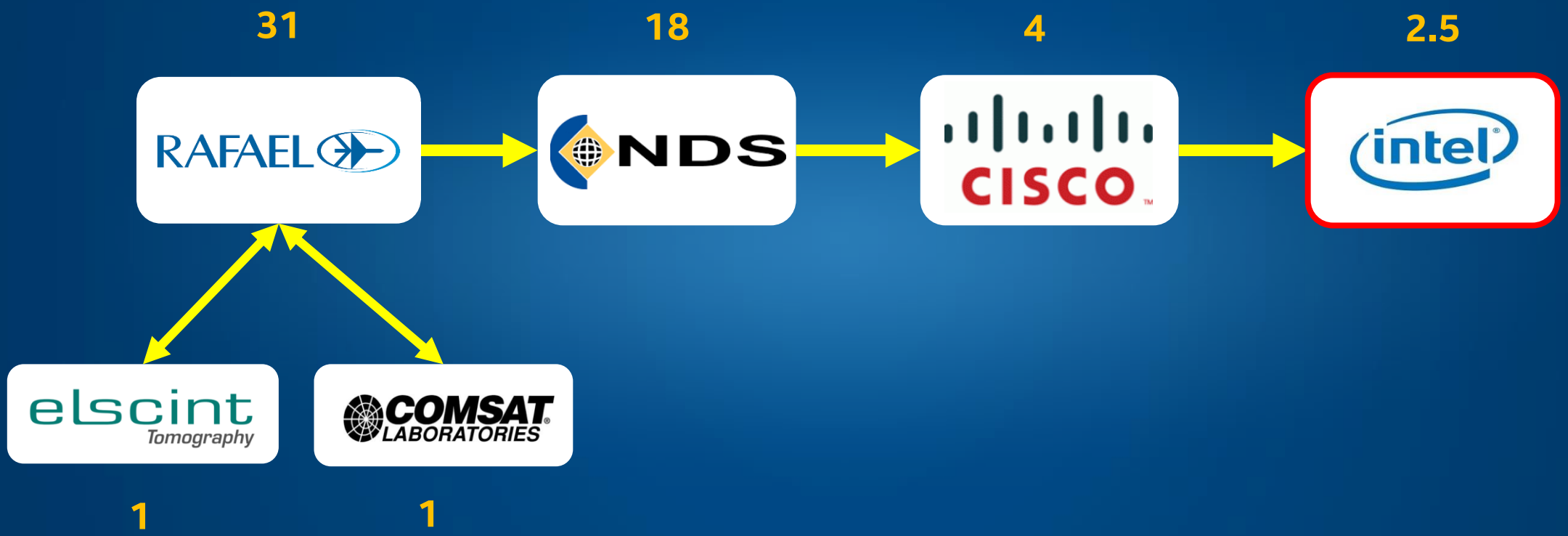
PHYSICAL ATTACKS

INDUSTRY VIEWS

Presented at 2019 FICHSA
Beer Sheba/ Tel Aviv

Chaim Shen-Orr
IPAS / iSTARE
MAY 2019

CHAIM SHEN-ORR



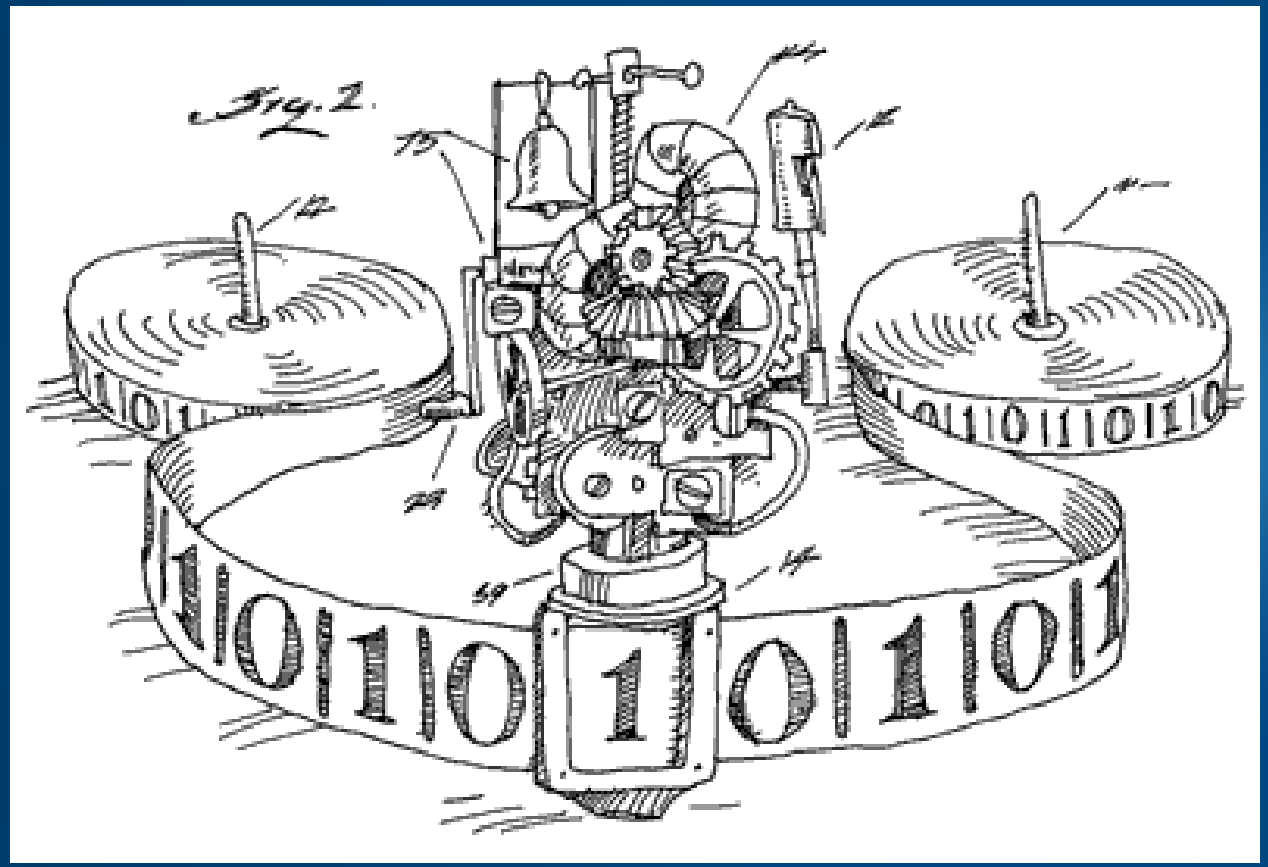
TOPICS

- ❑ Who & What
- ❑ Physical Attacks through the ages
- ❑ The Making of a Chip
- ❑ Problems, solutions and dilemmas
- ❑ Supply Chain through the ages
- ❑ Myth and reality
- ❑ Takeaways

WHO & WHAT

	Researchers	Nation States	Terrorist Orgs	Insiders
Motivation	Fame, academic research	Political / national	Fear, monetary advantage	Personal issues, forced collaboration
Type of damage	Perceived insecurity	Infrastructure destruction, secrets	Infrastructure destruction, finance	Exposure of key values, design details, design weaknesses. Trojan insertion
Means / equipment	Somewhat limited	Unlimited	unknown	Very limited
Attack dev timeframe	Large	Unlimited	?	Unlimited
Response dev timeframe	Embargo period	Zero	Zero	Zero
Collaboration	Researchers worldwide	None	None	With Nation States, Terrorist orgs.

IDEAL PLATFORM ?



No caches

No OOO

No speculation

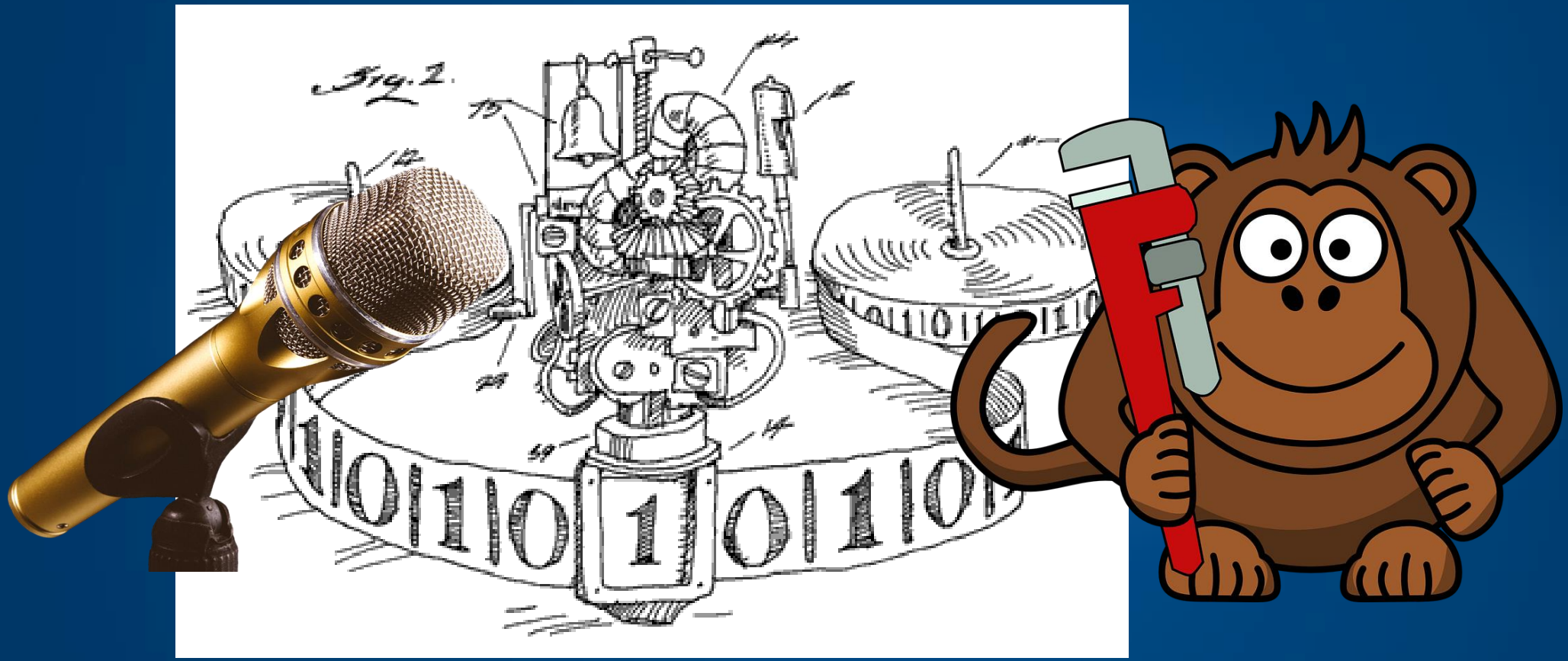
No KASLR attacks

No Spectre

No Meltdown

No Foreshadow

BUT . . .

