THE POWER OF
PASSIVE CYBER DEFENSE

Ralph Langner ▪ The Langner Group

WE LIVE IN THE DARK AGES OF CYBER SECURITY

History is static

Tomorrow will look the same like today

Promoting methods („best practices“)

that didn‘t work all that well

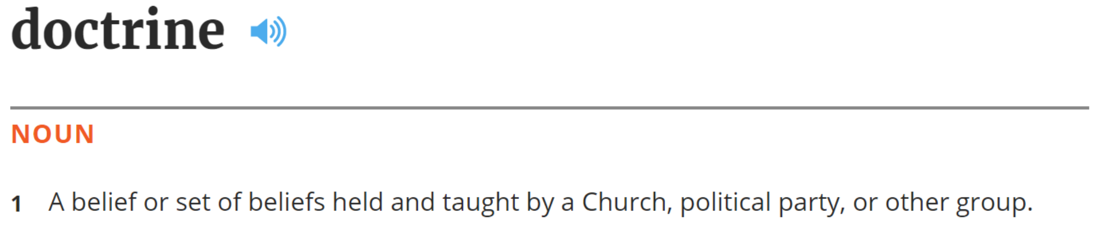
best practice in medicine for hundreds of years

best practice in IT security for decades

SECURITY PATCHES

ANTI-VIRUS

PASSWORD POLICIES



doctrine

NOUN

1 A belief or set of beliefs held and taught by a Church, political party, or other group.

hackers & malware

endpoints & networks

information security (C/I/A)

security awareness raising

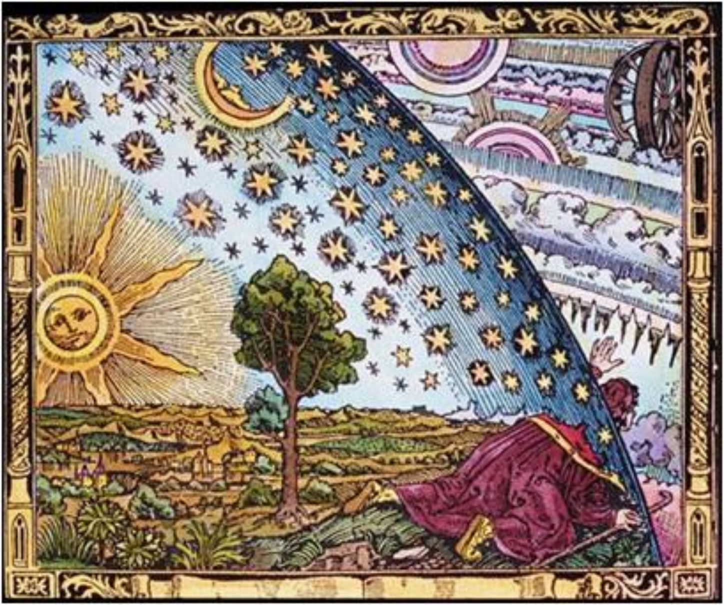
information sharing

risk management

Data artifacts

Hacking

Risk



Hybrid systems

Context & metadata

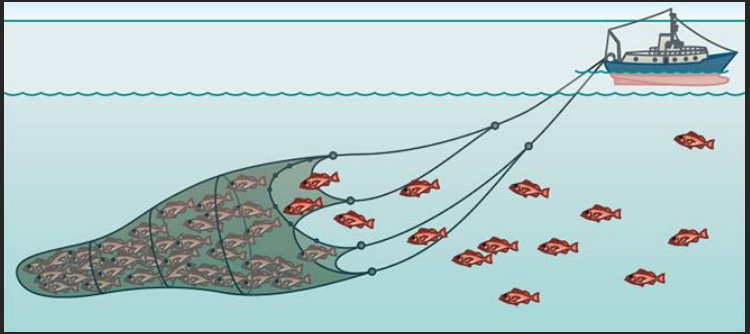
User behavior analytics

Crowdsourcing

Anti-dogma

(risk management, C/I/A)

