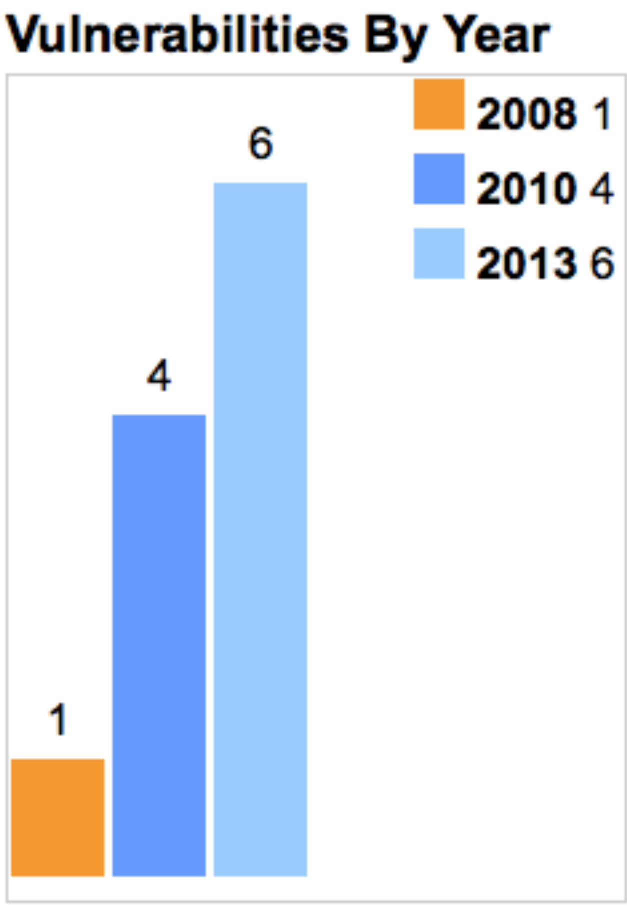
“On the Security and Safety of Collaborative Intelligent Vehicles” or “An explosion of problems”

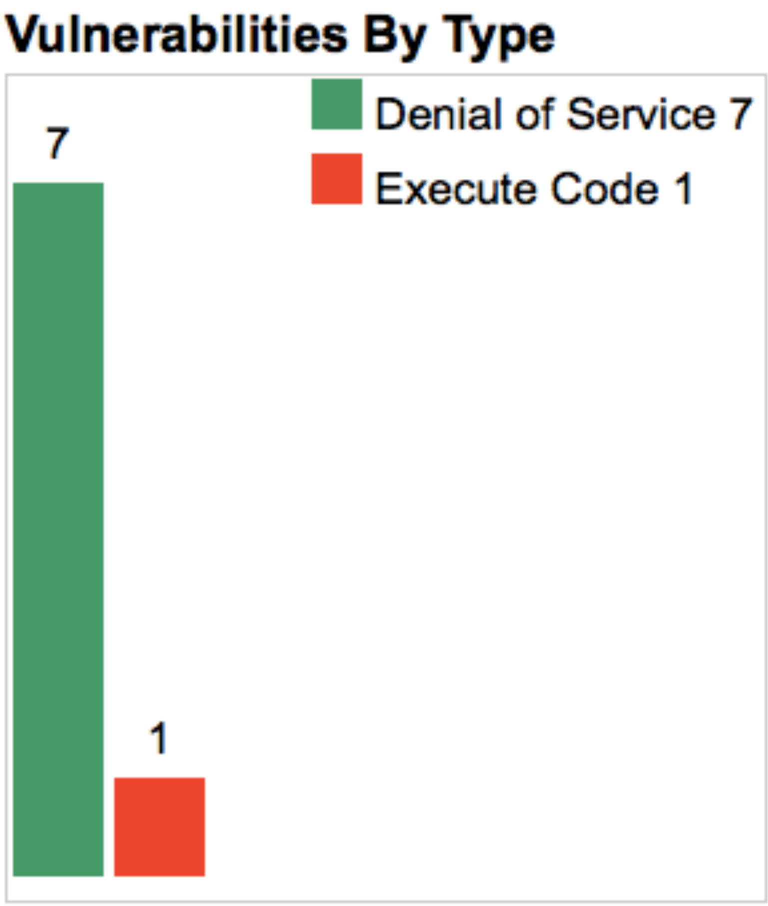
Dr. Roberto Gallo
Unicamp, Kryptus

INSECURITY AND ADVANCED THREATS


مرگ بر
PRESSTV

VxWorks Cyber-Issues





Advisory (ICSA-15-169-01)

Wind River VXWorks TCP Predictability Vulnerability in ICS Devices

Original release date: June 18, 2015

AFFECTED PRODUCTS

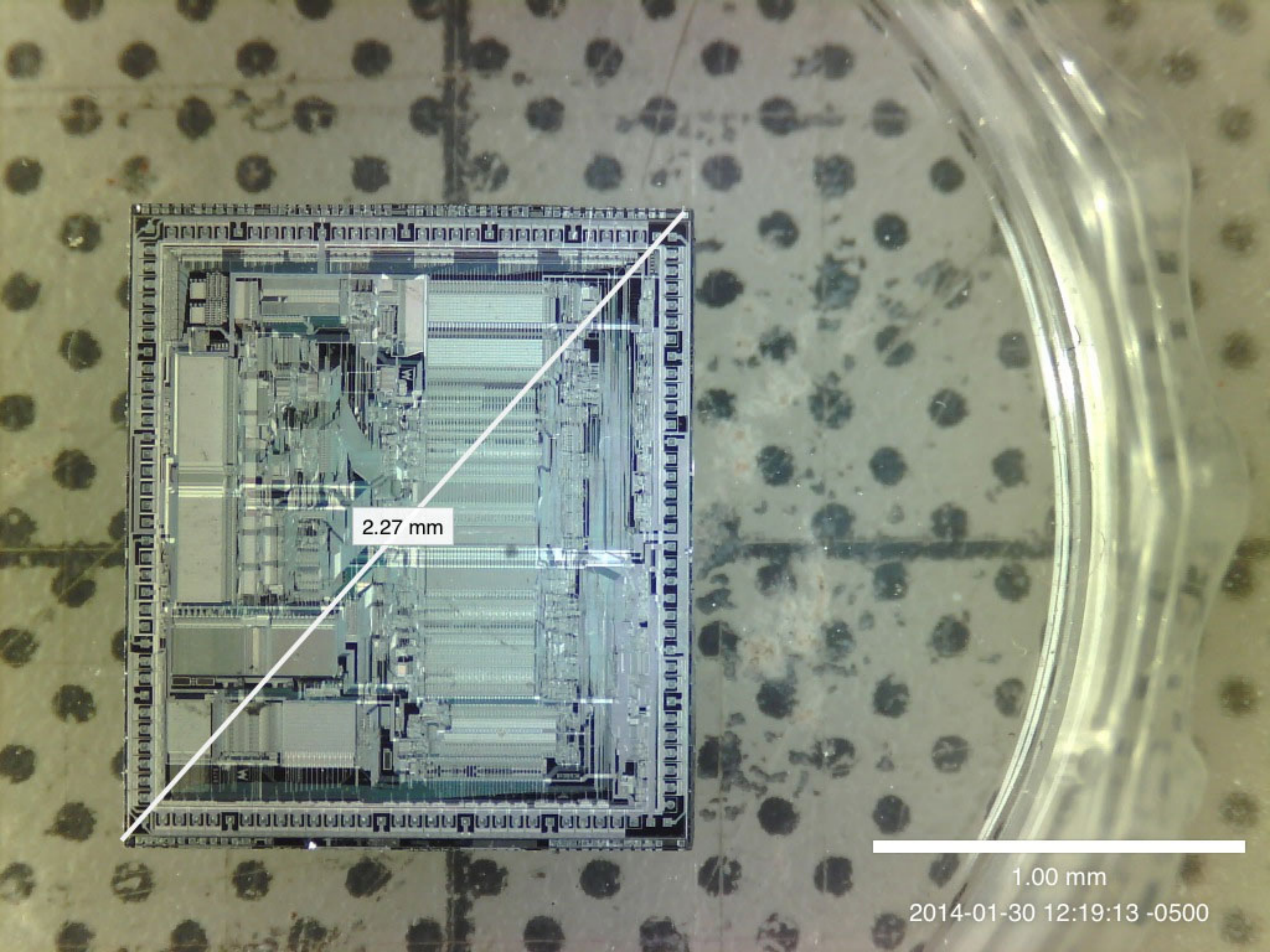
The following versions of VxWorks are affected:

