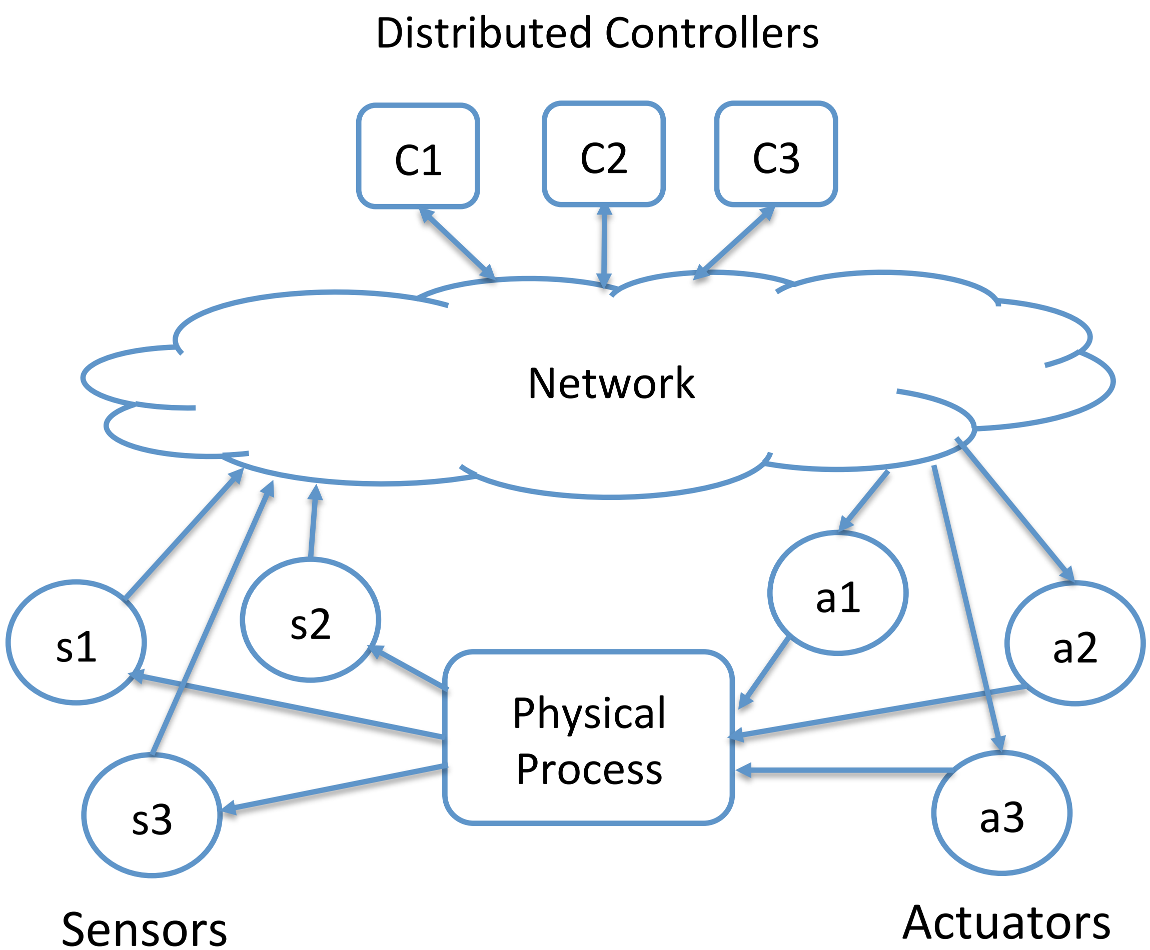
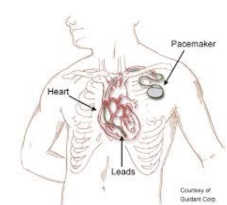
ARTINALI: Dynamic Invariant Detection for Cyber-Physical System Security

Maryam Raiyat Aliabadi, *Amita Kamath,*

Julien Gascon-Samson, Karthik Pattabiraman

Cyber-Physical Systems





Motivation

CPS Security Requirements

Real-time constraints

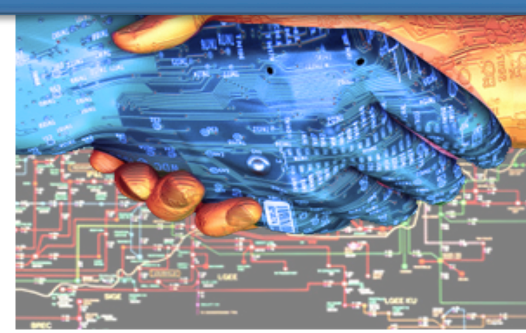
Resource constraints

Goal :

