Device Interrogation at TVA Discussion

Paul Trachian
MGR, Control Center Design

Open Discussion Topics

SOFTWARE

- openMIC
- openPDC
- openXDA
- eDNA

NETWORKS

- High security
- Low security
- Field

SECURITY

- On-prem vs cloud auth
- Encryption
- CIP

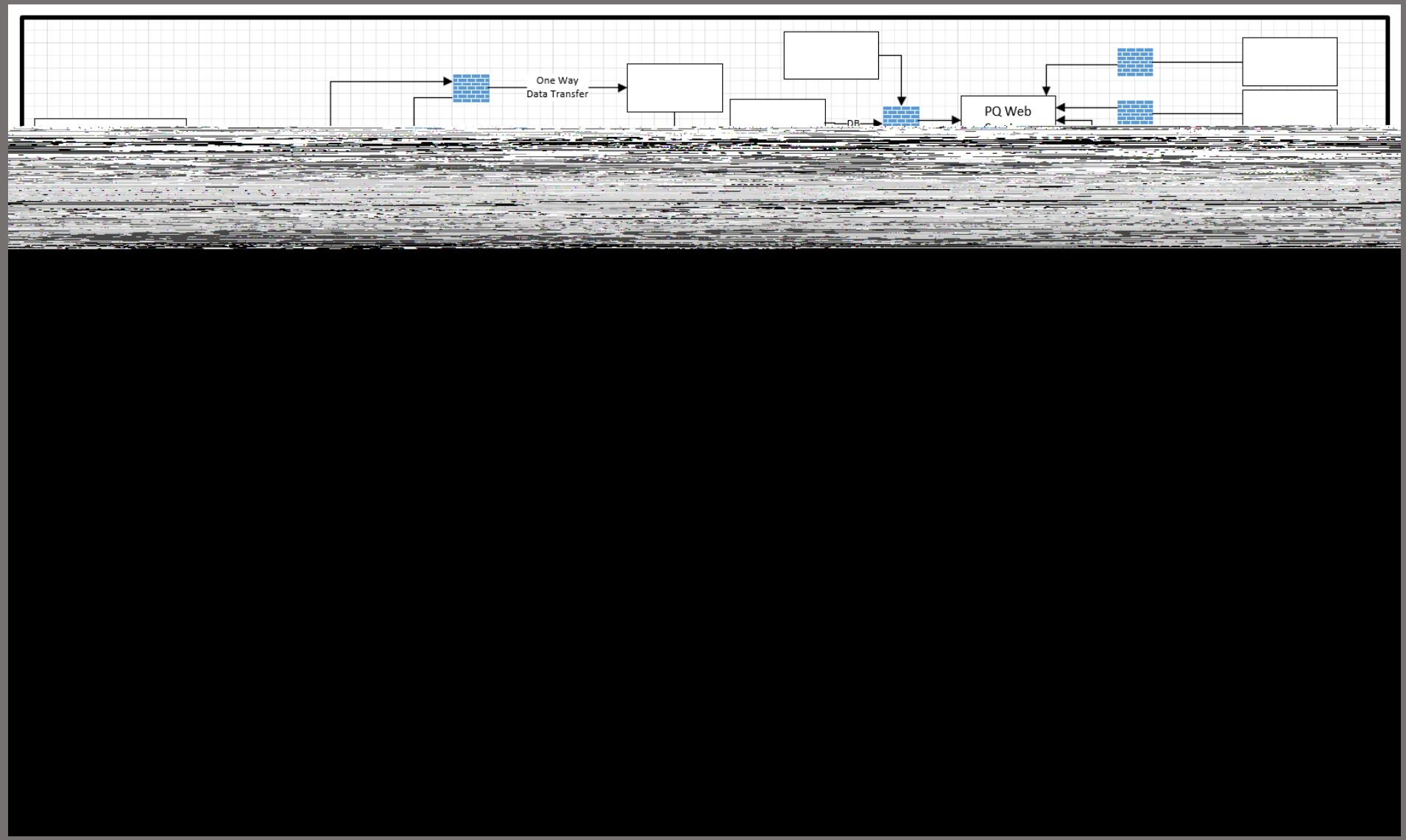
USER ACCESS

- Remote vs local
- Admin accounts vs user vs power user

OPERATIONS

- Bandwidth
- Redundancy and Failover
- Patching
- Resource Utilization

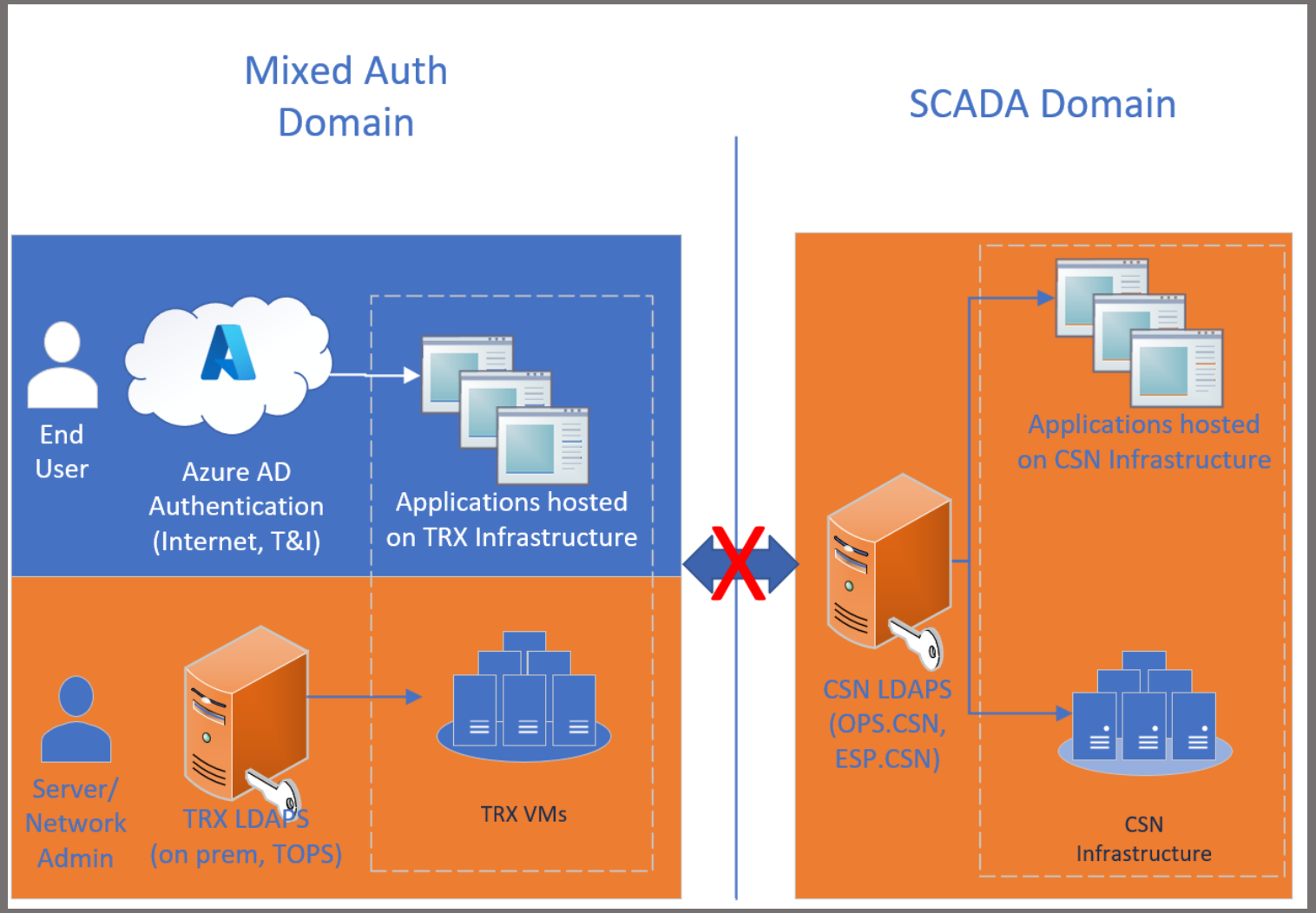
Data Flow Complexity



Due to the number of firewalls, data entry points, CIP considerations, and internal policies the flow of data is extremely complicated.

TVA TENNESSEE VALLEY AUTHORITY

Authentication and Domains



Internal policy mandates that all systems must work (and be effectively managed) even when disconnected from the internet, and the IT owned corporate network. This requires on-prem redundant use case architecture that also necessarily differs in technology selection.

TVA TENNESSEE VALLEY AUTHORITY

Operations

- Control Centers with redundant clustered hardware
- Utilizes HCI and vSAN, moving away from blade chassis and SAN
- Bandwidth has only been a problem for remote sites over cell, microwave, or other older technologies
- Microsoft Server Fail-over clustering
- Tiered storage arrays utilizing data de-dup
- 3 levels of software assurance – dev, acc, prod
- Patching done monthly using failover to switch nodes when patches are to be applied
- No need was seen for especially high performance hardware
- Encryption at the network level (DMVPN, TLS, etc)

TVA TENNESSEE VALLEY AUTHORITY

Hard Spots and Talking Points

- Large amount of storage possibly required, determine retention policy upfront
- Connections to control devices (relays) can force onerous controls on all other non-control assets/connections
- Disconnection requirements can complicate authentication
- Movement of data between domains with different levels of trust should be carefully examined for bi-directional feeds
- Device management software is often best separated out from polling software for more robust configuration management control

TVA TENNESSEE VALLEY AUTHORITY