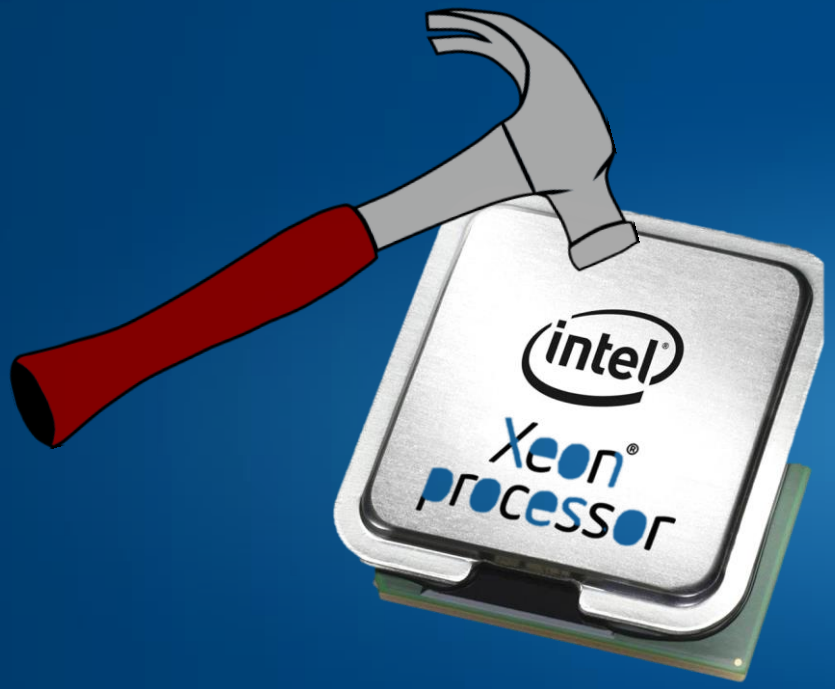


PHYSICAL ATTACKS

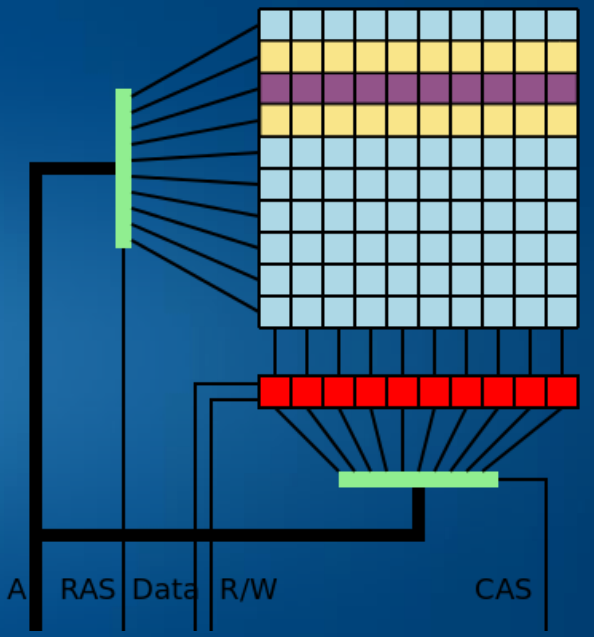
a) An attack that requires physical access to the attacked device

b) An attack that relies on the physical properties of the attacked device

PHYSICAL ATTACKS



a) Hammer



b) RowHammer

https://commons.wikimedia.org/wiki/User:Dsimic

BORE (Break One, Run Everywhere)

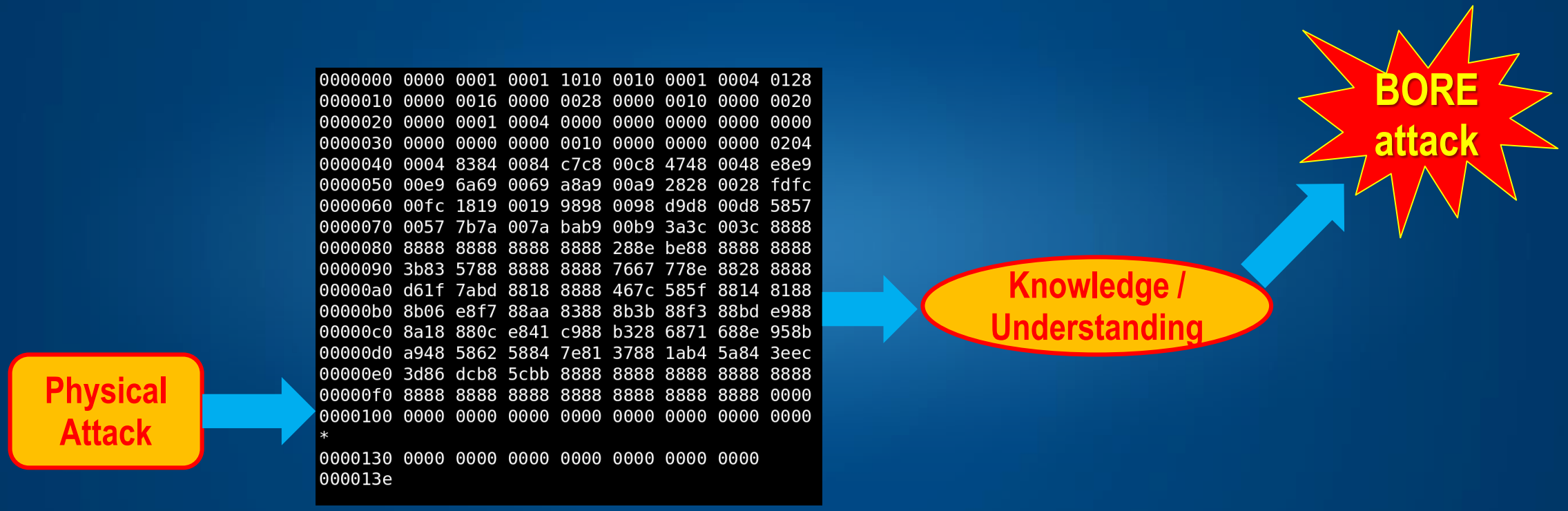
BORE - equivalent

PDOS (Permanent Denial of Service)

