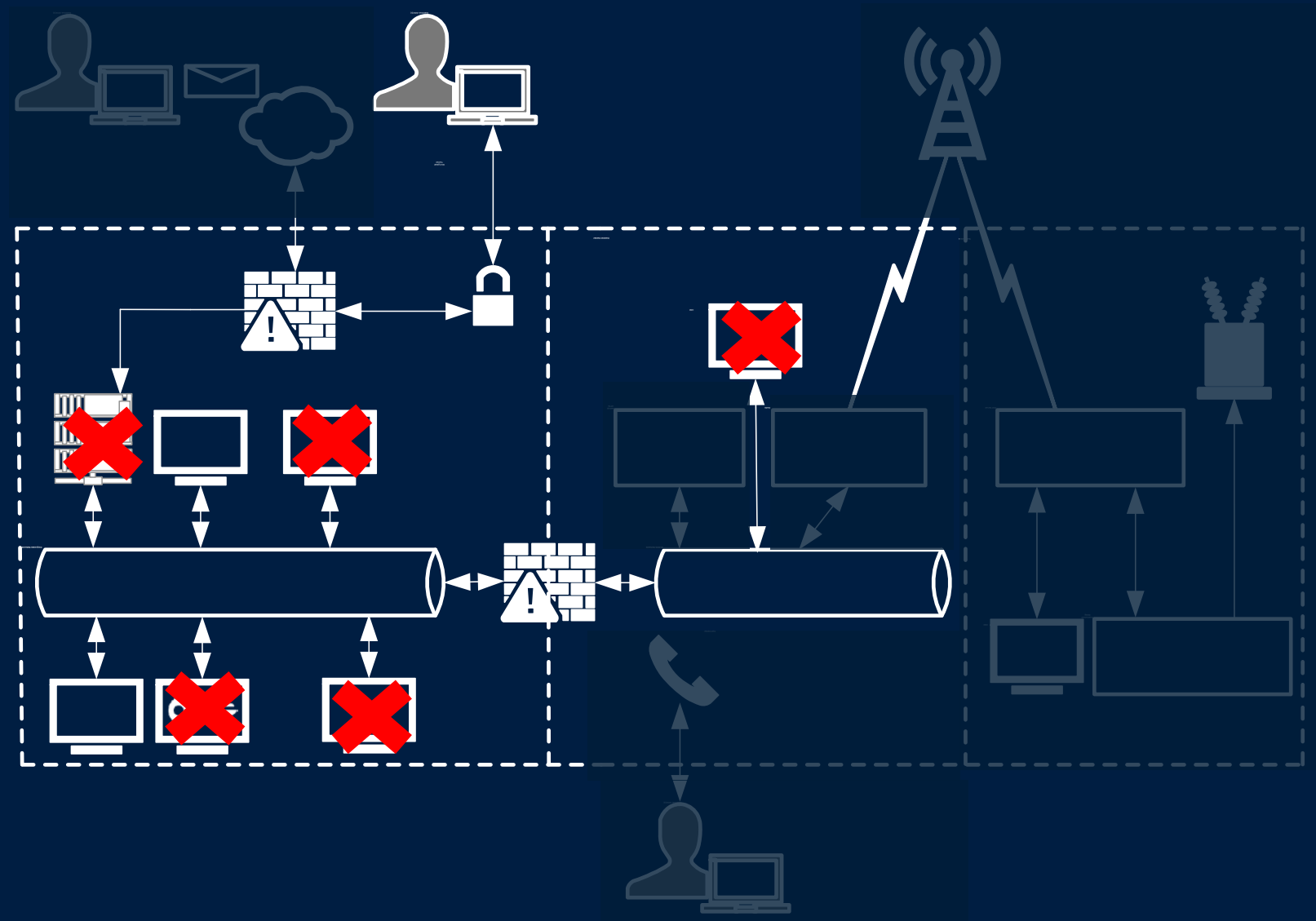
Stage 7: Additional Attack Actions

- Attacked call centers
- Switched off UPSs
- Corrupted RTU HMI firmware
- Corrupted port server firmware



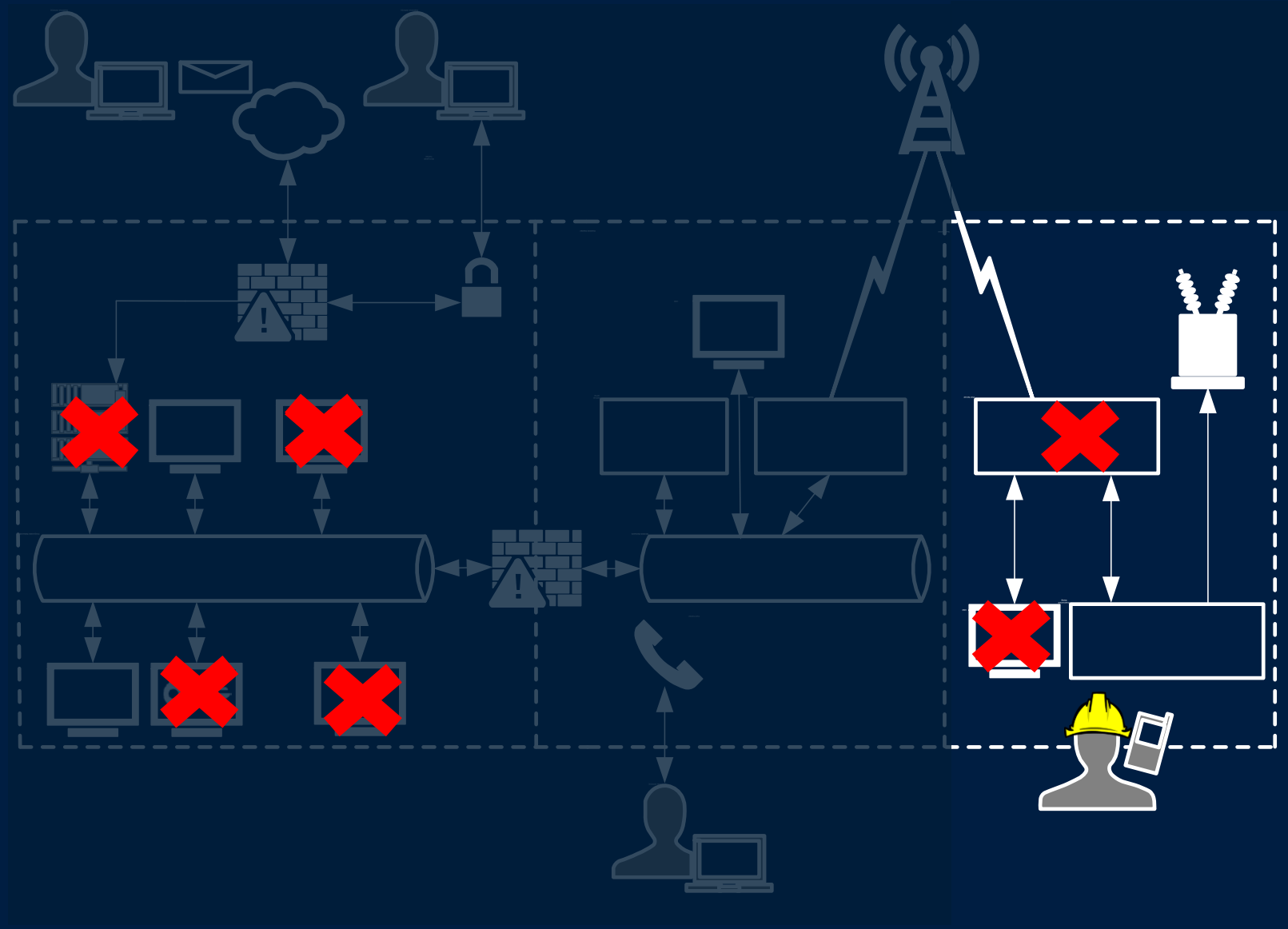
Stage 8: Destroy Hard Drives

Used KillDisk malware to corrupt hard drives



Power Restored Within Six Hours!

