IM-DISCO: Invariant Mining for Detecting IntrusionS in Critical Operations

GUILHERME SARAIVA [1], **FILIPE APOLINÁRIO [1]**, MIGUEL L. PARDAL [2]
INOV INESC INOVAÇÃO [1], INESC-ID [2], Instituto Superior Técnico (IST), Lisboa

CPS4CIP 2023, Hague, Netherlands - 28, Sep., 2023

STARLIGHT

Cyber-Physical Systems

Monitor and control physical processes

Contained in **Critical Infrastructures**

- Transportation Networks

Cyber-Physical Systems

Monitor and control physical processes

Contained in **Critical Infrastructures**

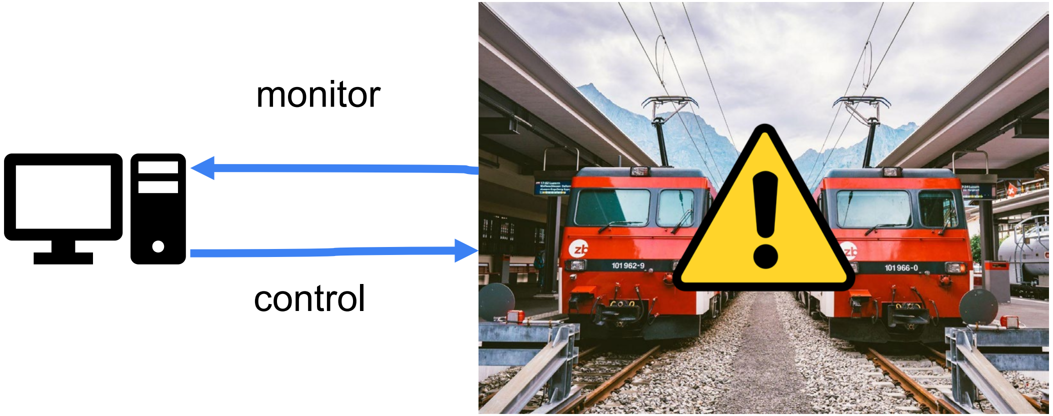
- Transportation Networks

Cyber-Physical Systems - Problem

Vulnerable to **cyber-physical attacks**

- Ex: **Ransomware** attack on a railway in Denmark

Access the actuators to disrupt operations

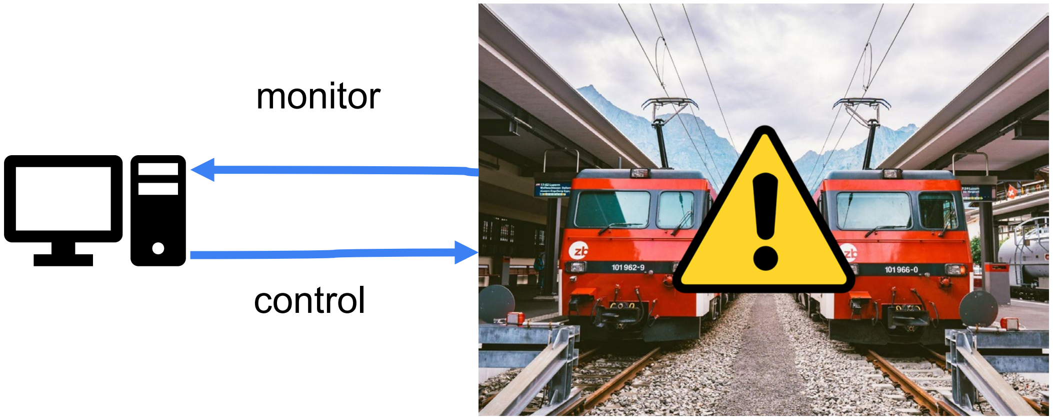


Cyber-Physical Systems - Problem

Vulnerable to **cyber-physical attacks**

- Ex: **Ransomware** attack on a railway in Denmark

Access the actuators to disrupt operations



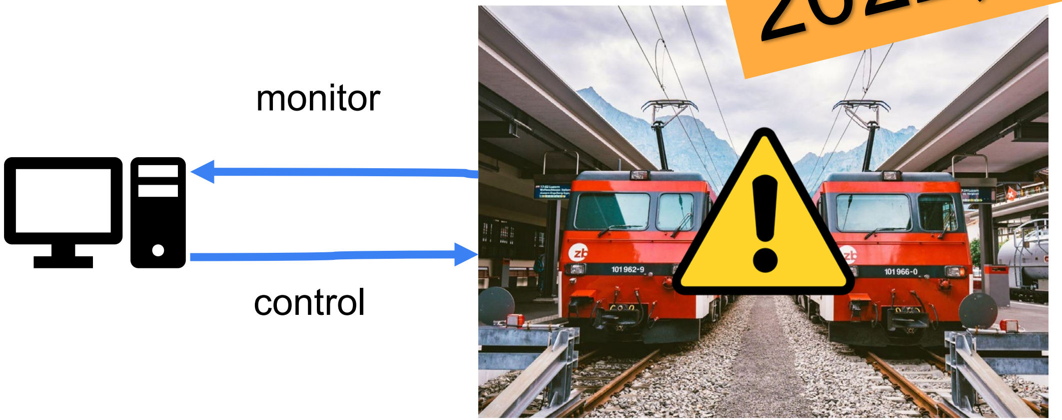
Cyber-Physical Systems - Problem

Vulnerable to **cyber-physical attacks**

- Ex: **Ransomware** attack on a railway in Denmark

Access the actuators to disrupt operati

2022, Denmark



Cyber-Physical Systems - Problem

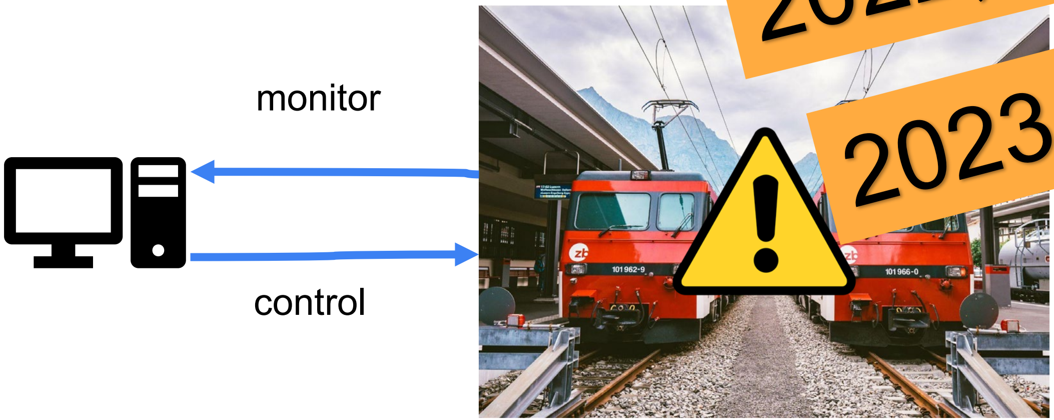
Vulnerable to **cyber-physical attacks**

- Ex: **Ransomware** attack on a railway in Denmark

2022, Denmark

2023, Poland

Access the actuators to disrupt operati



Cyber-Physical Systems - Example

Train cyber-physical system

Cyber-Physical Systems - Example

Train cyber-physical system

Sensors
- velocity
- acceleration
- temperature
- …

Cyber-Physical Systems - Example

Train cyber-physical system

Sensors
- velocity
- acceleration
- temperature
- …

Actuators
- brakes
- throttle
- doors
- …

Cyber-Physical Systems - Example

Train cyber-physical system

Sensors
- velocity
- acceleration
- temperature
- …

Actuators
- brakes
- throttle
- doors
- …

Operational Modes

- Riding
- arriving station
- on station
- leaving station

Cyber-Physical Systems - Example

Train cyber-physical system

Sensors
- velocity
- acceleration
- temperature
- ...

Actuators
- brakes
- throttle
- doors
- ...

Operational Modes

- riding
- arriving station
- on station
- leaving station

Cyber-Physical Systems - Example

Train cyber-physical system

Sensors
- velocity
- acceleration
- temperature
- …

Actuators
- brakes
- throttle
- doors
- …

Operational Modes

- riding
- arriving station
- on station
- leaving station

Cyber-Physical Systems - Example

Train cyber-physical system

Sensors
- velocity
- acceleration
- temperature
- ...

Actuators
- brakes
- throttle
- doors
- ...