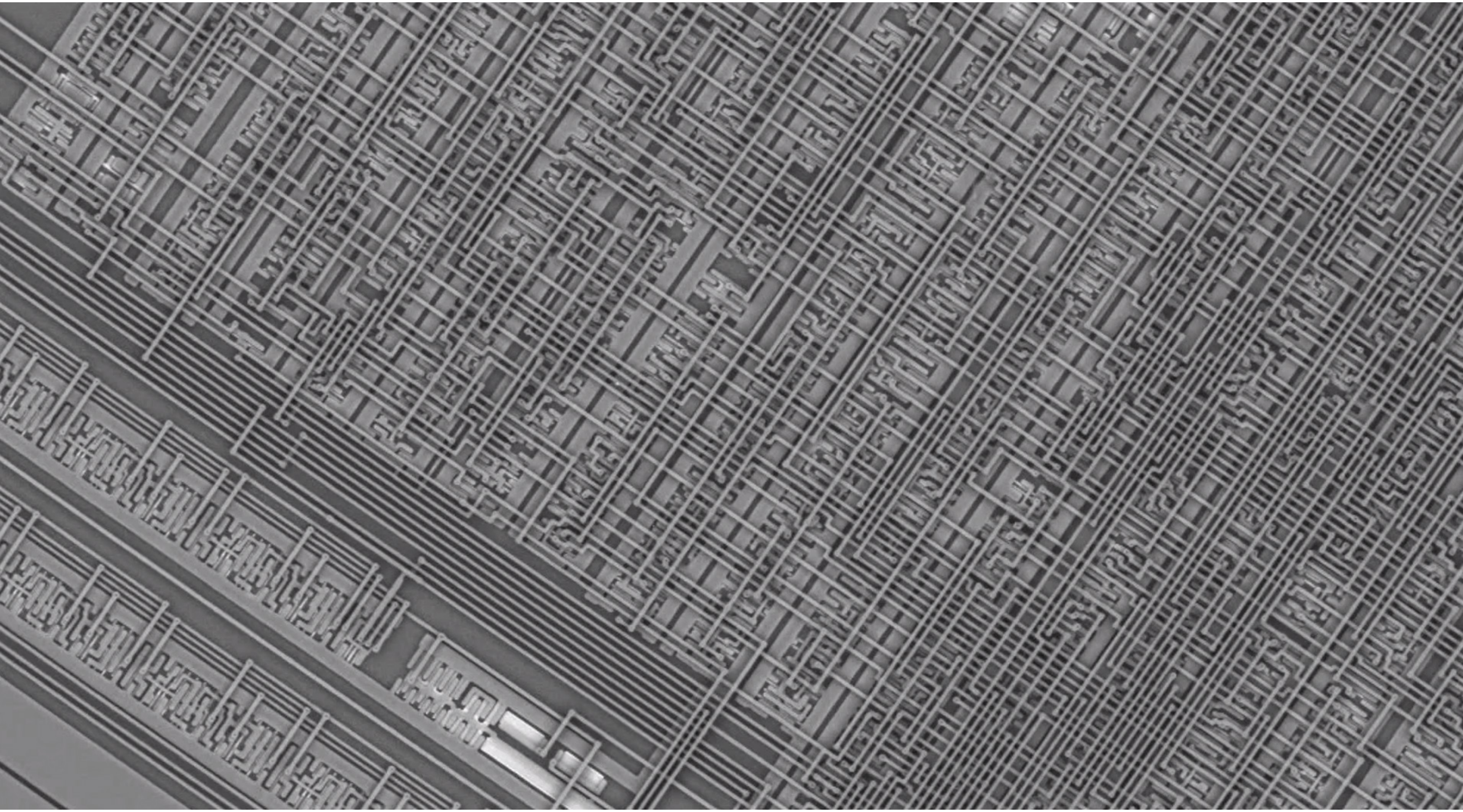
- Wind River VxWorks, Version 7, released prior to February 13, 2015,
- Wind River VxWorks, Version 6.9 releases prior to Version 6.9.4.4,
- Wind River VxWorks, Version 6.8 releases prior to Version 6.8.3,
- Wind River VxWorks, Version 6.7 releases prior to Version 6.7.1.1, and
- Wind River VxWorks, Version 6.6 and prior versions, but NOT to include Version 5.5.1 with PNE2.2 and Version 6.0 through Version 6.4.

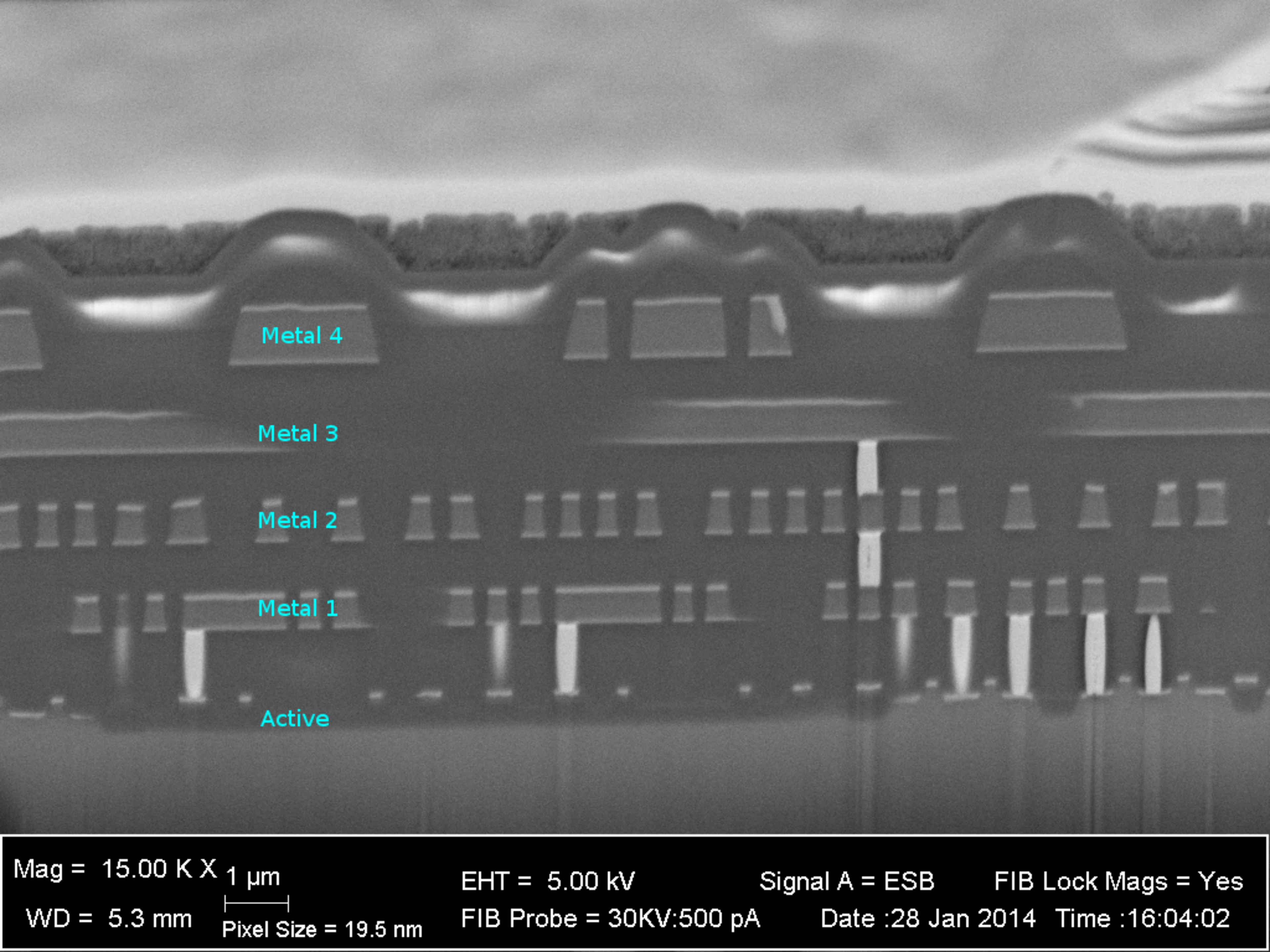
IMPACT

Successful exploitation of this vulnerability may allow an attacker to spoof or disrupt TCP connections of affected devices.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.


