



# “Computer Glitch in a Maximum Security Prison” Brief on Accident

Naja Green  
@02665005

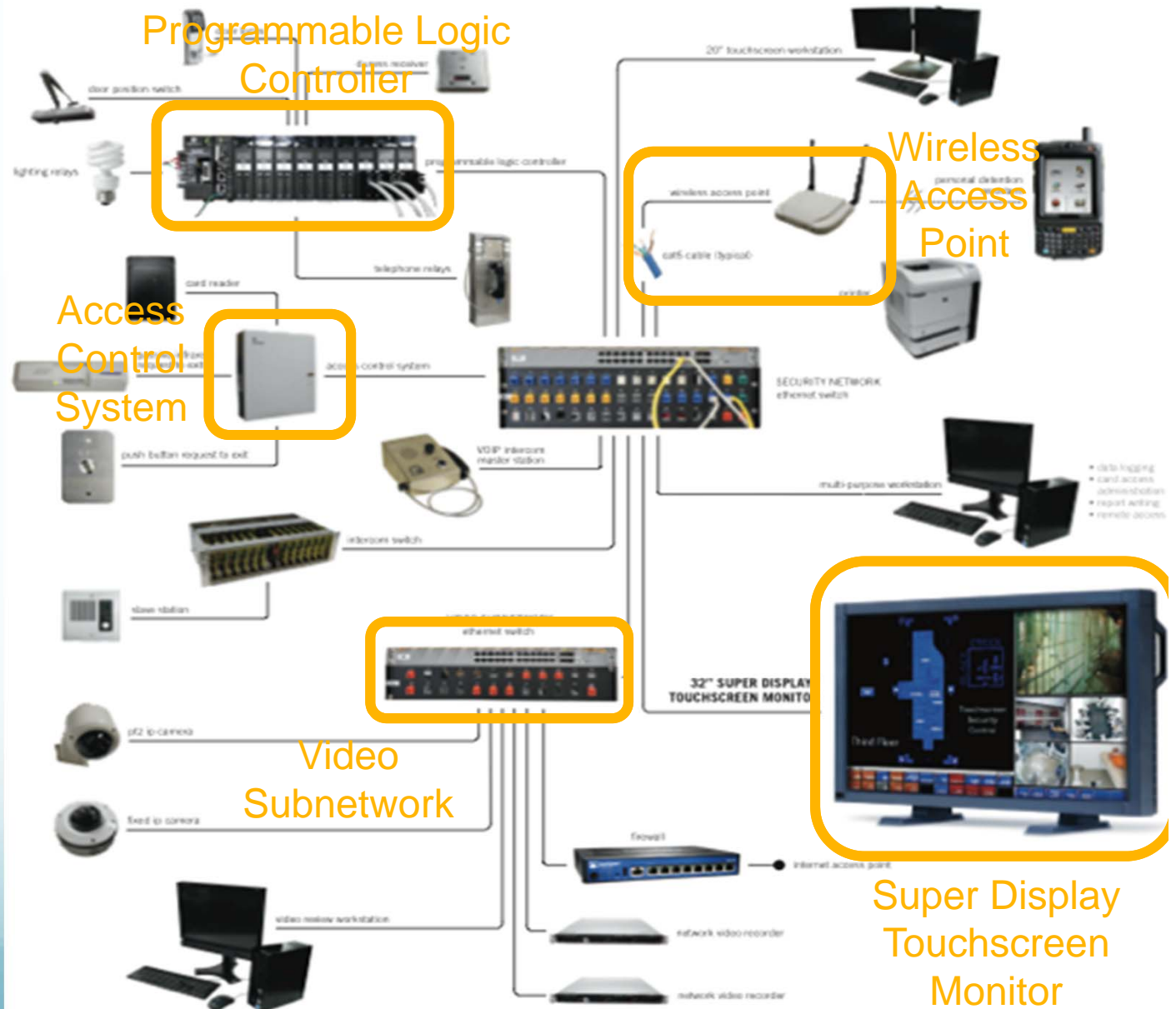
- All doors opened in maximum-security wing of prison
- Prisoners were free to leave their cells
- Two inmates attempted to attack rival gang member
- Targeted inmate suffered broke ankle and fractured vertebrae
- Took 3 minutes for additional guards to assist new guard on duty when system failed

# Computer System

Super Display System

by

Black Creek Integrated Systems



# Normal Functions & Operations

- System can control any electronic or electric device
  - Video surveillance
  - Intercoms
  - Water
  - Showers
  - Lighting
  - Card readers
  - Inmate phones
  - Doors
- Suspect glitch in “group release” feature
- Feature allows a guard to open cell doors simultaneously
- System should prompt guard to confirm action before opening all doors (implemented safeguard)

# Hazards

- Unauthorized access to control room
- Touchscreen not calibrated
- Network accessible via Internet



# Possible Failures & Faults

- Human Error
  - Security control room left unlocked or unattended
  - Guard accidentally triggers group release
- Vulnerabilities in architecture & configuration
- Infected USB
- Phishing attack
- Access to control system from another computer in the facility

# Conclusions

- Prison network should be secure, from inside and outside
- Black Creek needs to complete full assessment on group release feature
- Consider configuration of system and how computers on network can be used against main control system