Operational Modes

- riding
- arriving station
- on station
- leaving station

Cyber-Physical Systems - Example

Train cyber-physical system

Sensors
- velocity
- acceleration
- temperature
- ...

Actuators
- brakes
- throttle
- doors
- ...

Operational Modes
- riding
- arriving station
- on station
- leaving station

Cyber-Physical Systems - Example

Train cyber-physical system

Sensors
- velocity
- acceleration
- temperature
- ...

Actuators
- brakes
- throttle
- doors
- ...

Operational Modes

- riding
- arriving station
- on station
- leaving station

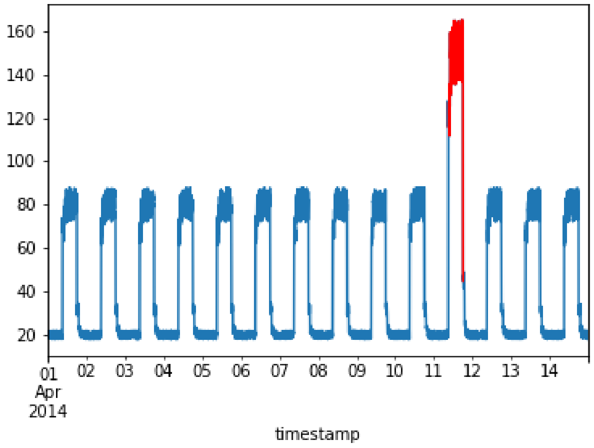
Intrusion Detection Systems

Passively collects and analyzes different data source

Anomaly Detectors:

[+] Detect novel attacks

[-] Incomprehensible alarms



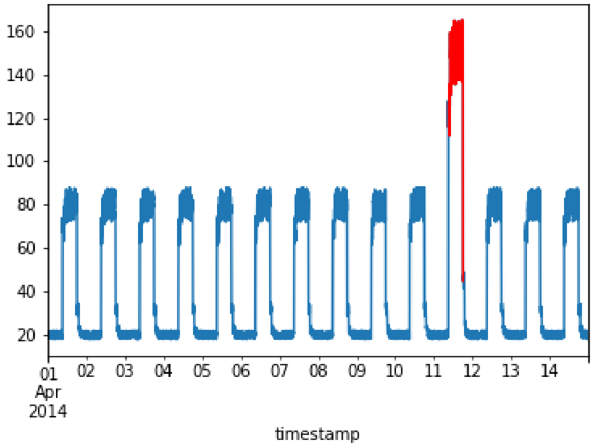
Intrusion Detection Systems

Passively collects and analyzes different data source

Anomaly Detectors:

[+] Detect novel attacks

[-] Incomprehensible alarms



Anomaly!

Invariant Rules

Physical conditions that must be sustained to maintain the normal functioning of the system

Anomaly - process value that violates the rules

Ex:

$$\textbf{(velocity > 20m/s} \wedge \textbf{station\_distance > 40m)} \vee \textbf{(station\_distance < 40m)} \Rightarrow \textbf{brakes = ON}$$

Invariant Rules

Physical conditions that must be sustained to maintain the normal functioning of the system

Anomaly - process value that violates the rules

Ex:

$$(velocity > 20m/s \land station\_distance > 40m) \lor (station\_distance < 40m) \Rightarrow brakes = ON$$

Invariant Rules

Physical conditions that must be sustained to maintain the normal functioning of the system

Anomaly - process value that violates the rules

Ex:

$$(\text{velocity} > 20\text{m/s} \wedge \text{station\_distance} > 40\text{m}) \vee (\text{station\_distance} < 40\text{m}) \Rightarrow \boxed{\text{brakes} = \text{ON}}$$

Invariant Rules

Physical conditions that must be sustained to maintain the normal functioning of the system

Anomaly - process value that violates the rules

Ex:

$$\boxed{(\text{velocity} > 20m/s \land \text{station\_distance} > 40m)} \lor (\text{station\_distance} < 40m) \Rightarrow \text{brakes} = \text{ON}$$

Invariant Rules

Physical conditions that must be sustained to maintain the normal functioning of the system

Anomaly - process value that violates the rules

Ex:

$$(\text{velocity} > 20\text{m/s} \land \text{station\_distance} > 40\text{m}) \lor \boxed{(\text{station\_distance} < 40\text{m})} \Rightarrow \text{brakes} = \text{ON}$$

Invariant Rules

Physical conditions that must be sustained to maintain the normal functioning of the system

Anomaly - process value that violates the rules

Ex:

(velocity > 20m/s ∧ station_distance > 40m) ∨ (station_distance < 40m) ⇒ brakes = ON

…

velocity = 26m/s, station_distance = 50, brakes = OFF, … ANOMALY!!

Invariant Rules - Problem

Complex rules may difficult the interpretation of the alarm

Ex:

$$(velocity > 20m/s \wedge station\_distance >= 40m \wedge acceleration > 1m/s^2 \wedge doors = OFF) \vee (station\_distance < 40m \wedge acceleration <= 1m/s^2) \vee (station\_distance = 0m \wedge doors = ON \wedge velocity = 0m/s \wedge acceleration = 0m/s^2) \Rightarrow brakes = ON$$

Invariant Rules - Problem

Complex rules may difficult the interpretation of the alarm

Ex:

$$(velocity > 20m/s \land station\_distance >= 40m \land \boxed{acceleration} > 1m/s^2 \land \boxed{doors = OFF}) \lor (station\_distance < 40m \land acceleration <= 1m/s^2) \lor (station\_distance = 0m \land doors = ON \land velocity = 0m/s \land acceleration = 0m/s^2) \Rightarrow brakes = ON$$

Invariant Rules - Problem

Complex rules may difficult the interpretation of the alarm

Ex:

(velocity > 20m/s ∧ station_distance >= 40m ∧ acceleration > 1m/s^2 ∧ doors = OFF) ∨ (station_distance < 40m ∧ acceleration <= 1m/s^2) ∨ (station_distance = 0m ∧ doors = ON ∧ velocity = 0m/s ∧ acceleration = 0m/s^2) ⇒ $\boxed{\text{brakes = ON}}$

Invariant Rules - Problem

Complex rules may difficult the interpretation of the alarm

Ex:

$$\boxed{(velocity > 20m/s \land station\_distance >= 40m \land acceleration > 1m/s^2 \land doors = OFF)} \lor (station\_distance < 40m \land acceleration <= 1m/s^2) \lor (station\_distance = 0m \land doors = ON \land velocity = 0m/s \land acceleration = 0m/s^2) \Rightarrow brakes = ON$$

Invariant Rules - Problem

Complex rules may difficult the interpretation of the alarm

Ex:

$$(velocity > 20m/s \land station\_distance >= 40m \land acceleration > 0m/s^2 \land doors = OFF) \lor \boxed{(station\_distance < 40m \land acceleration >= 0m/s^2)} \lor (station\_distance = 0m \land doors = ON \land velocity = 0m/s \land acceleration = 0m/s^2) \Rightarrow brakes = ON$$

Invariant Rules - Problem

Complex rules may difficult the interpretation of the alarm

Ex:

$$(velocity > 20m/s \wedge station\_distance >= 40m \wedge acceleration > 0m/s^2 \wedge doors = OFF) \vee (station\_distance < 40m \wedge acceleration >= 0m/s^2) \vee (station\_distance = 0m \wedge \boxed{doors = ON \wedge velocity = 0m/s \wedge acceleration = 0m/s^2)} \Rightarrow brakes = ON$$

Invariant Rules - Solution

Creation of invariants for modeling the observable operation mode of the CPS

Ex:

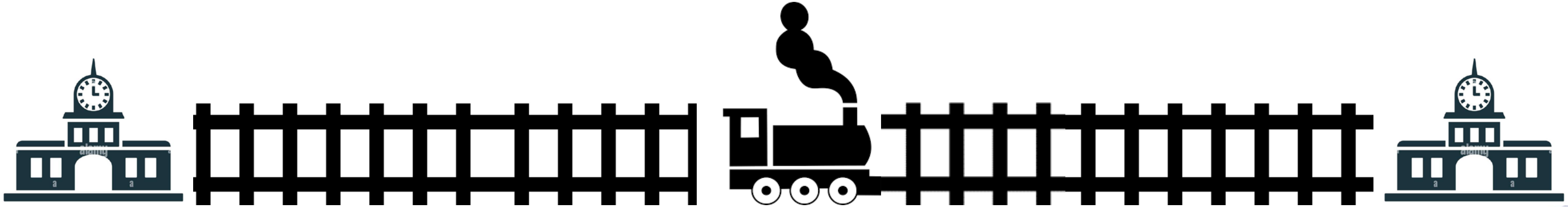
$$\textbf{doors} = \textbf{ON} \;\land\; \textbf{velocity} < \textbf{1m/s} \;\land\; \textbf{brakes} = \textbf{ON} \;\Rightarrow\; \textbf{M} = \textbf{on\_station}$$

