CERIAS

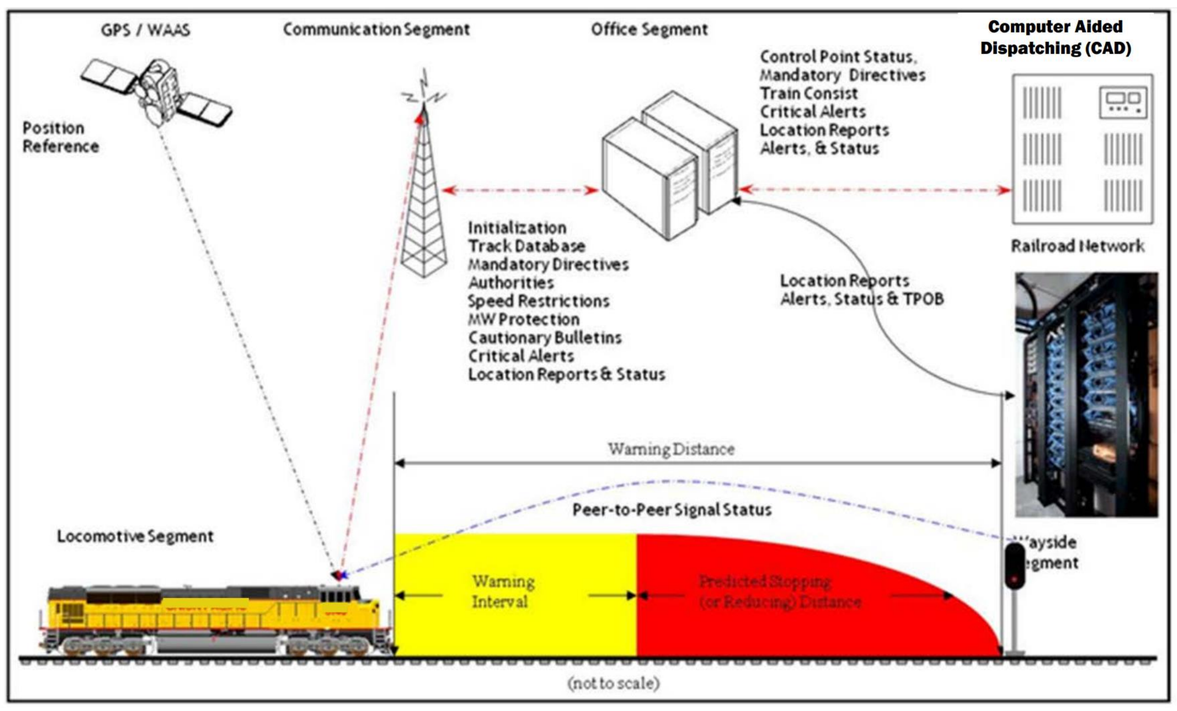
The Center for Education and Research in Information Assurance and Security

Small Trains, Big Risk: Physically Modeling Critical Freight Rail Infrastructure

Kira Sun, Courtney Falk

Motivation

According to the Association of American Railroads, freight rail accounts for 40% of freight in the US. And hazardous materials arrive safely more than 99% of the time. But the geographic scale of freight rail in the US, coupled with the need for many companies to interoperate, creates a large attack surface for adversaries. Our research is building a physical simulation of freight rail to model the cyber-physical risk and understand its impact. The final model will allow other researchers to interact with the cyber layer to test attacks.



The major components of a modern freight rail system. This diagram is from Meteorcomm's "ITCR 1.1 System Architecture Specification".

Threats

Rail networks rely on legacy components. These systems may lack key features such as cryptography and authentication needed to build a secure network. Newer components must interoperate with the legacy components to keep the rail lines working. Freight rail companies also operate the same business systems as other organizations which bring with them a whole host of new attack vectors. Freight rail companies are targets of ransomware gangs like Akira just the same as any other large enterprise.

The final model will include components designed to allow security researchers to test attack scenarios with the physical environment for immediate feedback. Virtualized enterprise desktop computer systems to handle the dispatching and planning tasks. Two software defined radios will form the wireless backhaul link along with a HackRF box to allow researchers access.

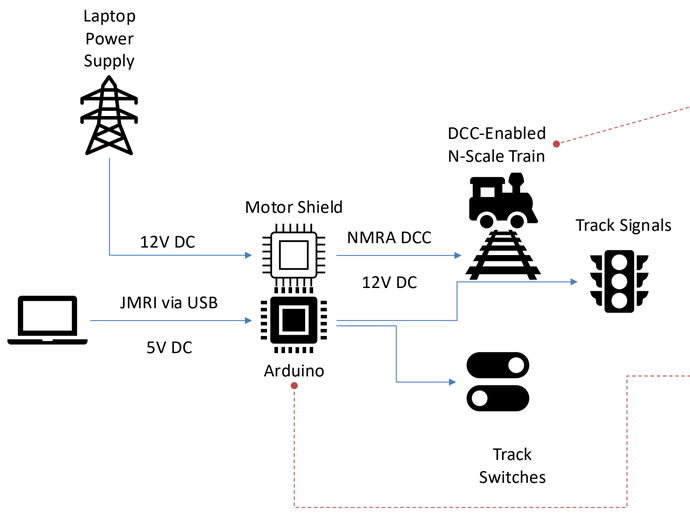
The derailed tank cars of a Norfolk Southern freight train in East Palestine, Ohio. The cars were carrying hazardous liquids that polluted the community.

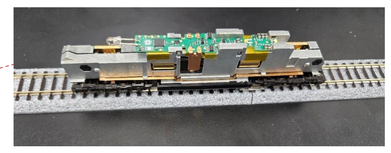
Implementation

Our implementation leverages commercial off-the-shelf technologies. Model railroad enthusiasts maintain a healthy ecosystem of open-source hardware and software solutions. Central to this is the DCC-EX package, which runs on an Arduino single-board microcontroller. DCC-EX can be remotely controlled via the JMRI library and tools.

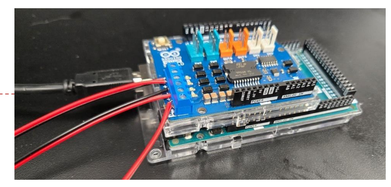
The Arduino requires an additional motor shield component because the Arduino itself runs on 5V DC but all the train components expect 12V DC. The motor shield passes the 12V power to the N gauge Kato tracks. Turnouts and signal lights also expect a 12V source.

Model train engines use the varying voltage of an analog controller to determine their speed. This also means that every engine on the same track will move in unison. These engines must be modified by inserting a digital decoder board. Digital decoder boards allow DCC-EX to individually address engines, allowing for independent movement around the track.





A Kato SD70M engine with a Digitrax decoder installed.



Arduino with motor shield running DCC-EX.

Thanks

Thanks to the Pacific Northwest National Laboratory (PNNL) for their CELR platform which served as motivation for this project. A special thanks to Bill Hoffer for taking the time to answer so many questions.

https://youtu.be/y9PO4ntUhn8?si=zDqvhApSmDJpjI0b

PURDUE UNIVERSITY

CERIAS