Stepping Stones

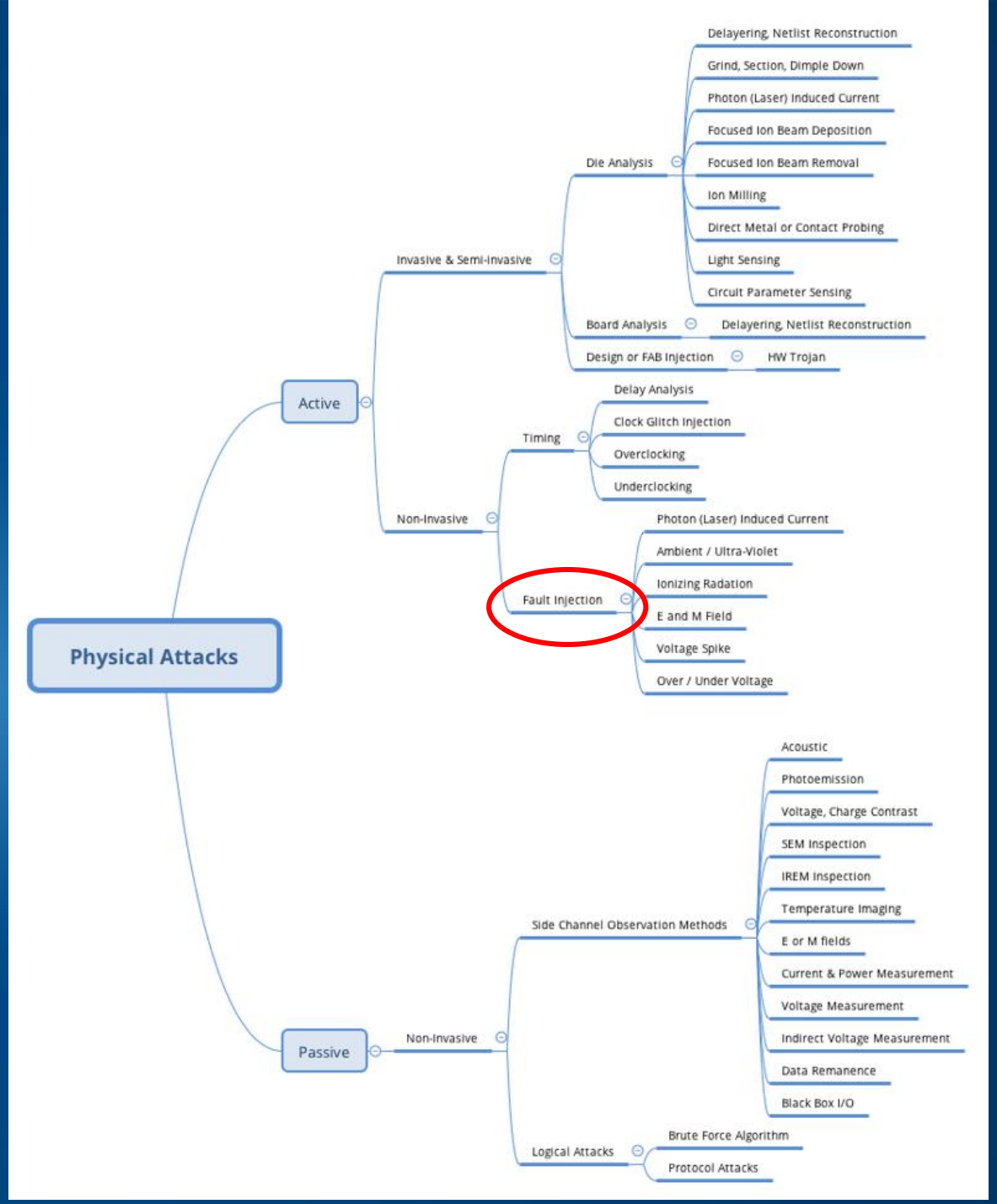
Hansaushermargor

STEPPING STONES



Mwtoews

PHYSICAL ATTACKS

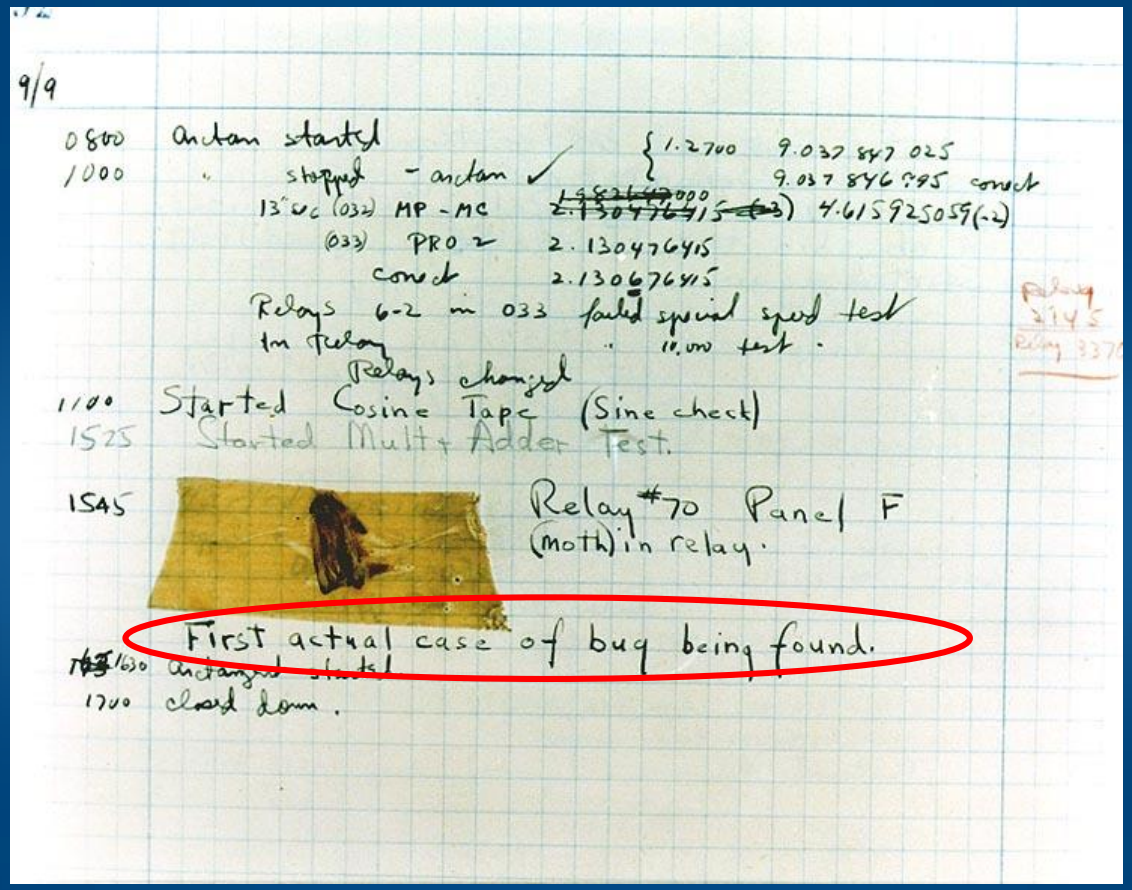


WHAT IS FAULT INJECTION ?

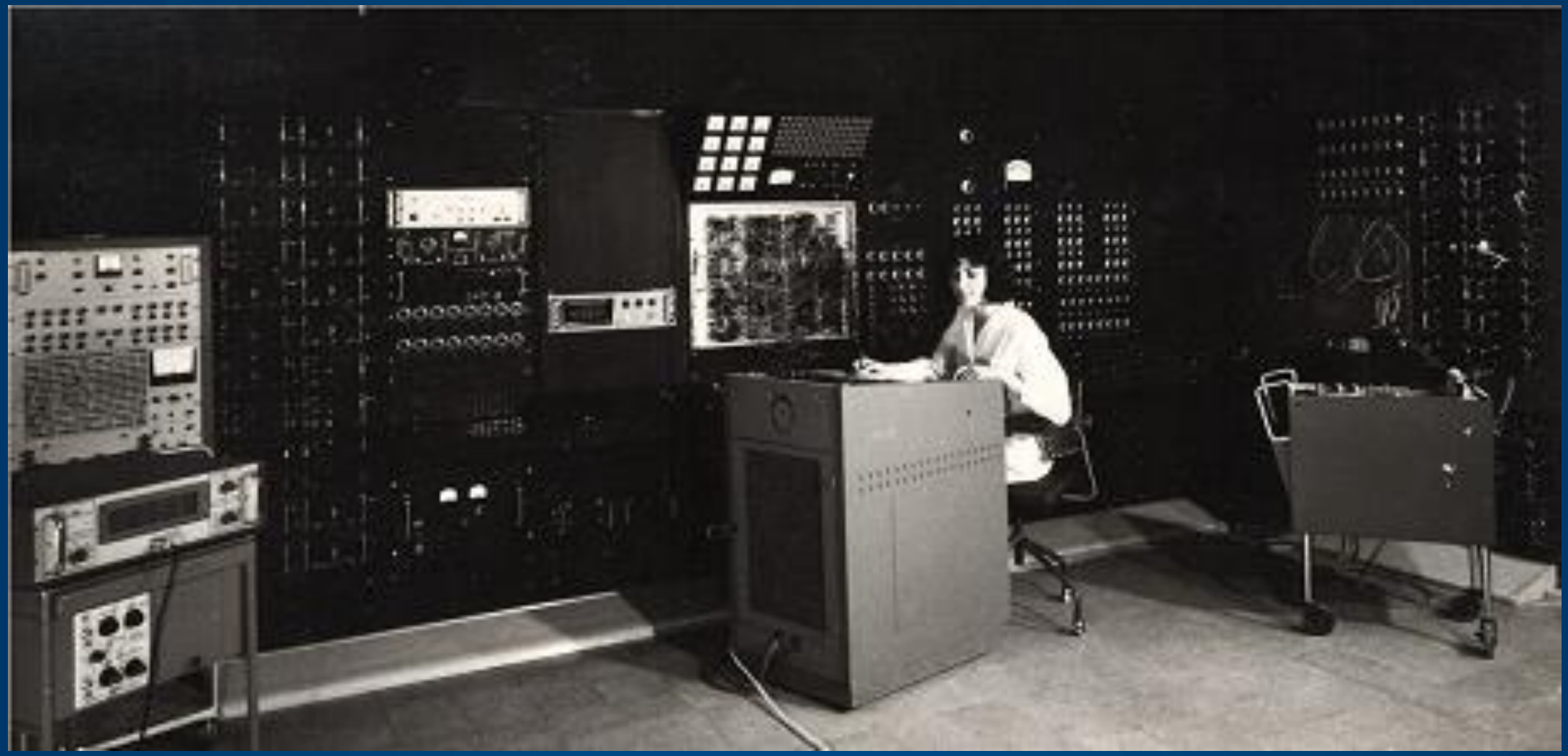
A < Die / Package / Computer >
Data Sheet specifies / implies a set of physical and logical inputs and environmental conditions

Any other inputs or environmental conditions are *potential* causes of a fault condition

EARLY FAULT INJECTION (1)