Invariant Rules - Solution

Creation of invariants for modeling the observable operation mode of the CPS

Ex:

doors = ON ∧ velocity = 0m/s ∧ brakes = ON , ∧ distance=0 ⇒
M = on_station



Invariant Rules - Solution

Creation of invariants for modeling the observable operation mode of the CPS

Ex:

$$\boxed{\textbf{doors} = \textbf{ON}} \wedge \textbf{velocity} = \textbf{0m/s} \wedge \textbf{brakes} = \textbf{ON} , \wedge \textbf{distance}=\textbf{0} \Rightarrow \textbf{M} = \textbf{on\_station}$$

Invariant Rules - Solution

Creation of invariants for modeling the observable operation mode of the CPS

Ex:

$$\textbf{doors = ON} \wedge \boxed{\textbf{velocity = 0m/s} \wedge \textbf{brakes = ON ,}} \wedge \textbf{distance=0} \Rightarrow \textbf{M = on\_station}$$

Invariant Rules - Solution

Creation of invariants for modeling the observable operation mode of the CPS

Ex:

$$\textbf{doors} = \textbf{ON} \ \wedge \ \textbf{velocity} = \textbf{0m/s} \ \wedge \ \textbf{brakes} = \textbf{ON} \ , \wedge \ \boxed{\textbf{distance=0}} \Rightarrow \textbf{M} = \textbf{on\_station}$$

Invariant Rules - Solution

Creation of invariants for modeling the observable operation mode of the CPS

Ex:

doors = ON ∧ velocity = 0m/s ∧ brakes = ON , ∧ distance=0 ⇒ M = on_station

doors = OFF ∧ velocity > 0m/s ∧ acceleration>0m/s ∧ brakes = OFF , ∧ distance<40 ⇒ M = leaving station

doors = OFF ∧ 0 m/s < velocity < 20m/s ∧ distance>40 ⇒ M = riding

doors = OFF ∧ velocity > 0m/s ∧ acceleration>0m/s, ∧ distance<40 ⇒ M = reaching station

Invariant Rules - Solution

Creation of invariants for modeling the observable operation mode of the CPS

Ex:

doors = ON ∧ velocity = 0m/s ∧ brakes = ON , ∧ distance=0 ⇒ M = on_station

doors = OFF ∧ velocity > 0m/s ∧ acceleration>0m/s ∧ brakes = OFF , ∧ distance<40 ⇒ M = leaving station

doors = OFF ∧ 0 m/s < velocity < 20m/s ∧ distance>40 ⇒ M = riding

doors = OFF ∧ velocity > 0m/s ∧ acceleration>0m/s, ∧ distance<40 ⇒ M = reaching station

Invariant Rules - Solution

Creation of invariants for modeling the observable operation mode of the CPS

Ex:

$\text{doors} = \text{ON} \wedge \text{velocity} = 0\text{m/s} \wedge \text{brakes} = \text{ON}, \wedge \text{distance}=0 \Rightarrow M = \text{on\_station}$

$\text{doors} = \text{OFF} \wedge \text{velocity} > 0\text{m/s} \wedge \text{acceleration}>0\text{m/s} \wedge \text{brakes} = \text{OFF}, \wedge \text{distance}<40 \Rightarrow M = \text{leaving station}$

$\text{doors} = \text{OFF} \wedge 0\text{ m/s} < \text{velocity} < 20\text{m/s} \wedge \text{distance}>40 \Rightarrow M = \text{riding}$

$\boxed{\text{doors} = \text{OFF} \wedge \text{velocity} > 0\text{m/s} \wedge \text{acceleration}>0\text{m/s}, \wedge \text{distance}<40 \Rightarrow M = \text{reaching station}}$

Invariant Rules - Solution

Creation of invariants for modeling the observable operation mode of the CPS

Ex:

doors = ON ∧ velocity = 0m/s ∧ brakes = ON , ∧ distance=0 ⇒ M = on_station
doors = OFF ∧ velocity > 0m/s ∧ acceleration>0m/s ∧ brakes = OFF , ∧ distance<40 ⇒ M = leaving station
doors = OFF ∧ 0 m/s < velocity < 20m/s ∧ distance>40 ⇒ M = riding
doors = OFF ∧ velocity > 0m/s ∧ acceleration>0m/s, ∧ distance<40 ⇒ M = reaching station

Invariant Rules - Solution

Creation of invariants for modeling the observable operation mode of the CPS

Ex:

doors = ON ∧ velocity = 0m/s ∧ brakes = ON , ∧ distance=0 ⇒ M = on_station
doors = OFF ∧ velocity > 0m/s ∧ acceleration>0m/s ∧ brakes = OFF , ∧ distance<40 ⇒ M = leaving station
doors = OFF ∧ 0 m/s < velocity < 20m/s ∧ distance>40 ⇒ M = riding
doors = OFF ∧ velocity > 0m/s ∧ acceleration>0m/s, ∧ distance<40 ⇒ M = reaching station

doors = OFF ∧ velocity = 0m/s ∧ brakes = ON, M = on_station

Invariant Rules - Solution

Creation of invariants for modeling the observable operation mode of the CPS

Ex:

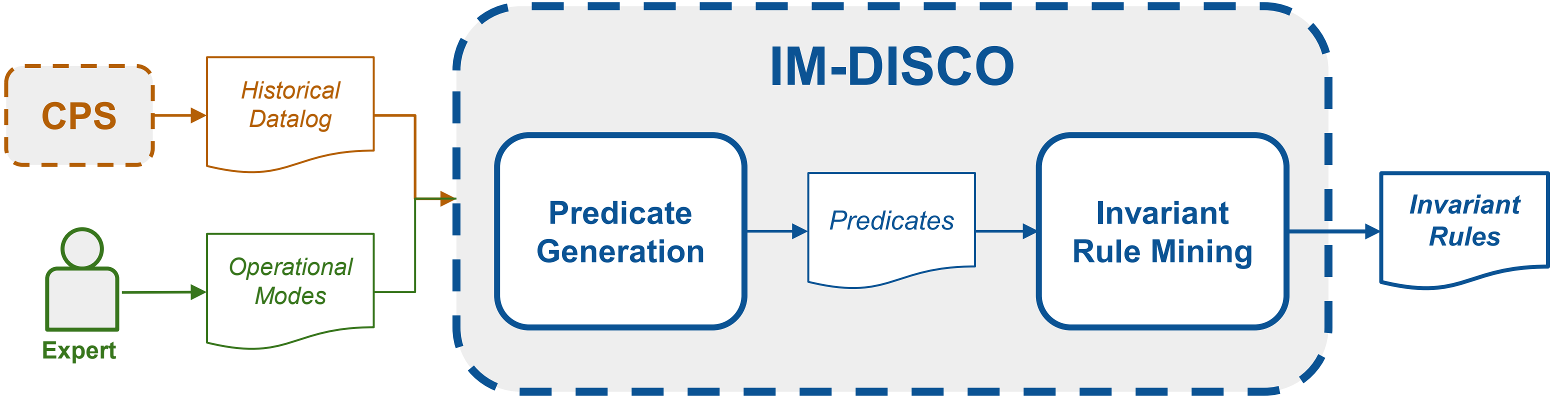
doors = ON ∧ velocity = 0m/s ∧ brakes = ON , ∧ distance=0 ⇒ M = on_station
doors = OFF ∧ velocity > 0m/s ∧ acceleration>0m/s ∧ brakes = OFF , ∧ distance<40 ⇒ M = leaving station
doors = OFF ∧ 0 m/s < velocity < 20m/s ∧ distance>40 ⇒ M = riding
doors = OFF ∧ velocity > 0m/s ∧ acceleration>0m/s, ∧ distance<40 ⇒ M = reaching station

