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

Joseph Hallett

University of
BRISTOL

How Can We Avoid Having Everything Being On Fire?

Joseph Hallett

University of BRISTOL

Cyber Physical Systems are *Everywhere*

50,000,000,000

Smart Offices

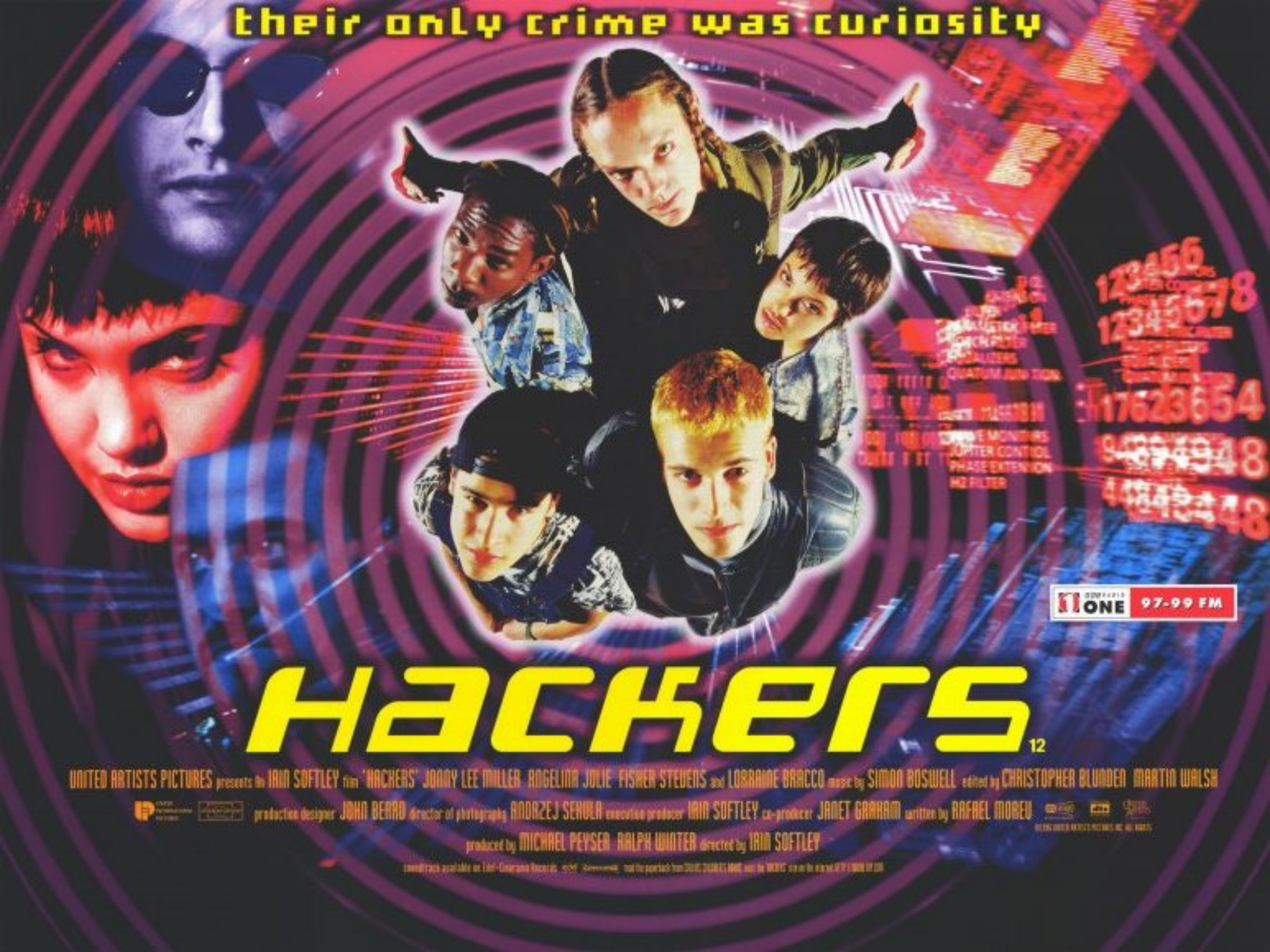
Smart Water Treatment Plants

Smart Power Generation

Smart Factories

Autonomous Vehicles

IOT



their only crime was curiosity

HACKERS