2.27 mm
1.00 mm
2014-01-30 12:19:13 -0500




Metal 4
Metal 3
Metal 2
Metal 1
Active
Mag = 15.00 K X
1 µm
WD = 5.3 mm
Pixel Size = 19.5 nm
EHT = 5.00 kV
FIB Probe = 30KV:500 pA
Signal A = ESB
Date :28 Jan 2014
FIB Lock Mags = Yes
Time :16:04:02

Remote disablaing

Actions were taken to contain the Exocet threat. During the preparation for the war, Britain benefited from the help of France, which gave the Exocet's code and homing radar.[16] A major intelligence operation was also initiated to prevent the Argentine Navy from acquiring more of the weapons on the international market.[17] The operation included British intelligence agents claiming to be arms dealers able to supply large numbers of Exocets to Argentina, who diverted Argentina from pursuing sources which could genuinely supply a few missiles. France denied deliveries of Exocet AM39s purchased by Peru to avoid the possibility of Peru giving them to Argentina, because they knew that payment would be made with a Credit card from the Central Bank of Peru. British intelligence had detected the guarantee was a deposit of two hundred million dollars from the Andean Lima Bank, an owned subsidiary of the Banco Ambrosiano.[18][19]

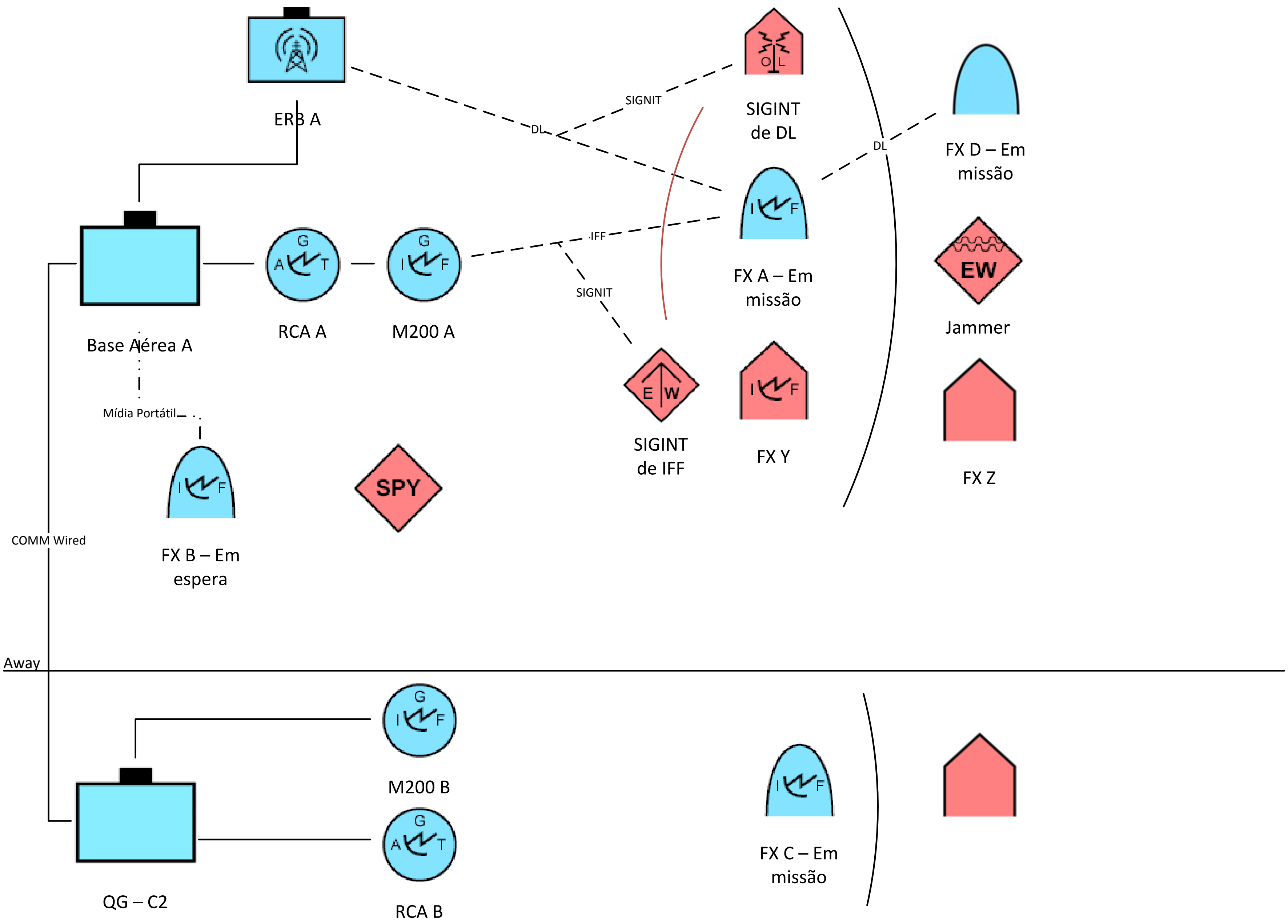
Some scary facts

- "Certified" UAV military-grade ground control station running on MS-Windows!
  - 50 Mio LoC (wrong number at SSIV!)
- Intrinsic complexity of crypto
  - 85 K LoC on a high efficient asymmetric + symmetric library, very complex to model
- Rice's theorem
  - there exists no automatic method that decides with generality non-trivial questions on the behavior of computer programs.
- Subverted ICs found on F-16 and F-35 programs!
  - Hardware trojan horses
- Failure model vs. threat model

OBJECTIVE PROBLEMS

Working in three problems

1. IFF mode 4 (identification foe or friend)
   - Prevent friend fire from any platform
   - Works in tandem with radars
   - Used also in traffic control



ERB A
SIGNIT
DL
SIGINT
de DL
FX D – Em
missão
DL
Base Aérea A
RCA A
M200 A
IFF
SIGNIT
FX A – Em
missão
Jammer
EW
Mídia Portátil
SIGINT
de IFF
FX Y
FX Z
SPY
COMM Wired
FX B – Em
espera
Away
M200 B
RCA B
QG – C2
FX C – Em
missão

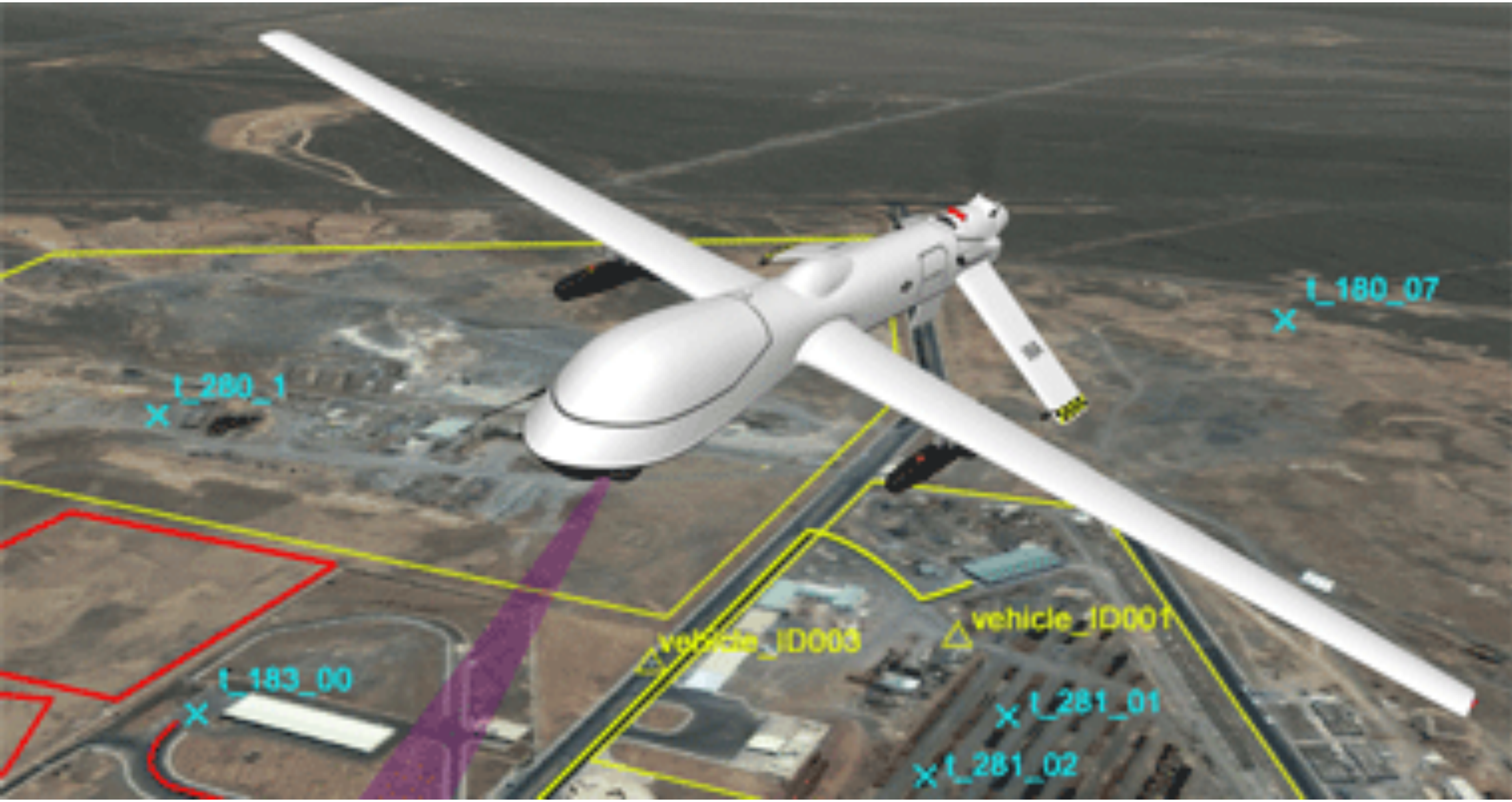
Working in three problems

1. IFF mode 4 (identification foe or friend)
   – Prevent friend fire from any platform
   – Works in tandem with radars
   – Used also in traffic control
2. Netcentric warfare system
   – All-to-all communications (air, ground, sea)
   – All platforms (manned, unmanned)