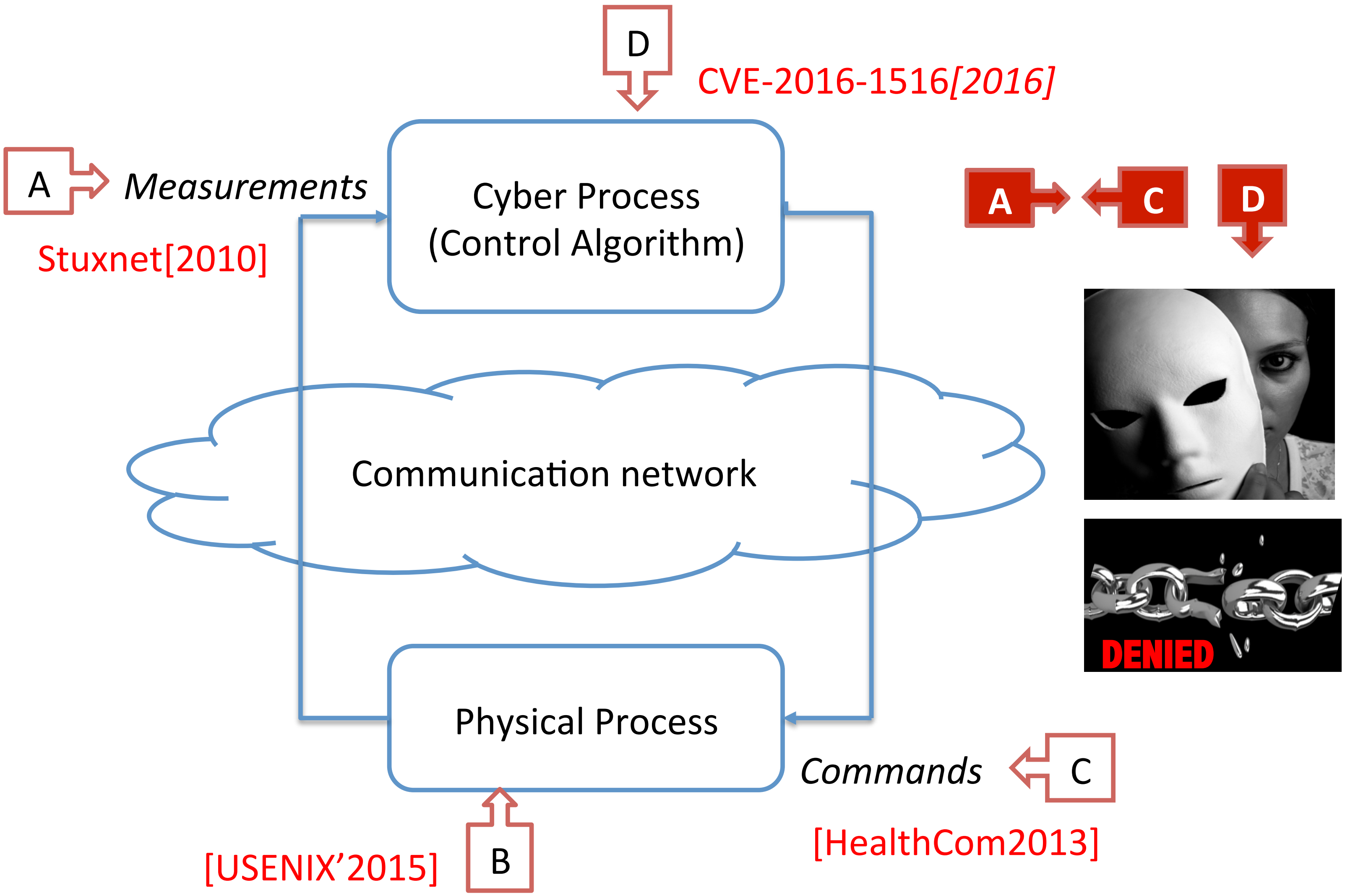
Design an **Automated, Real-time** and **Attack-neutral** security solution for CPSes with respect to their **resource constraints**

Zero-day attacks

No human-in-the-loop



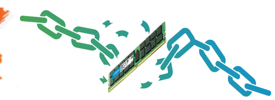
Threat Model



Previous work

- Intrusion Detection System (IDS)
  - Signature-based IDSs [CSUR2014]

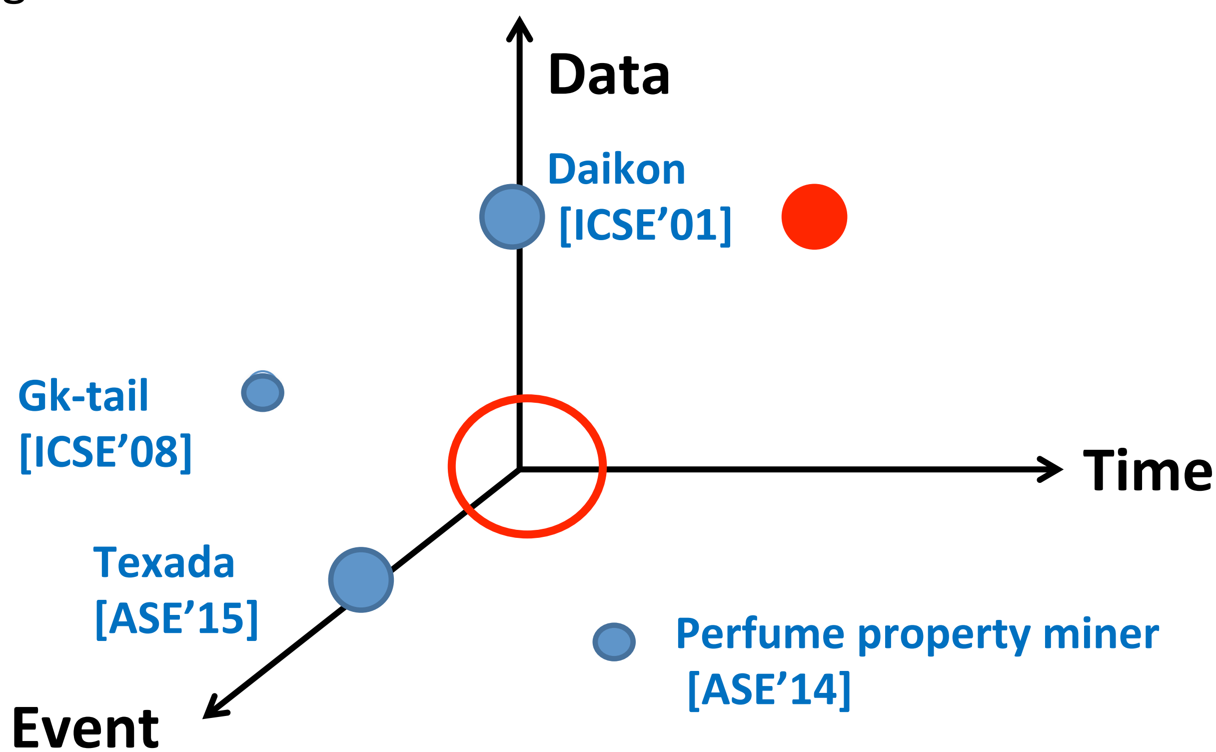
  - Anomaly-based IDSs [Computers&Security2009]