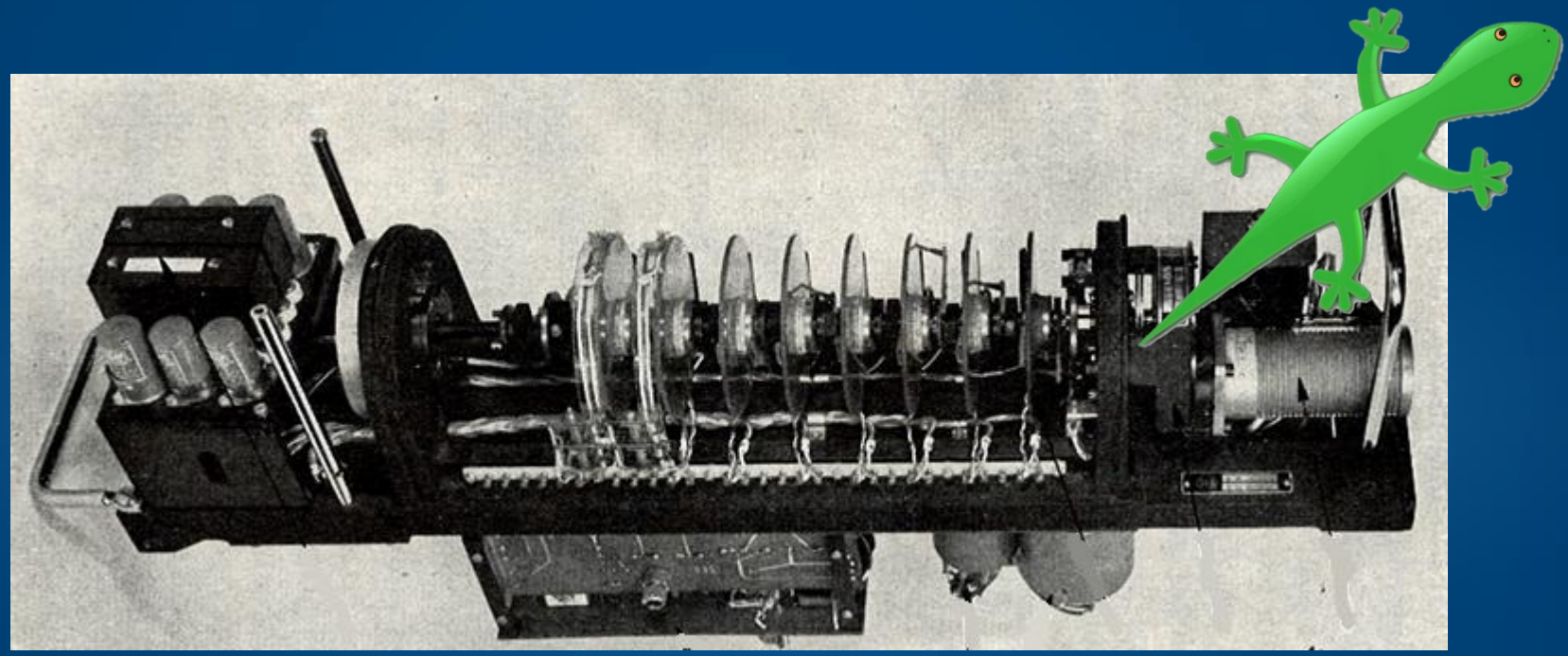


Bug (Harvard Mark II Aiken Relay Calculator, 9/1947)



RAFAEL’s “Itsik” analog computer (~1966)

EARLY FAULT INJECTION (2)

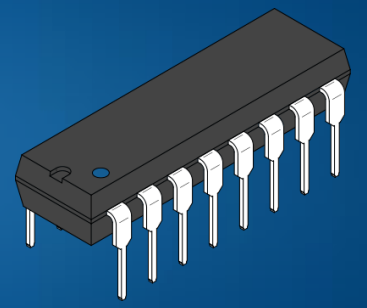


Lizard’s tail caught in servo-multiplier

M. PELEGRIN, Machines à calculer électroniques – Arithmétiques et Analogiques, © Dunod, 1959, Paris

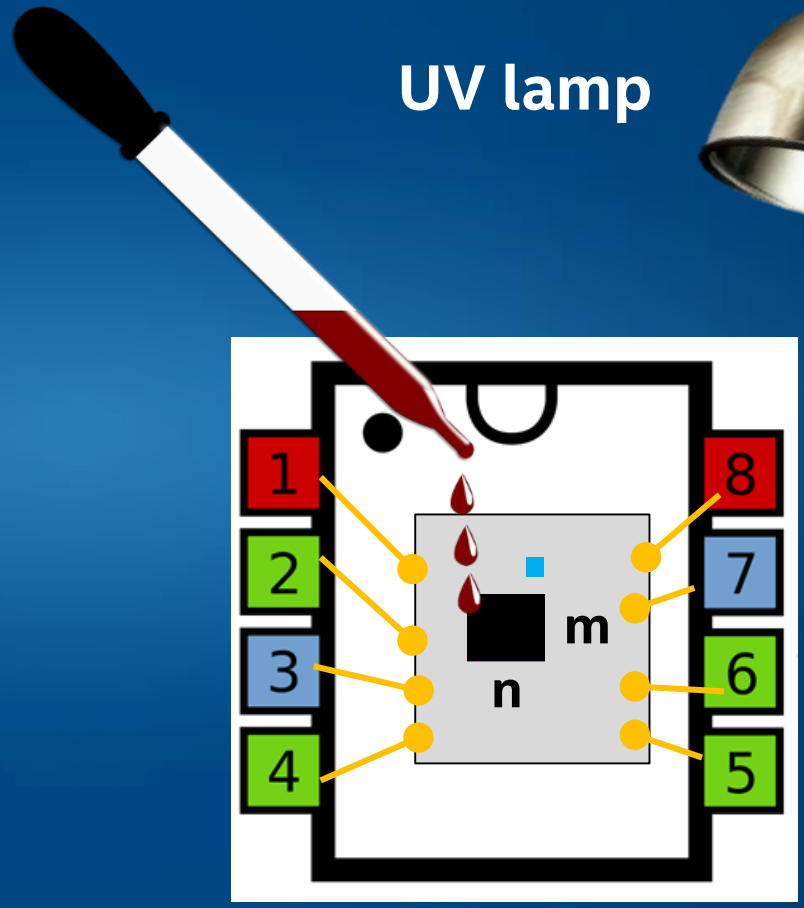
LATER FAULT INJECTION ATTACKS

- ❑ Ionizing radiation
- ❑ Photons
- ❑ Electro-magnetic fields
- ❑ Voltage spikes
- ❑ Over / under voltage
- ❑ Temperature



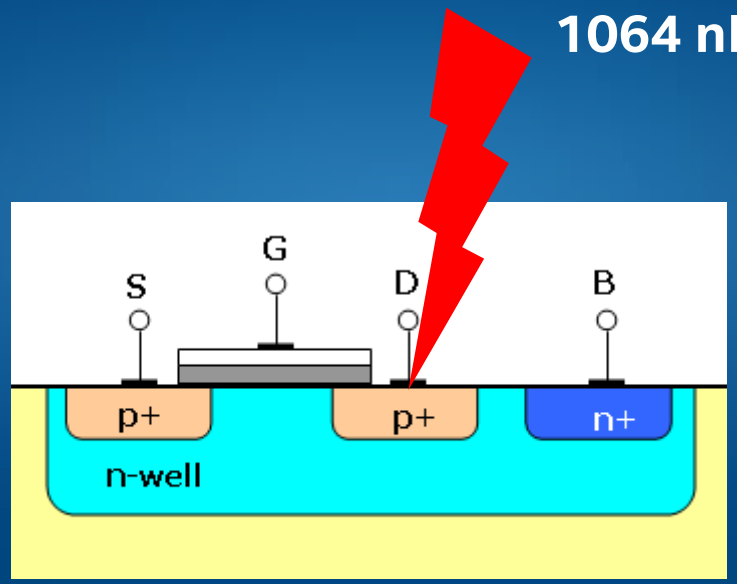
MORE ADVANCED FAULT INJECTION ATTACKS

- ❑ Ionizing radiation
- ❑ Photons
- ❑ Electro-magnetic field
- ❑ Voltage spike
- ❑ Over / under voltage
- ❑ Temperature