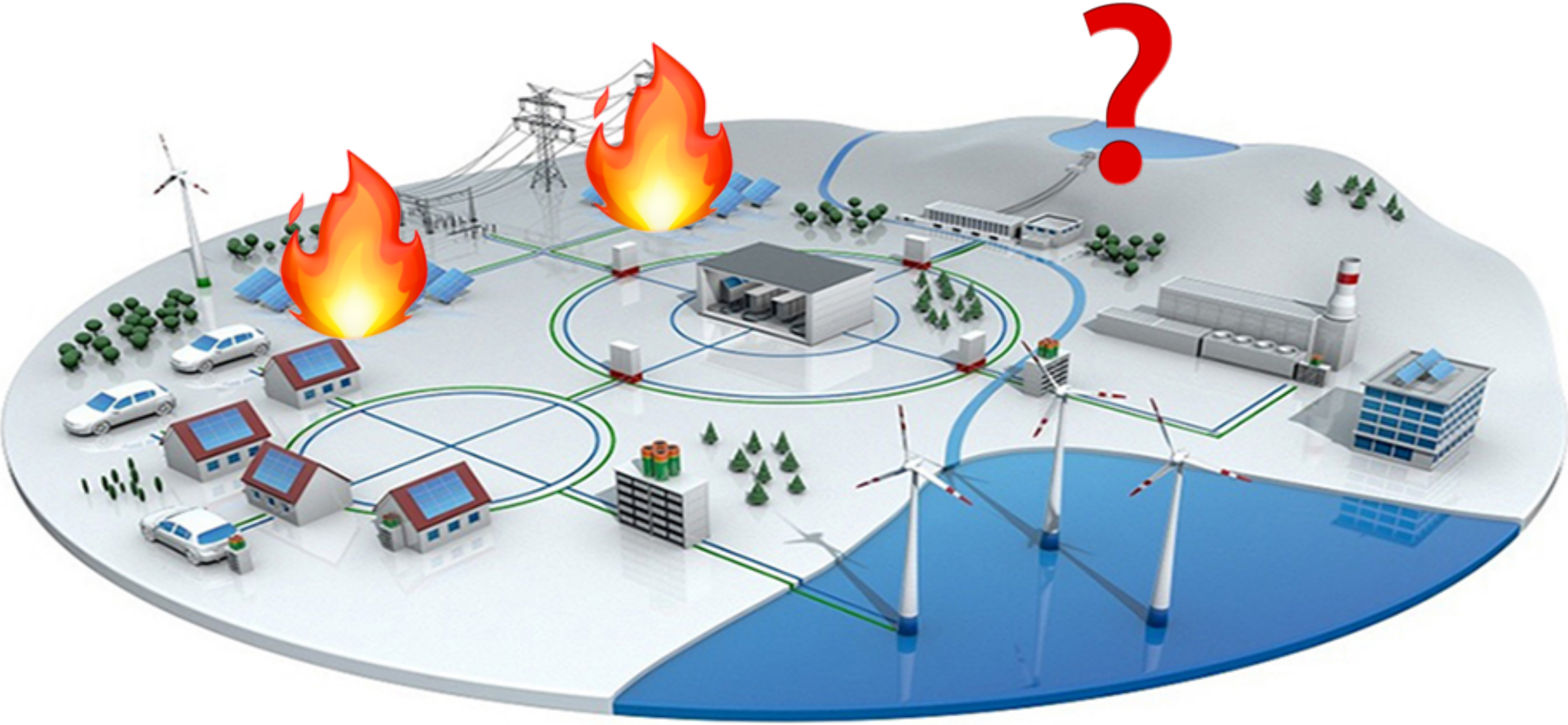
12

UNITED ARTISTS PICTURES presents An IAIN SOFTLEY film "HACKERS" JONNY LEE MILLER ANGELINA JOLIE FISHER STEVENS and LORRAINE BRACCO music by SIMON BOSWELL edited by CHRISTOPHER BLUNDEN MARTIN WALSH

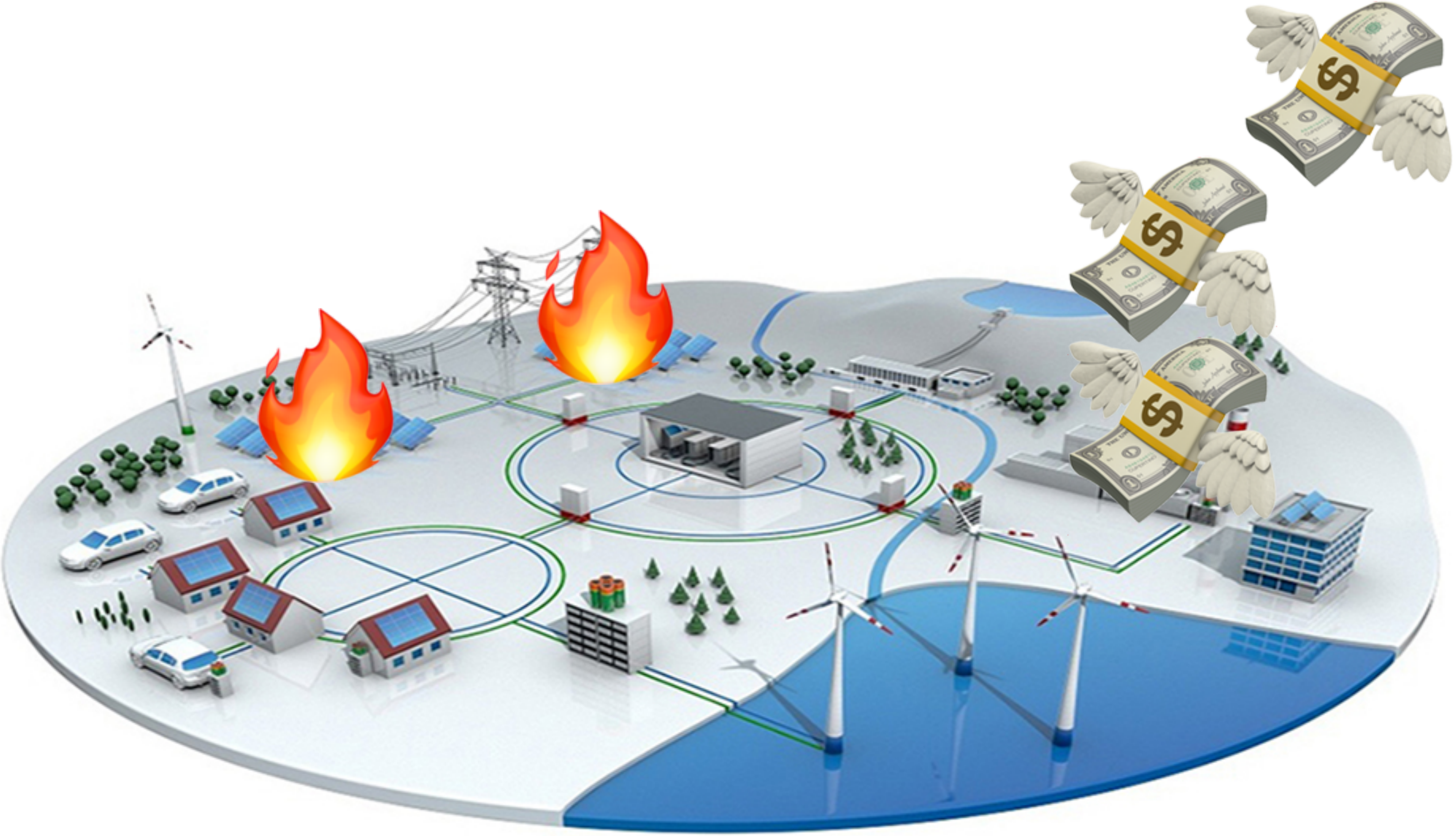
production designer JOHN BEARD director of photography ANDRZEJ SEKULA executive producer IAIN SOFTLEY co-producer JANET GRAHAM written by RAFAEL MOREU

