SePanner: Analyzing Semantics of Controller Variables in Industrial Control Systems based on Network Traffic

Jie Meng[1] Zeyu Yang[1] Zhenyong Zhang[2] Yangyang Geng[3]

Ruilong Deng[1] Peng Cheng[1] Jiming Chen[1] Jianying Zhou[4]

[1] Zhejiang University

[2] Guizhou University

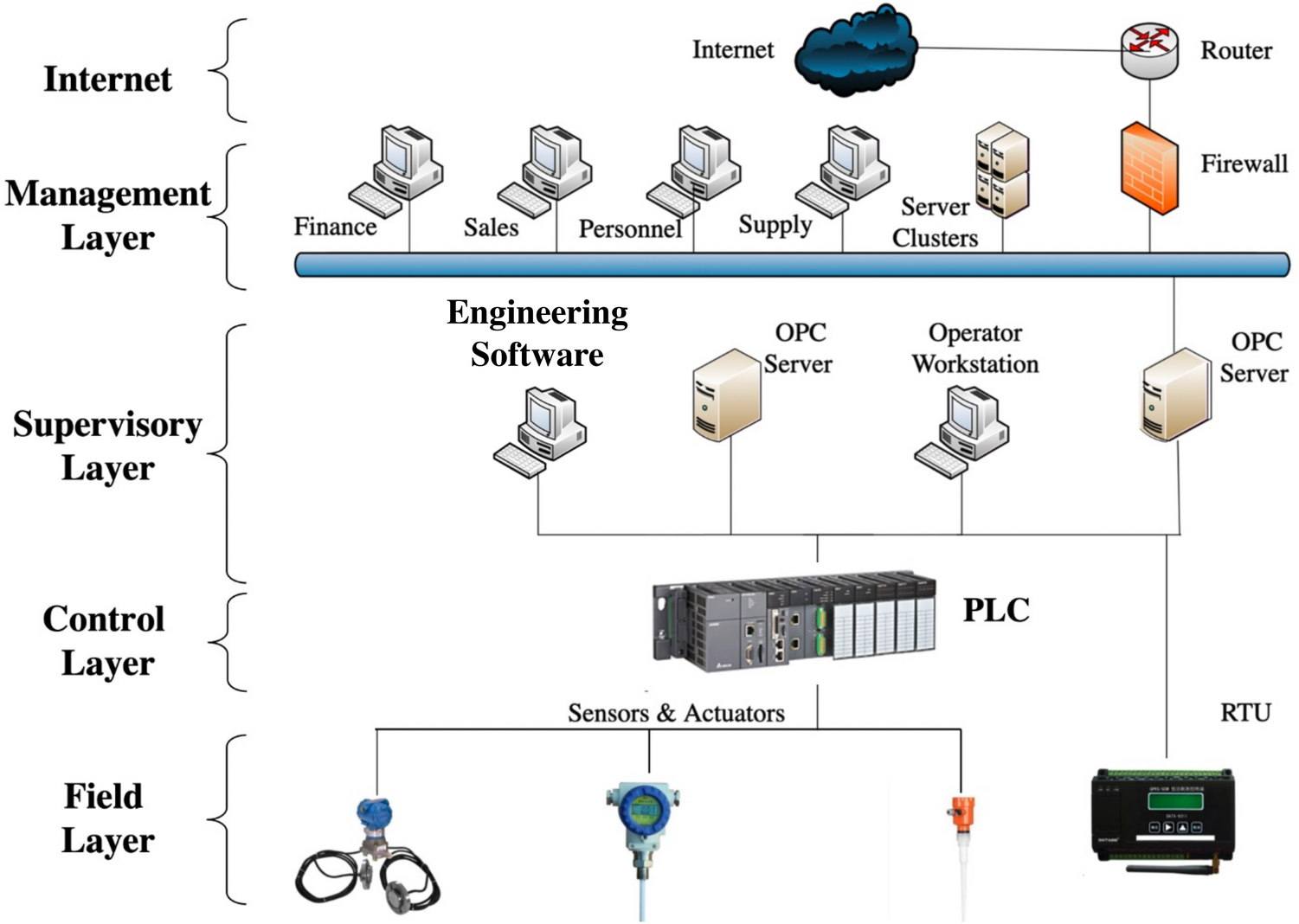
[3] Information Engineering University

[4] Singapore University of Technology and Design

ACSAC 2023 December 4 – 8 Austin, Texas, USA

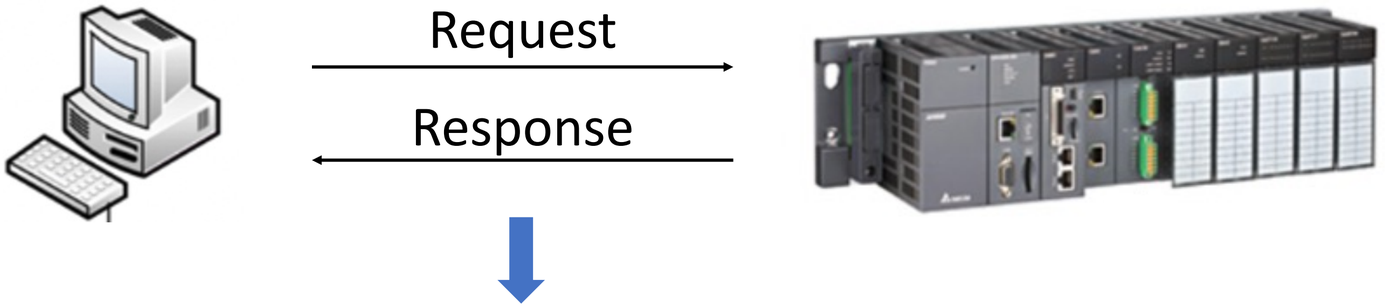
Programmable Logic Controller (PLC)

- **Sense and drive** the physical processes of Industrial Control System (ICS)



PLC Communication

- **Engineering Software:** configure, program, and monitor PLCs



Label	Time(s)	SRC	DST	Len(B)	Data
E6	0.031881	192.168.1.77	192.168.1.21	10	68 C5 00 00 00 04 01 5A 00 02
I6	0.03273	192.168.1.21	192.168.1.77	52	68 C5 00 00 00 2E 01 5A 00 FE 14 30 8D 07 11 54 4D 32 32 31 43 45 32 ...