CROWDSOURCING: EARLY DETECTION



How modern cyber attack campaigns work

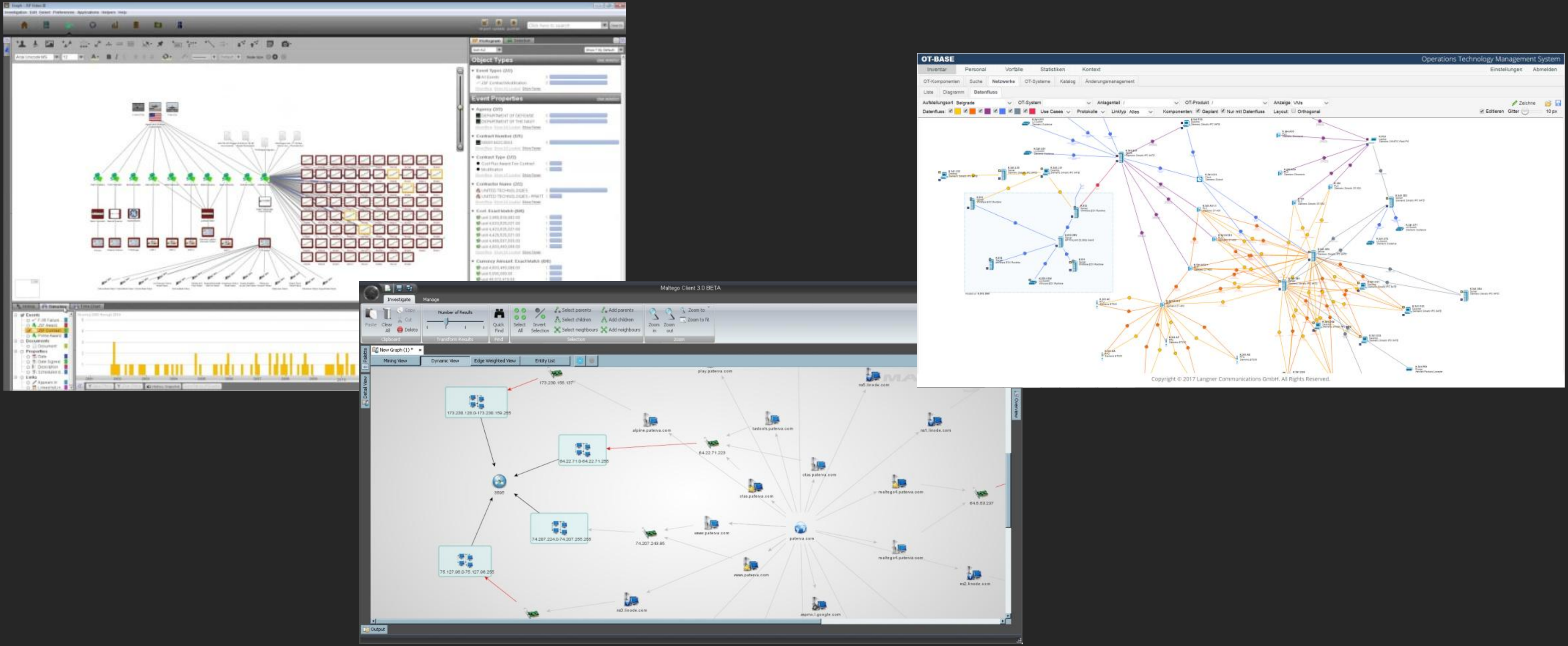
Time and effort to compromise must not be substantially lower than time and effort to detection of breach

How modern IoC analytics works

SECURITY AUTOMATION: SCALEABILITY

DARPA Cyber Grand Challenge 2016

ADVANCED ANALYTICS OF HYBRID SYSTEMS: TAMING COMPLEXITY



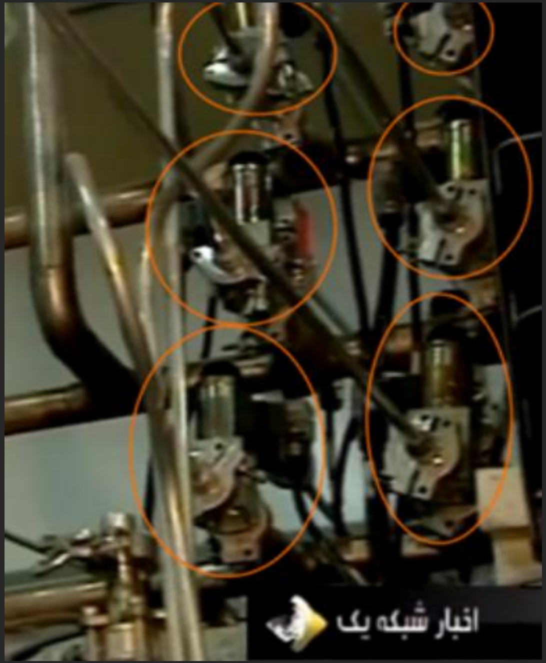
MODEL-DRIVEN SYSTEMIC VULNERABILITY ANALYSIS

This doesn't work – because physical objects and processes have LOW ENTROPY.