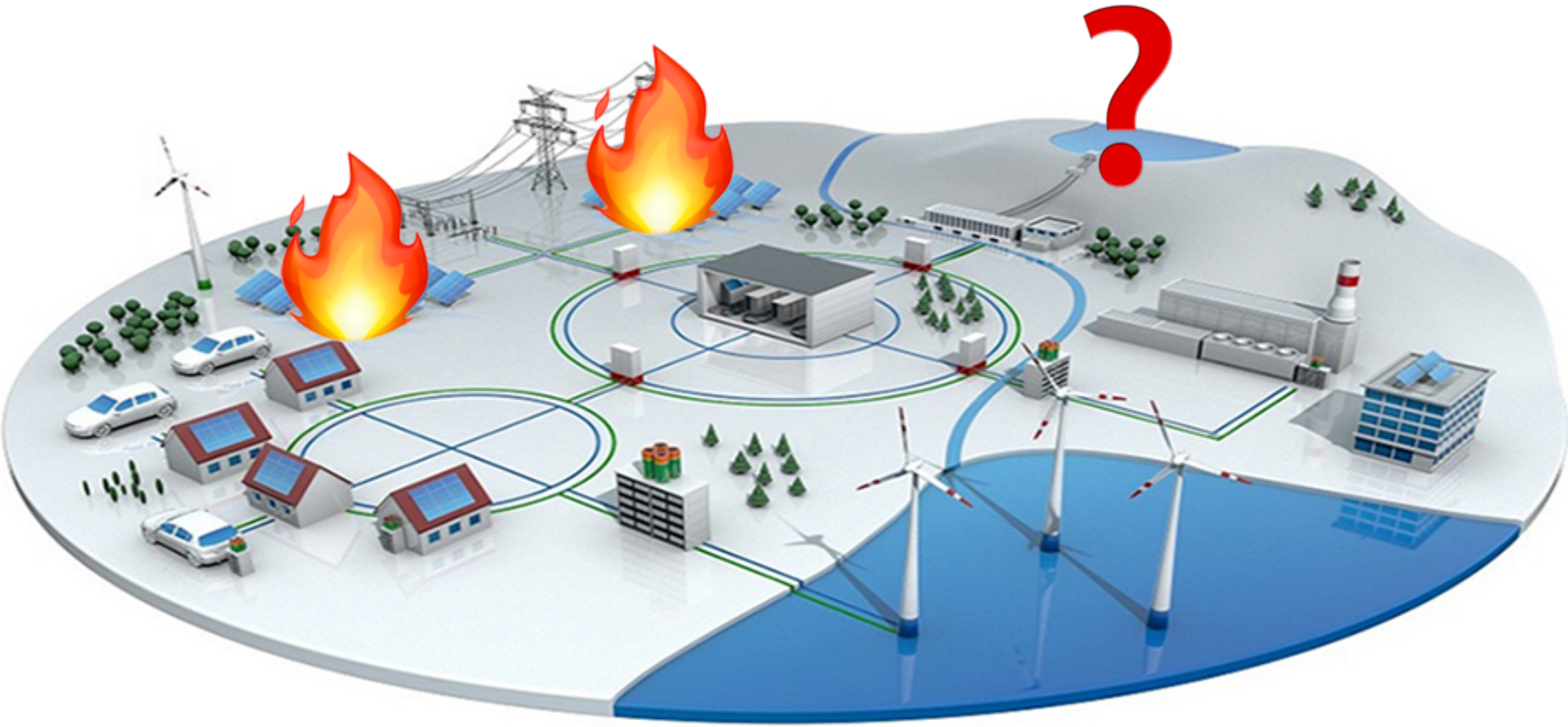
produced by MICHAEL PEYSER RALPH WINTER directed by IAIN SOFTLEY

soundtrack available on Edel-Cinerama Records [illegible]



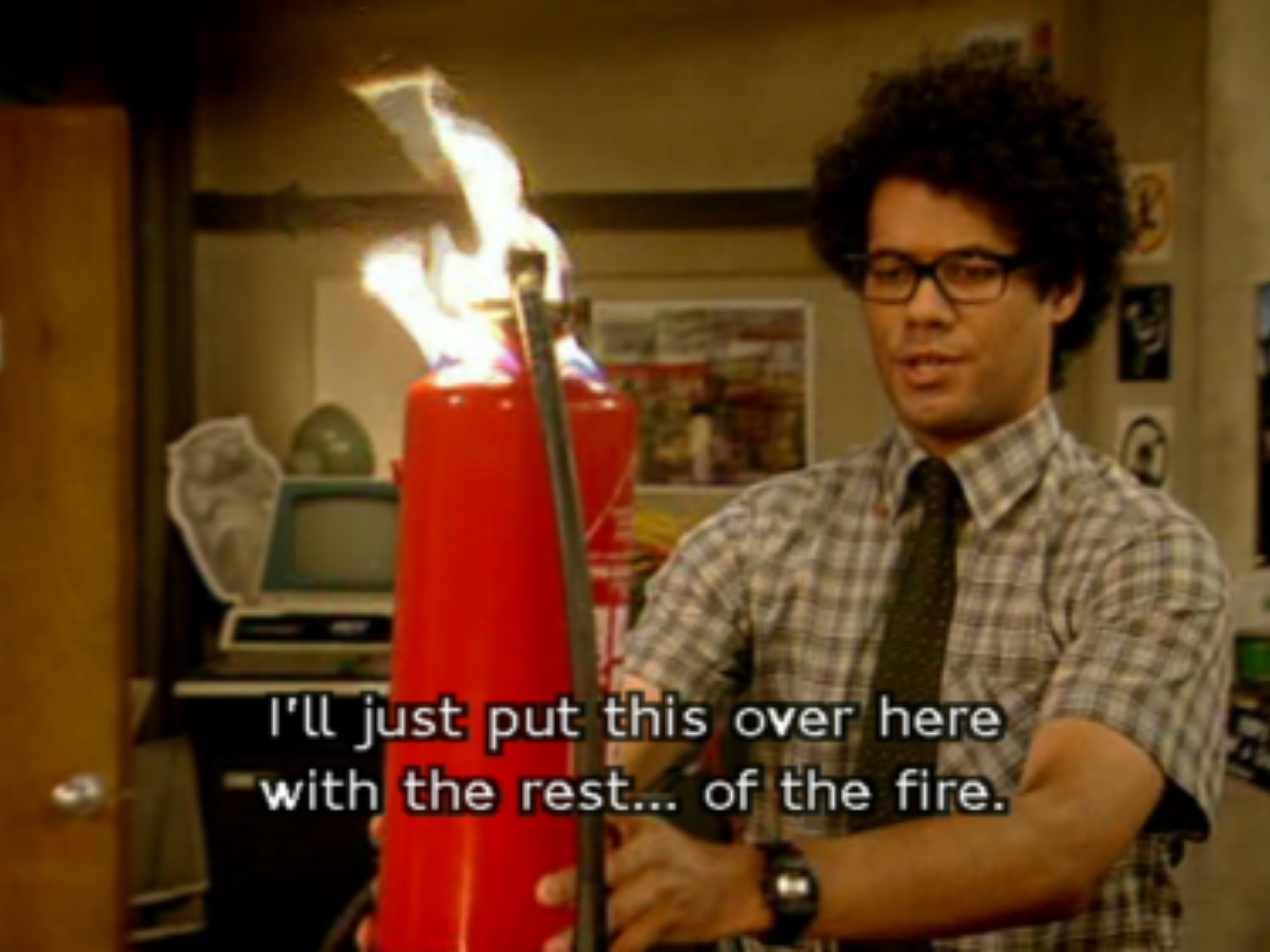
Windows is shutting down...