System operated manually



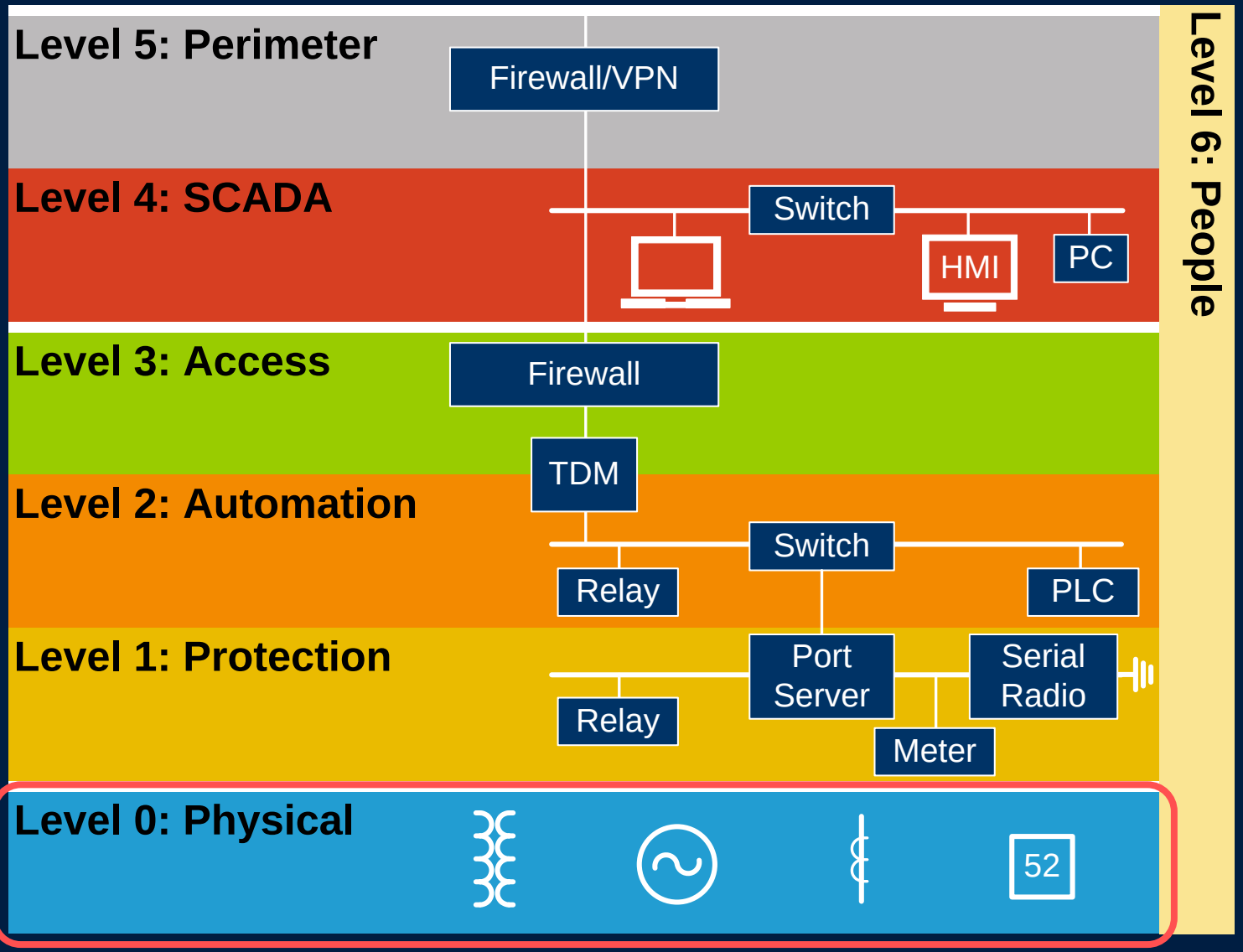
SCADA Systems Are Still Operating in a Degraded State

- Still replacing corrupted equipment
- Enhancing network security
- According to ICS-CERT
  - Adversary most likely still present
  - Other sectors are probably vulnerable

Creating a Robust Control System Architecture

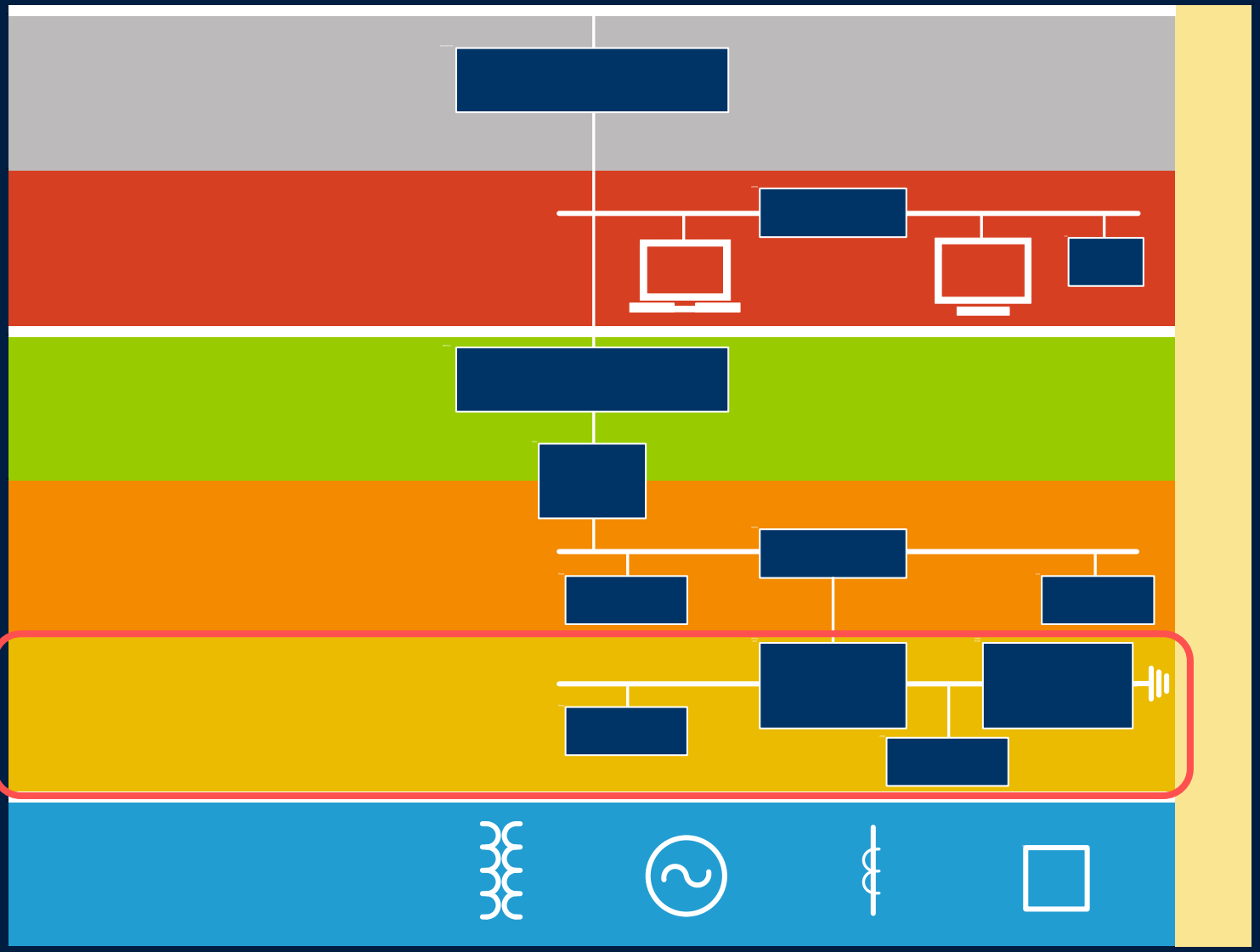
- Identify risk
- Create a defense-in-depth model
- Implementing effective controls