Optus C1
JSF
HALE UAV
JSF
JSF
JSF
Wedgetail
INGARA
TUAV
UCAV
Parakeet
NORCOM
Tiger
M113
Seahawk
Air Warfare
Destroyer
JSF

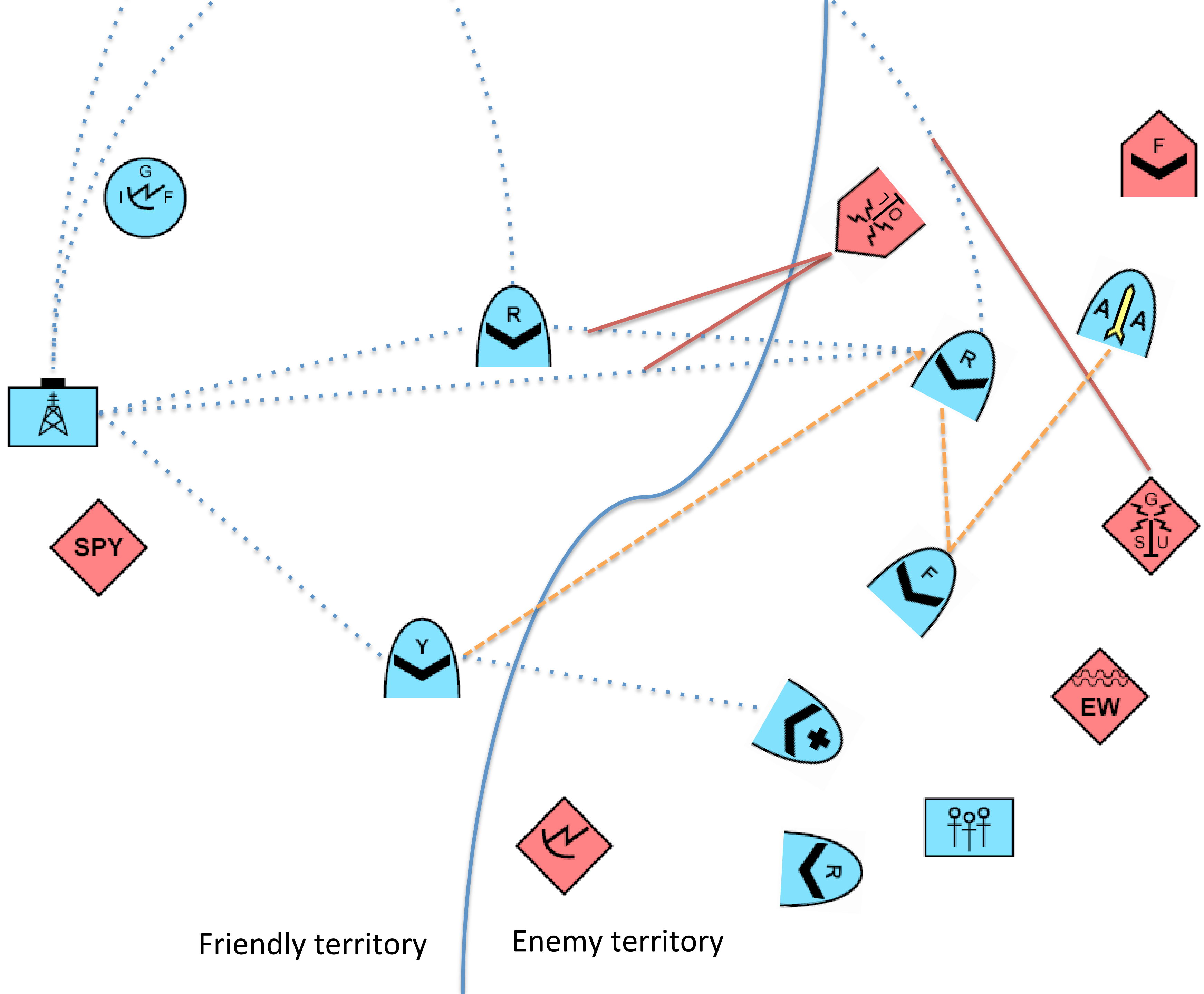
Working in three problems

1. IFF mode 4 (identification foe or friend)
   - Prevent friend fire from any platform
   - Works in tandem with radars
   - Used also in traffic control
2. Netcentric warfare system
   - All-to-all communications (air, ground, sea)
   - All platforms (manned, unmanned)
3. Drone cyber security
   - From ground station to airborne sensors

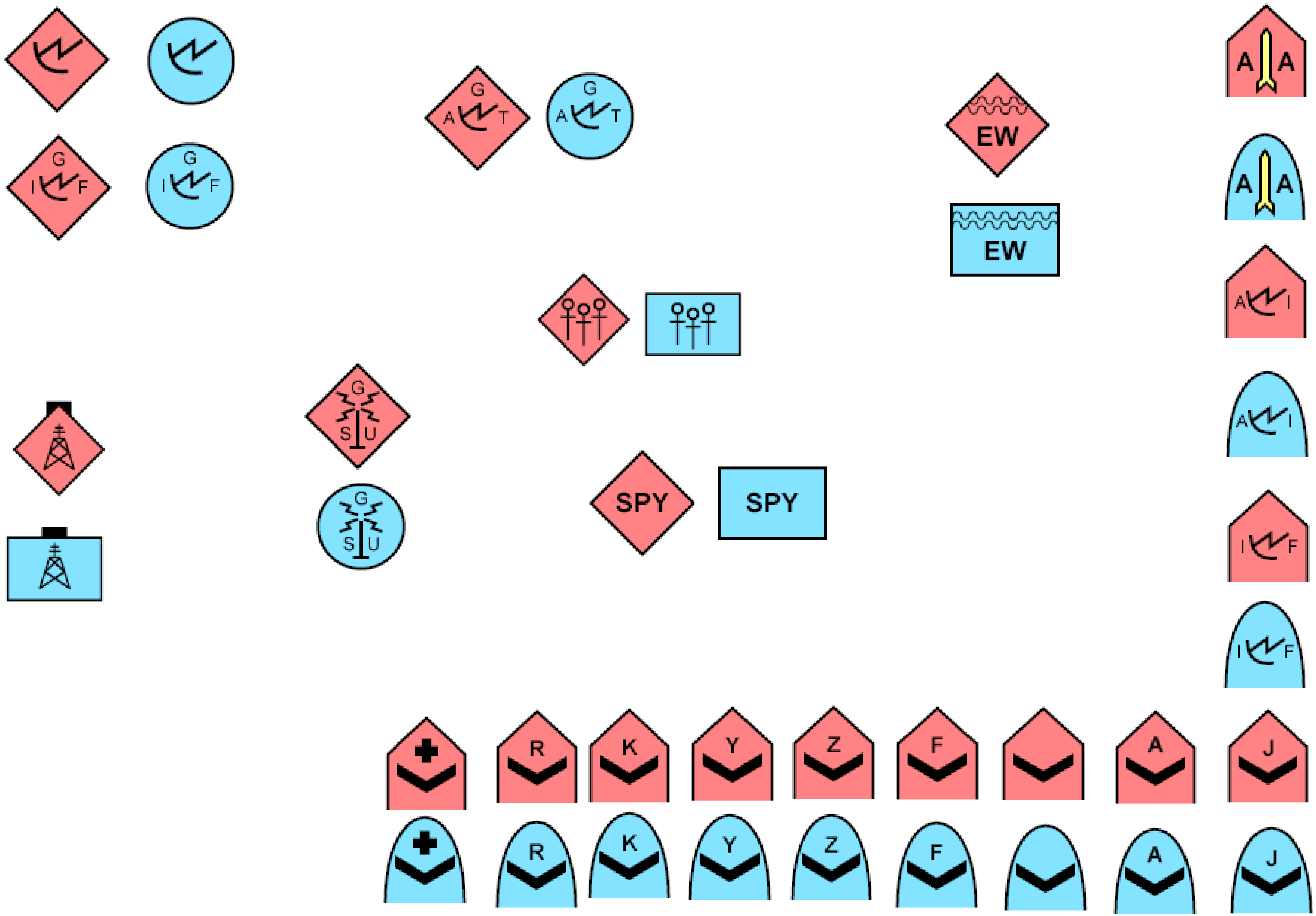


t_180_07
t_280_1
vehicle_ID001
vehicle_ID003
t_183_00
t_281_01
t_281_02

privacy or confidentiality	keeping information secret from all but those who are authorized to see it.
data integrity	ensuring information has not been altered by unauthorized or unknown means.
entity authentication or identification	corroboration of the identity of an entity (e.g., a person, a computer terminal, a credit card, etc.).
message authentication	corroborating the source of information; also known as data origin authentication.
signature	a means to bind information to an entity.
authorization	conveyance, to another entity, of official sanction to do or be something.
validation	a means to provide timeliness of authorization to use or manipulate information or resources.
access control	restricting access to resources to privileged entities.
certification	endorsement of information by a trusted entity.
timestamping	recording the time of creation or existence of information.
witnessing	verifying the creation or existence of information by an entity other than the creator.
receipt	acknowledgement that information has been received.
confirmation	acknowledgement that services have been provided.
ownership	a means to provide an entity with the legal right to use or transfer a resource to others.
anonymity	concealing the identity of an entity involved in some process.
non-repudiation	preventing the denial of previous commitments or actions.
revocation	retraction of certification or authorization.