Low entropy limits the system's state space and attack opportunities.

It makes these systems defendable.

UNDERSTANDING ENTROPY

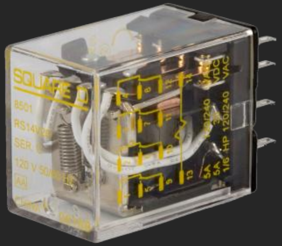


From: R. Langner, „To kill a centrifuge"

Typical actuators have a small set of normal states and of abnormal states, for example:

-open/close

-cycle/stick

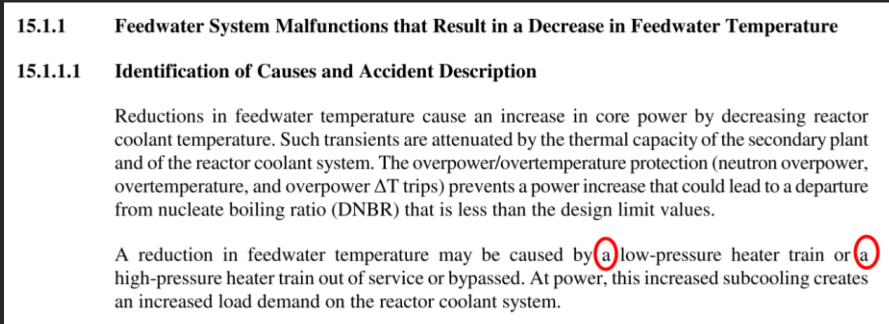


UNDERSTANDING ENTROPY

Most physical processes used in critical infrastructure are surprisingly simple and static

PROVOKING RARE EVENTS DIGITALLY: NPP EXAMPLE

Safety analysis



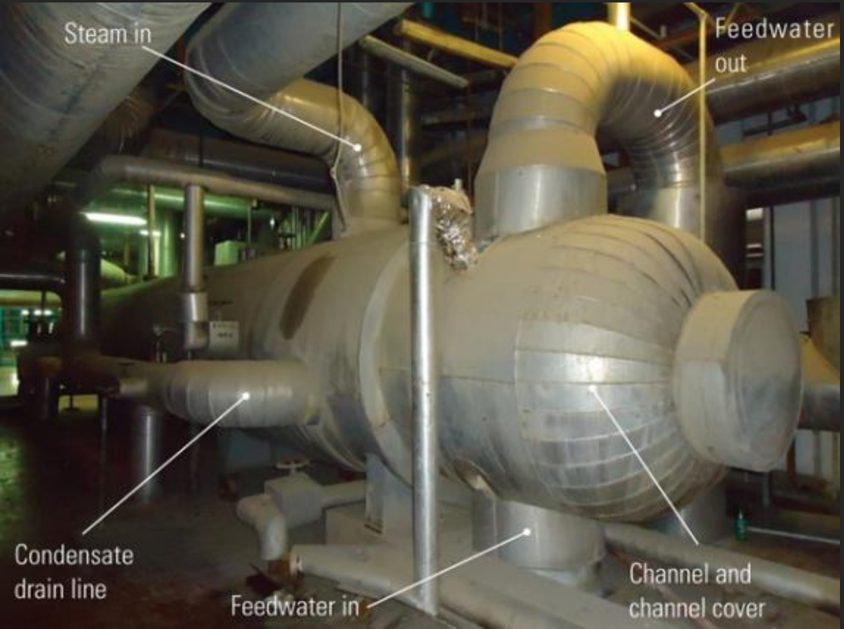
15.1.1 Feedwater System Malfunctions that Result in a Decrease in Feedwater Temperature