Level 0: Physical – Measures and Operates



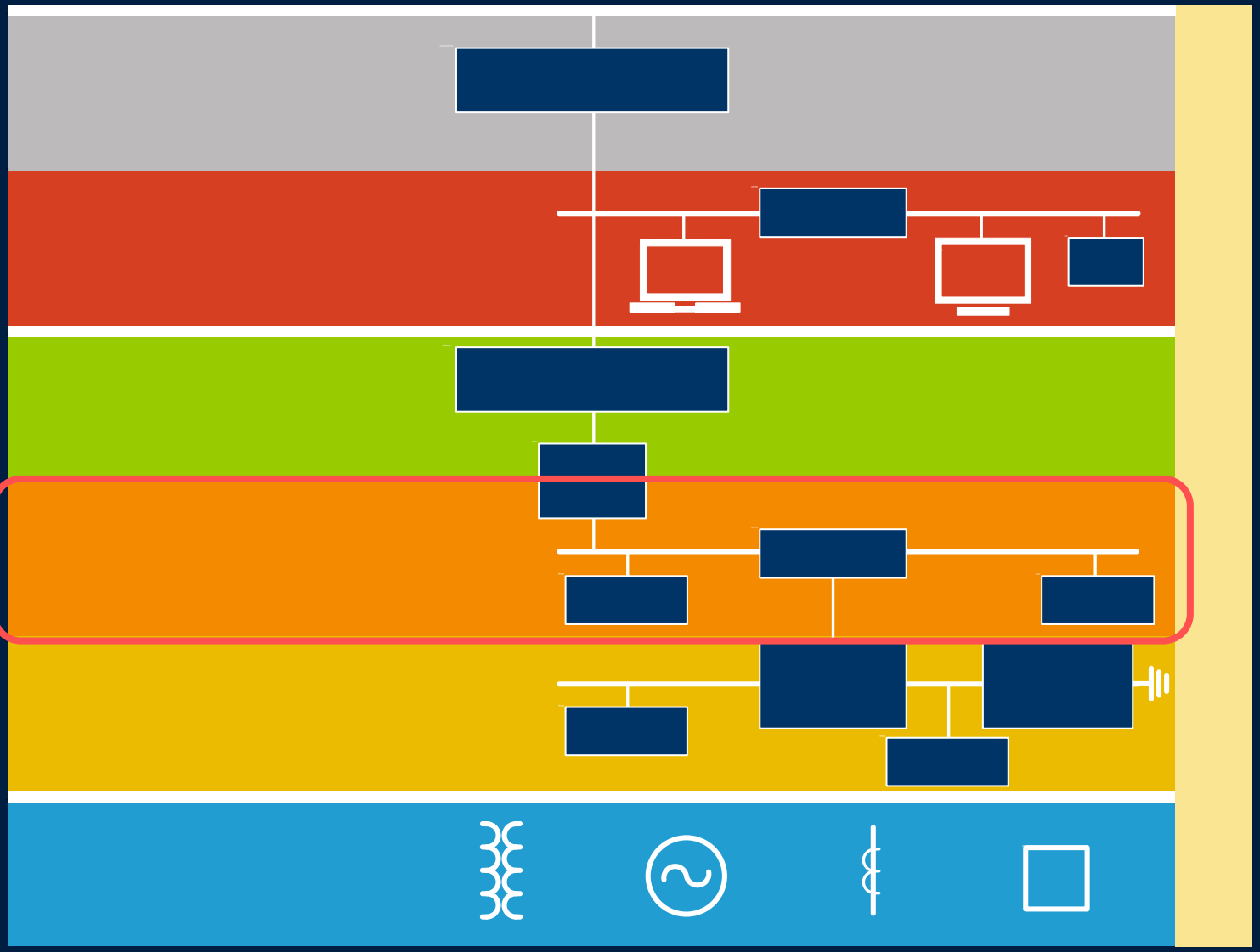
- Typically no digital communication
- Limit physical access

Level 1: Protection – Isolates and Clears Faults



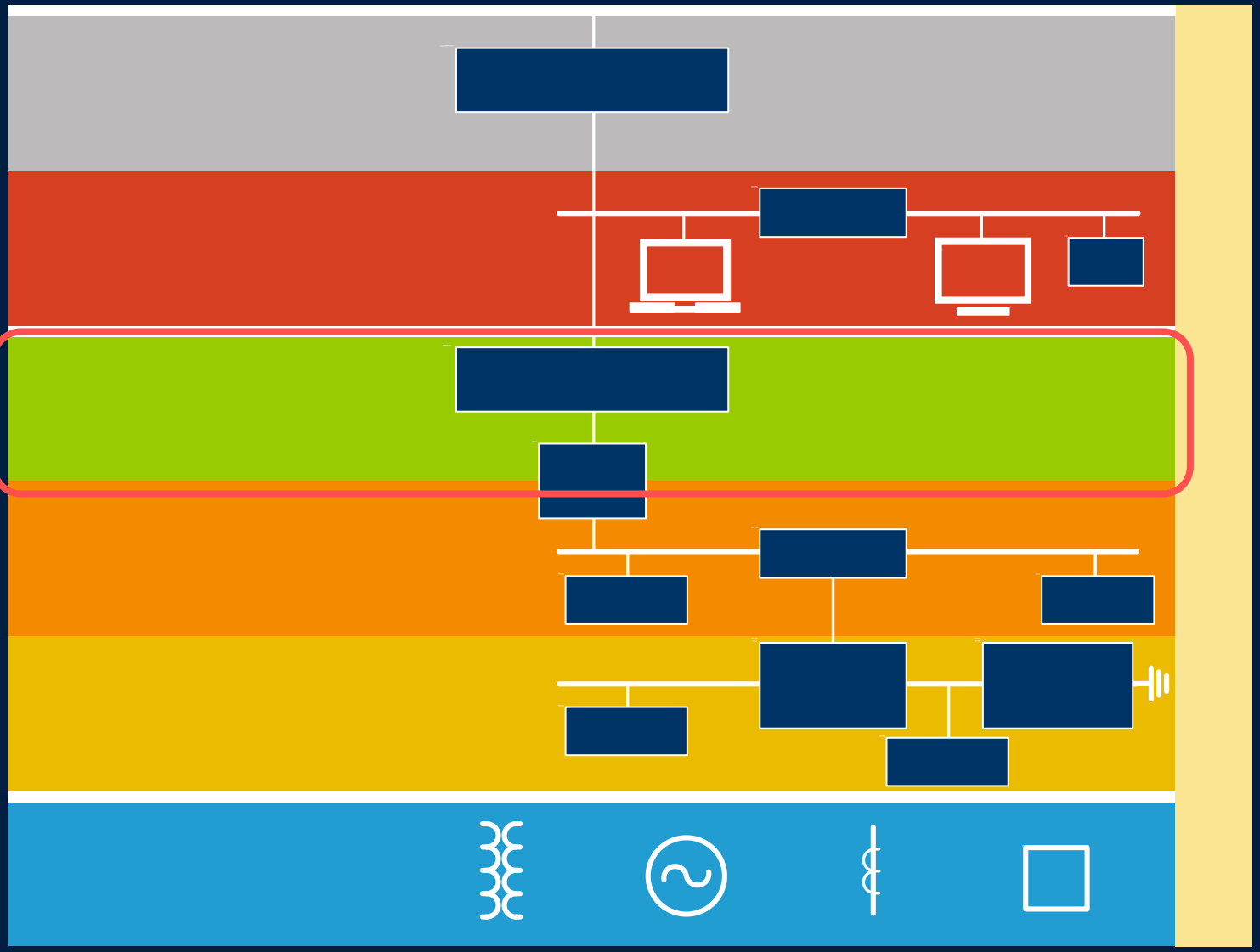
- Limit direct user interaction
- Monitor internal diagnostics
- Monitor alarms

Level 2: Automation – Protection and Control



- Continuously monitor
  - Settings
  - Firmware configurations
- Collect and aggregate alarms

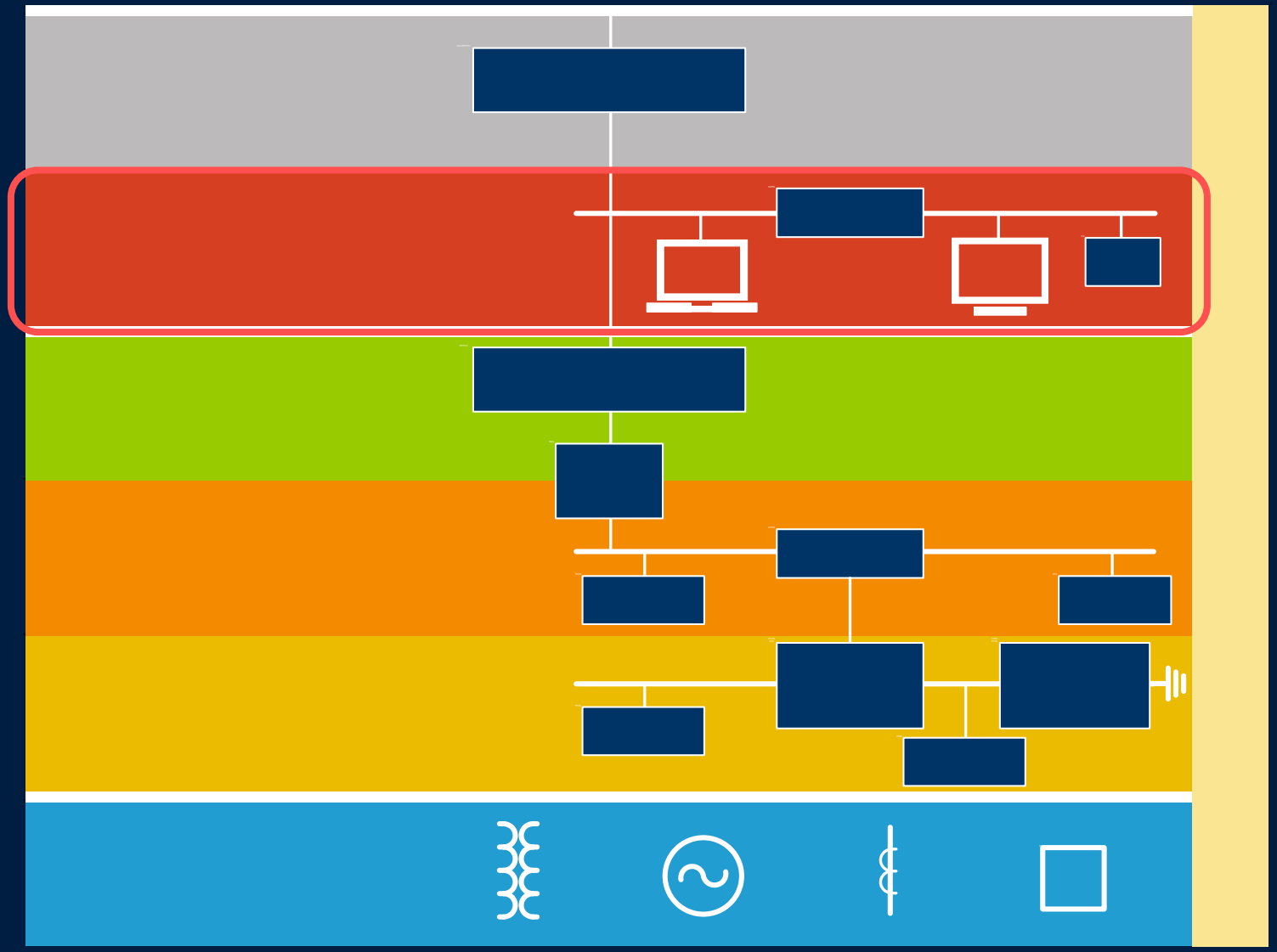
Level 3: Access – Segregates H2M From M2M