SPY
EW
Friendly territory
Enemy territory

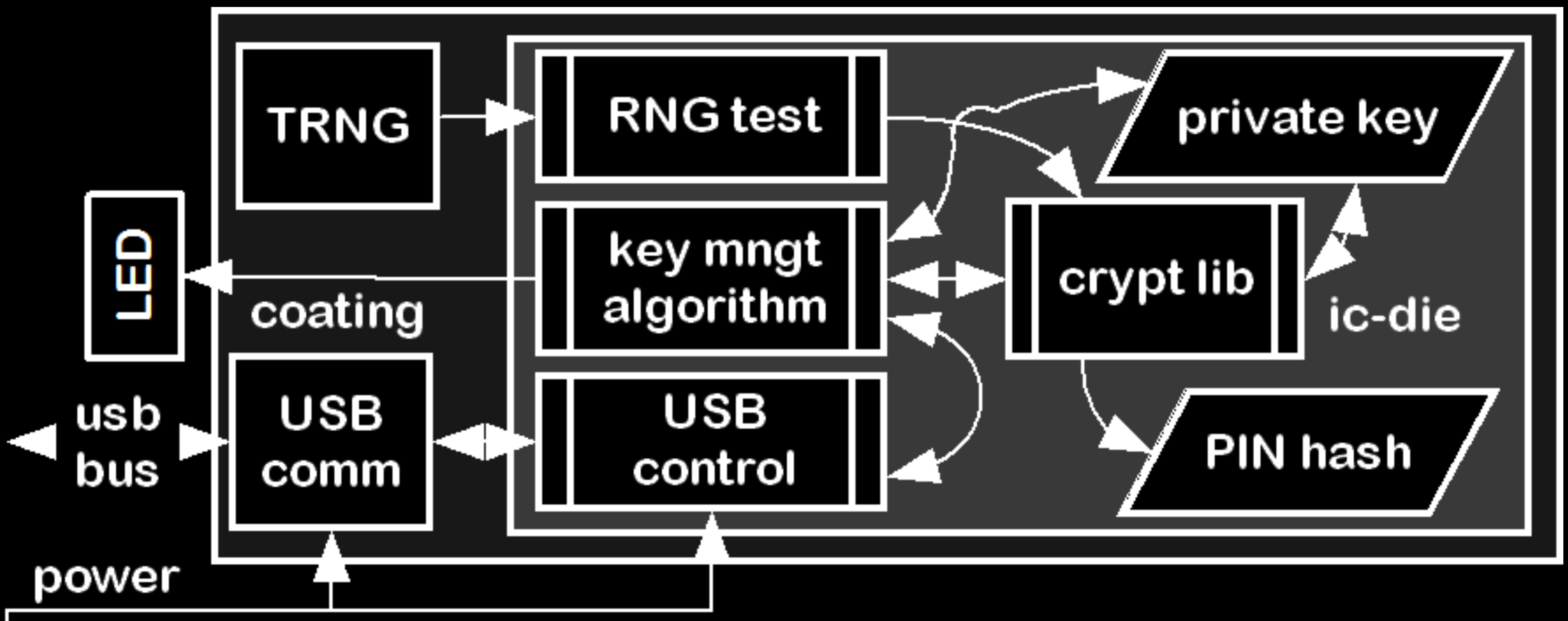

G
I F
A T
EW
EW
A A
A I
G
S U
SPY
SPY
R
K
Y
Z
F
A
J

A FEW STRATEGIES

FORTUNA Framework

- 5^{th} IEEE NSS, Milan, 2011
  - Initial version
  - Model plus tool
- JSS Elsevier, 2013
  - Model expansion
  - More tools
  - Architectural flaw on SPARC processor found

Example – Crypto Token



System Observations

1. A secure system can be composed of other systems (or components);
2. The security of systems has a probabilistic nature (not the attacks);
3. Individually insecure (with respect to a given policy) components can be arranged in the form of a secure system;
4. Secure components (with respect to a given policy) may be arranged into an insecure system;
5. Ultimately, all components are physical. Logical components are abstractions represented in a particular physical component configuration (or state);
6. There are no complete descriptions of non-trivial practical systems;
7. Every component has an associated cost for its deployment;
8. Certain (typically local) components are associated with adversary rewards;

Extracted Properties I

B1. Interaction channel: every subsystem that can be composed with others has one interaction channel. This interaction channel may be a logical abstraction, providing a communication channel. The channel can be directed or not.

B2. Entropic potential: represents the information assets that generate benefits for the opponent. Measured in bits.

B3. Entropic impedance (or resistance to leakage): quantifies the permeability of components and interaction channels to entropy. It is given as the probability that a given entropy amount migrates in a given timeframe from A to B trough an channel AB.

Extracted Properties II

B4. Implicit security: components with a certain set of security policies are subject to different attacks. Each attack has a different cost and a different success probability.

B5. Security provided: expresses the ability an (directional) interaction has of transporting the implicit security experienced by a component A to a component B. Together with the implicit security, it expresses the ``protection relationship''.

Models

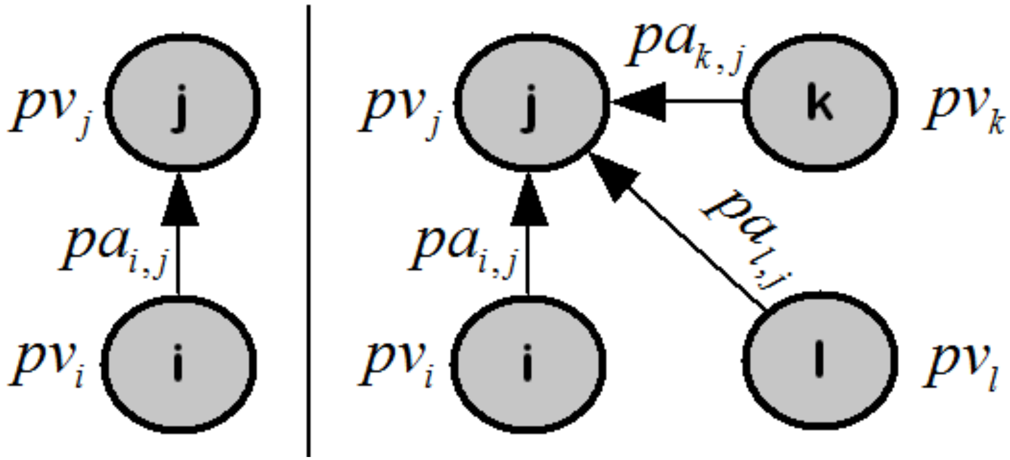
- Our observations and properties are used to produce models where security characteristics can be explored
- We investigated three models:
  - Two are graph-based:
    - Model 1: Bit leakage
    - Model 2: Adversary path
  - One is based on Decision Theoretic Probabilistic ProLog - DTProbLog

Graph Model 1 – Bit-Leakage

- Uses Properties B1, B2, and B3: interaction channel, entropic potential, and entropic impedance
- Let *D = (V, A)* be a digraph representing a related system and external agents that interact with it
- Each vertex *i* from V represents a system component or a principal. Each arc *ij* from *A* represents a interaction channels (B1).
- Let *s* be a bit of the secret (B2) which the system protects and that the adversary aims