HOW DO WE DEFEND AGAINST THIS?

So what’s the problem?


I'll just put this over here
with the rest... of the fire.

50,000,000,000

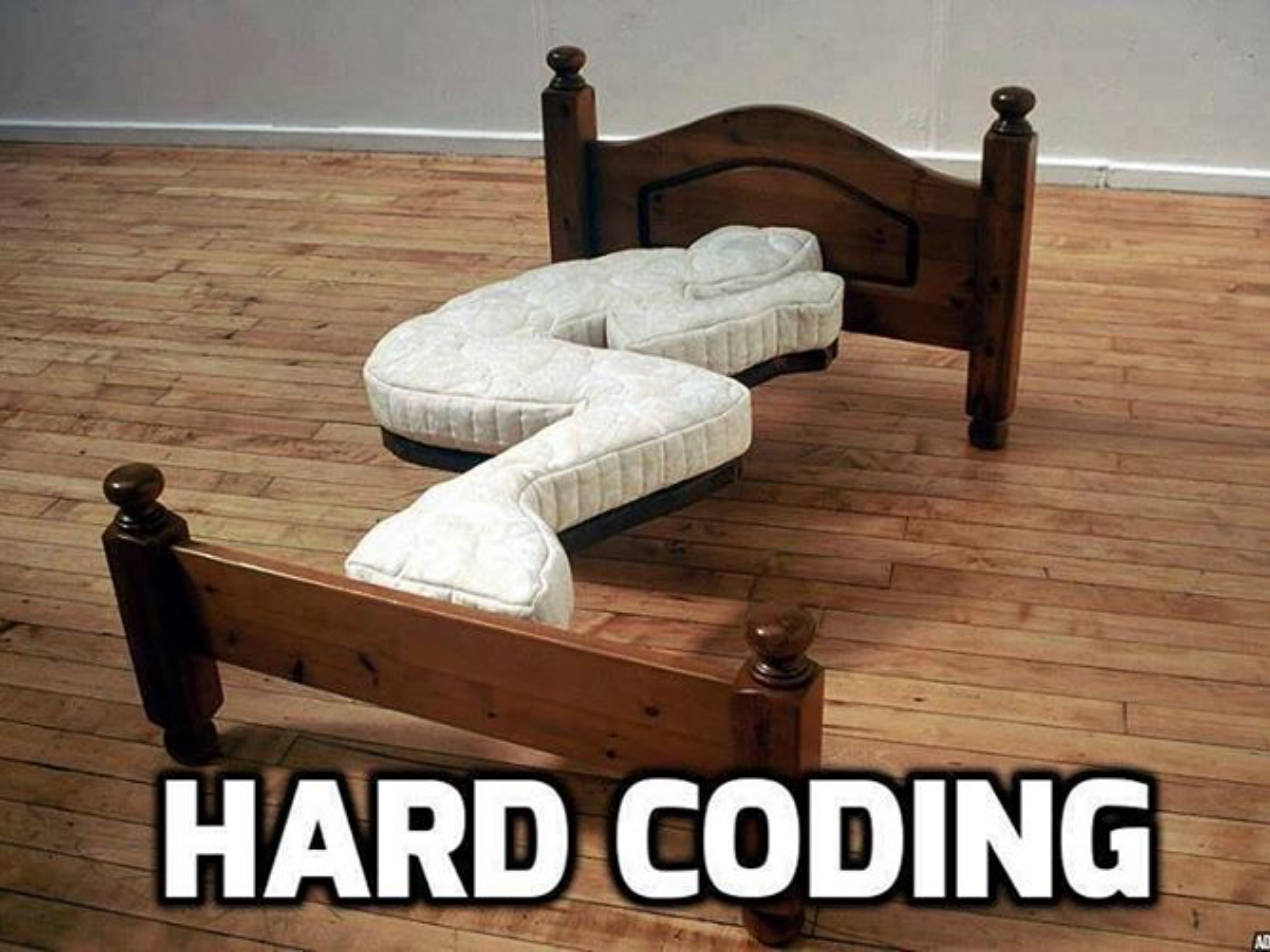
Handwritten policies do not scale

50,000,000,000

The threat landscape isn't static

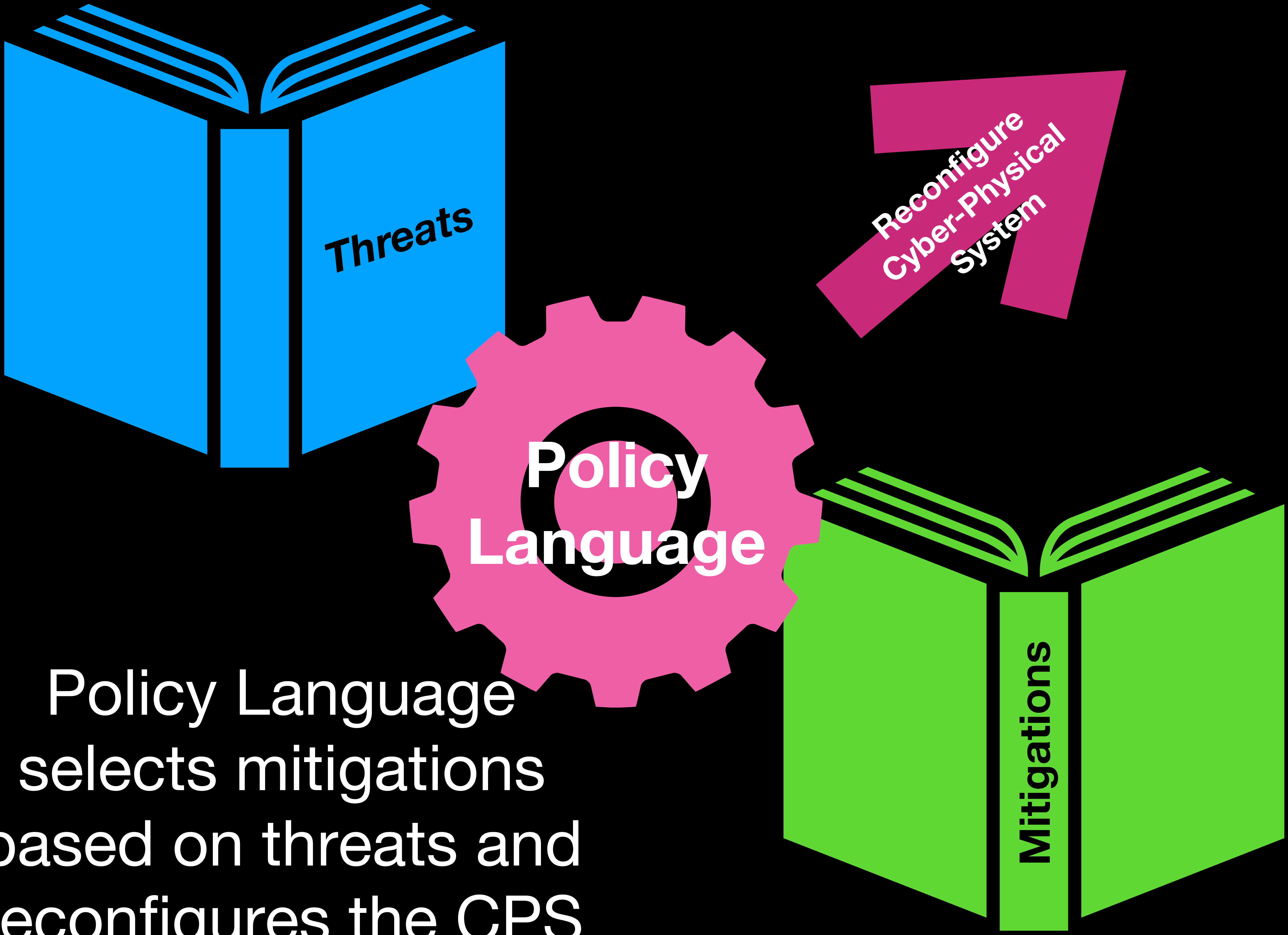