Separate, restrict, and filter H2M from M2M

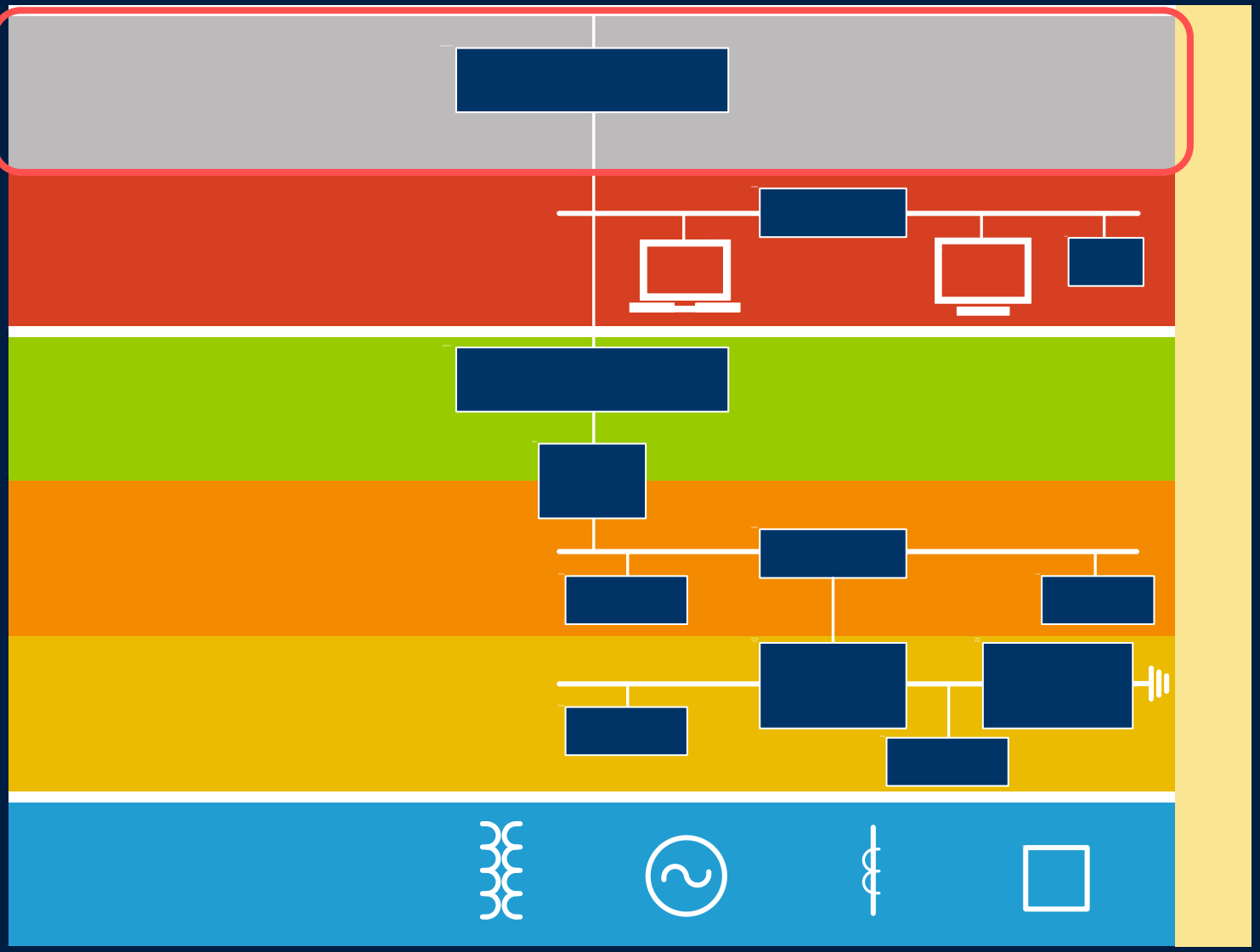
- Authorization
- Authentication
- Accountability

Level 4: SCADA – Interfaces With Control System



- Integrate traditional IT controls
- Monitor networks with IDS/IPS/NAC

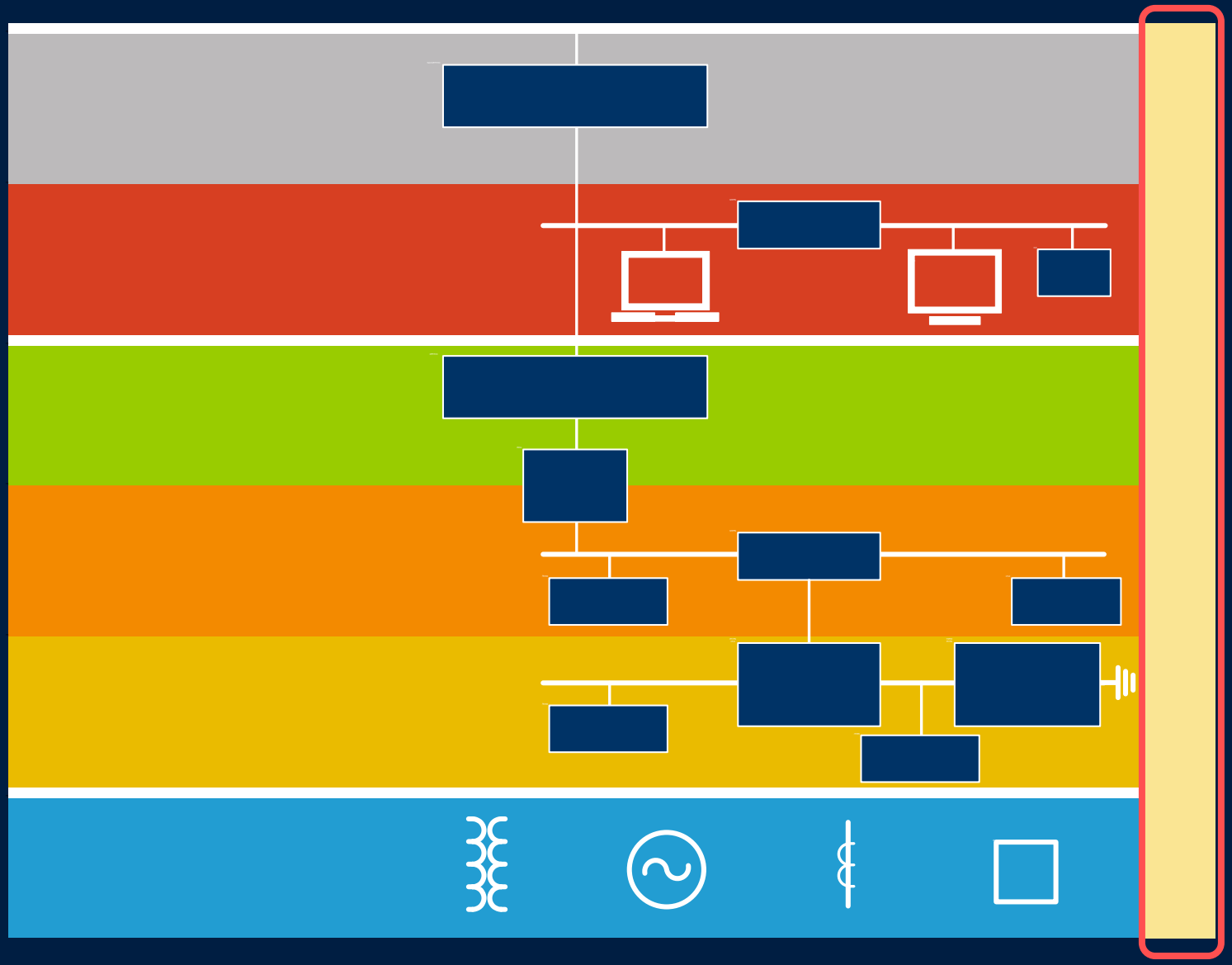
Level 5: Perimeter – Isolates Control System