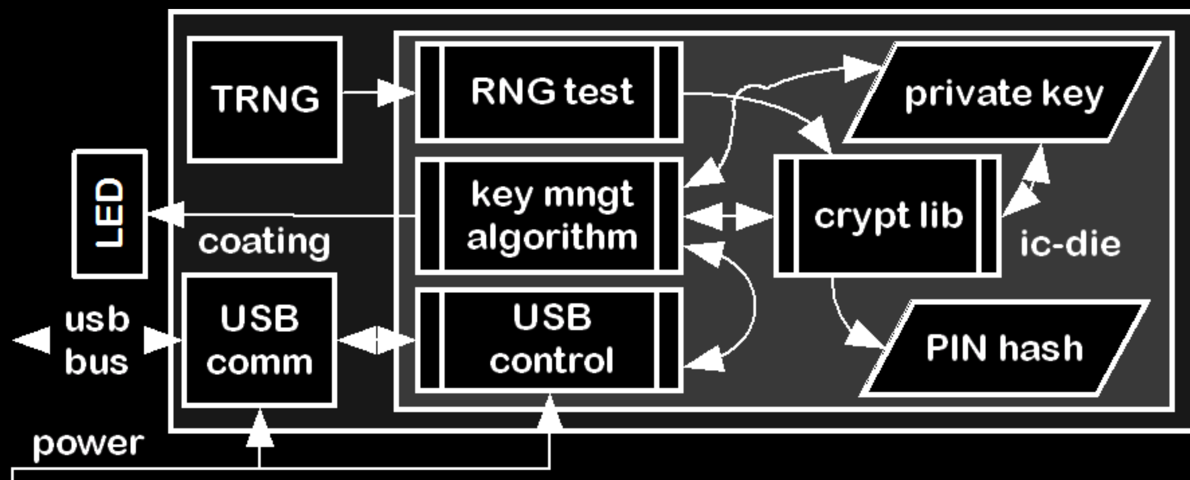
Graph Model 1 – Bit-Leakage II

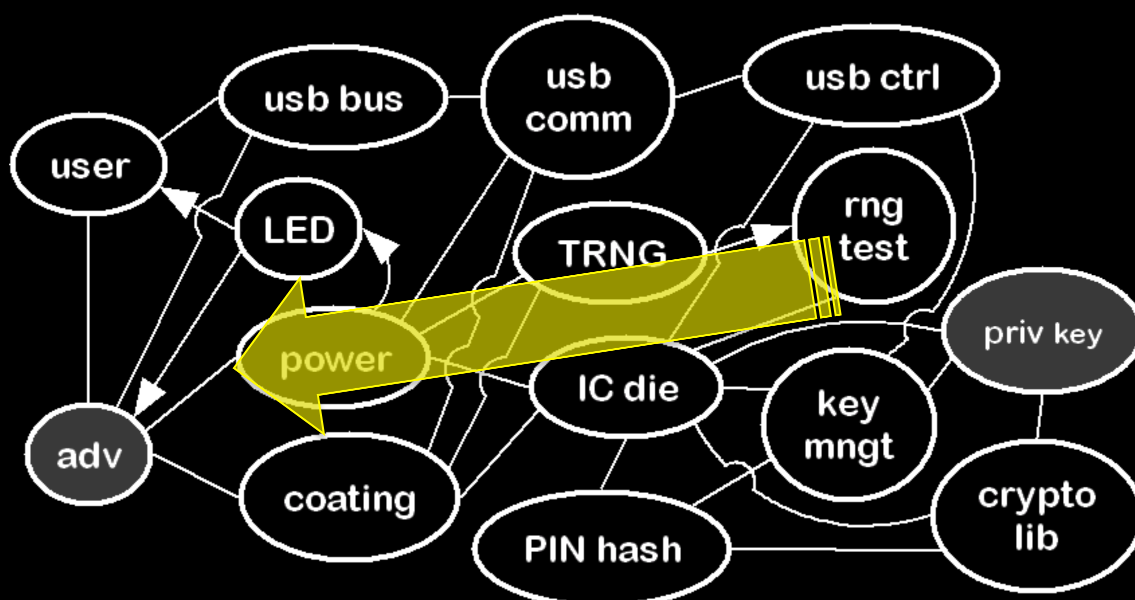
- Vertex *i* has probability pv_i of knowing *s*
- By properties B1 and B3, *s* leaks from its container (say i) through the arcs *ij* with probability $pa_{i,j}$
- We are interested in minimizing pv_k for the vertex *k* that represents the attacker



$$pv_j = pa_{i,j} \times pv_i$$

$$pv_j = 1 - \prod_{i \in N_D^-(j)} (1 - pv_i \times pa_{i,j})$$


TRNG
RNG test
private key
LED
key mngt
algorithm
crypt lib
coating
ic-die
usb
bus
USB
comm
USB
control
PIN hash
power

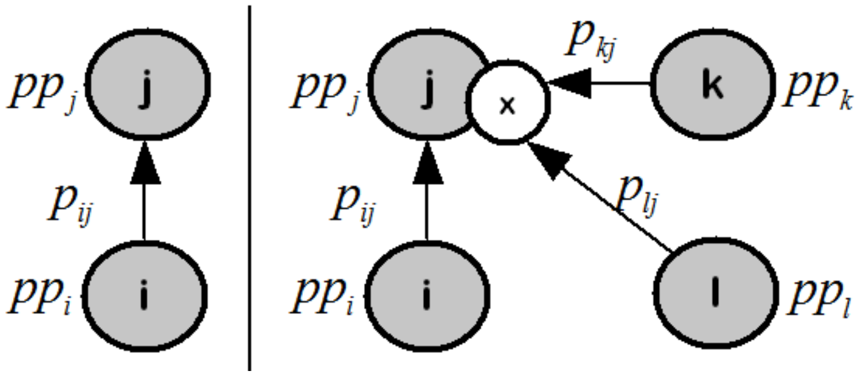

usb bus
usb
comm
usb ctrl
user
LED
TRNG
rng
test
priv key
power
IC die
key
mngt
adv
coating
crypto
lib
PIN hash

Graph Model 2 – Attack Path

- Uses Properties B1, B4, and B5: implicit security, security provided
- Let $D = (V, A)$ be a connected digraph representing part of a system.
- Each vertex *i* of V represents a system component that can establish relations of protection. To each vertex *i* there is a related cost e_v. Each arc *ij* of A represents protection relationships.

Graph Model 2 – Attack Path

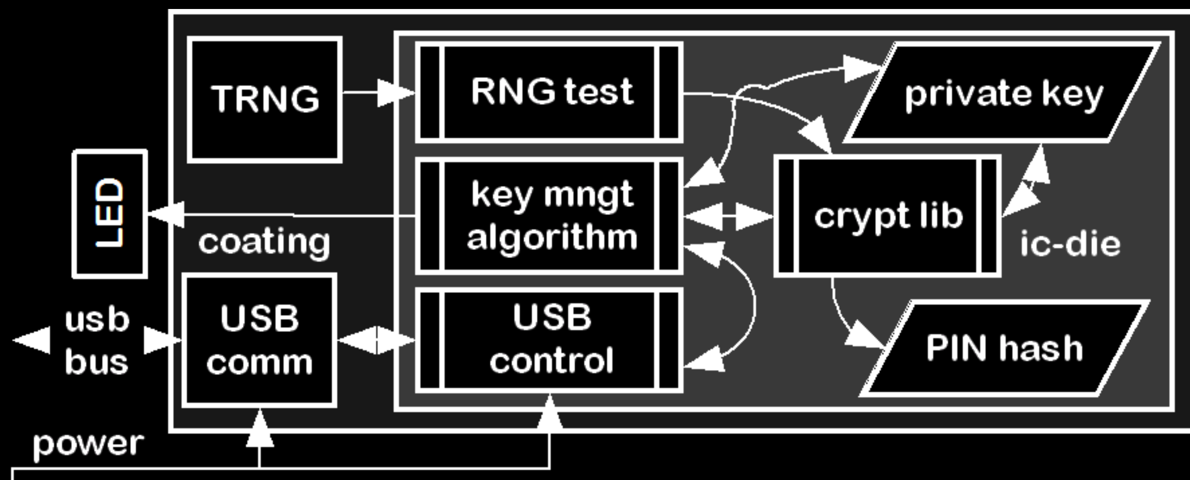
- By B4, for each arc *ij* of *A* there is a violation cost c_{ij} associated with a given probability of succesful attack pp_{ij}.
- The arcs incident on *j* can be composed in and/or form.
- Let C be a subset of V representing the system's CSP. To each vertex *j* of *C* is associated a gain g_j.
- We are interested in making the best attack plan more expensive than the expected gain for the adversary.

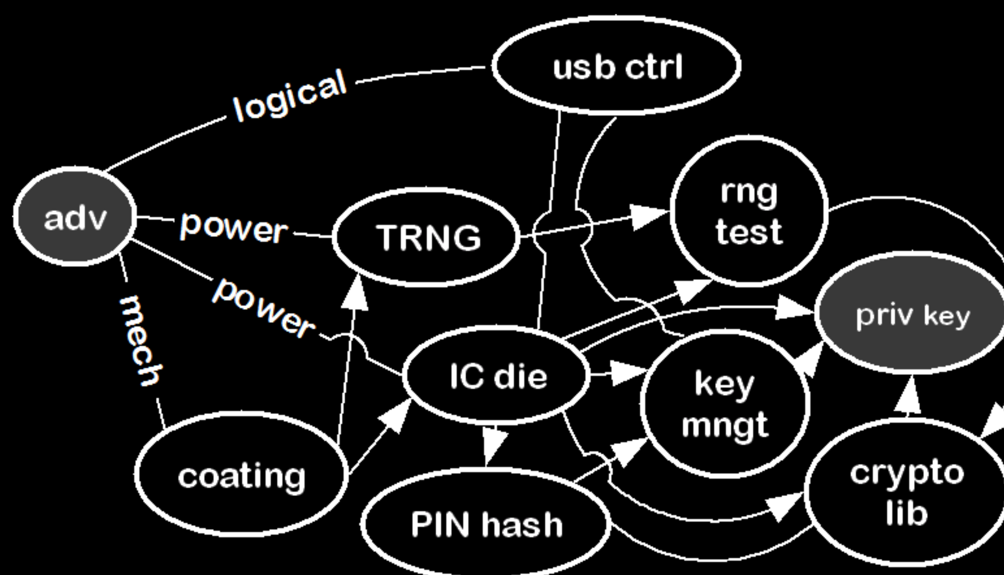


$$pp_j = 1 - \prod_{X \in N_D^-} \left(1 - \prod_{i \in X} p_{ij} \right)$$

$$e_j = e_{ij} = \frac{f(p_{ij})}{p_{ij}} + e_i$$

$$e_j = min \left(\sum_{x \in X} e_{xj}, \sum_{y \in Y} e_{yj}, ..., \sum_{z \in Z} e_{zj} \right)$$