50,000,000,000

How do we fix this?


HARD CODING

Catalogue of identified threats against the running of the system

Mitigation controls for handling the threats

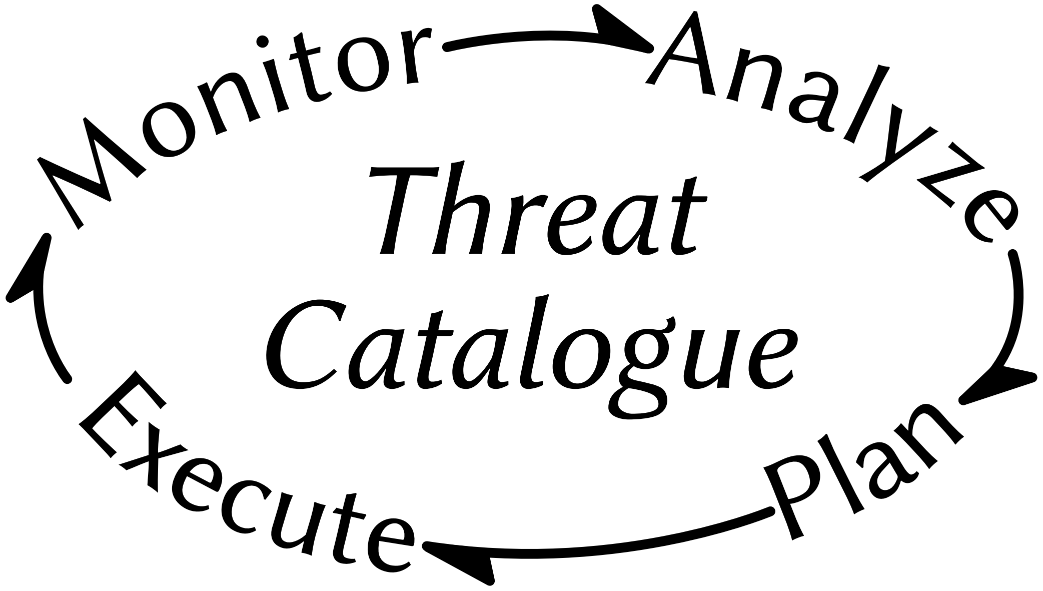


Policy Language selects mitigations based on threats and reconfigures the CPS

Running in a MAPE-K loop...