  - Specification-based IDSs [SmarGridCom2010]
    - Static analysis
    - Dynamic analysis

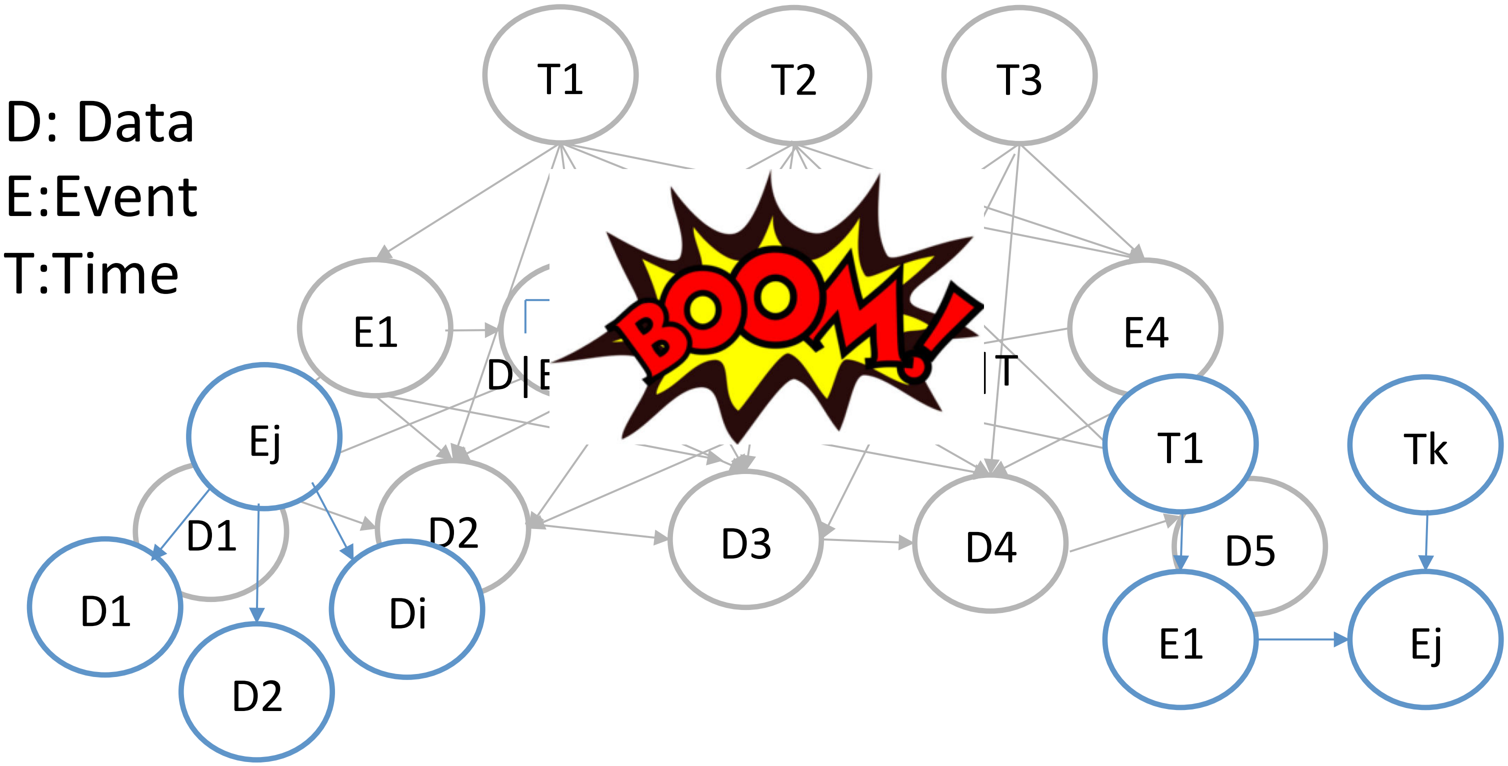
Dynamic Analysis-based Techniques
(Invariant-based)