E7	0.034434	192.168.1.77	192.168.1.21	10	68 C6 00 00 00 04 01 5A 00 04
I7	0.03569	192.168.1.21	192.168.1.77	32	68 C6 00 00 00 1A 01 5A 00 FE 02 0A 80 03 C2 6A D4 0D C2 6A D4 0D ...
...	...	...	...	...	...
E24	1.866162	192.168.1.77	192.168.1.21	10	68 DD 00 00 00 04 01 5A 00 04
I24	1.867145	192.168.1.21	192.168.1.77	32	68 DD 00 00 00 1A 01 5A 00 FE 02 0A 80 03 C2 6A D4 0D C2 6A D4 0D ...
E25	1.867364	192.168.1.77	192.168.1.21	17	68 DE 00 00 00 0B 01 5A 00 24 01 02 00 0B 00 01 00
I25	1.868945	192.168.1.21	192.168.1.77	14	68 DE 00 00 00 08 01 5A 00 FE 01 00 00 00

- **Industrial Control protocol (ICP):** binary protocol for PLC communication

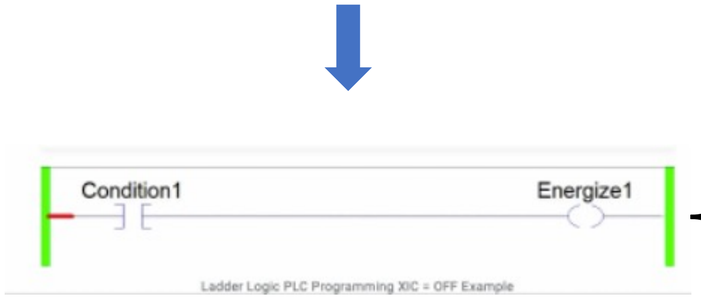
Controller Variable of PLC

- **Device Status:** current status of PLC
- **Program Component:** the components in the internal program logic of PLC

Operating Mode (Run, Stop)

Protection Level (Write, Read/Write Protect)

LED Status (ON, OFF)