- Implement multifactor authentication
- Segment network

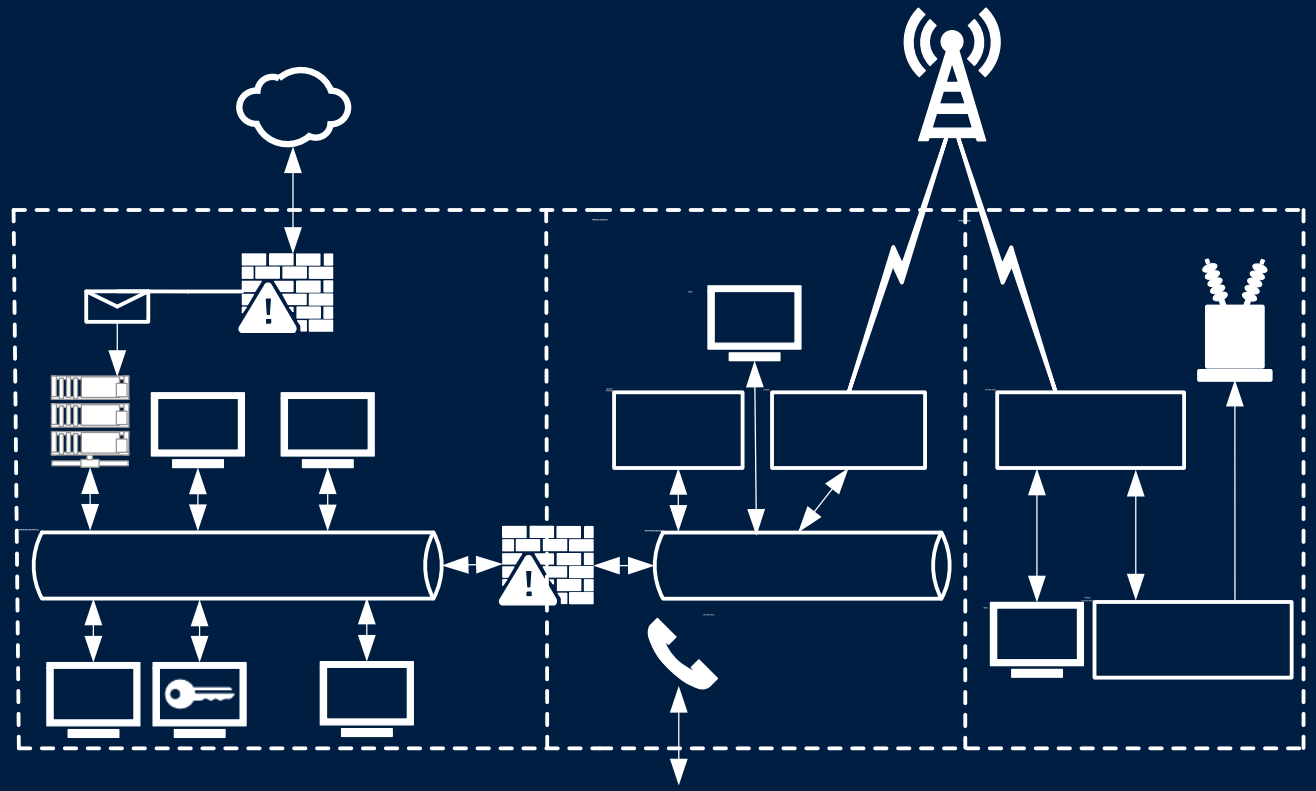
***NEVER** connect your ICS to the Internet!*

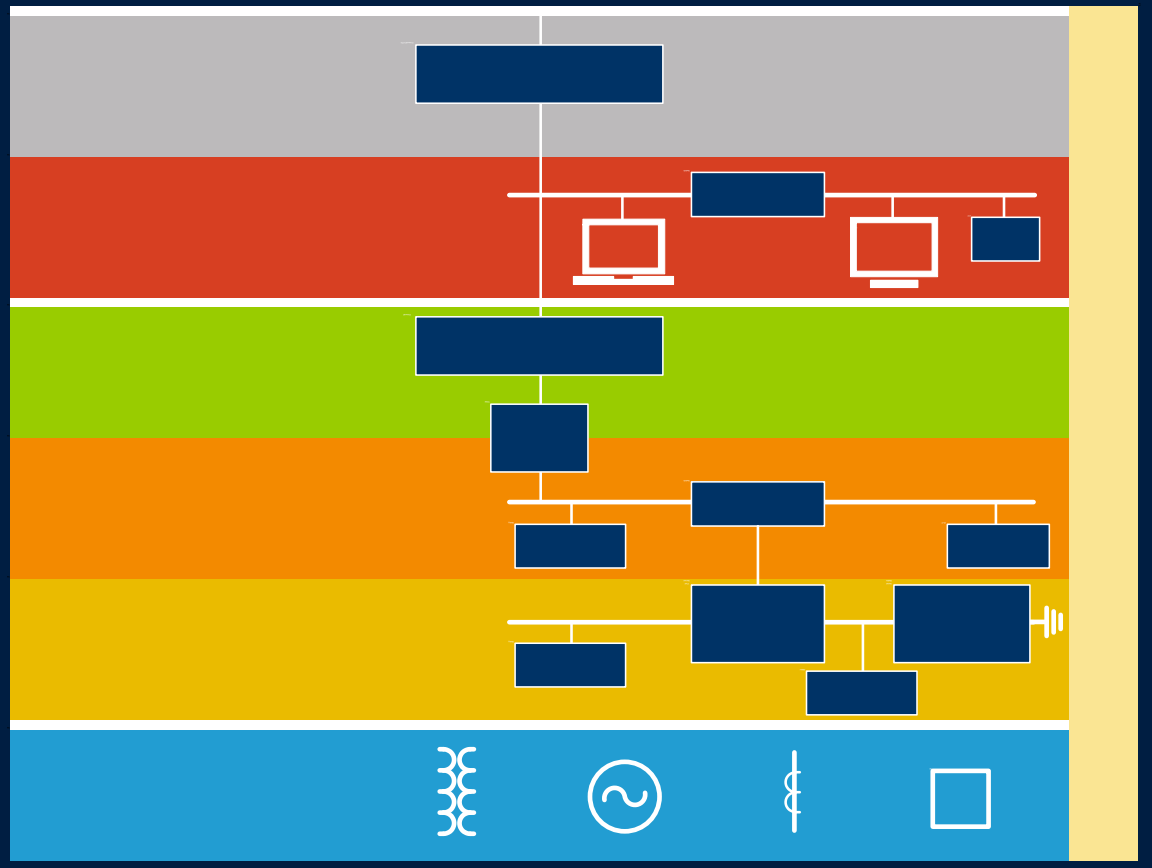
Level 6: People – Policies, Procedures, Training



- Apply least privilege
- Create awareness
- Develop and exercise contingency plans

