How Can We Evolve Cyber Physical Security Policies to Automatically Manage Changing Threats?

Joseph Hallett
How Can We Avoid Having Everything Being On Fire?

Joseph Hallett
Cyber Physical Systems are *Everywhere*
Smart Water Treatment Plants
Smart Power Generation
Smart Factories
Autonomous Vehicles

IOT
Windows is shutting down...
HOW DO WE DEFEND AGAINST THIS?
So what's the problem?
I'll just put this over here with the rest... of the fire.
Handwritten policies do not scale
The threat landscape isn’t static

50,000,000,000,000
How do we fix this?
HARD CODING
Catalogue of identified threats against the running of the system
Mitigation controls for handling the threats
Policy Language selects mitigations based on threats and reconfigures the CPS.
Running in a MAPE-K loop...

threat posture
policy deployment and enforcement

Monitor → Analyze → Plan → Execute

Threat Catalogue

best practices and standards
policy adaptation
Automation
Automation

(should scale)
No ad-hoc reconfiguration
No ad-hoc reconfiguration

(should react faster too)
Why is this controversial?
Dynamic reconfiguration in a MAPE-K loop is not new
I CAN RECONFIGURE UR TOWN?
MR. STARK...
I DON'T FEEL SO GOOD
THIS WILL INCREASE THE ATTACK SURFACE
50,000,000,000,000