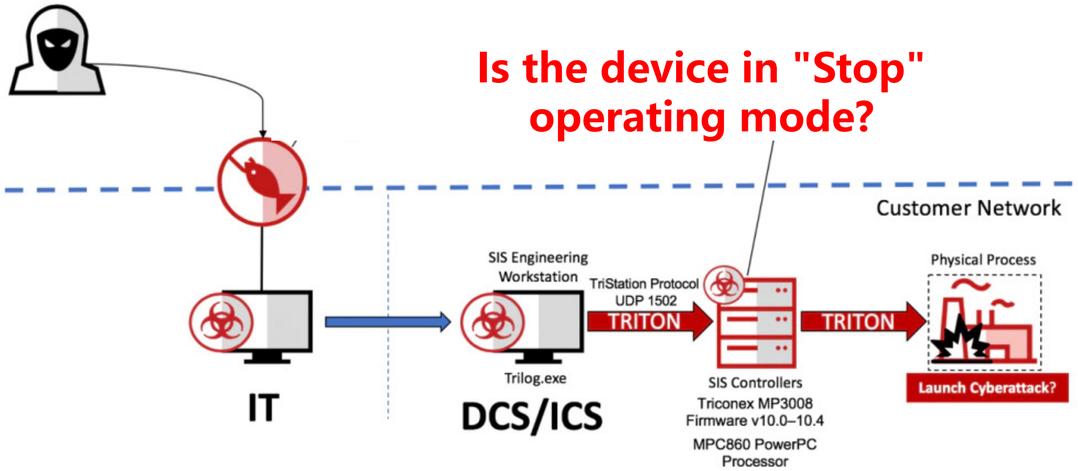
Type (Input, Output)

Number

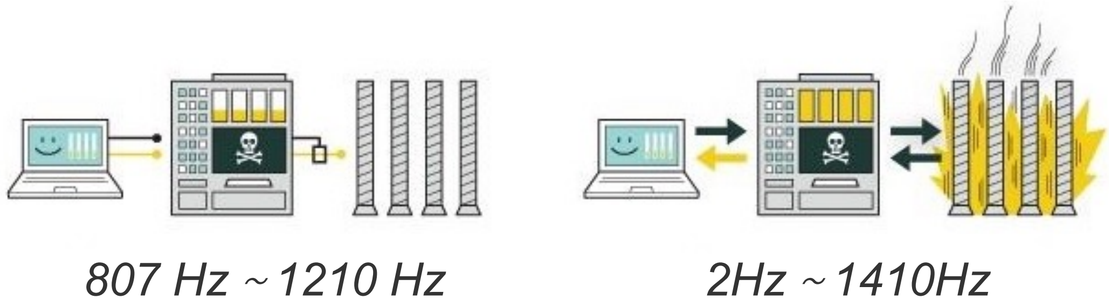
Value (ON, OFF)

Attack on Controller Variable

- **Reconnaissance:** Search for suitable attack targets
- **Tampering:** Modify the state of controller Variable



Triton Malware - 2017



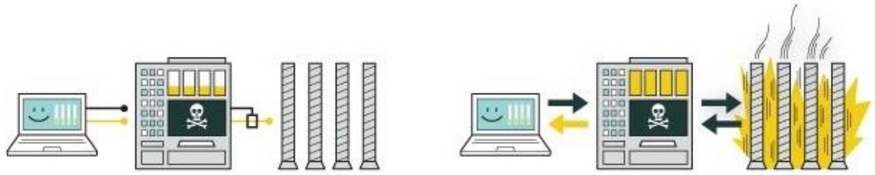
Stuxnet Malware - 2010

- **Sending specific ICP messages containing controller variables information**

Defend

- **Monitoring** abnormal changes in controller variables
- **Detecting** anomalous traffic in ICS that acquires or modifies controller variables

Attack: Sending specific ICS protocol packets containing controller variables information



807 Hz ~ 1210 Hz　　2Hz ~ 1410Hz

Defend: Monitor controller variables and detect anomalous traffic in network traffic

Label	Time(s)	SRC	DST	Len(B)	Data
E6	0.031881	192.168.1.77	192.168.1.21	10	68 C5 00 00 00 04 01 5A 00 02
I6	0.03273	192.168.1.21	192.168.1.77	52	68 C5 00 00 00 2E 01 5A 00 FE 14 30 8D 07 11 54 4D 32 32 31 43 45 32 ...
E7	0.034434	192.168.1.77	192.168.1.21	10	68 C6 00 00 00 04 01 5A 00 04
I7	0.03569	192.168.1.21	192.168.1.77	32	68 C6 00 00 00 1A 01 5A 00 FE 02 0A 80 03 C2 6A D4 0D C2 6A D4 0D ...
...	...	...	...	...	...
E24	1.866162	192.168.1.77	192.168.1.21	10	68 DD 00 00 00 04 01 5A 00 04
I24	1.867145	192.168.1.21	192.168.1.77	32	68 DD 00 00 00 1A 01 5A 00 FE 02 0A 80 03 C2 6A D4 0D C2 6A D4 0D ...
E25	1.867364	192.168.1.77	192.168.1.21	17	68 DE 00 00 00 0B 01 5A 00 24 01 02 00 0B 00 01 00
I25	1.868945	192.168.1.21	192.168.1.77	14	68 DE 00 00 00 08 01 5A 00 FE 01 00 00 00