threat posture

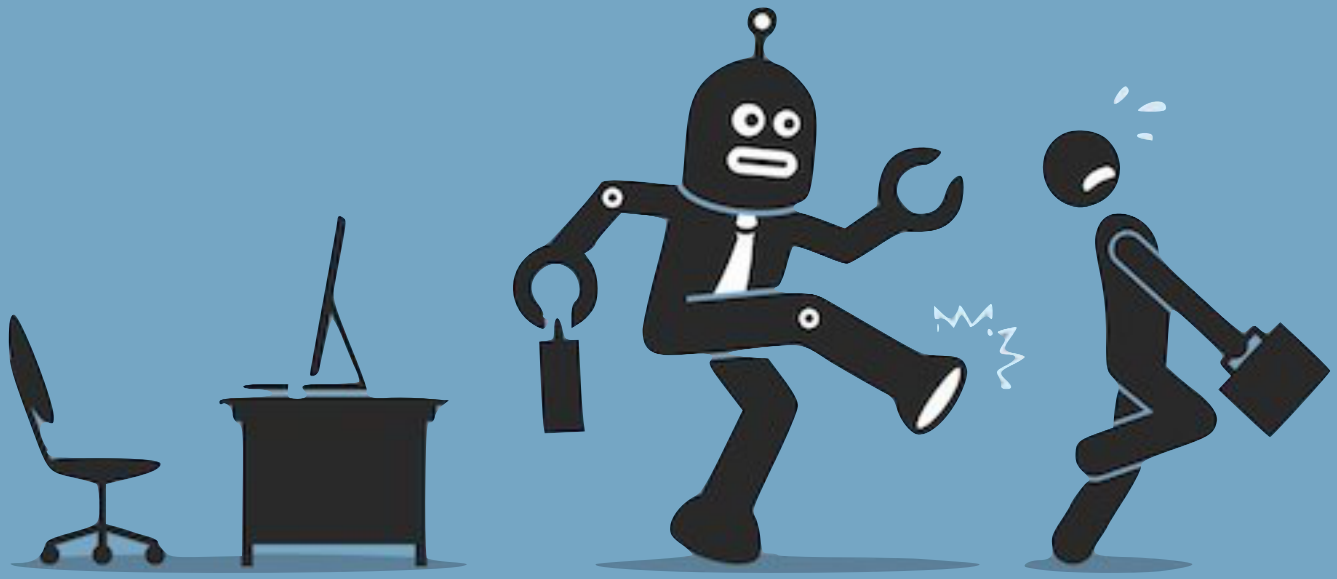
best practices
and standards



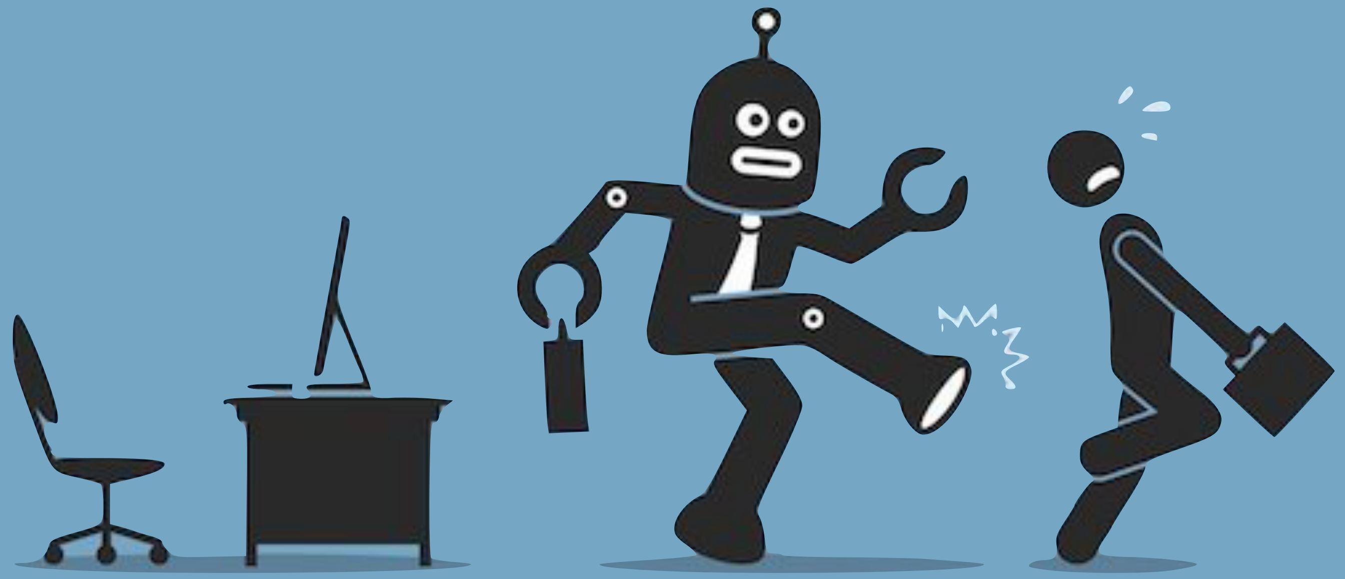
policy deployment
and enforcement

policy adaptation

Automation

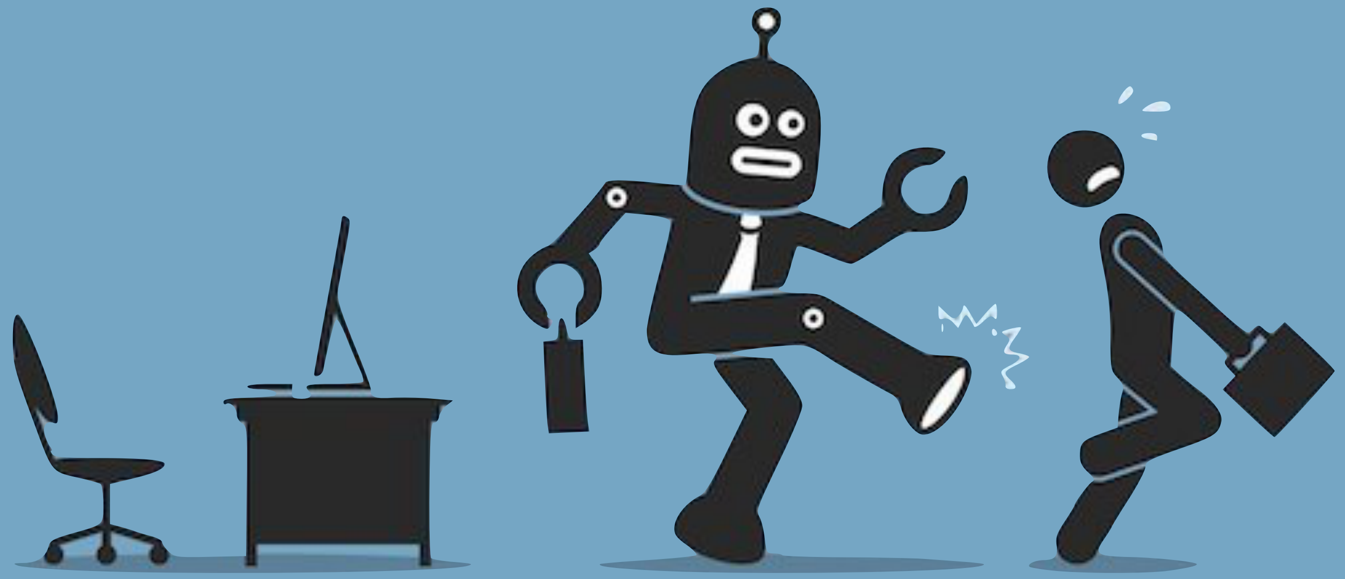