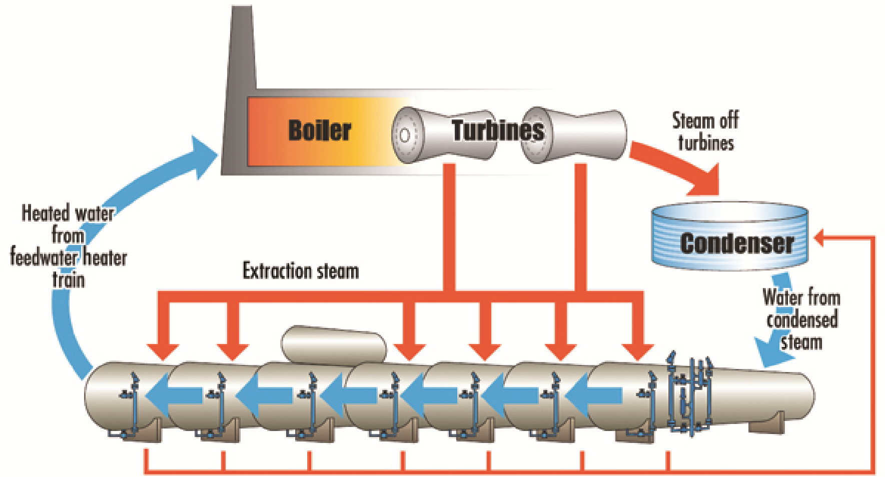
15.1.1.1 Identification of Causes and Accident Description

Reductions in feedwater temperature cause an increase in core power by decreasing reactor coolant temperature. Such transients are attenuated by the thermal capacity of the secondary plant and of the reactor coolant system. The overpower/overtemperature protection (neutron overpower, overtemperature, and overpower ΔT trips) prevents a power increase that could lead to a departure from nucleate boiling ratio (DNBR) that is less than the design limit values.

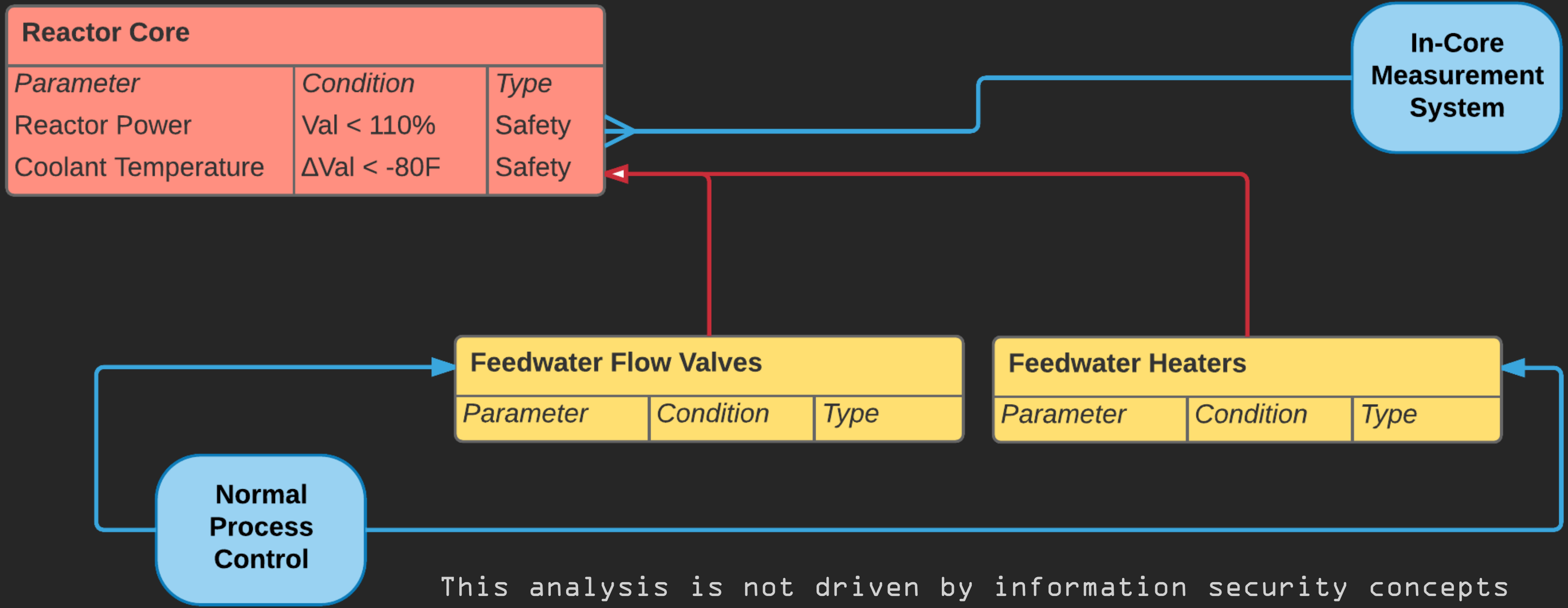
A reduction in feedwater temperature may be caused by a low-pressure heater train or a high-pressure heater train out of service or bypassed. At power, this increased subcooling creates an increased load demand on the reactor coolant system.