doors = OFF ∧ velocity = 30 m/s ∧ brakes = OFF, M = riding

IM-DISCO

Provides invariant rules for inferring operational modes within CPS

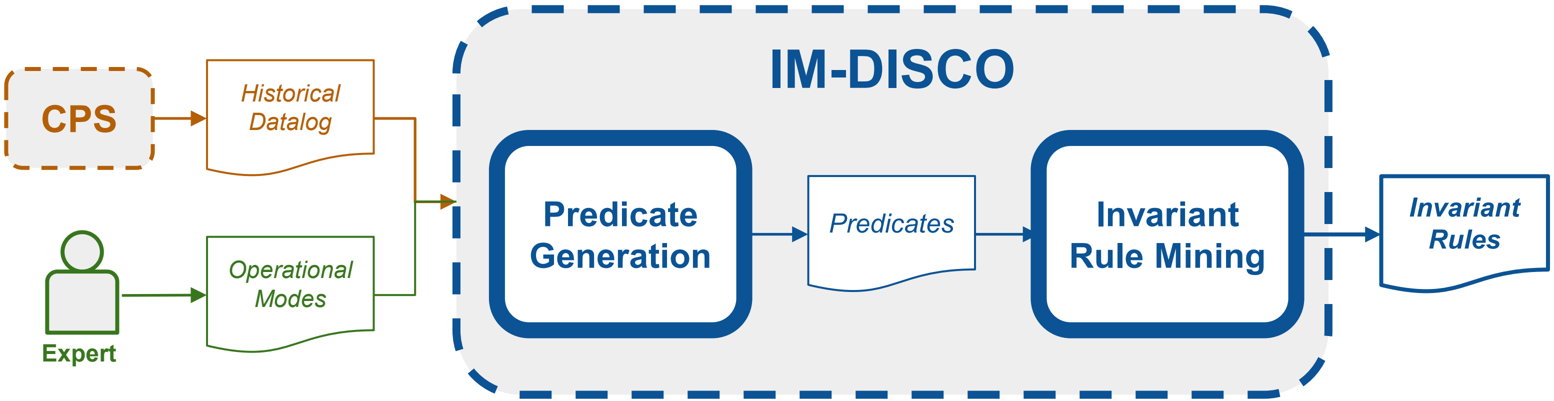
Allows the detection of anomalies that can be verified by human experts



IM-DISCO Invariant rule mining

Two main phases:

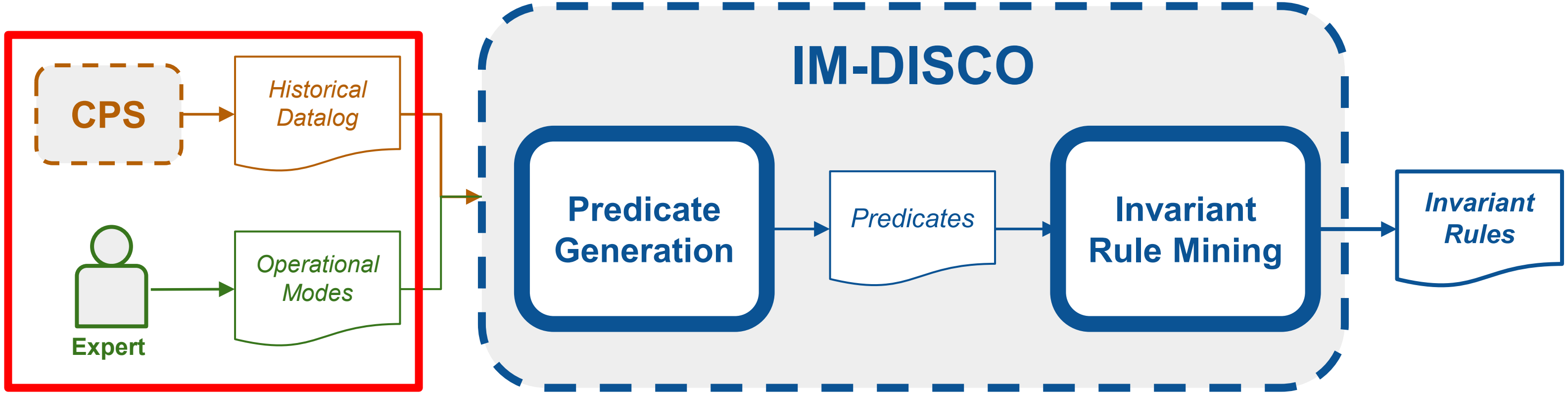
- **Predicate Generation**
- **Invariant Rule Mining**



IM-DISCO Invariant rule mining

Two main phases:

- **Predicate Generation**
- **Invariant Rule Mining**

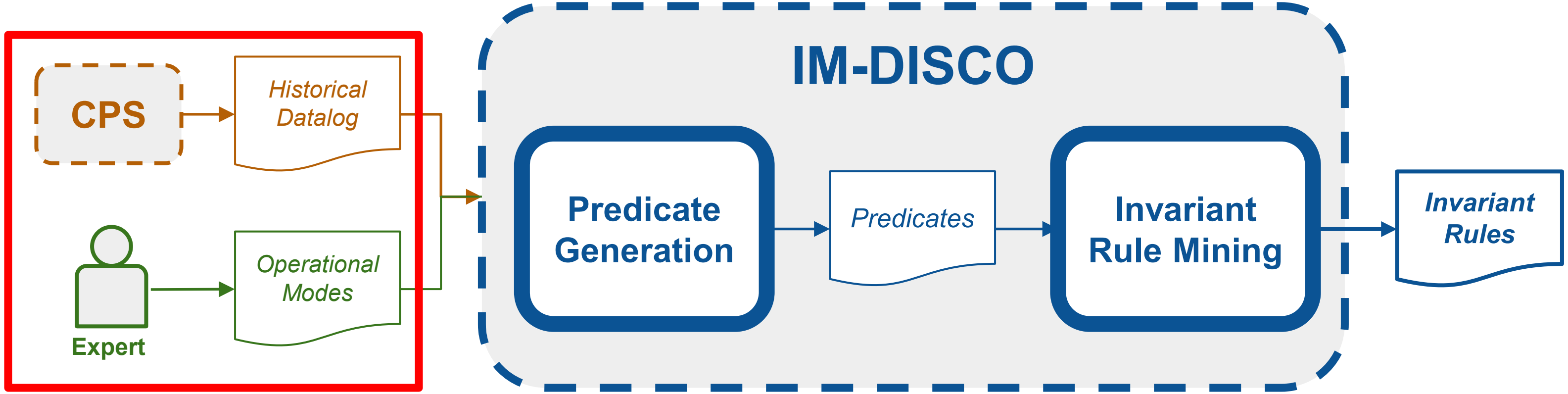


IM-DISCO Invariant rule mining

Two main phases:

- **Predicate Generation**
- **Invariant Rule Mining**

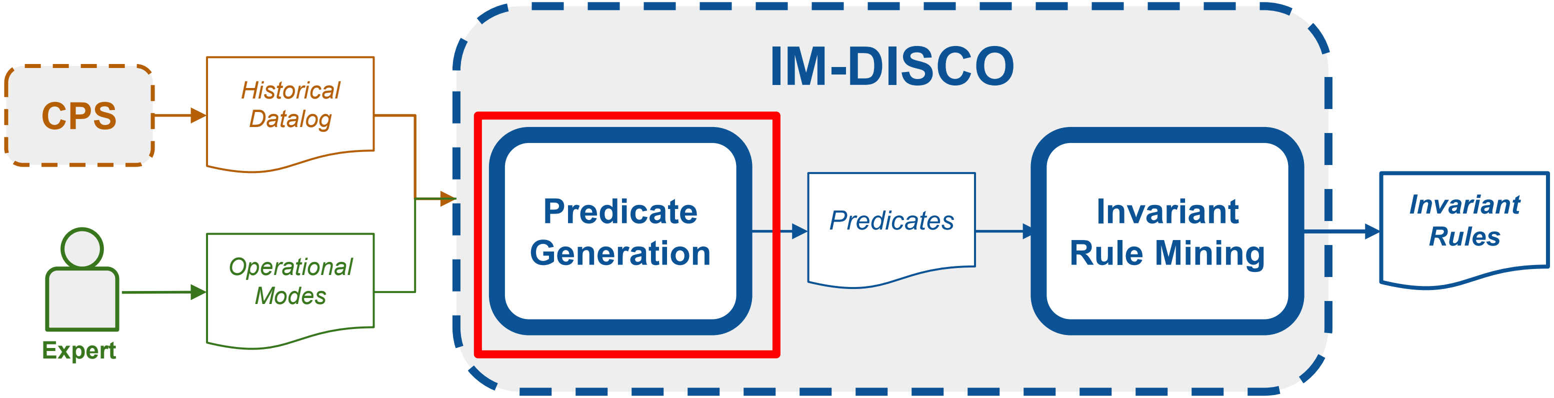
Velocity=20m/s, acceleration=2m/s; riding
Velocity=20m/s, acceleration=3m/s; riding