Automation

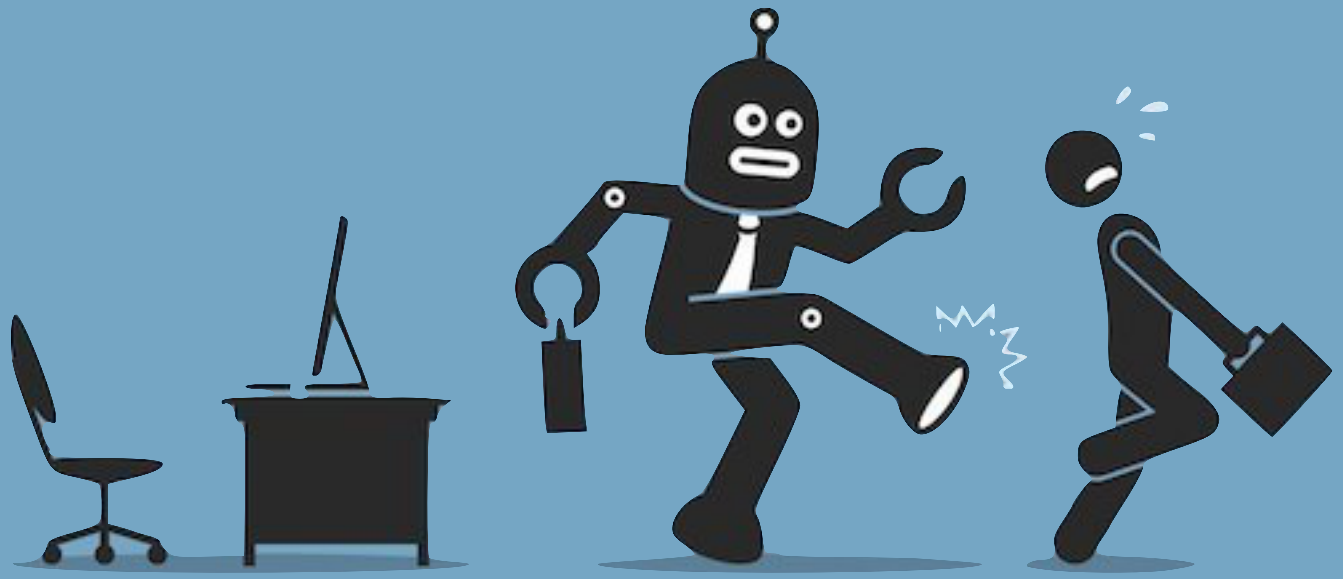


(should scale)

No ad-hoc reconfiguration



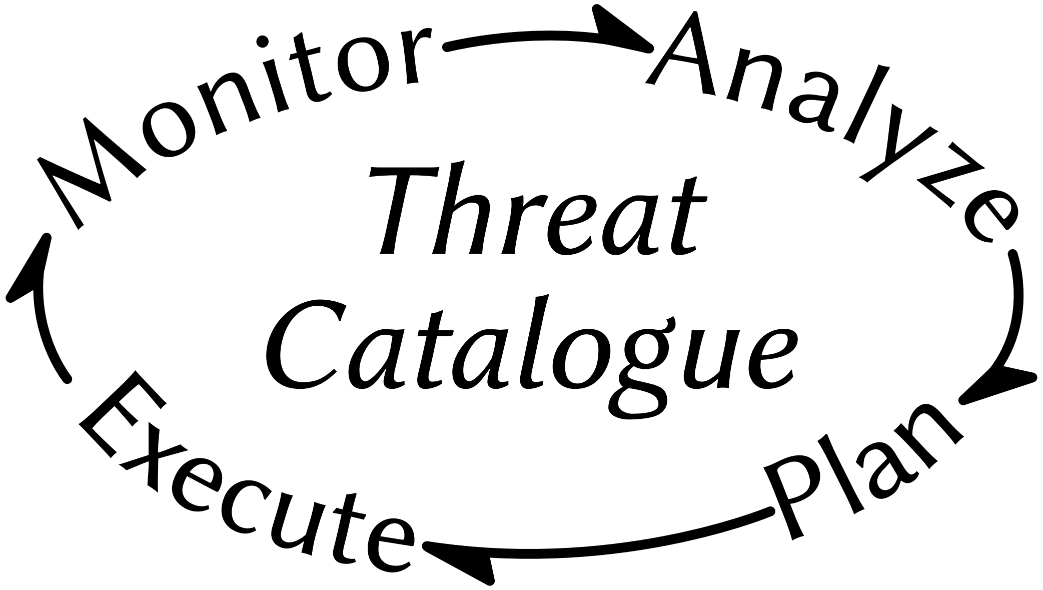
No ad-hoc reconfiguration



(should react faster too)

Why is this controversial?