TRNG
RNG test
private key
LED
key mngt
algorithm
crypt lib
coating
ic-die
usb
bus
USB
comm
USB
control
PIN hash
power


usb ctrl
logical
adv
power
TRNG
rng
test
power
priv key
mech
IC die
key
mngt
coating
crypto
lib
PIN hash

Model Results – Policy 1

- Policy 1: "Grant system principals the least privileges necessary to perform their jobs"
- Theorem 1: Policy 1 either does not affect, or it improves the overall system security regarding confidentiality CSPs
- Proof 1: Comes from equation for pv_j in model 1 by arc removal where *j* is the vertex that represents the adversary

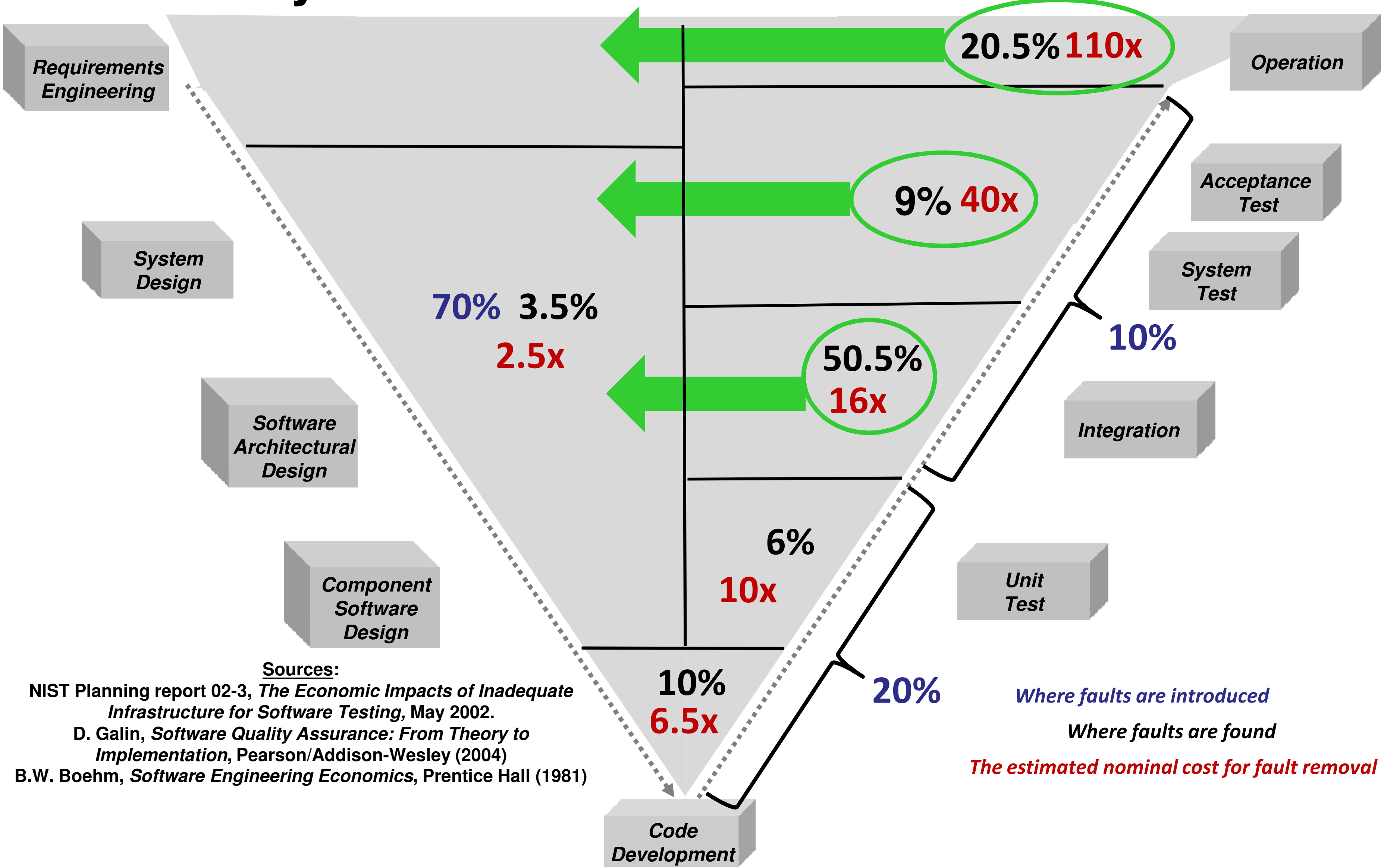
Model Results – Policy 2

- Policy 2: "Minimize the size of the Trusted Computing Base"
- Theorem 2: Policy 2 does not always hold for integrity CSPs
- Proof 2: We use model 2. It suffices to show that we can arbitrarily increase system security by increasing the size of the TCB

Assurance Cases

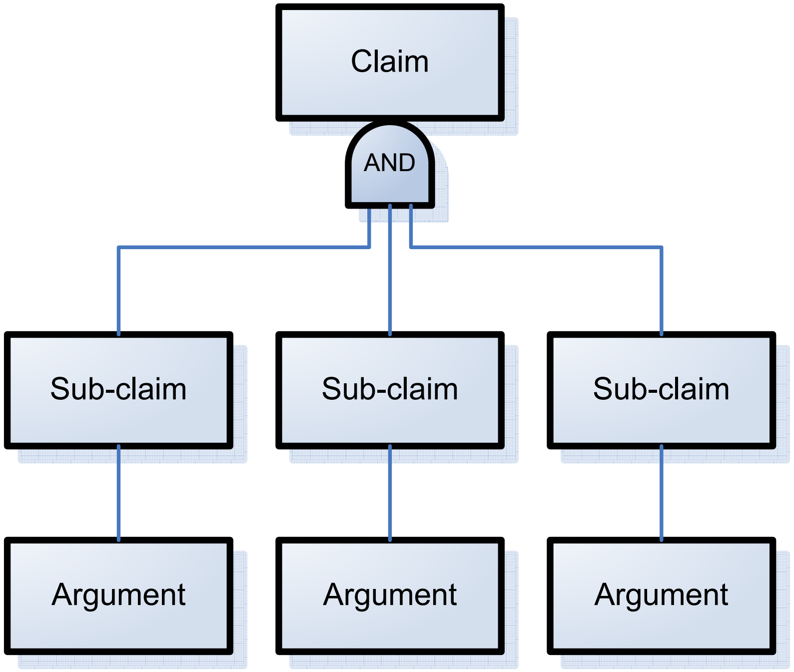
- Showed how to train and coordinate highly-productive team by using AC (IFIP WISE 9, 2015, Hamburg)
- Novel ability to *predict* hardware architectural security flaws on Intel microprocessor (ARES 2015, to appear, Toulouse)
- Analysis automation (undergoing work)

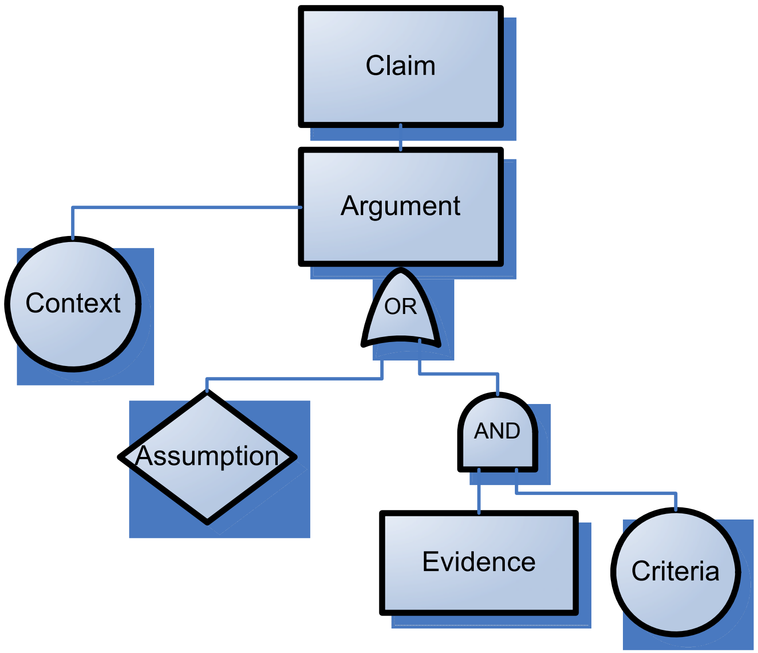
Cost & Time Reduction due to Early Fault Discovery