UV lamp

SEMICONDUCTOR PHYSICS

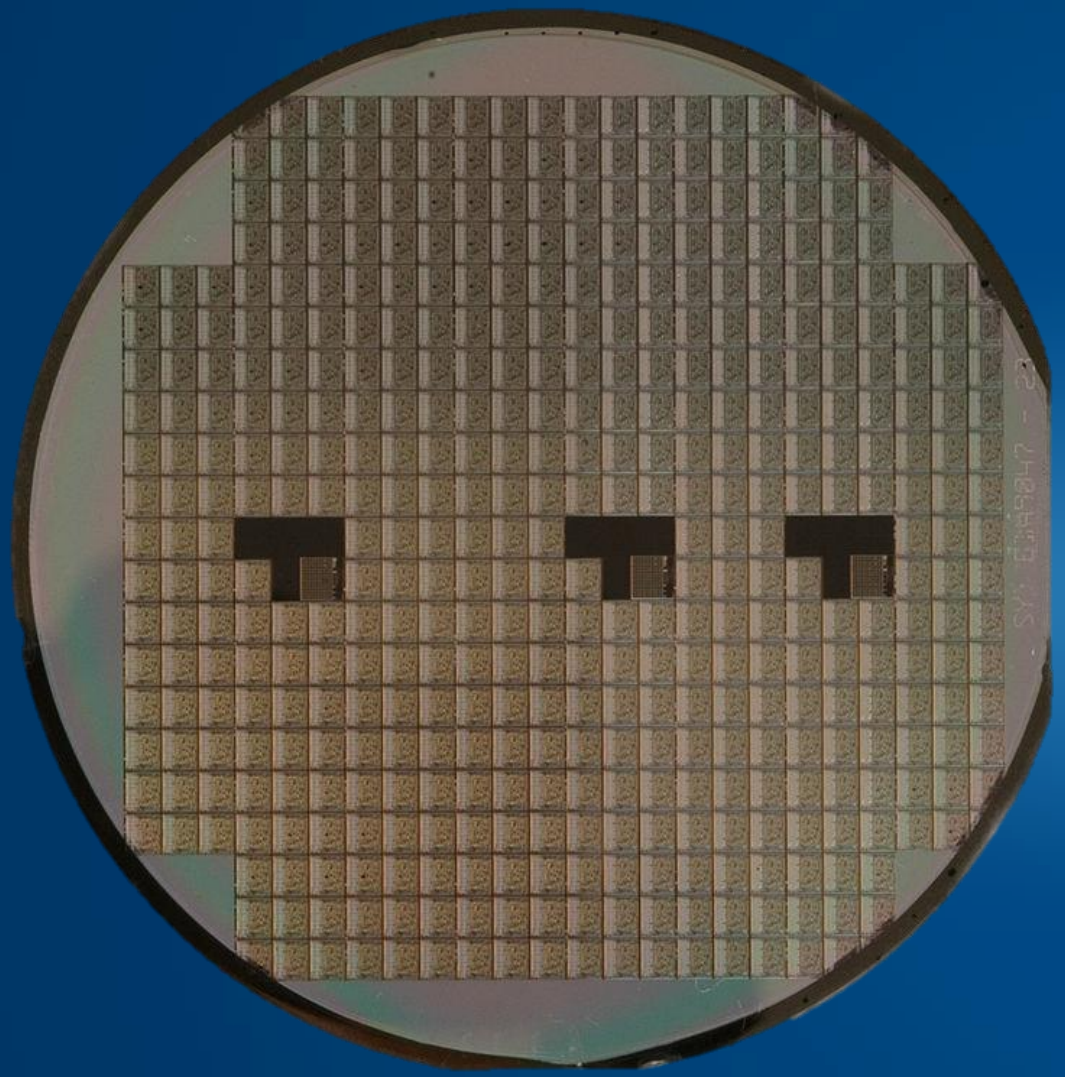


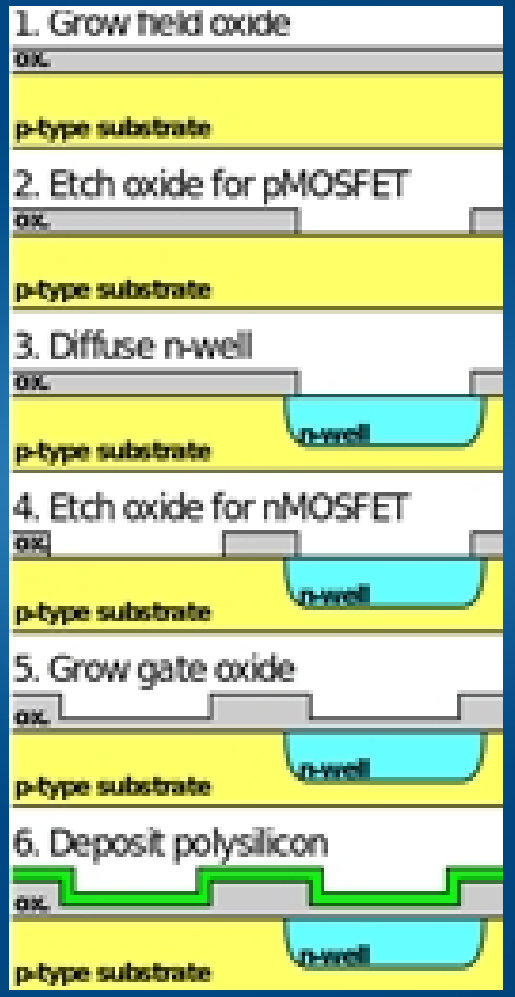
LASER STATION

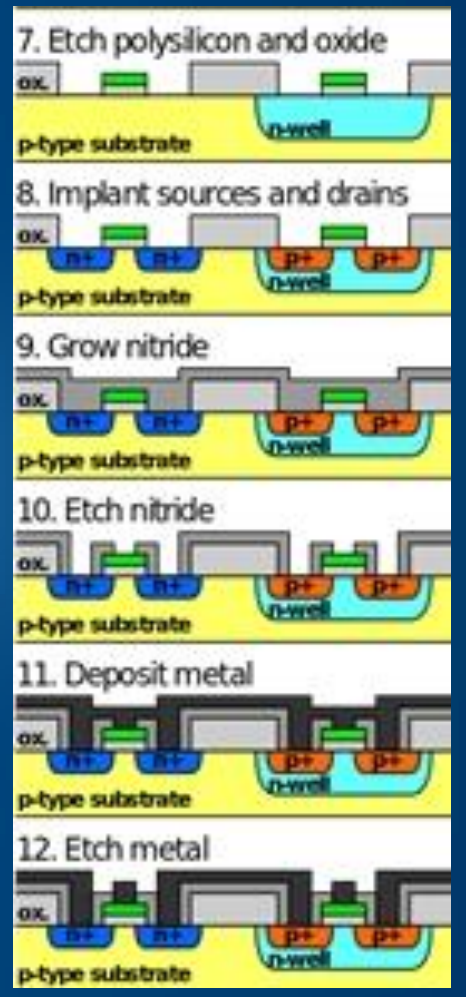
Riscure

THE MAKING OF A CHIP

THE MAKING OF A CHIP

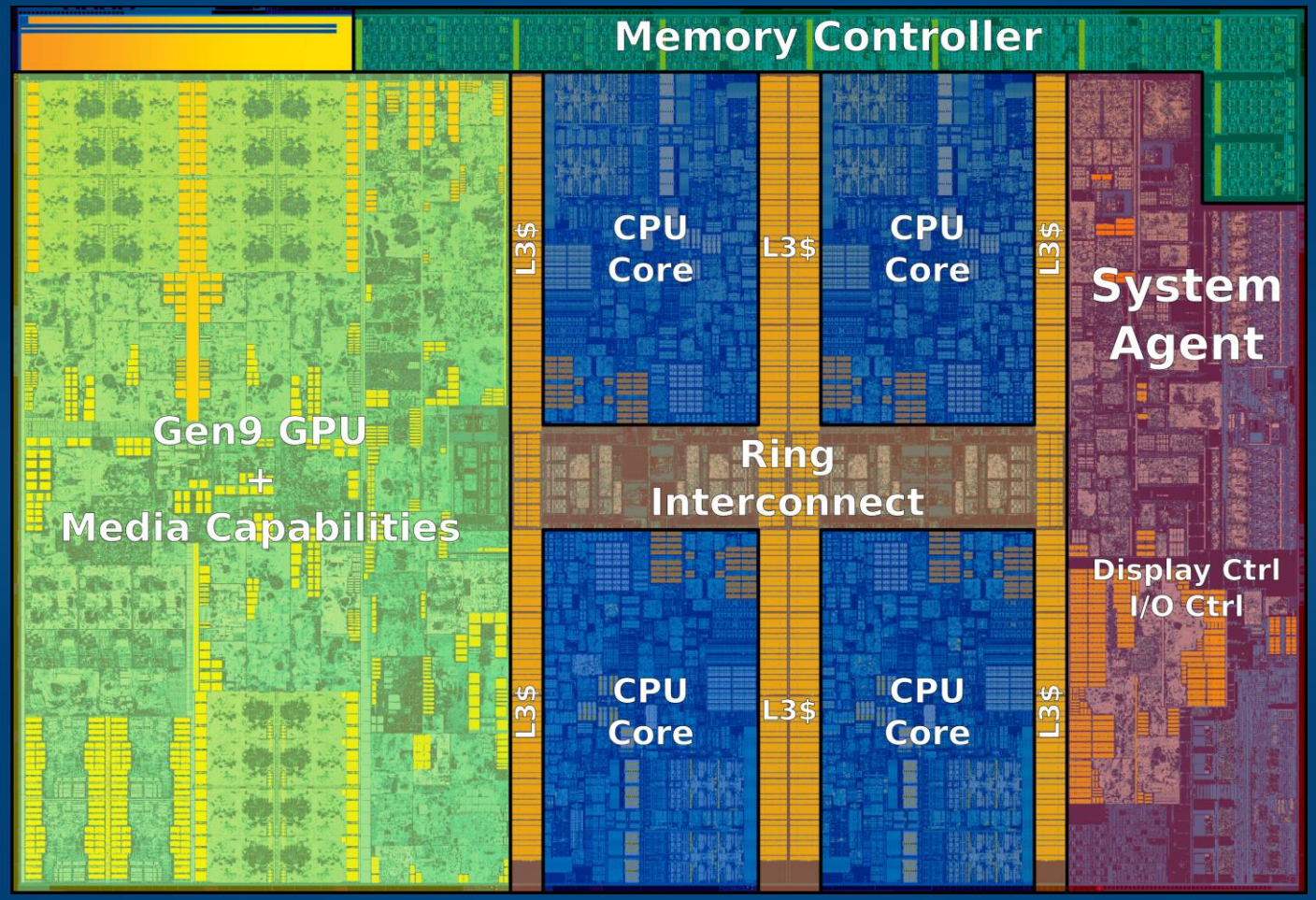






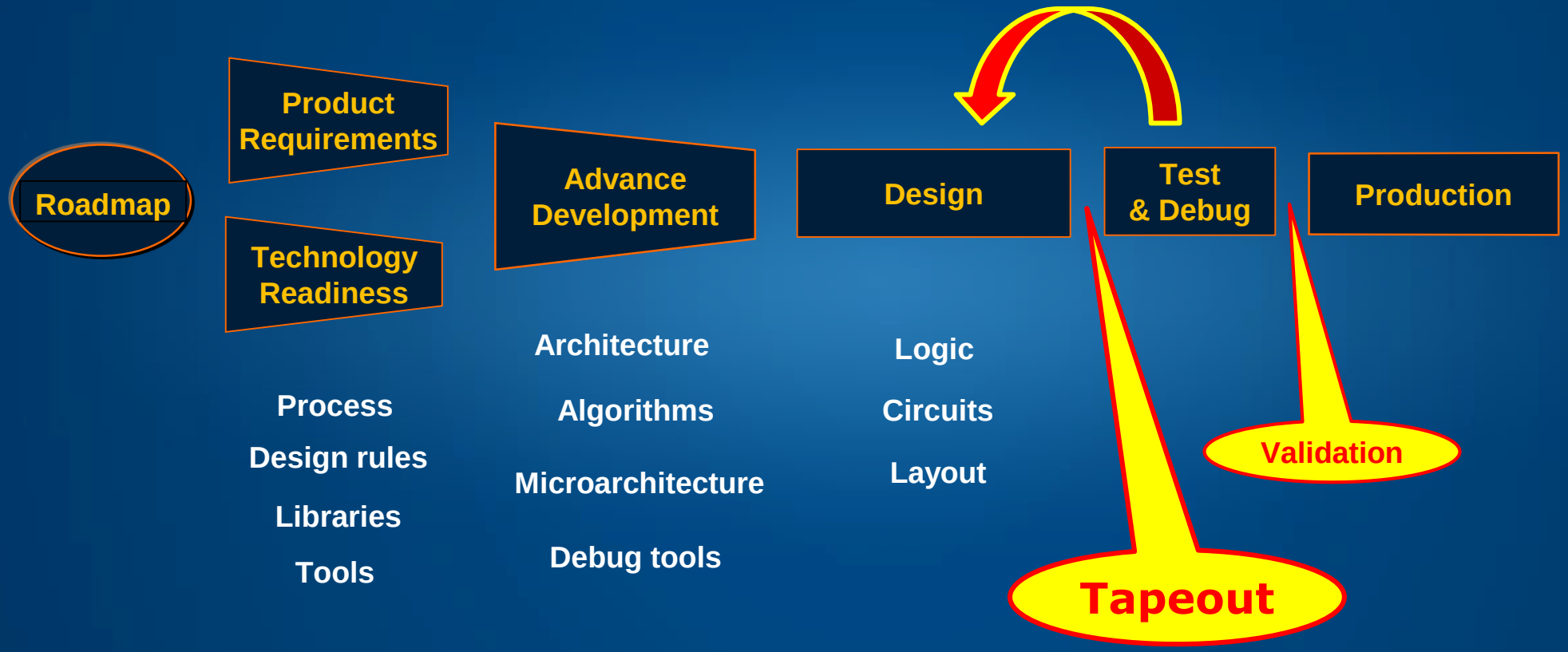
https://commons.wikimedia.org/wiki/User:Cmglee

A CHIP



Intel® Skylake quad-core

IT'S A LONG WAY . . .