- Invariant
  - Energy usage >=0



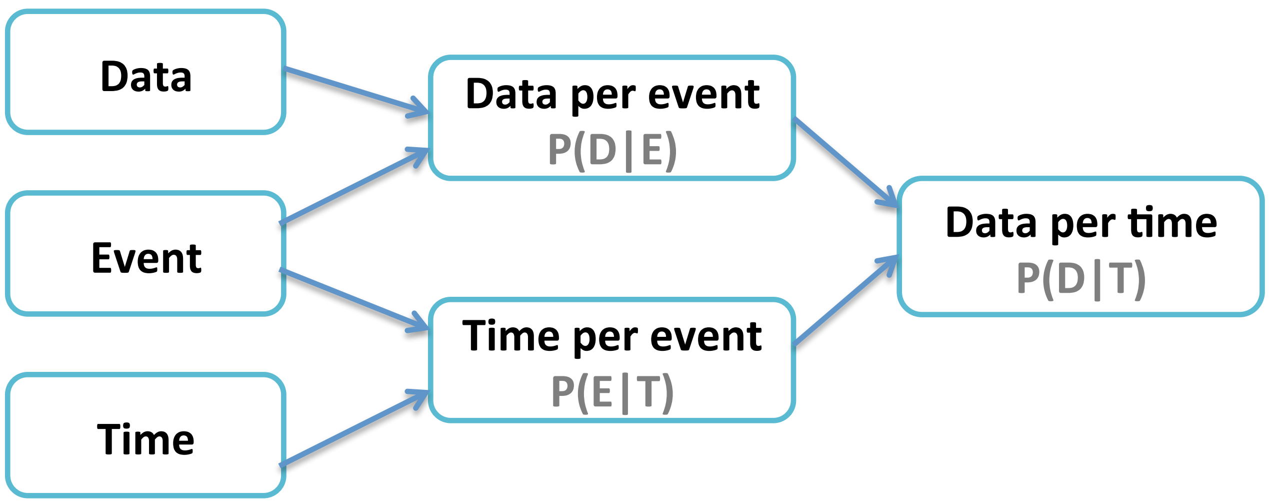
Main Idea: Break down the search space

D: Data
E:Event
T:Time



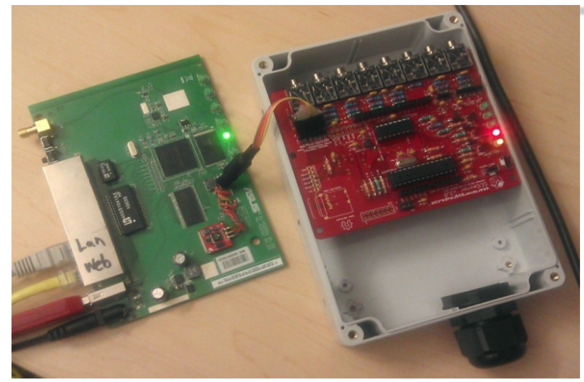
Methodology

- **ARTINALI**: **A** **R**eal **T**ime-specific **I**nvariant i**N**ference **AL**gor**I**thm
  - 3 dimensions and 6 classes of invariants

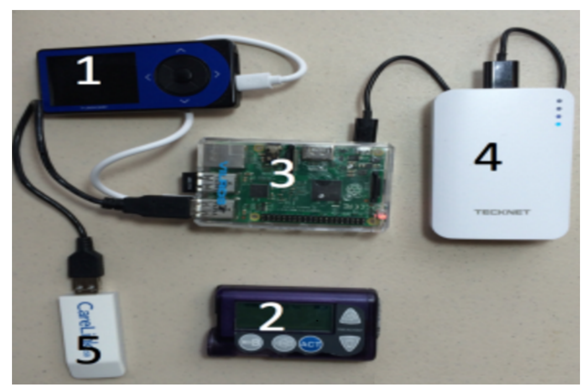


CPS platforms

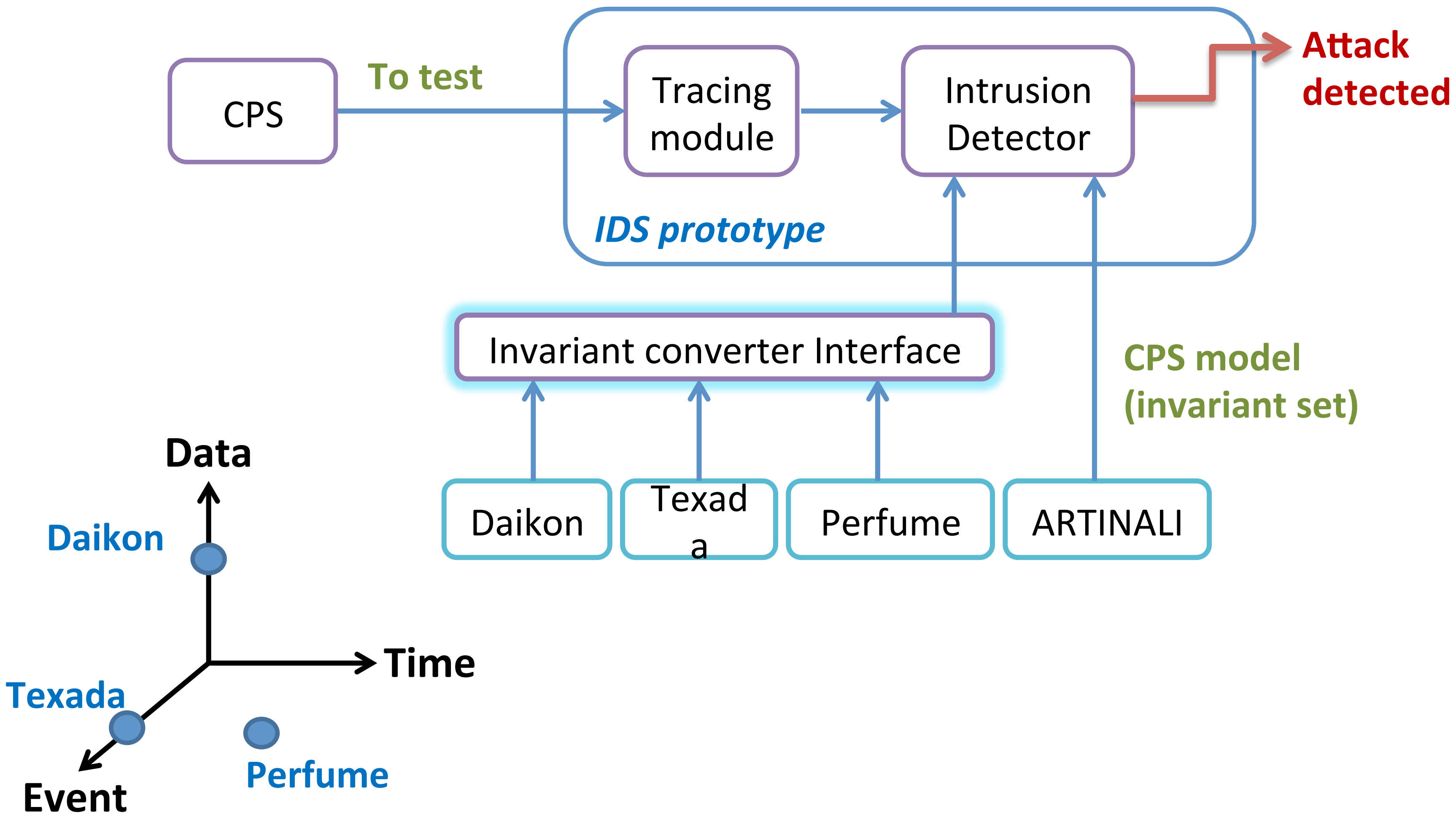
- Advanced metering infrastructure (AMI)
  - SEGMeter
    - http://smartenergygroups.com