IM-DISCO Rule generation

Two main phases:

- **Predicate Generation**
- **Invariant Rule Mining**

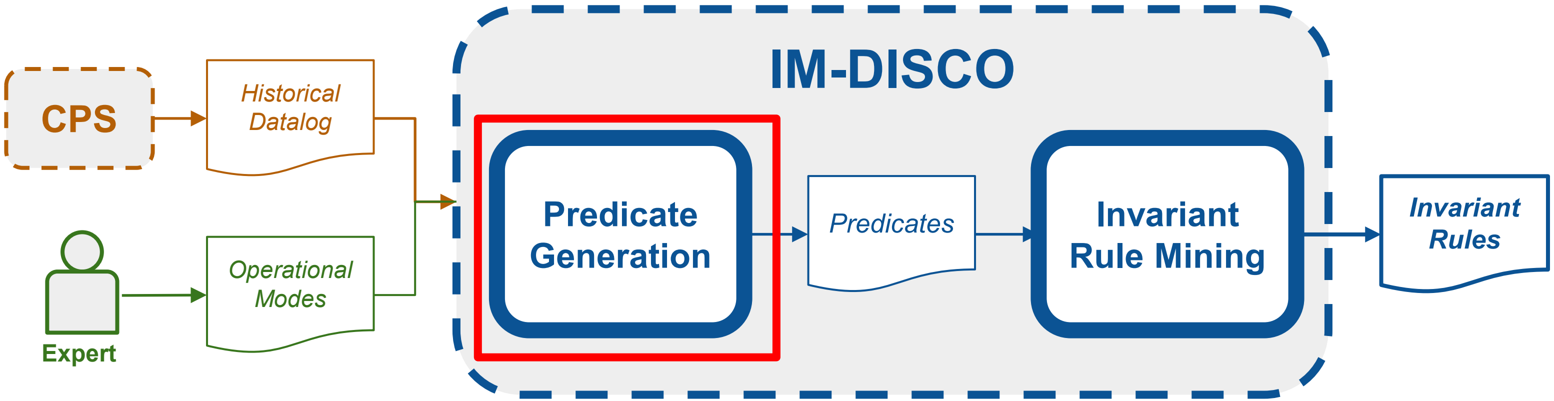


IM-DISCO Rule generation

Two main phases:

- **Predicate Generation**
- **Invariant Rule Mining**

distance<40m (leaving station)

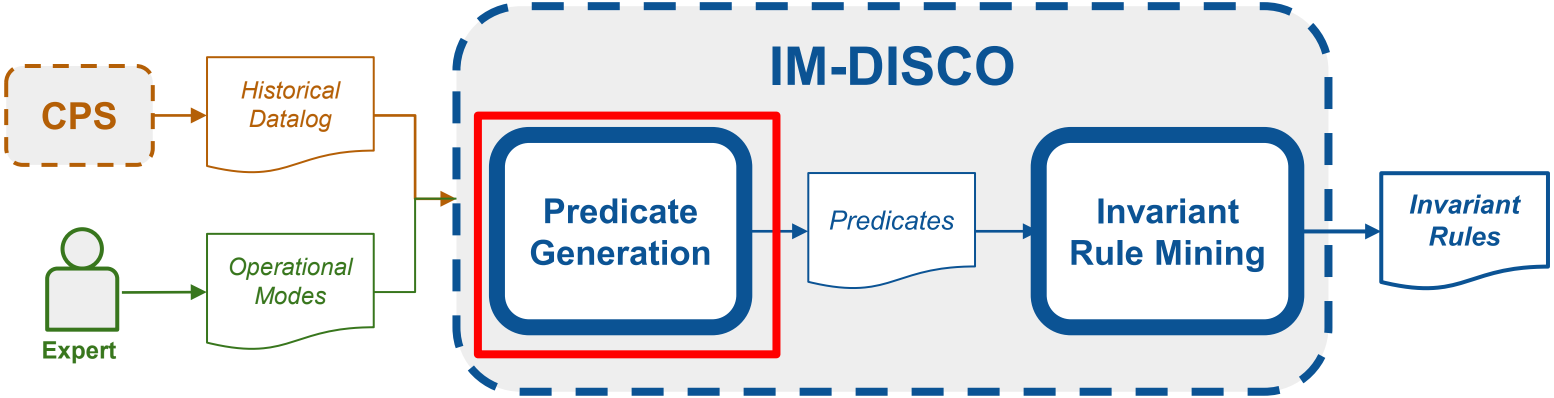


IM-DISCO Rule generation

Two main phases:

- **Predicate Generation**
- **Invariant Rule Mining**

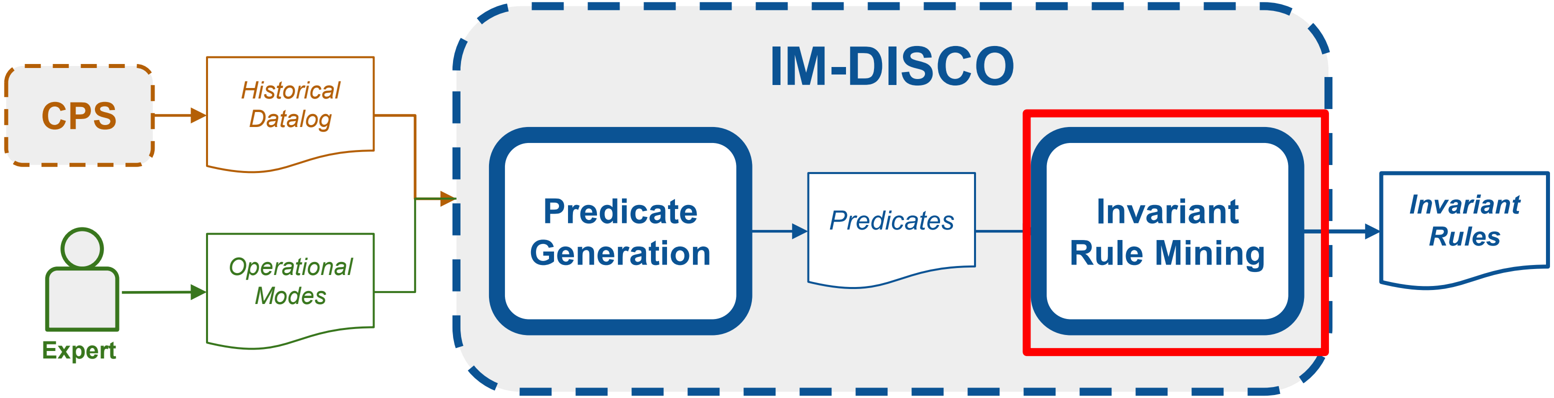
distance<40m (leaving station)
Velocity<20m/s (riding)



IM-DISCO Rule generation

Two main phases:

- **Predicate Generation**
- **Invariant Rule Mining**



IM-DISCO Rule generation

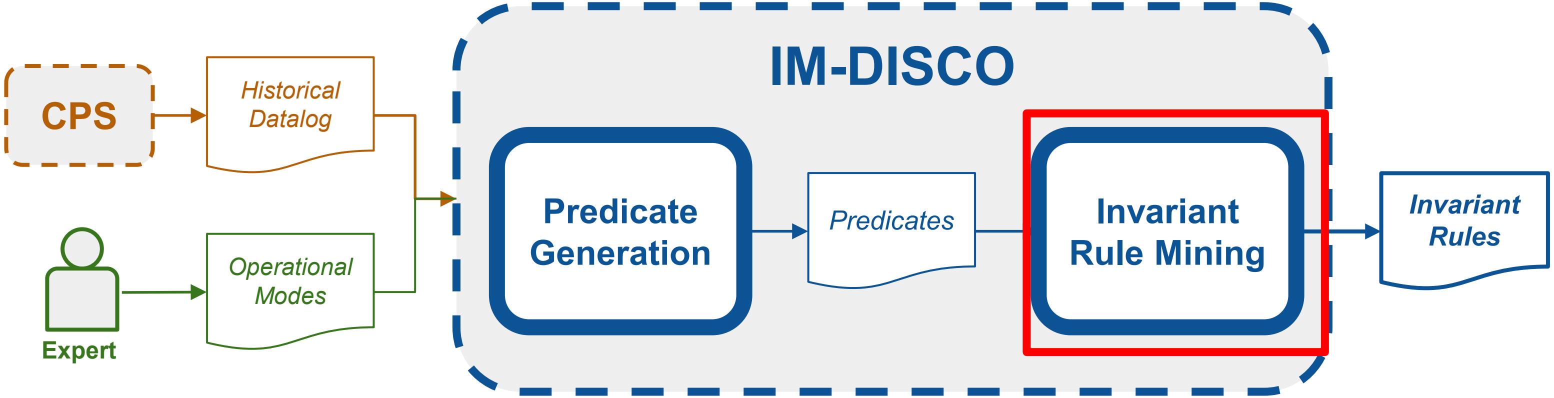
Two main phases:

- **Predicate Generation**
- **Invariant Rule Mining**

doors = ON ∧ velocity = 0m/s ∧ brakes = ON , ∧ distance=0 ⇒ M = on_station

doors = OFF ∧ velocity > 0m/s ∧ acceleration>0m/s ∧ brakes = OFF , ∧ distance<40 ⇒ M = leaving station

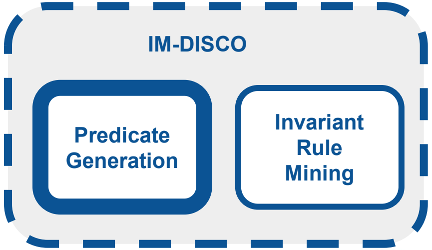
doors = OFF ∧ 0 m/s < velocity < 20m/s ∧ distance>40 ⇒ M = riding



IM-DISCO - Predicate Generation

Approach:

- Define different thresholds for each sensor/actuator based on their characteristics, using the techniques proposed by **SIMPLE-IDS** [1]:
    - **MinMax**
    - **Gradient**
    - **SteadyTime**
    - **Actuator States**

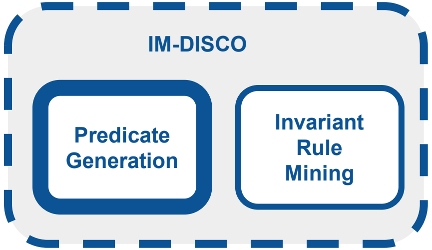


1. Wolsing, K., Thiemt, L., Sloun, C.v., Wagner, E., Wehrle, K., Henze, M.: Can industrial intrusion detection be simple? In: Atluri, V., Di Pietro, R., Jensen, C.D., Meng, W. (eds.) Computer Security – ESORICS 2022. pp. 574–594. Springer Nature Switzerland, Cham (2022)

IM-DISCO - Predicate Generation

Approach:

- Define different thresholds for each sensor/actuator based on their characteristics, using the techniques proposed by **SIMPLE-IDS** [1]:
    - **MinMax -** Extracts the minimum and maximum values observed by each sensor
    - **Gradient**
    - **SteadyTime**
    - **Actuator States**



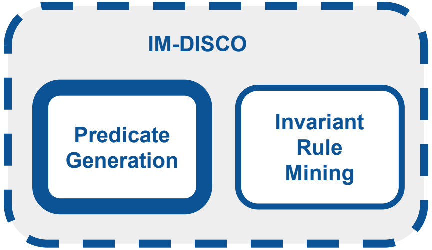
1. Wolsing, K., Thiemt, L., Sloun, C.v., Wagner, E., Wehrle, K., Henze, M.: Can industrial intrusion detection be simple? In: Atluri, V., Di Pietro, R., Jensen, C.D., Meng, W. (eds.) Computer Security – ESORICS 2022. pp. 574–594. Springer Nature Switzerland, Cham (2022)

IM-DISCO - Predicate Generation

Approach:

- Define different thresholds for each sensor/actuator based on their characteristics, using the techniques proposed by **SIMPLE-IDS** [1]:
  - **MinMax -** Extracts the <u>minimum</u> and <u>maximum</u> values observed by each sensor
  - **Gradient**
  - **SteadyTime**
  - **Actuator States**

0<Velocity<20m/s (riding)

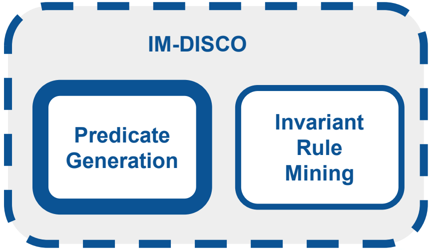


1. Wolsing, K., Thiemt, L., Sloun, C.v., Wagner, E., Wehrle, K., Henze, M.: Can industrial intrusion detection be simple? In: Atluri, V., Di Pietro, R., Jensen, C.D., Meng, W. (eds.) Computer Security – ESORICS 2022. pp. 574–594. Springer Nature Switzerland, Cham (2022)

IM-DISCO - Predicate Generation

Approach:

- Define different thresholds for each sensor/actuator based on their characteristics, using the techniques proposed by **SIMPLE-IDS** [1]:
    - **MinMax**
    - **Gradient -** Regarding it establishes the limits of each sensor's observed slope
    - **SteadyTime**
    - **Actuator States**

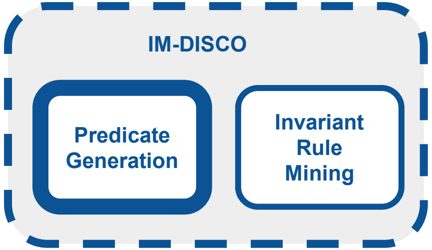


1. Wolsing, K., Thiemt, L., Sloun, C.v., Wagner, E., Wehrle, K., Henze, M.: Can industrial intrusion detection be simple? In: Atluri, V., Di Pietro, R., Jensen, C.D., Meng, W. (eds.) Computer Security – ESORICS 2022. pp. 574–594. Springer Nature Switzerland, Cham (2022)

IM-DISCO - Predicate Generation

Approach:

- Define different thresholds for each sensor/actuator based on their characteristics, using the techniques proposed by **SIMPLE-IDS** [1]:
    - **MinMax**
    - **Gradient -** Regarding it establishes the limits of each sensor's observed <u>slope</u>
        - **2 m/s < slope(S.velocity) < 4 m/s (riding)**
    - **SteadyTime**
    - **Actuator States**

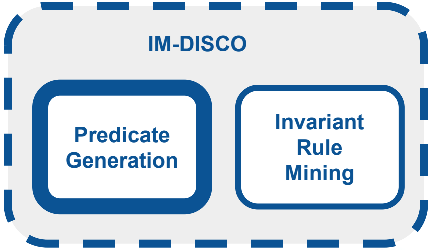


1. Wolsing, K., Thiemt, L., Sloun, C.v., Wagner, E., Wehrle, K., Henze, M.: Can industrial intrusion detection be simple? In: Atluri, V., Di Pietro, R., Jensen, C.D., Meng, W. (eds.) Computer Security – ESORICS 2022. pp. 574–594. Springer Nature Switzerland, Cham (2022)

IM-DISCO - Predicate Generation

Approach:

- Define different thresholds for each sensor/actuator based on their characteristics, using the techniques proposed by **SIMPLE-IDS** [1]:
    - **MinMax**
    - **Gradient**
    - **SteadyTime -** Defines the limits of each actuator state duration
    - **Actuator States**



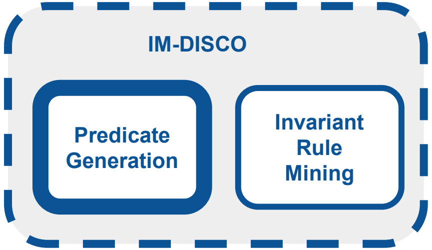
1. Wolsing, K., Thiemt, L., Sloun, C.v., Wagner, E., Wehrle, K., Henze, M.: Can industrial intrusion detection be simple? In: Atluri, V., Di Pietro, R., Jensen, C.D., Meng, W. (eds.) Computer Security – ESORICS 2022. pp. 574–594. Springer Nature Switzerland, Cham (2022)

IM-DISCO - Predicate Generation

Approach:

- Define different thresholds for each sensor/actuator based on their characteristics, using the techniques proposed by **SIMPLE-IDS** [1]:
  - **MinMax**
  - **Gradient**
  - **SteadyTime -** Defines the limits of each actuator state duration
  - **Actuator States**