VALIDATION

SECURITY VALIDATION

Metrics ?

Heuristics ?

We have not broken it YET

UNKNOWN UNKNOWNS

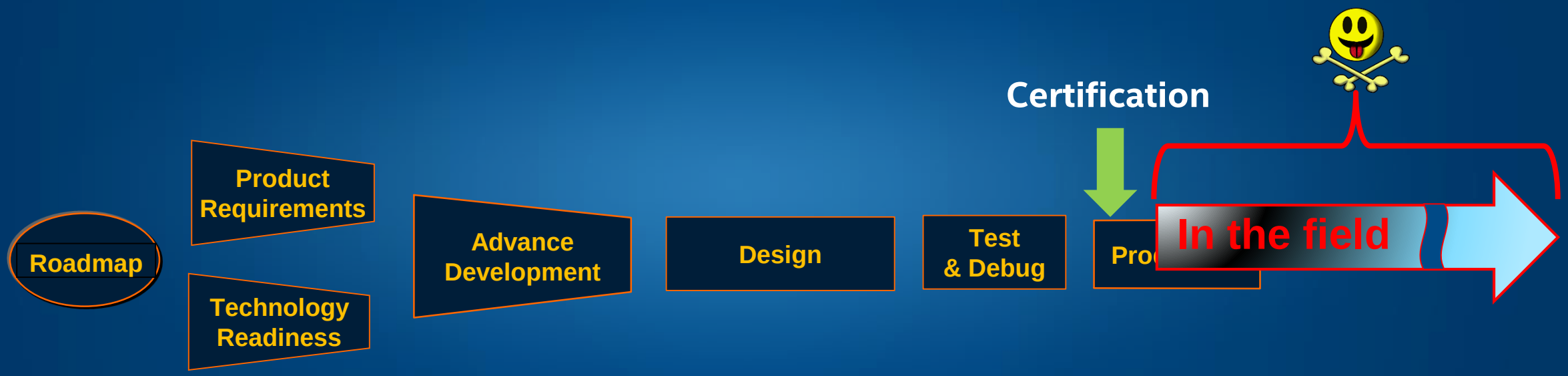
CERTIFICATION

FIPS	Federal Information Processing Standards
CC	Common Criteria
EMVCo	EuroPay, MasterCard, Visa

Commercially important, but . . .

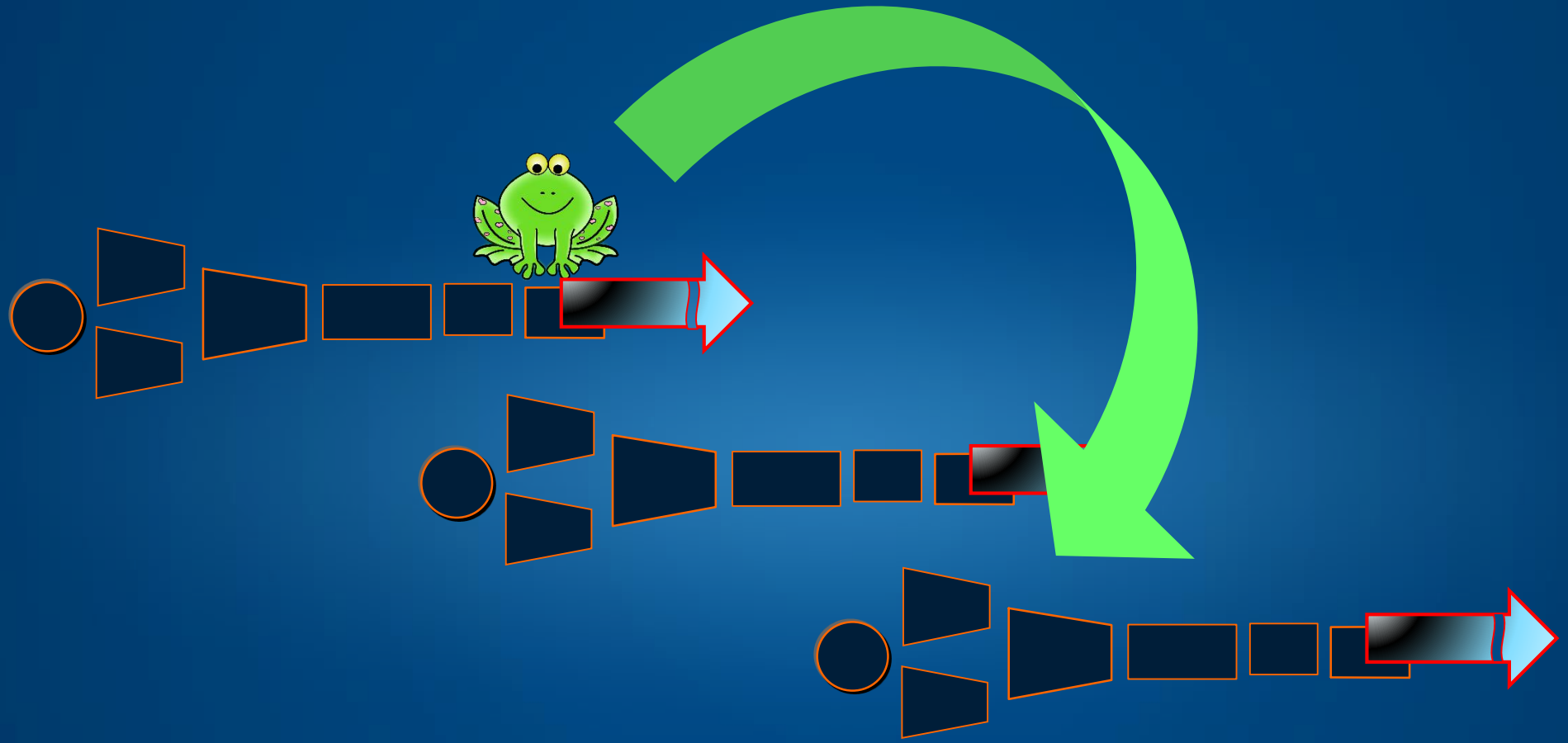
http://clipart-library.com/clipart/355565.htm

“WE” vs. “THEY”