Dynamic reconfiguration in a MAPE-K loop is not new



threat posture

Monitor

Analyze

best practices
and standards

*Threat
Catalogue*

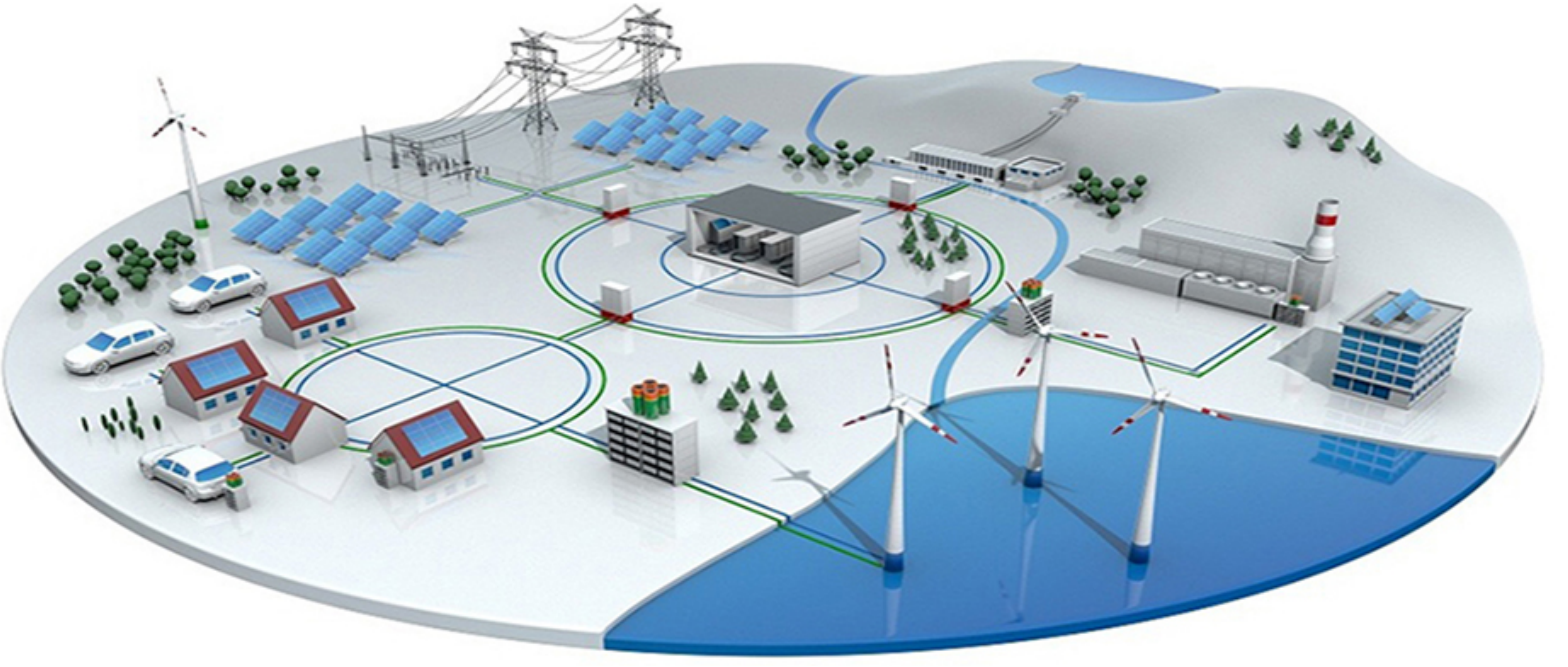
policy deployment
and enforcement

Execute

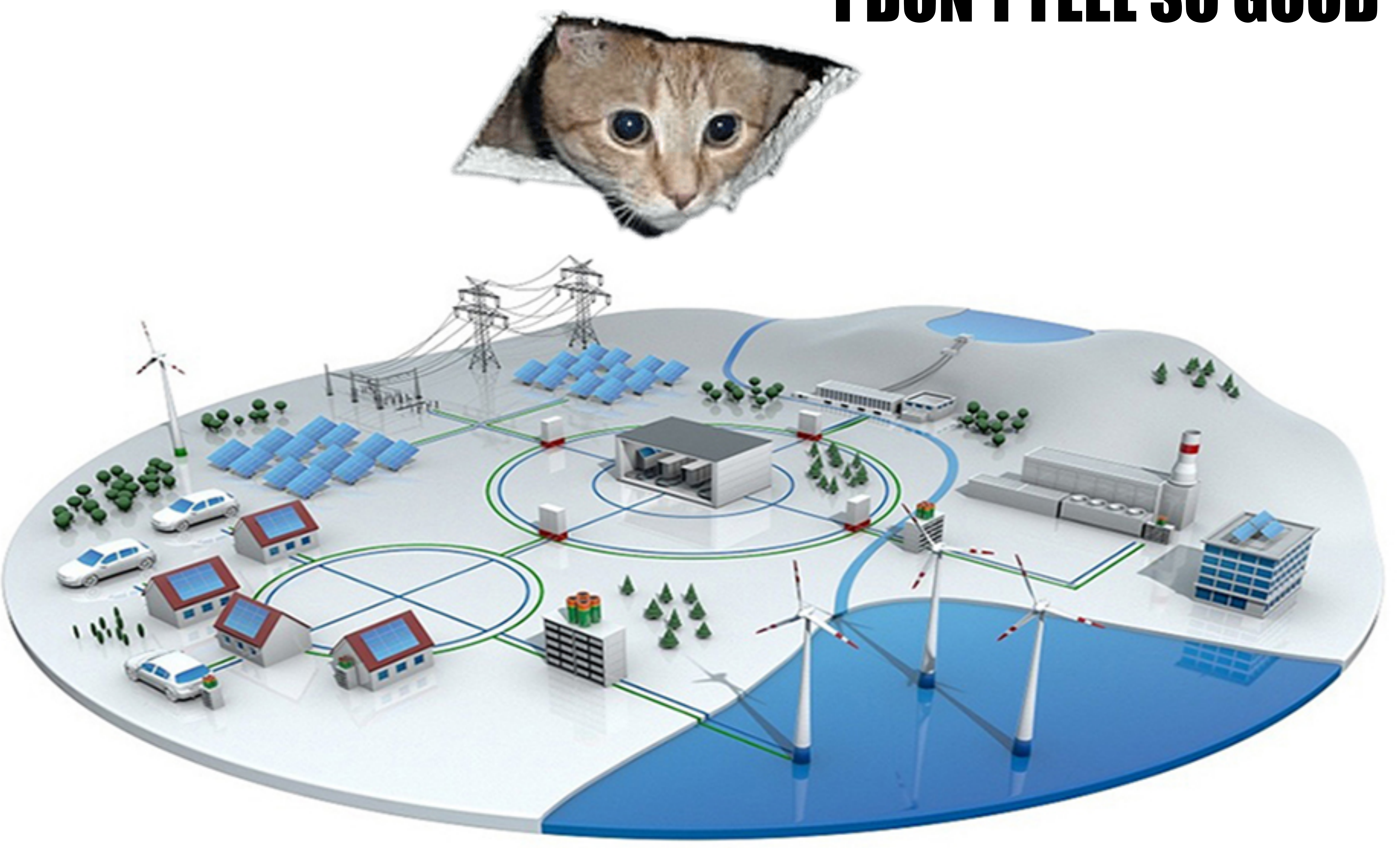
Plan

policy adaptation

I CAN RECONFIGURE UR TOWN?



MR. STARK...
I DON'T FEEL SO GOOD



THIS WILL INCREASE THE ATTACK SURFACE

50,000,000,000