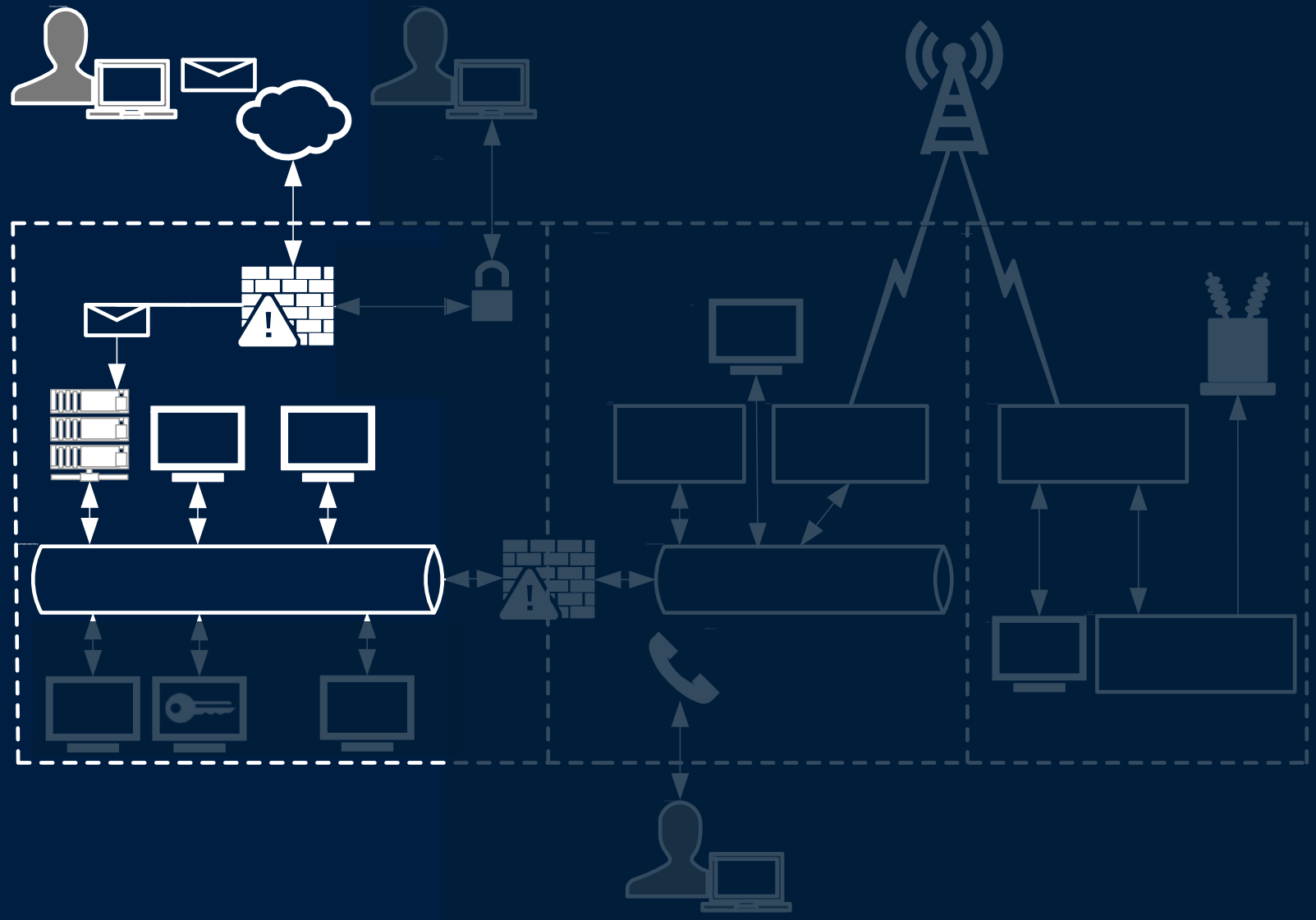
Comparing Ukraine System and Security Model