Ex: 10s < A.doors = OPEN < 50s

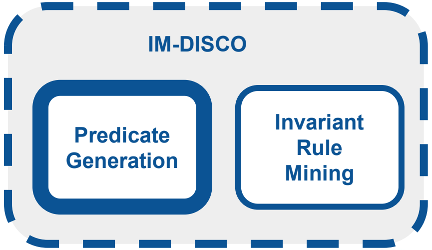


1. Wolsing, K., Thiemt, L., Sloun, C.v., Wagner, E., Wehrle, K., Henze, M.: Can industrial intrusion detection be simple? In: Atluri, V., Di Pietro, R., Jensen, C.D., Meng, W. (eds.) Computer Security – ESORICS 2022. pp. 574–594. Springer Nature Switzerland, Cham (2022)

IM-DISCO - Predicate Generation

Approach:

- Define different thresholds for each sensor/actuator based on their characteristics, using the techniques proposed by **SIMPLE-IDS** [1]:
    - **MinMax**
    - **Gradient**
    - **SteadyTime**
    - **Actuator States -** The different states that an actuator can assume



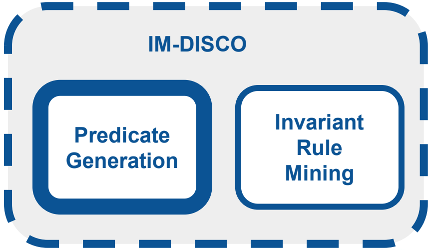
1. Wolsing, K., Thiemt, L., Sloun, C.v., Wagner, E., Wehrle, K., Henze, M.: Can industrial intrusion detection be simple? In: Atluri, V., Di Pietro, R., Jensen, C.D., Meng, W. (eds.) Computer Security – ESORICS 2022. pp. 574–594. Springer Nature Switzerland, Cham (2022)

IM-DISCO - Predicate Generation

Approach:

- Define different thresholds for each sensor/actuator based on their characteristics, using the techniques proposed by **SIMPLE-IDS** [1]:
    - **MinMax**
    - **Gradient**
    - **SteadyTime**
    - **Actuator States -** The different states that an actuator can assume

Ex: **A.Doors = CLOSED (riding)**



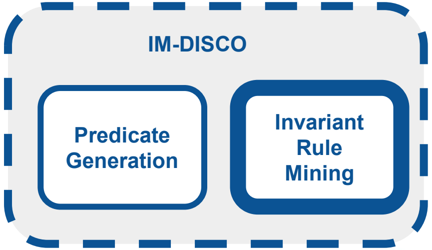
1. Wolsing, K., Thiemt, L., Sloun, C.v., Wagner, E., Wehrle, K., Henze, M.: Can industrial intrusion detection be simple? In: Atluri, V., Di Pietro, R., Jensen, C.D., Meng, W. (eds.) Computer Security – ESORICS 2022. pp. 574–594. Springer Nature Switzerland, Cham (2022)

IM-DISCO - Invariant Rule Mining

Approach:

- Use **Association Rule Mining** to discover associations between the predicates that characterize the operational modes

  1. *Frequent Itemsets Extraction*
  2. *Association Rules Generation*



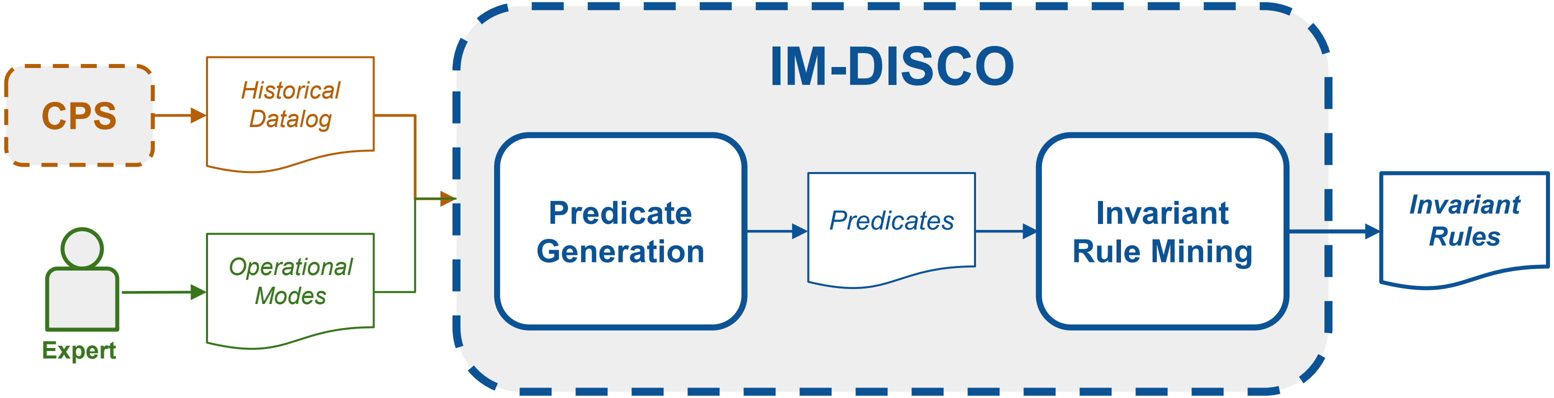
1. Wolsing, K., Thiemt, L., Sloun, C.v., Wagner, E., Wehrle, K., Henze, M.: Can industrial intrusion detection be simple? In: Atluri, V., Di Pietro, R., Jensen, C.D., Meng, W. (eds.) Computer Security – ESORICS 2022. pp. 574–594. Springer Nature Switzerland, Cham (2022)

IM-DISCO - Takeaways

Provides invariant rules for inferring operational modes within CPS

Allows the detection of anomalies that can be verified by human experts

40m/s < S.velocity < 100m/s ∧ 10s < A.throttle = ON < 50s ⇒ *riding*



Evaluation

Evaluation 1

Real Train Dataset:

- Data collection using *Strava* mobile app
- Sensors and actuators derived based on GPS coordinates
- Operation mode collected based on observation
- Dataset uses two train rides

Ride	Stops	Time	Datapoints
Departure ride	12	35 minutes 22 seconds	2122
Return ride	12	34 minutes 28 seconds	2068

Results 1 - Operational Mode Inference

Can IM-DISCO infer the correct operational mode?

- Trained IM-DISCO with 80% of the dataset, and tested with 20%

Table 1. Results of using invariant rules for detecting the operational modes for both rides

	Precision		Recall		F1-score		Accuracy	
	R_d	R_r	R_d	R_r	R_d	R_r	R_d	R_r
arriving_station	100%	100%	98.53%	97.89%	99.26%	98.94%		
leaving_station	100%	43.75%	100%	100%	100%	60.87%		
on_station	100%	100%	100%	100%	100%	100%		
riding	99.60%	100%	99.60%	93.21%	99.60%	96.48%		
IM-DISCO	99.90%	85.94%	99.53%	98.22%	99.71%	89.07%	**99.29%**	**95.17%**

Results 1 - Operational Mode Inference

Can IM-DISCO infer the correct operational mode?

- Trained IM-DISCO with 80% of the dataset, and tested with 20%

Table 1. Results of using invariant rules for detecting the operational modes for both rides

	Precision		Recall		F1-score		Accuracy	
	R_d	R_r	R_d	R_r	R_d	R_r	R_d	R_r
arriving_station	100%	100%	98.53%	97.89%	99.26%	98.94%		
leaving_station	100%	43.75%	100%	100%	100%	60.87%		
on_station	100%	100%	100%	100%	100%	100%		
riding	99.60%	100%	99.60%	93.21%	99.60%	96.48%		
IM-DISCO	99.90%	85.94%	99.53%	98.22%	99.71%	89.07%	**99.29%**	**95.17%**

Results 1 - Operational Mode Inference

Can IM-DISCO infer the correct operational mode?

- Trained IM-DISCO with 80% of the dataset, and tested with 20%

Table 1. Results of using invariant rules for detecting the operational modes for both rides

	Precision		Recall		F1-score		Accuracy	
	R_d	R_r	R_d	R_r	R_d	R_r	R_d	R_r
arriving_station	100%	100%	98.53%	97.89%	99.26%	98.94%		
leaving_station	100%	43.75%	100%	100%	100%	60.87%		
on_station	100%	100%	100%	100%	100%	100%		
riding	99.60%	100%	99.60%	93.21%	99.60%	96.48%		
IM-DISCO	99.90%	85.94%	99.53%	98.22%	99.71%	89.07%	**99.29%**	**95.17%**

Results 1 - Operational Mode Inference

Can IM-DISCO infer the correct operational mode?

