Site Locking and Alerting Mechanism for Doors (SLAM-Doors)

Christopher Son

Aiden Seay

Preston Smith

Ryan Todd

Sponsored by:
General Dynamics Mission Systems

Client:
Benjamin Walker

Team Mentor:
Bailey Hall

NAU NORTHERN ARIZONA UNIVERSITY

Problem Statement

Coast Guard

- 11 missions which contribute to the security of the United States of America
- Operates military facilities across the U.S.
- Needs to ensure access control to shelter, areas, and facilities

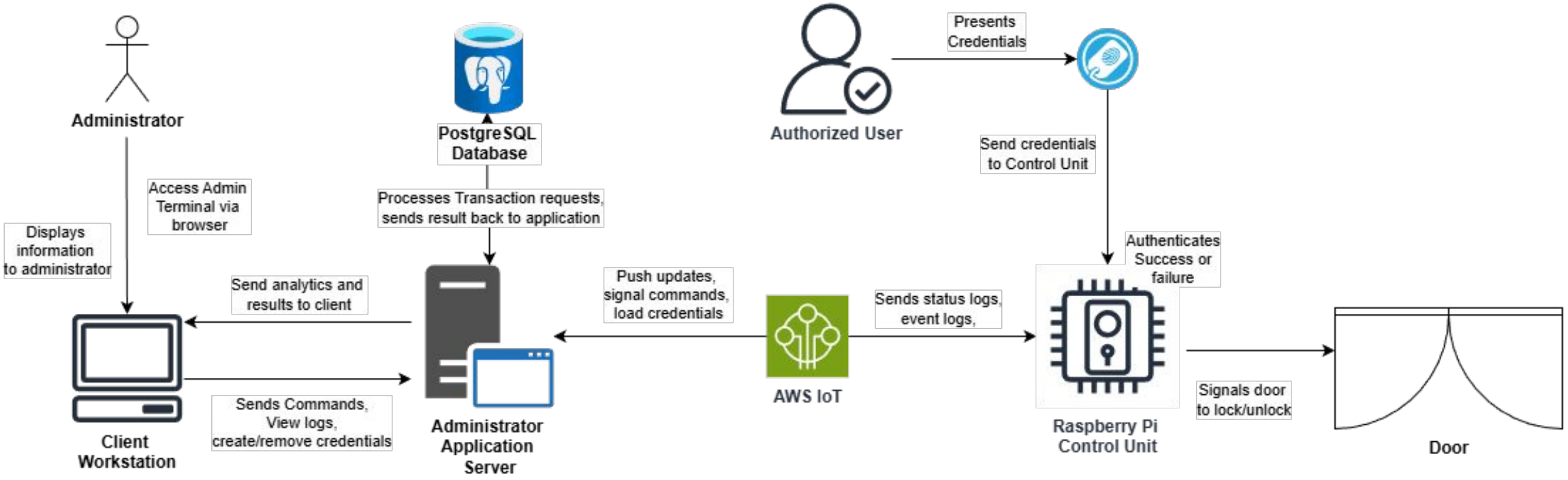
General Dynamics Mission Systems

- Uses Commercial Off-the-shelf (COTS) products to achieve secure access and control
- Current System's pitfalls
  - Unable to alert personnel of attempted access, unauthorized access, and external or internal attempts
  - Unable to save logs for audits
  - Unable to operate when power goes out