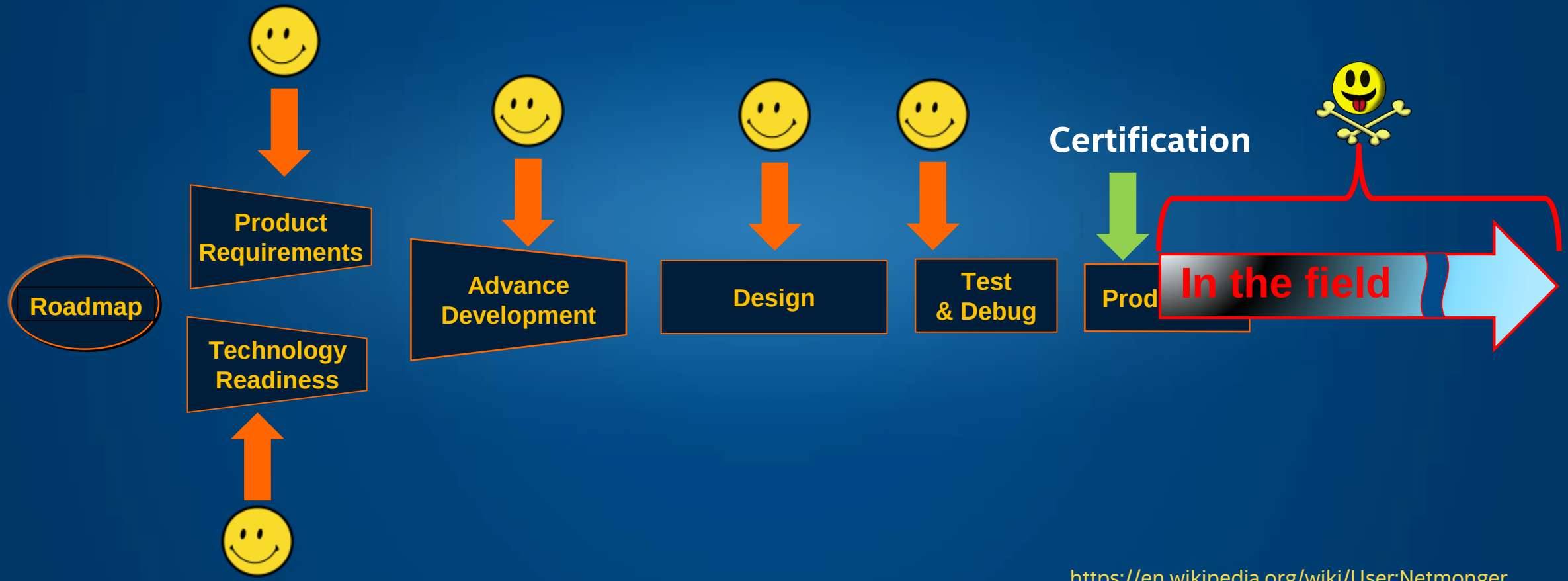
https://www.deviantart.com/red436/art/Pirate-Smilly-76239623

LEAPFROGGING

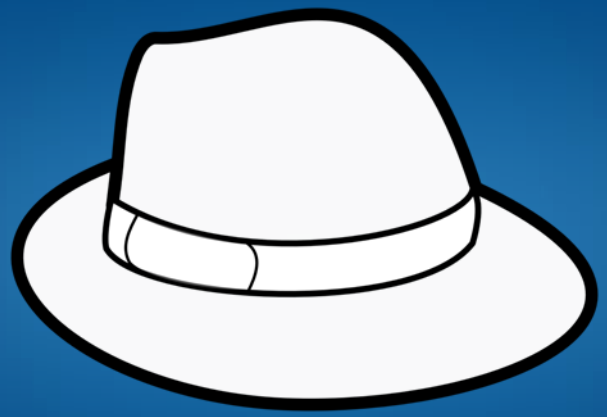


NEEDED: TIME MACHINE

EARLY BIRD

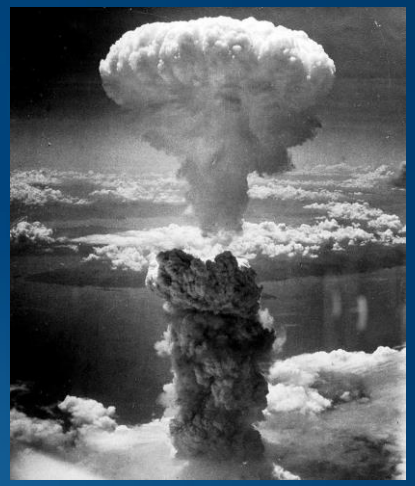


https://en.wikipedia.org/wiki/User:Netmonger



PROBLEMATICS

- Significance estimation
- Management attention



- Scalability
- Time

SCALABILITY & TIME

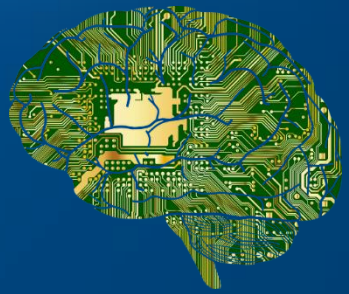
	Researchers	Nation States	Terrorist Orgs	Insiders
Motivation	Fame, academic research	Political / national	Fear, monetary advantage	Personal issues, forced collaboration
Type of damage	Perceived insecurity	Infrastructure destruction, secrets	Infrastructure destruction, finance	Exposure of key values, design details, design weaknesses. Trojan insertion
Means / equipment	Somewhat limited	Unlimited	unknown	Very limited
Attack dev timeframe	Large	Unlimited	?	Unlimited
Response dev timeframe	Embargo period	Zero	Zero	Zero
Collaboration	Researchers worldwide	None	None	With Nation States, Terrorist orgs.

SOLUTIONS ?

- ❑ Simulation / Emulation ?

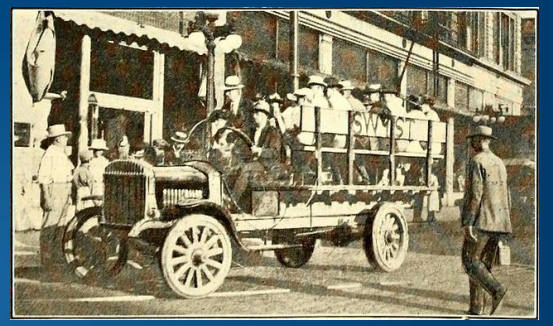
- ❑ Outsourcing ?

- ❑ Artificial Intelligence ?



MORE PROBLEMATICS

- ❑ Shared assumptions
- ❑ State of Mind

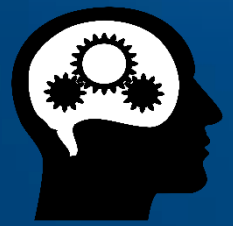


"Secure Bus"

- ❑ Contamination
- ❑ Hacker / Designer dilemma

https://commons.wikimedia.org/wiki/File:Indian_Election_Symbol_Bus.png

SIDE BENEFITS

- ❑ Discovery → Mitigation
- ❑ General advice / guidelines
- ❑ Spread the word
- ❑  Security State of Mind

AND NOW

Supply Chain Security

SOMETH LETELY DIFFERENT

Giovanni Domenico Tiepolo

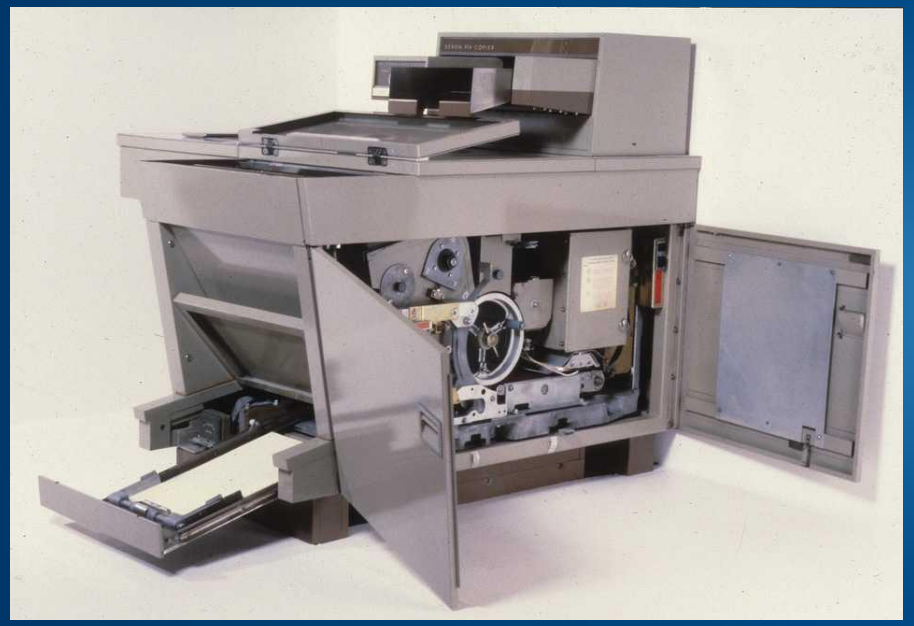
TROJAN TAXONOMY

(SNIPPET)

- Physical characteristics
  - ...
- Activation characteristics
  - Internal
    - ...
  - External
    - ...
- Action characteristics
  - Transmit
    - ...
  - Modify
    - Kill