- Smart Artificial Pancreas (SAP)
  - OpenAPS
    - https://openaps.org/



Intrusion Detection System



Targeted attacks

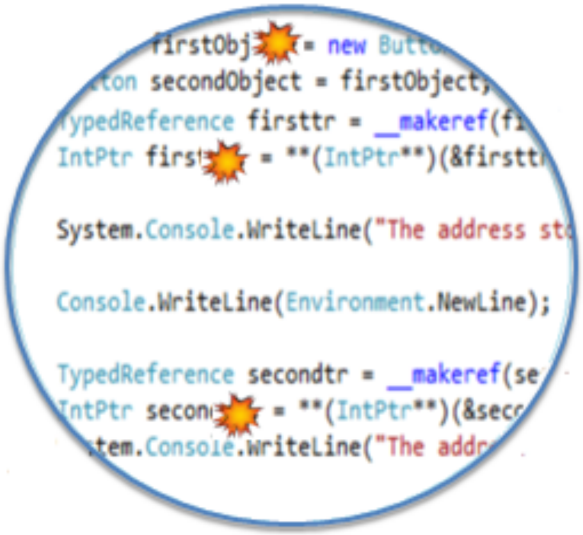
CPS Platform	Targeted attack	Attack entry point
AMI (SEGMeter)	Meter spoofing [ACSAC2010]	Deception on A
	Sync. Tampering [ACSAC2010]	Deception on D

Take away :

ARTINALI detected all targeted attacks successfully

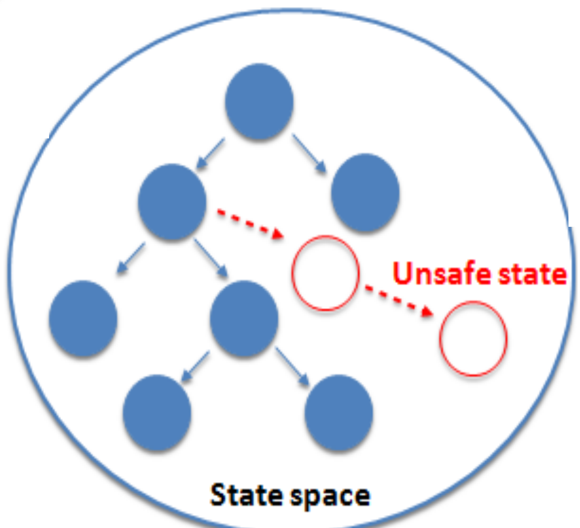
Arbitrary Attacks

Data mutations



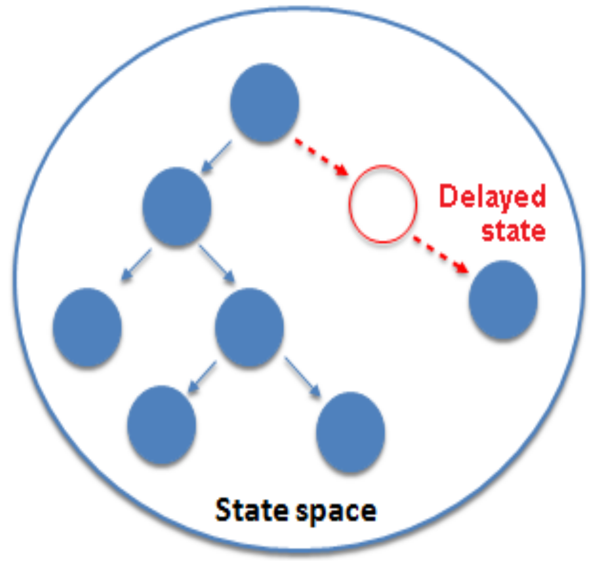
Smart facial recognition system (CVE-2016-1516)