GENERAL DYNAMICS
Mission Systems

Solution Overview

Overhaul of the entire system



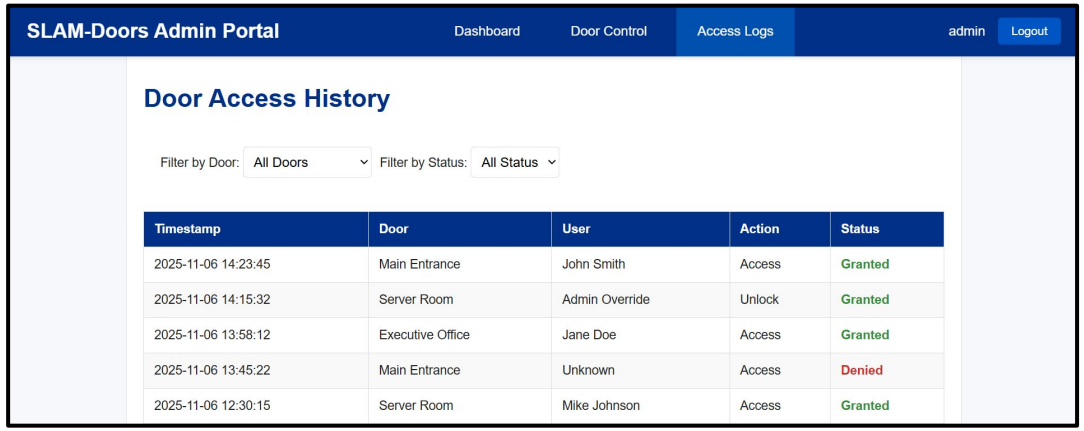
Key Requirements

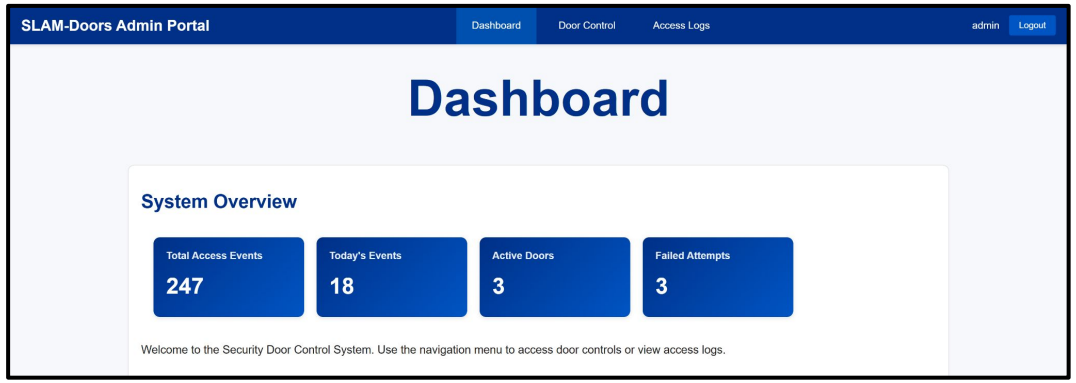
Requirements Development Process

- **GDMS** supplied a formal set of 15 system requirements defining **security**, **functionality**, and **performance** needs.
- Regular meetings with GDMS allowed us to clarify expectations and confirm our solution will align with their **technical** and **security standards**.
- Assessed **current** access-control **documentation** from GDMS to map out **missing capabilities** and define where enhanced logging, monitoring, and resilience are needed.

Minimum Viable Product (*MVP*)

- Secure **authentication** and **access control**.
- **Intrusion-state** monitoring and event reporting
- **Reliable** operation under **high latency** and outages.
- **Encrypted communication** and long-term event logging.





Requirements Breakdown

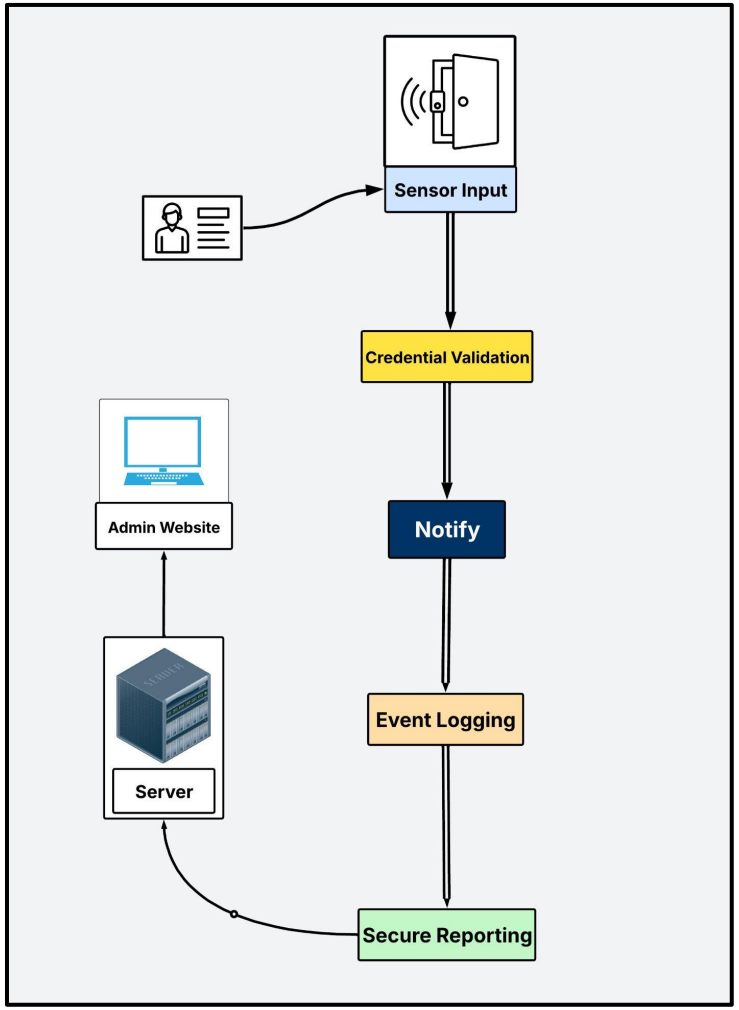
Access Events:

High-Level Requirement:

- *"The system shall detect and classify access events as (no-access, authorized, or unauthorized.)"*

Breakdown:

1. **Sensor Input** - Monitor door status, intrusion events, and tamper signals.
2. **Credential Validation** – Confirm RFID card ownership and corresponding user record.
3. **Classify –** Determine access state: authorized, unauthorized, or no-access.
4. **Notify** – Trigger cautionary alerts for unauthorized or abnormal events.
5. **Event Logging** – Forward events to the central server and database, storing them locally only when connectivity is unavailable.
6. **Secure Reporting** – Transmit classified events via encrypted communication channels.



Risks

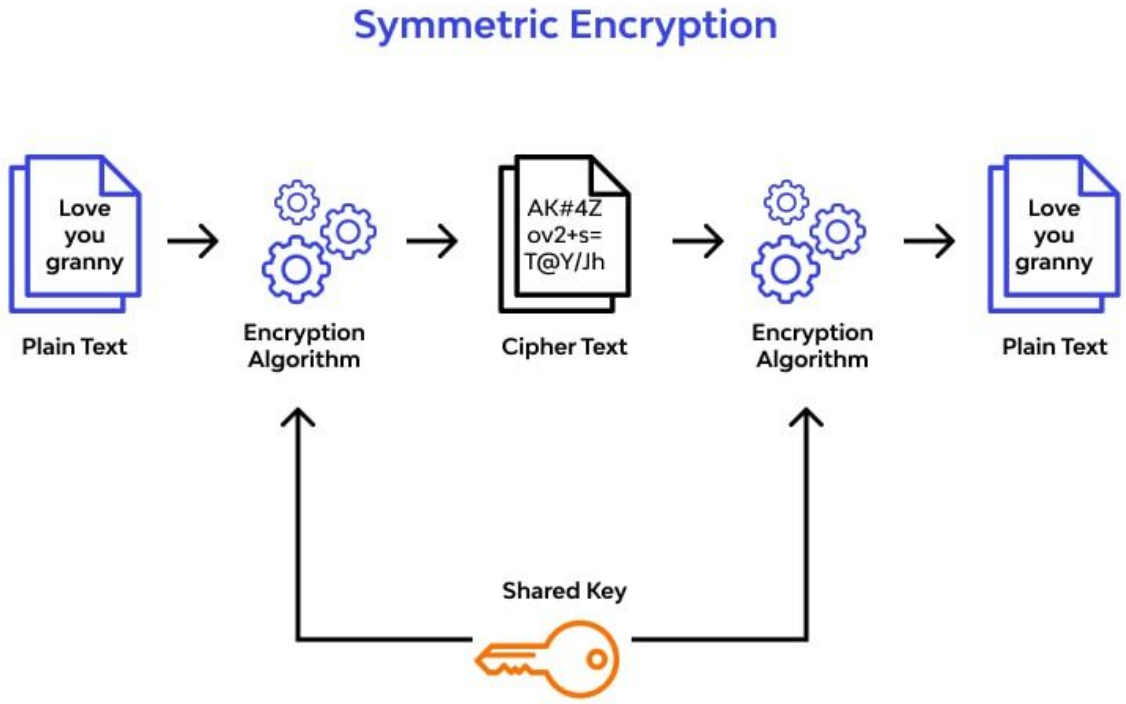
This project deals with a key government institution, and with that comes many **security** and **reliability** concerns.

Security concerns

- End to end encryption

Reliability concerns

- Backup power supply
- Redundant local storage



Source: https://www.wallarm.com/what/what-is-end-to-end-encryption

Feasibility

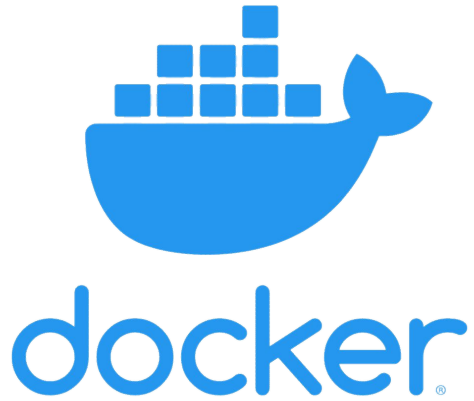
The technology and hardware have been thoroughly evaluated to ensure compatibility with the requirements of this system.