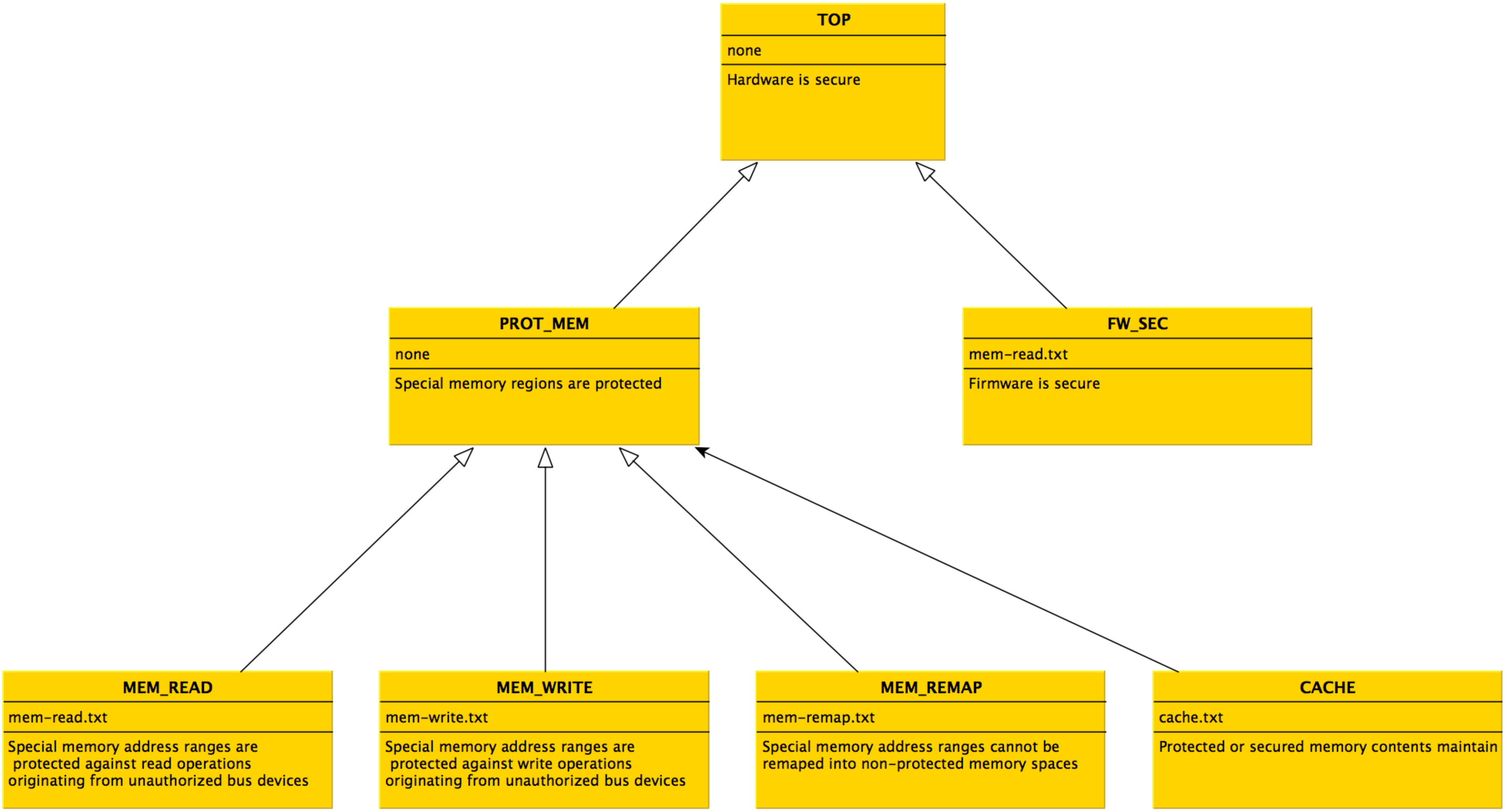
<u>Sources</u>:
NIST Planning report 02-3, *The Economic Impacts of Inadequate Infrastructure for Software Testing,* May 2002.
D. Galin, *Software Quality Assurance: From Theory to Implementation*, Pearson/Addison-Wesley (2004)
B.W. Boehm, *Software Engineering Economics*, Prentice Hall (1981)

Tech Enabler: Assurance Cases NATO AEP-67



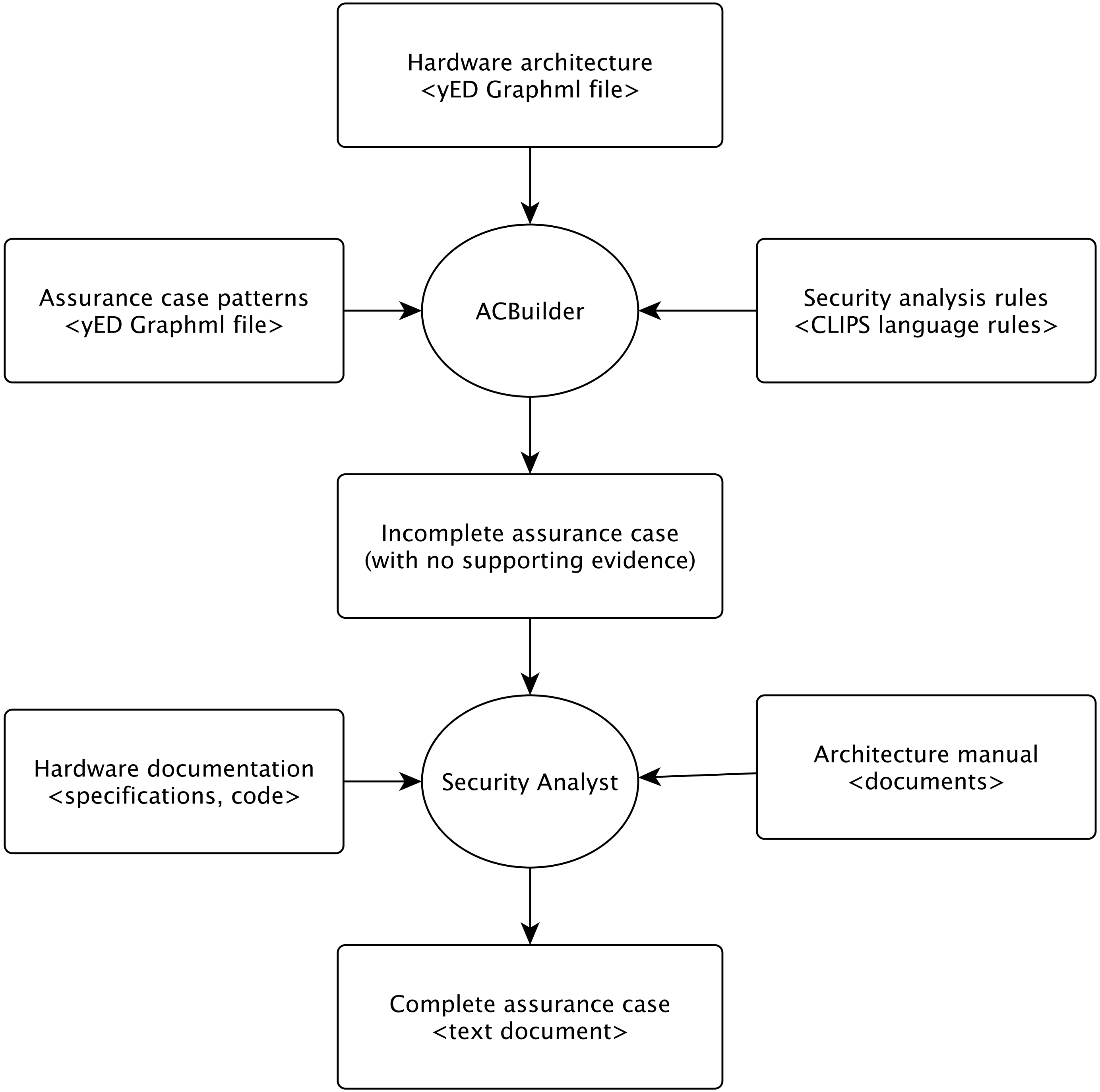


KAMM Example



Semi-formal, text-based

- **CLAIM A**: "The software implementation abides to its specifications", with **"medium assurance"**
  - "AND" **SUB-CLAIM-1**: "The software binary correctly corresponds to the source code", with **"high assurance"**
    - **CONTEXT-1.1**: "All source code is interpreted as ISO/IEC 9899:1999 standard";
    - **ARGUMENT-1.1**: "The source code is compiled with a compiler that correctly translates the source code to binaries" with **"high assurance"**
      - **EVIDENCE-1.1**: "The used compiler is CompCert, which is formally verified"
      - **CRITERION**: "Compiler with formal verification" for "high assurance"
  - "AND" **SUB-CLAIM-2**: "The source code abides to its specifications", with **"high assurance"**
    - ...
  - ...
- **CLAIM B**: ...


Hardware architecture
<yED Graphml file>
Assurance case patterns
<yED Graphml file>
ACBuilder
Security analysis rules
<CLIPS language rules>
Incomplete assurance case
(with no supporting evidence)
Hardware documentation
<specifications, code>
Security Analyst
Architecture manual
<documents>
Complete assurance case
<text document>