Stage 1: Spear Phishing

- Training
- Email security controls
  - Remove attachments
  - Scan attachments

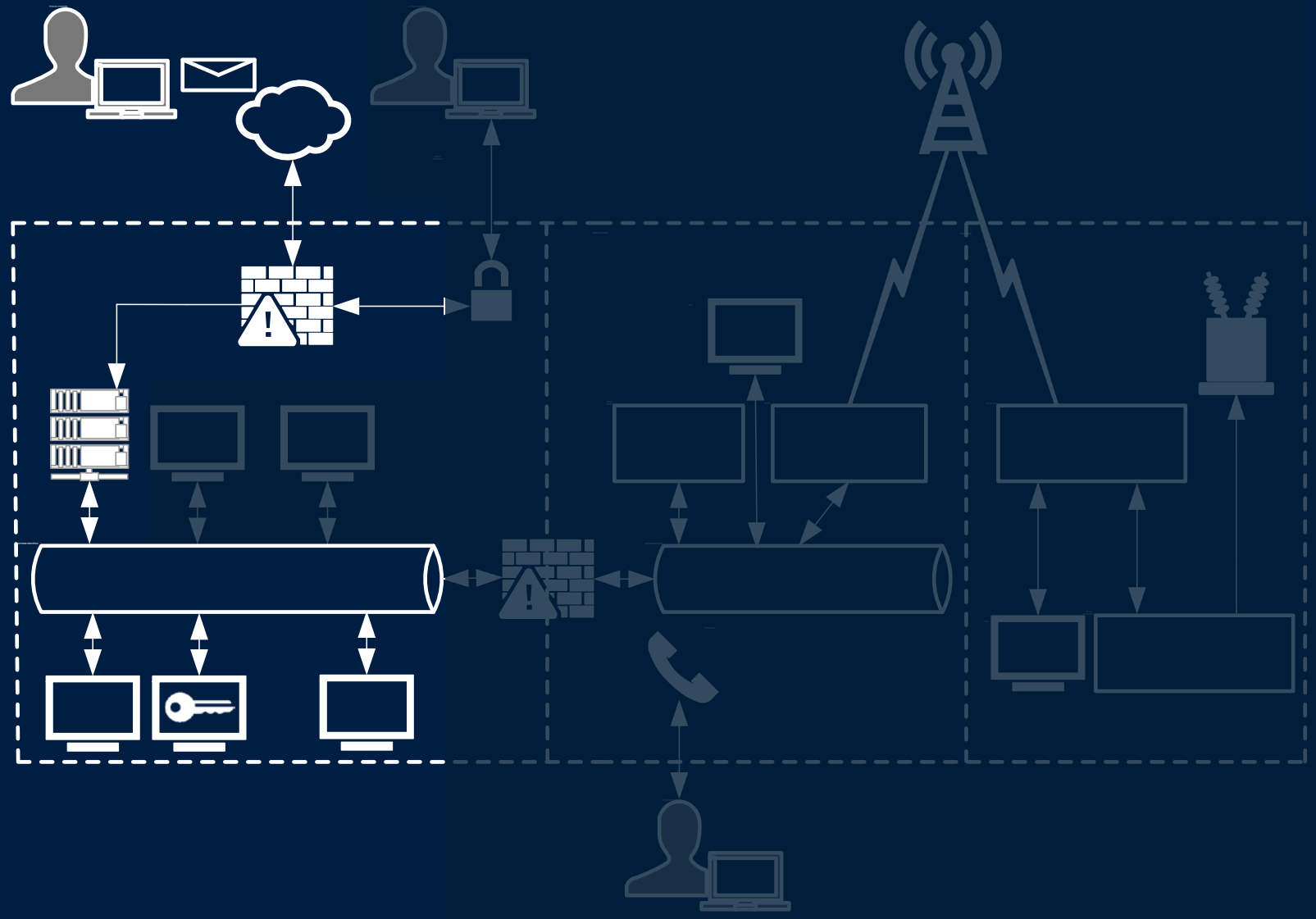


Stage 2: Access Corporate Network

- Antivirus
- IDS/IPS/NAC
- Host-based firewalls

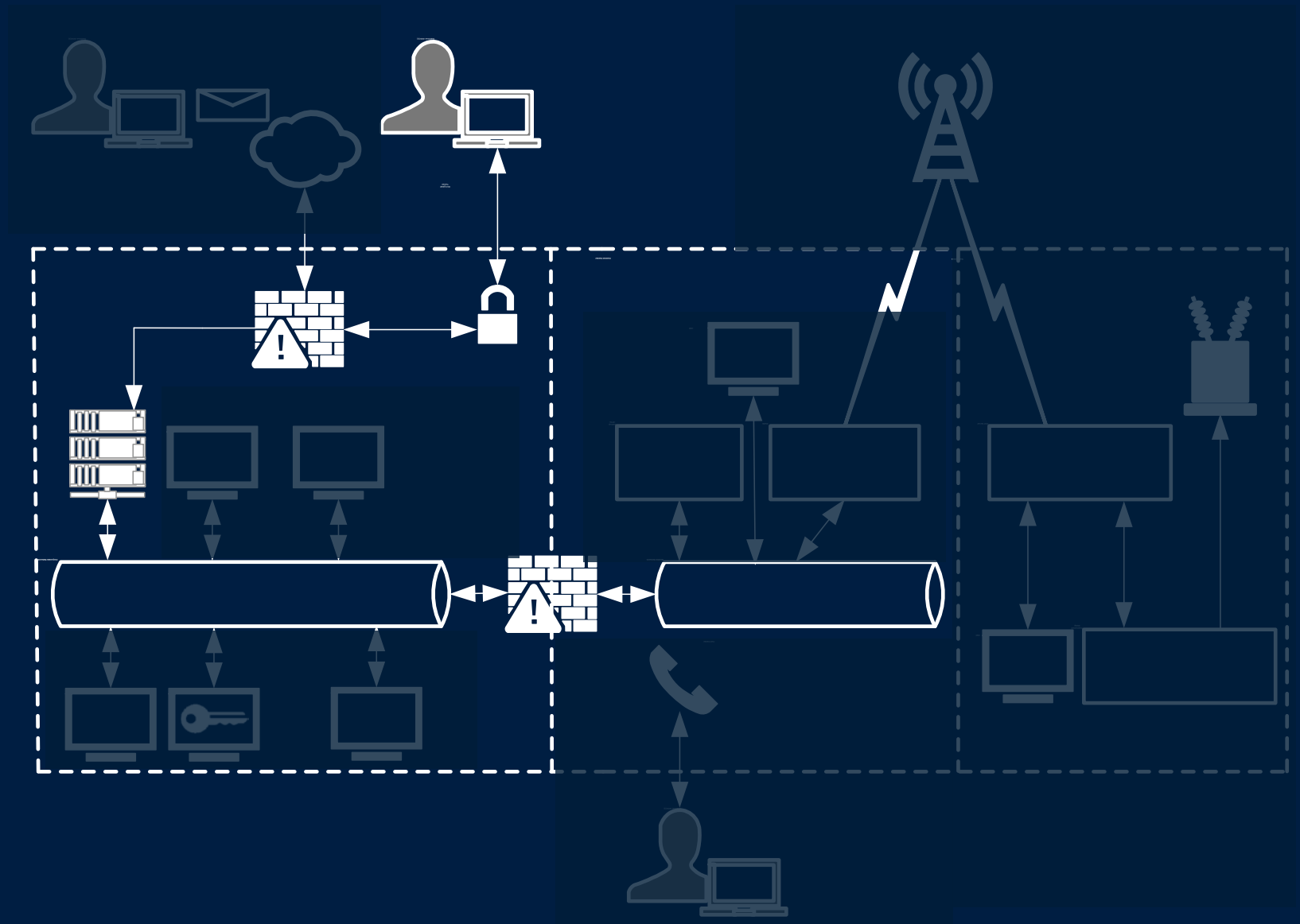
Stage 3: Theft of User Credentials

- User least privilege
- Password rotation
- Strong credentials
- IDS
- Syslogs



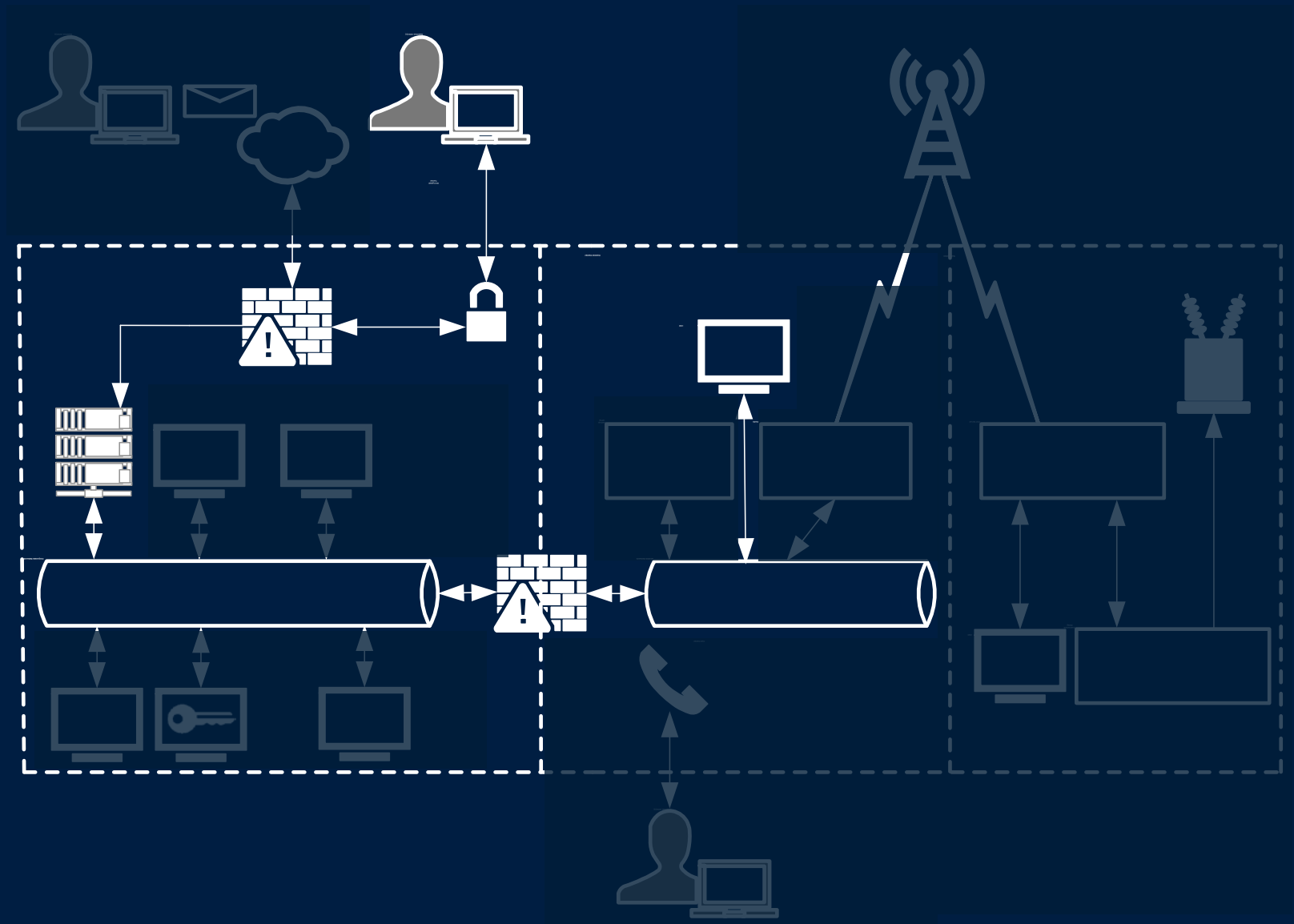
Stage 4: Create Encrypted Tunnels

- Granular VPN rules
- Multifactor authentication
- Monitoring



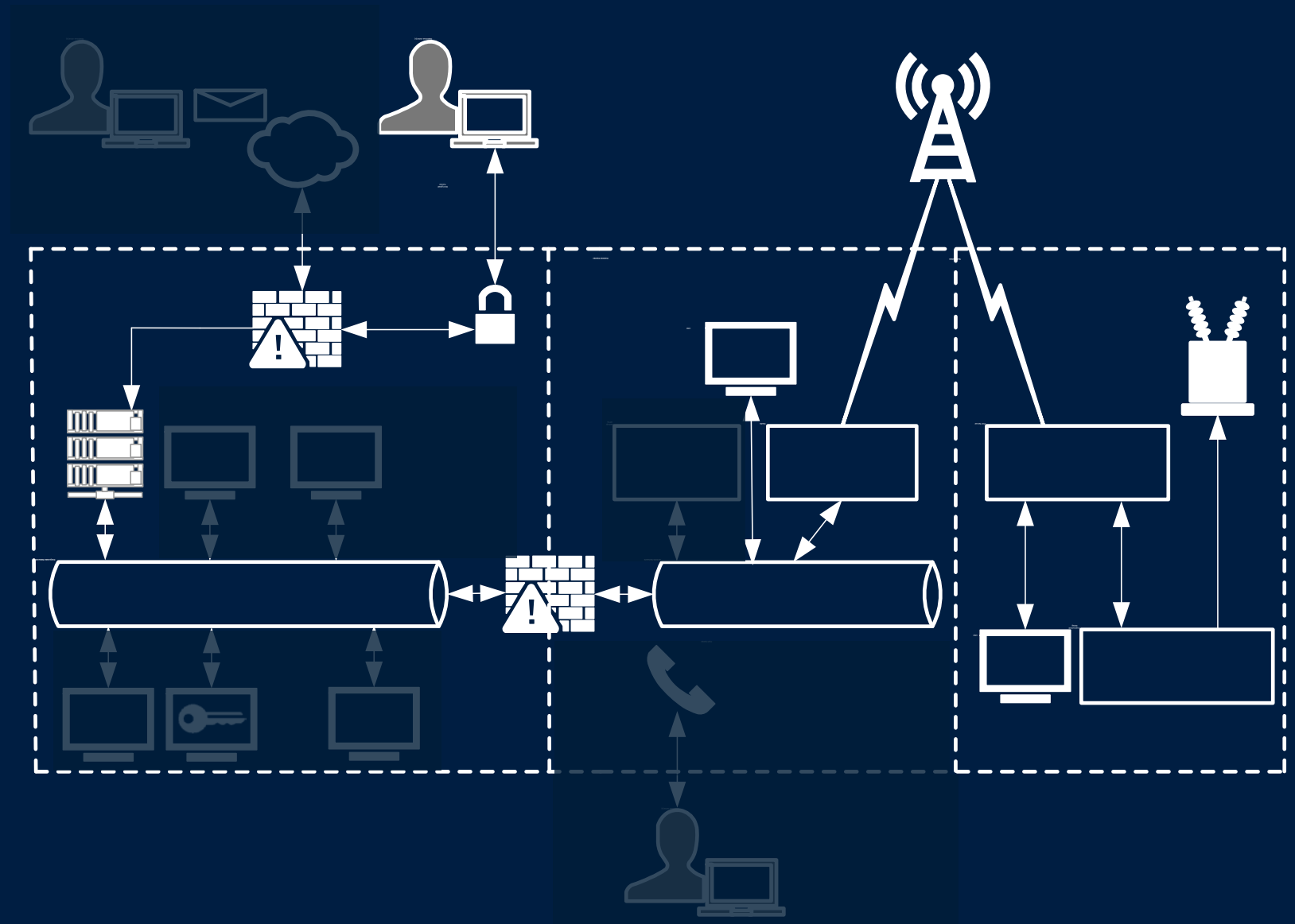
Stage 5: Gain Access to HMIs

- Network segmentation
- Strong firewall rules
- User least privilege



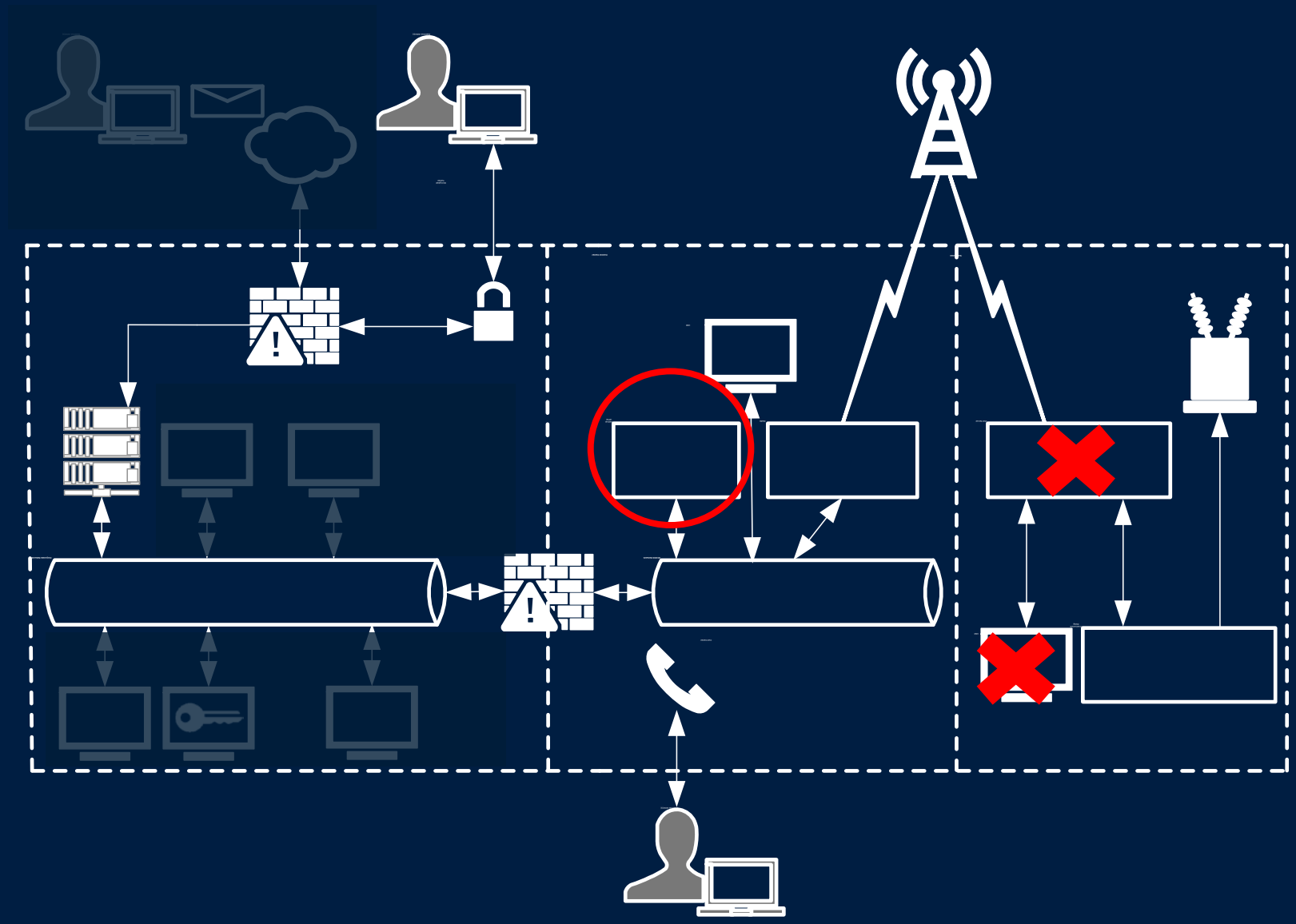
Stage 6: Manipulate Circuit Breakers

- Strong authentication
- Quick isolation