- Trained IM-DISCO with 80% of the dataset, and tested with 20%

Table 1. Results of using invariant rules for detecting the operational modes for both rides

	Precision		Recall		F1-score		Accuracy	
	R_d	R_r	R_d	R_r	R_d	R_r	R_d	R_r
arriving_station	100%	100%	98.53%	97.89%	99.26%	98.94%		
leaving_station	100%	43.75%	100%	100%	100%	60.87%		
on_station	100%	100%	100%	100%	100%	100%		
riding	99.60%	100%	99.60%	93.21%	99.60%	96.48%		
IM-DISCO	99.90%	85.94%	99.53%	98.22%	99.71%	89.07%	**99.29%**	**95.17%**

Evaluation 2

Simulated Train Dataset:

- Data artificially generated
- Same sensors, actuators and operational modes
- Dataset uses one train ride
- Includes an attack that disrupts the brakes of the train

Ride	Stops	Time	Datapoints
Simulated ride	13	48 minutes	1697

Results 3 - Anomaly Detection

Can IM-DISCO be used for anomaly detection?

- Trained IM-DISCO with 80% of the dataset, and tested with 20% containing an attack

Table 2. Results of using invariant rules for anomaly detection in a simulated ride

	Precision	Recall	F1-score	Accuracy
anomaly	95.24%	100%	97.56%	
arriving_station	100%	99.56%	99.78%	
leaving_station	100%	100%	100%	
on_station	100%	100%	100%	
riding	100%	100%	100%	
IM-DISCO	99.05%	99.91%	99.47%	**99.86%**

Results 3 - Anomaly Detection

Can IM-DISCO be used for anomaly detection?

- Trained IM-DISCO with 80% of the dataset, and tested with 20% containing an attack

Table 2. Results of using invariant rules for anomaly detection in a simulated ride

	Precision	Recall	F1-score	Accuracy
anomaly	95.24%	100%	97.56%	
arriving_station	100%	99.56%	99.78%	
leaving_station	100%	100%	100%	
on_station	100%	100%	100%	
riding	100%	100%	100%	
IM-DISCO	99.05%	99.91%	99.47%	**99.86%**

Results 3 - Anomaly Detection

Can IM-DISCO be used for anomaly detection?

- Trained IM-DISCO with 80% of the dataset, and tested with 20% containing an attack

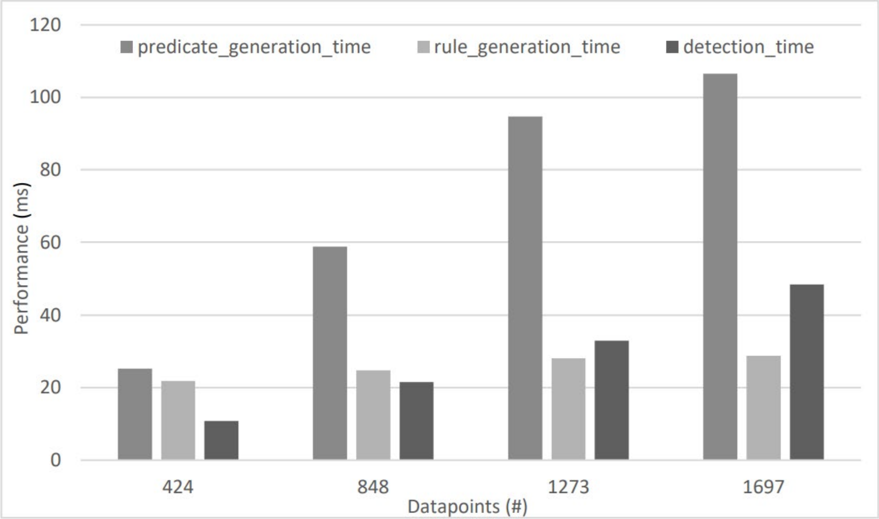
Table 2. Results of using invariant rules for anomaly detection in a simulated ride

	Precision	Recall	F1-score	Accuracy
anomaly	95.24%	100%	97.56%	
arriving_station	100%	99.56%	99.78%	
leaving_station	100%	100%	100%	
on_station	100%	100%	100%	
riding	100%	100%	100%	
IM-DISCO	99.05%	99.91%	99.47%	**99.86%**

Results 4 - Rules Verification and Validation

How much time does IM-DISCO take to generate and verify rules?

- Trained IM-DISCO with different training sizes

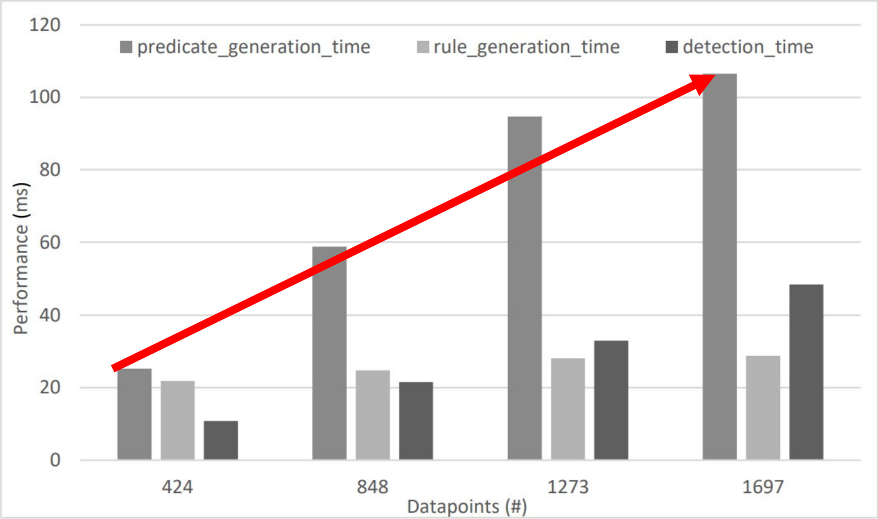


Graph 2. Performance of our solution across different dataset sizes

Results 4 - Rules Verification and Validation

How much time does IM-DISCO take to generate and verify rules?

- Trained IM-DISCO with different training sizes

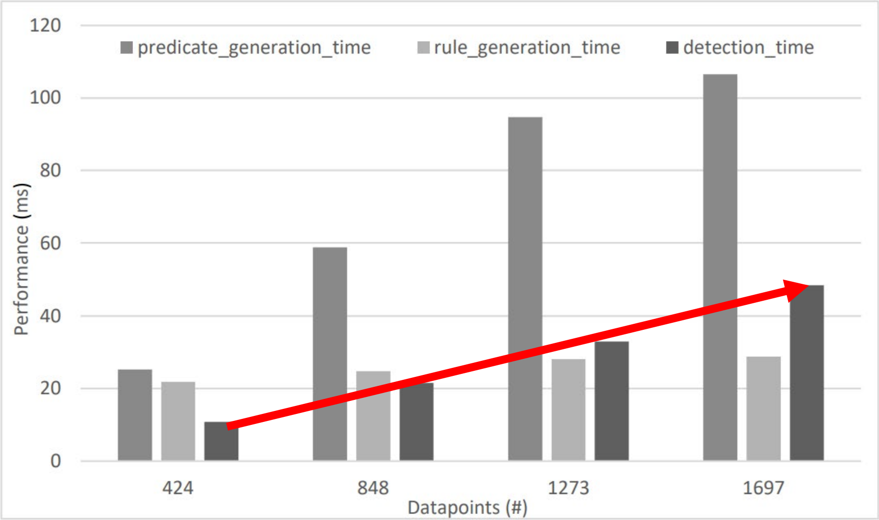


Graph 2. Performance of our solution across different dataset sizes

Results 4 - Rules Verification and Validation

How much time does IM-DISCO take to generate and verify rules?

- Trained IM-DISCO with different training sizes



Graph 2. Performance of our solution across different dataset sizes

Conclusion

- IM-DISCO generates rules that infer operational modes based on sensors and actuators
- Allows anomaly detection with understandable alerts
- IM-DISCO is accurate and real-time
- Adequate for detecting cyberphysical attacks

Thank you for listening!

E-MAIL: FILIPE.APOLINARIO@TECNICO.ULISBOA.PT
WEBPAGE: HTTPS://WEB.TECNICO.ULISBOA.PT/FILIPE.APOLINARIO/