After Wang, Tehranipoor, Plusquelic – HOST 2008

OLD TROJANS



1959 - Xerox 914 copier {1961 – 1969}

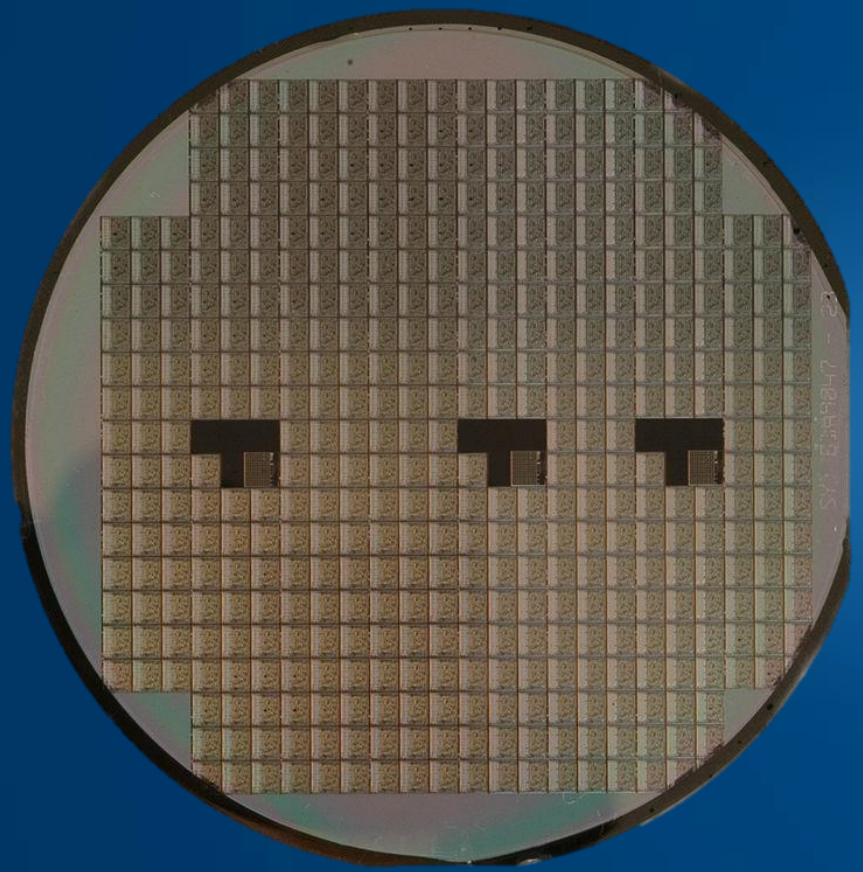
1961 - IBM Selectric II typewriter {1976 – 1984}

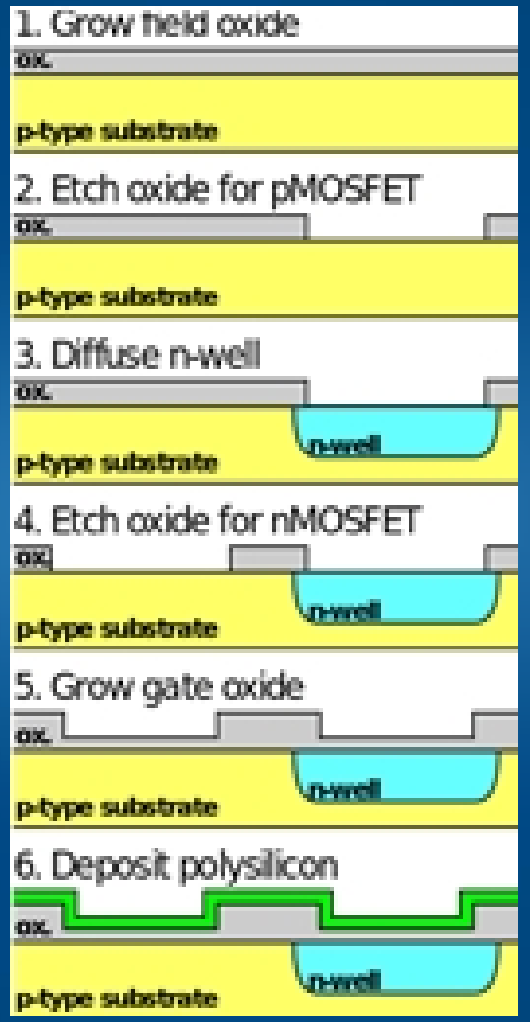
https://en.wikipedia.org/wiki/IBM_Selectric_typewriter#/media/File:IBM_Selectric.jpg (Oliver Kurmis)

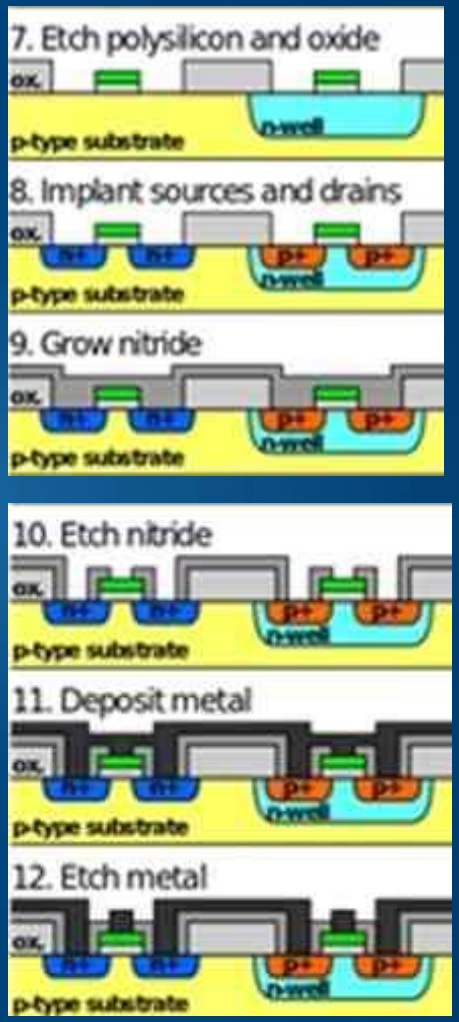
Bug - www.cryptomuseum.com

Smithsonian National Museum of American History

SPLIT FABRICATION







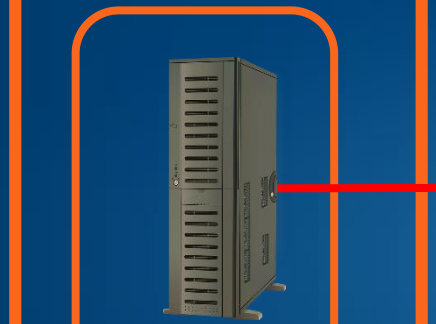
https://commons.wikimedia.org/wiki/User:Cmglee

Bloomberg Businessweek

BORE - EQUIVALENT

Teradyne® UltraFLEX tester

MYTH



Black Box

Secure Rack

Secure room

Optical Fiber

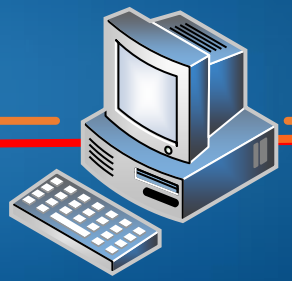
Teradyne® UltraFLEX tester

REALITY

Production System

Engineering System

Optical Fiber



Windows XP PC

Black Box

Secure Rack

Secure room

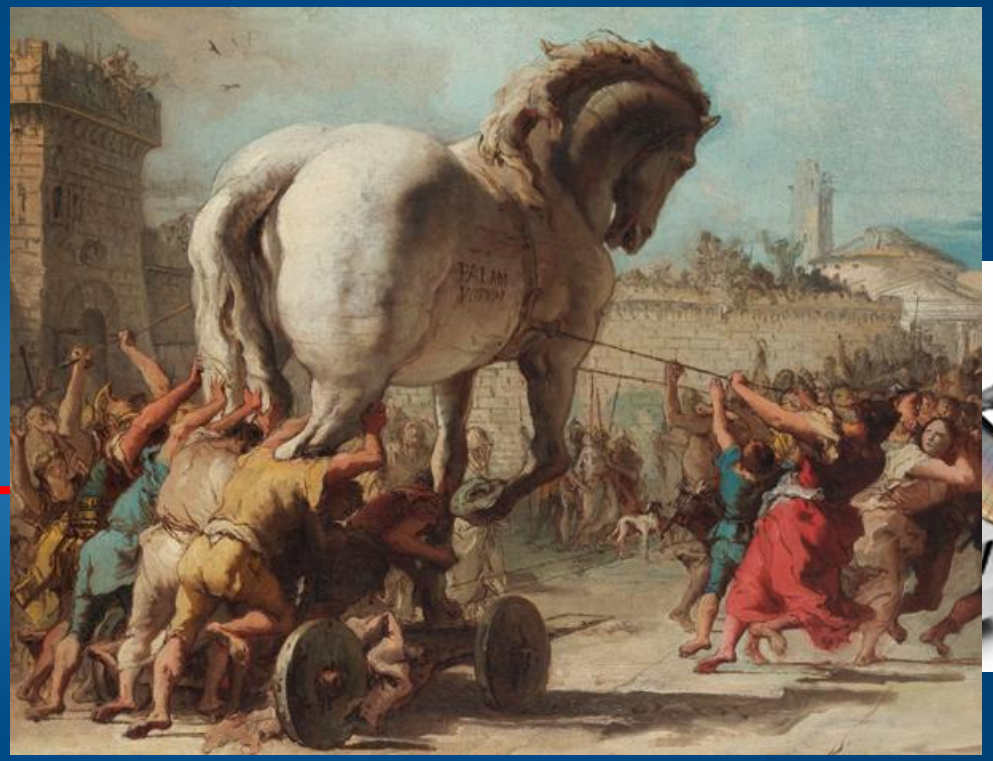
Teradyne® UltraFLEX tester

REALITY

Black Box

Secure Rack

Secure room



Teradyne® UltraFLEX tester

BUT DON'T WORRY . . .

TAKEAWAYS

- ❑ Physical attacks – especially FI – are verrry powerful
- ❑ Bore is a SYSTEM property
- ❑ Scalability and time problems
- ❑ Need metrics
- ❑ Solutions, but no panacea
- ❑ “Security State of Mind” is important
- ❑ Security and the “Ninja circle”

Performance

Manufacturability

Cost

Power

Testability

Usability