Branch flipping



CGM spoofing in SAP, [BHC2011]

Artificial delay insertion



Synchronization tampering in smart meter, [ACSAC2010]

Accuracy Metrics

- False Negative Rate (FNR)

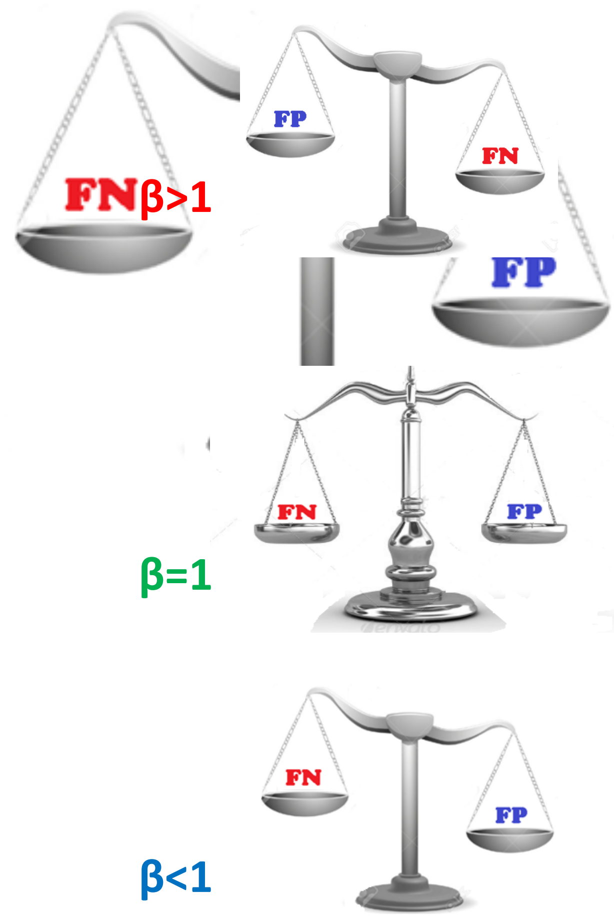
$$\frac{\textit{Number of detected attacks}}{\textit{Total number of injected attacks}} \times 100$$

- False Positive Rate (FPR)

$$\frac{\textit{Number of raised alarms}}{\textit{Total number of attack-free tests}} \times 100$$

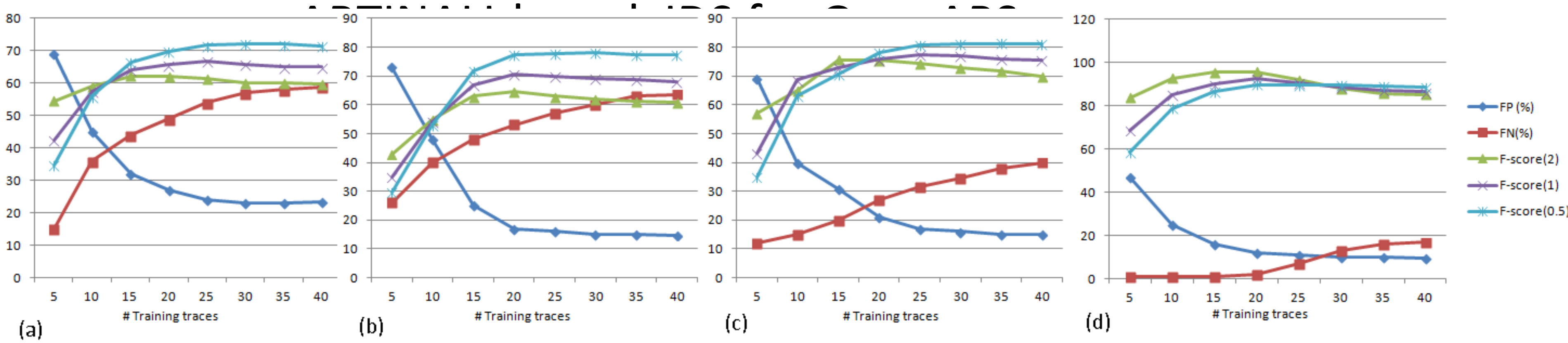
- F-Score(β)