- Incident planning



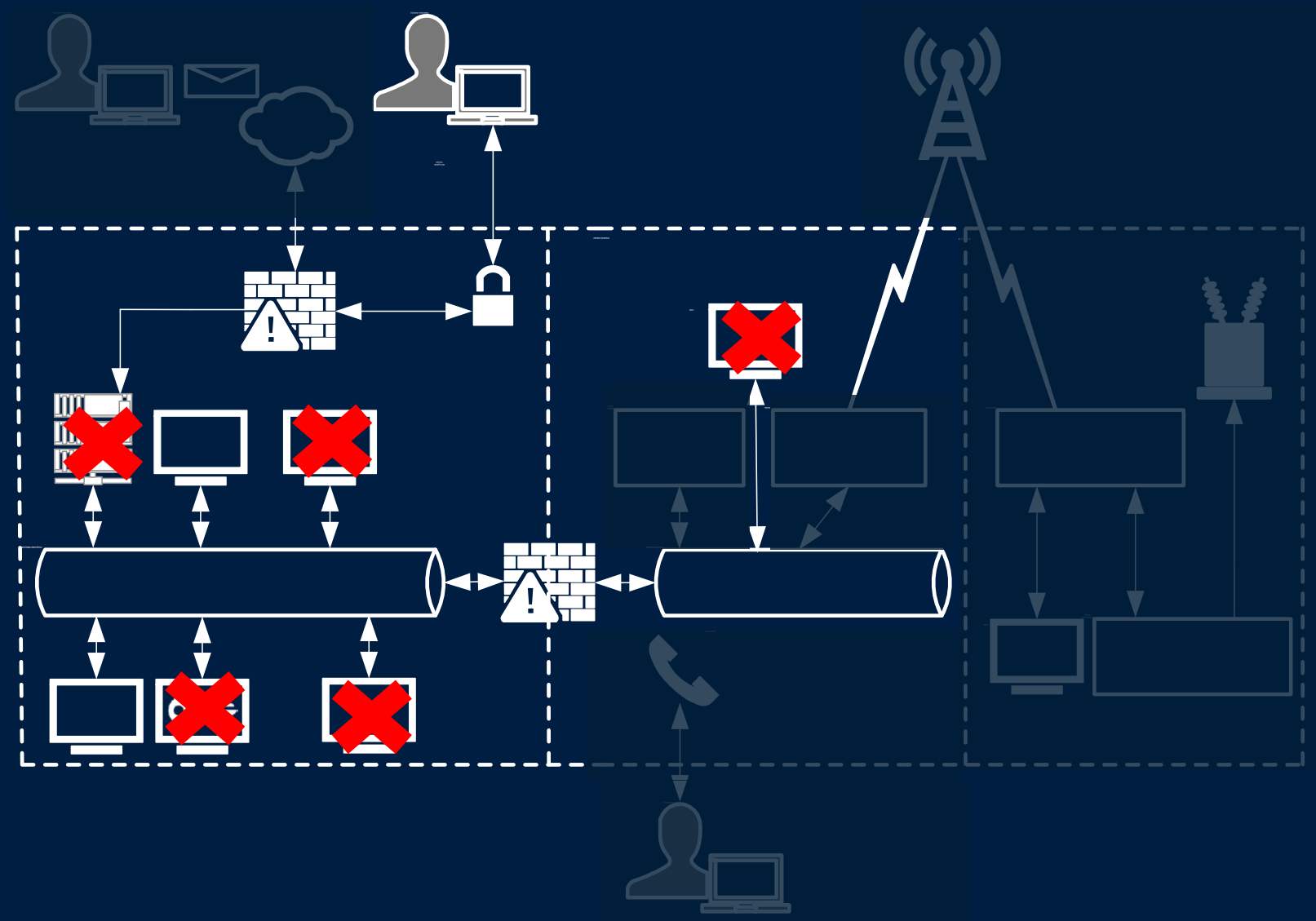
Stage 7: Additional Attack Actions

- Firmware validation
- Hardware backups
- Data backups
- Recovery procedures



Stage 8: Destroy Hard Drives

- Antivirus
- Hardware backups
- Data backups



Ukraine Incident Summary

- Unfortunate event that disrupted numerous households
- No single security or network deficiency allowed malicious actors to achieve their objective
- Determined malicious actors can exploit a system that is not based on defense-in-depth design principles

Conclusions

- Use a layered security approach
- Proper cybersecurity includes *people*, hardware, software, policies, and procedures
- Ukraine incident encourage all of us to reevaluate our security measures protecting our cyber-based assets


Questions