Feedwater pre-heater




Boiler
Turbines
Steam off turbines
Condenser
Heated water from feedwater heater train
Extraction steam
Water from condensed steam

MODEL-DRIVEN SYSTEMIC VULNERABILITY ANALYSIS



Reactor Core

Parameter	*Condition*	*Type*
Reactor Power	Val < 110%	Safety
Coolant Temperature	ΔVal < -80F	Safety

Feedwater Flow Valves

Parameter	*Condition*	*Type*

Feedwater Heaters

Parameter	*Condition*	*Type*

This analysis is not driven by information security concepts but by cybernetics

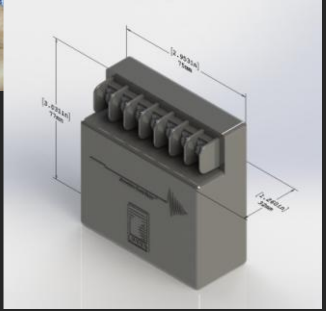
ANALOG CONTROL

One of these can't be hacked

ANALOG CONTROL

Operation Rock Ridge

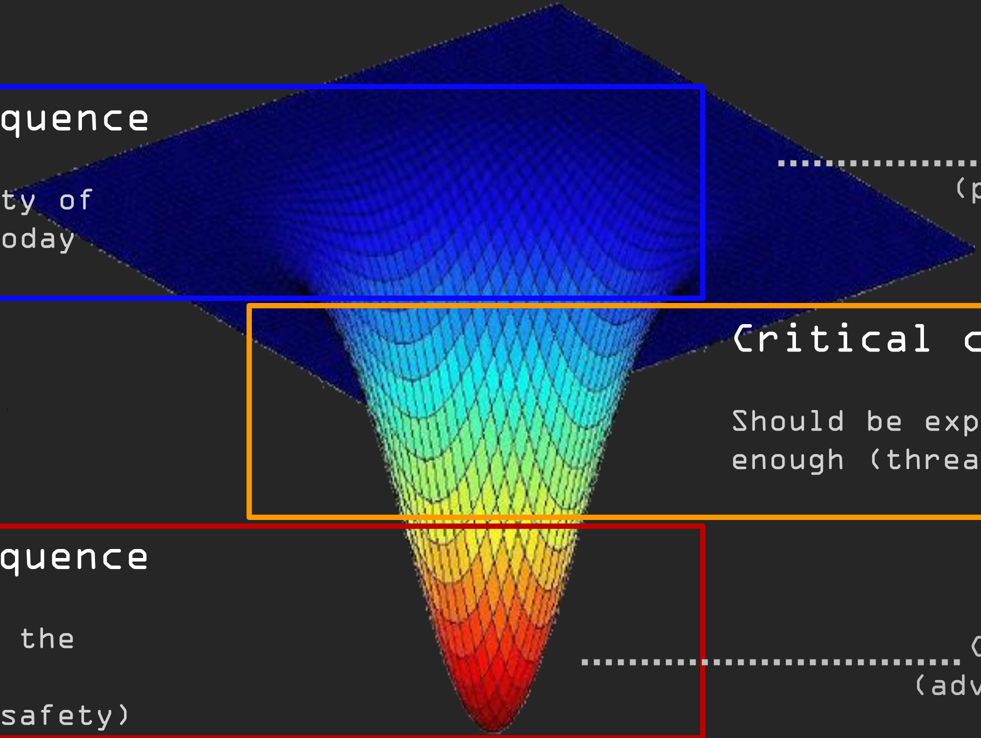
(Tim Roxey)



Westinghouse ALS

(FPGA based)

CYBERSPACE IS NON-LINEAR



Non-critical consequence

This is where the majority of „cyber attacks“ happen today

Efficiency (positive non-linearity / anti-fragility)

Critical consequence

Should be expensive and unreliable enough (threat actor triage)

Unacceptable consequence

Should be impossible for the attacker to achieve (Baseline reliability & safety)

Core functionality (adverse non-linearity / fragility)

Q&A

Ralph Langner ▪ The Langner Group

www.langner.com ▪ rl@langner.com ▪ @langnergroup