$$\frac{(1+\beta^2)\times TP}{(1+\beta^2)\times TP+\beta^2\times FN+FP}$$

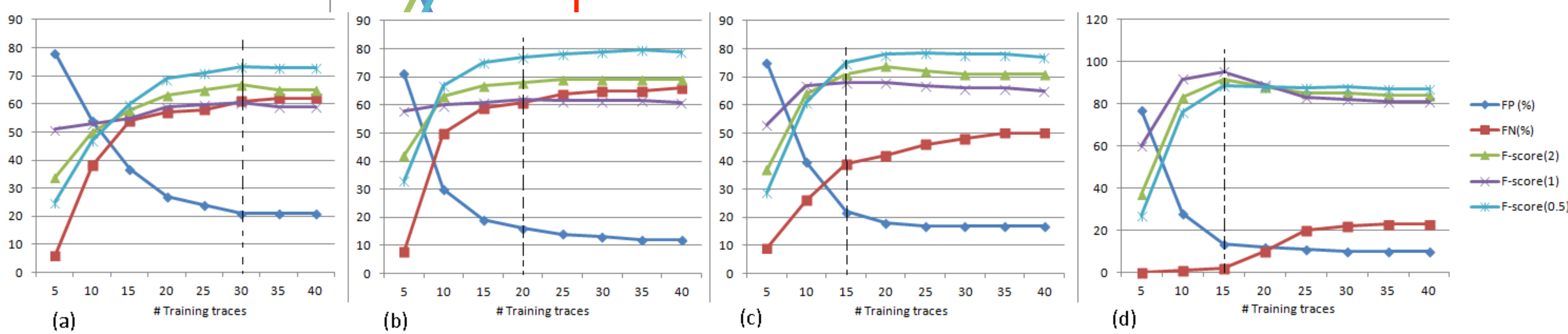


F-Score(β)- Tuning/Training

SEGMeter



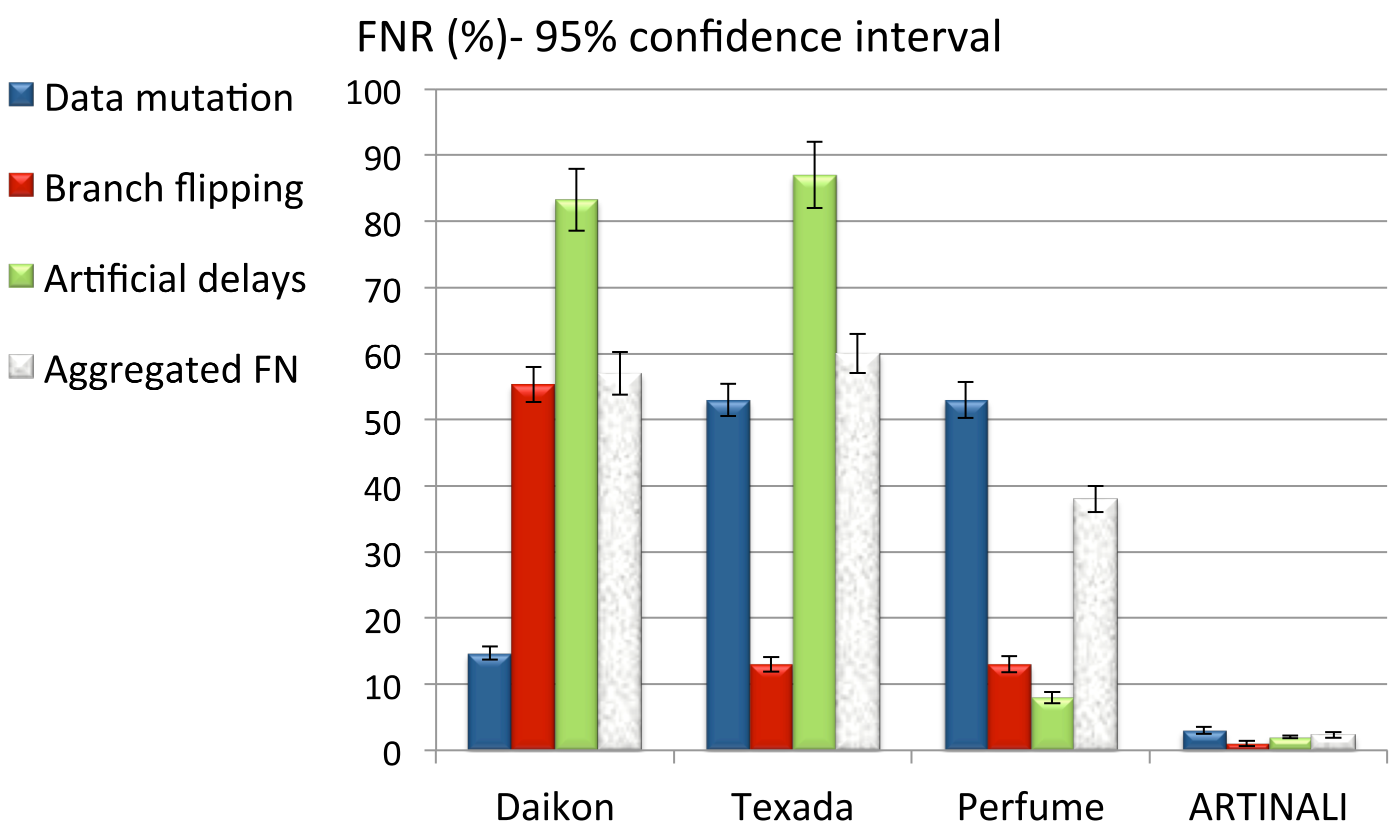
OpenAPS



(a) Daikon (b) Texada (c) Perfume (d) ARTINALI

False Negatives' Rate

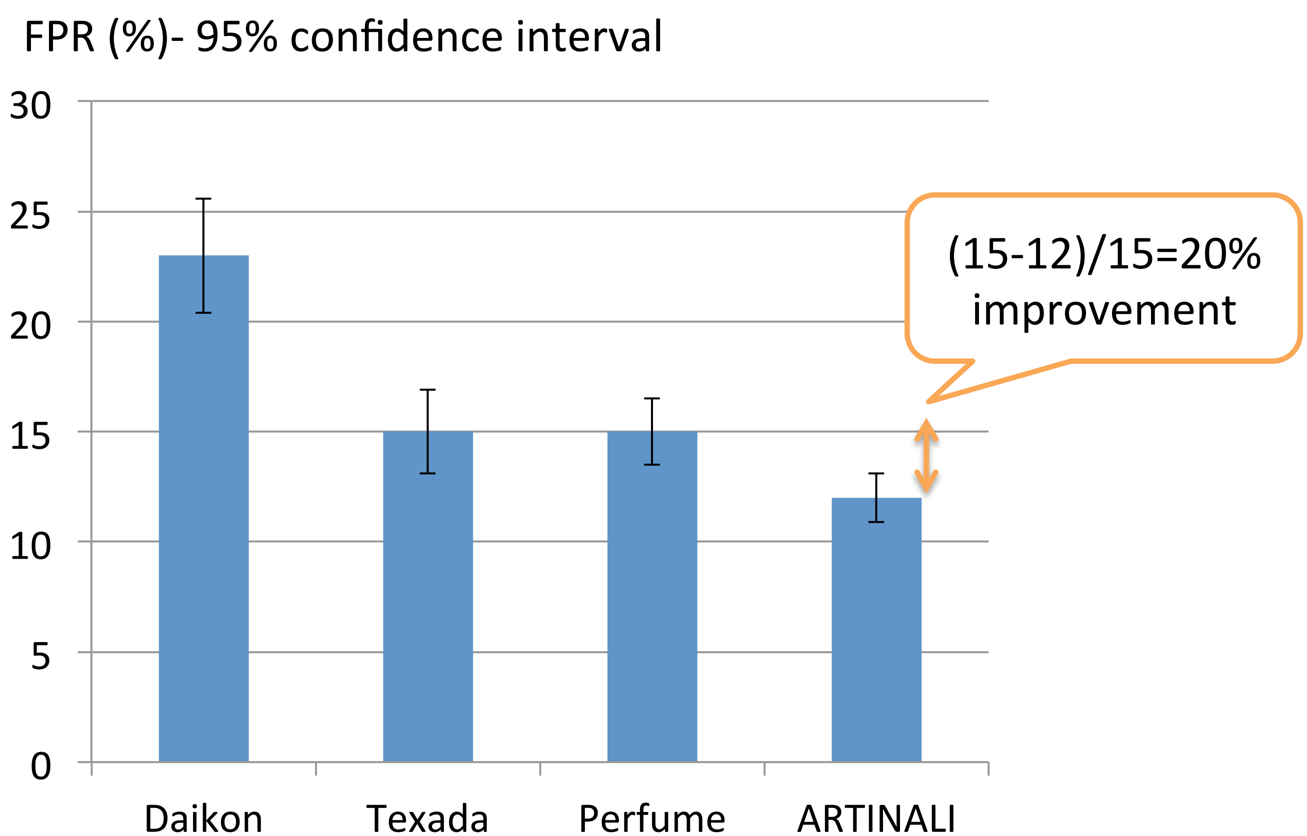
- ARTINALI-based IDS reduces the ratio of FN by 89 to 95% compared with the other tools across both platforms.
  - SEGMeter



False Positives' Rate

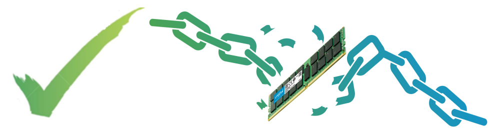
- ARTINALI-based IDS reduces the ratio of FP by 20 to 48% compared with the other tools across both platforms.

  - SEGMeter