Amazon Web Services (AWS)

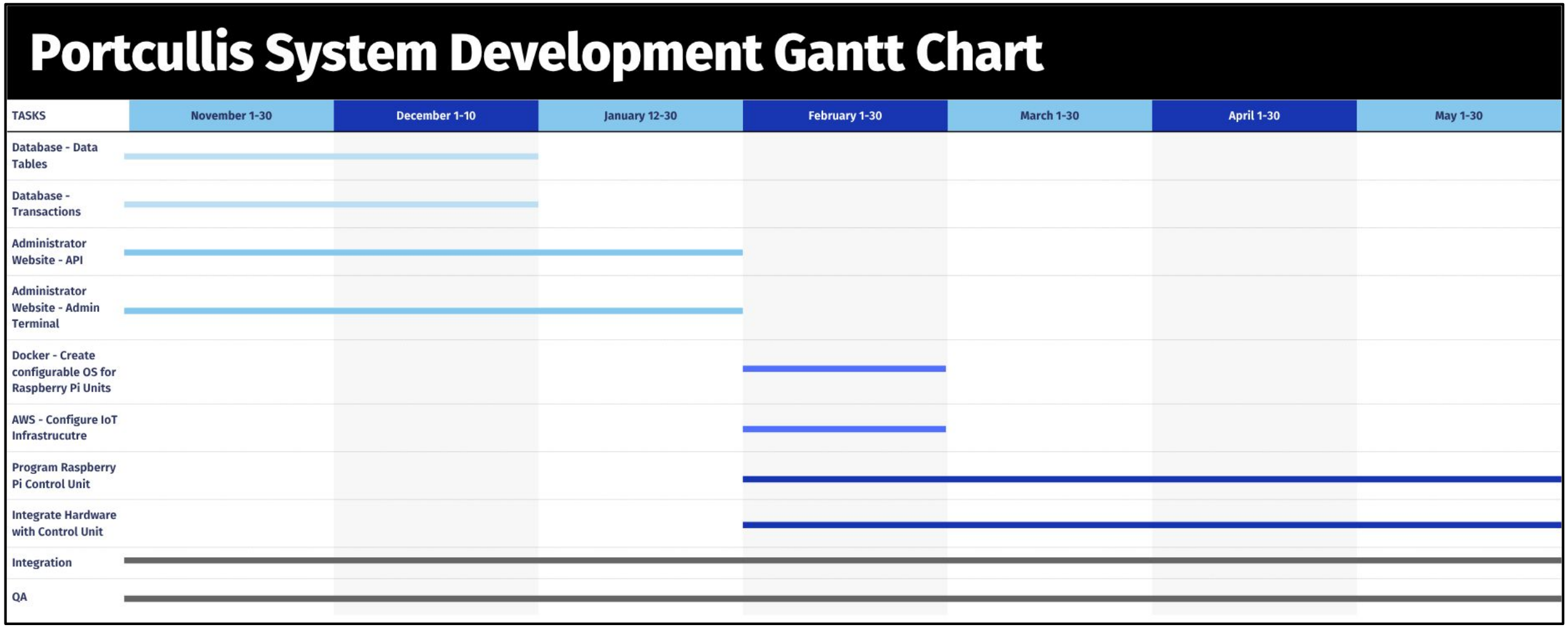
- Tool to host services
- Database, server, endpoints, etc.

Docker

- Containerized software
- Run on any system
- Simplifies updates



Schedule


Portcullis System Development Gantt Chart
TASKS
November 1-30
December 1-10
January 12-30
February 1-30
March 1-30
April 1-30
May 1-30
Database - Data Tables
Database - Transactions
Administrator Website - API
Administrator Website - Admin Terminal
Docker - Create configurable OS for Raspberry Pi Units
AWS - Configure IoT Infrastrucutre
Program Raspberry Pi Control Unit
Integrate Hardware with Control Unit
Integration
QA

Conclusion

- The Coast Guard requires a solution that addresses various pitfalls of current COTS systems
- The Portcullis team plans to build a new system from the ground up, utilizing:
  - Raspberry Pi
  - AWS
  - Web Application
  - And more…
- The new system addresses the pitfalls by
  - Logging access events
  - Alerting users of intrusion detection/attempts
  - Custom Raspberry Pi control unit
  - Access control system continues operation with no network or power

Thank you

NAU NORTHERN ARIZONA UNIVERSITY