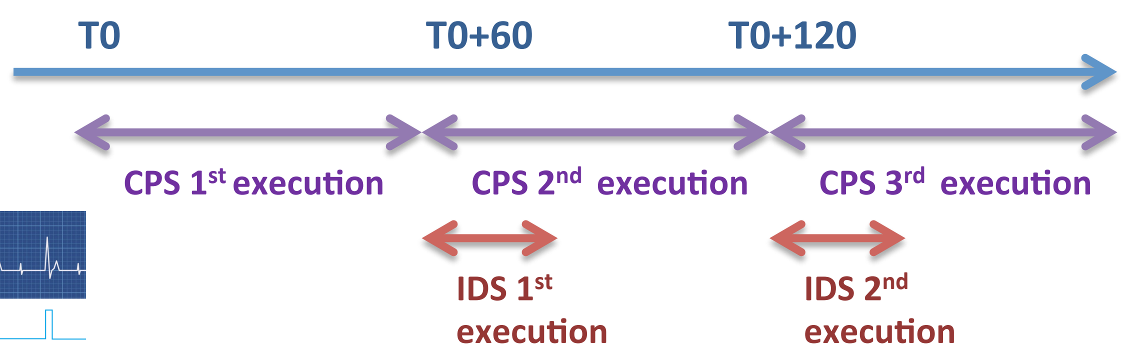


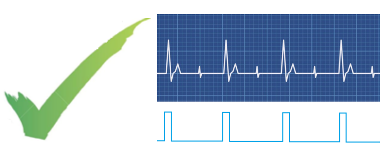
Overheads

SEGMeter



	Performance Overhead (%)	Detection time (sec)	Memory usage
Daikon	27.3	16.63	1.24 MB
Texada	23.7	14.45	3.21 MB
Pefume	32.08	19.57	3.94 MB
ARTINALI	31.6	19.25	2.96 MB





Summary and Future Work

- ARTINALI: A Multi-Dimensional model for CPS
  - Captures *data-event-time* interplay
  - Introduces *Real-time data invariants*
  - Increases the *coverage* of IDS
  - Decreases the rate of *false positives*
  - Imposes comparable *overheads*
- Examine generalizability of ARTINALI
  - Unmanned Aerial Vehicle (UAV)
- https://github.com/karthikp-ubc/Artinali