Base: The domain knowledge of the semantics of controller variables

- **Semantic messages**
- **Semantic fields**

Domain knowledge of the semantics of controller variables

- **Semantic messages**
- **Semantic fields**

Controller Variable: Operating Mode, **Message Template**: … 00 1A 01 5A 00 FE ... ,
Field Offset :10, **Correspondence**:{Run:03, Stop:02}

Label	Time(s)	SRC	DST	Len(B)	Data
E6	0.031881	192.168.1.77	192.168.1.21	10	68 C5 00 00 00 04 01 5A 00 02
I6	0.03273	192.168.1.21	192.168.1.77	52	68 C5 00 00 00 2E 01 5A 00 FE 14 30 8D 07 11 54 4D 32 32 31 43 45 32 ...
E7	0.034434	192.168.1.77	192.168.1.21	10	68 C6 00 00 00 04 01 5A 00 04
I7	0.03569	192.168.1.21	192.168.1.77	32	68 C6 00 00 00 1A 01 5A 00 FE 02 0A 80 03 C2 6A D4 0D C2 6A D4 0D ...
...	...	...	...	...	...
E24	1.866162	192.168.1.77	192.168.1.21	10	68 DD 00 00 00 04 01 5A 00 04
I24	1.867145	192.168.1.21	192.168.1.77	32	68 DD 00 00 00 1A 01 5A 00 FE 02 0A 80 03 C2 6A D4 0D C2 6A D4 0D ...
E25	1.867364	192.168.1.77	192.168.1.21	17	68 DE 00 00 00 0B 01 5A 00 24 01 02 00 0B 00 01 00
I25	1.868945	192.168.1.21	192.168.1.77	14	68 DE 00 00 00 08 01 5A 00 FE 01 00 00 00

The current operating mode of the PLC is "Stop"

Defend

- **Monitoring** abnormal changes in controller variables
- **Detecting** anomalous traffic in ICS that acquires or modifies controller variables

Attack: Sending specific ICS protocol packets containing controller variables information

Defend: Monitor controller variables and detect anomalous traffic in network traffic

Label	Time(s)	SRC	DST	Len(B)	Data
E6	0.031881	192.168.1.77	192.168.1.21	10	68 C5 00 00 00 04 01 5A 00 02
I6	0.03273	192.168.1.21	192.168.1.77	52	68 C5 00 00 00 2E 01 5A 00 FE 14 30 8D 07 11 54 4D 32 32 31 43 45 32 ...
E7	0.034434	192.168.1.77	192.168.1.21	10	68 C6 00 00 00 04 01 5A 00 04
I7	0.03569	192.168.1.21	192.168.1.77	32	68 C6 00 00 00 1A 01 5A 00 FE 02 0A 80 03 C2 6A D4 0D C2 6A D4 0D ...
...	...	...	...	...	...
E24	1.866162	192.168.1.77	192.168.1.21	10	68 DD 00 00 00 04 01 5A 00 04
I24	1.867145	192.168.1.21	192.168.1.77	32	68 DD 00 00 00 1A 01 5A 00 FE 02 0A 80 03 C2 6A D4 0D C2 6A D4 0D ...
E25	1.867364	192.168.1.77	192.168.1.21	17	68 DE 00 00 00 0B 01 5A 00 24 01 02 00 0B 00 01 00
I25	1.868945	192.168.1.21	192.168.1.77	14	68 DE 00 00 00 08 01 5A 00 FE 01 00 00 00

Base: The domain knowledge of the semantics of controller variables

- **Semantic messages**
- **Semantic fields**

✖ **Proprietary**

Industrial control protocol

How to analyze semantics of controller variables from proprietary ICPs?

Analyze semantics of controller variable

- **Observation: network traffic between Engineering Software and PLC is starting-aligned**

```
E0:   68 FF 00 00 00 05 01 5A 00 01 00
I0 :  68 FF 00 00 00 11 01 5A 00 FE FA 00 …
E1:   68 00 00 00 00 04 01 5A 00 11
I1 :  68 00 00 00 00 05 01 5A 00 FD 81
                        …
E7:   68 C6 00 00 00 04 01 5A 6A 04
I7 :  68 C6 00 00 00 1A 01 5A 6A FE 02 0A …
                        …
```

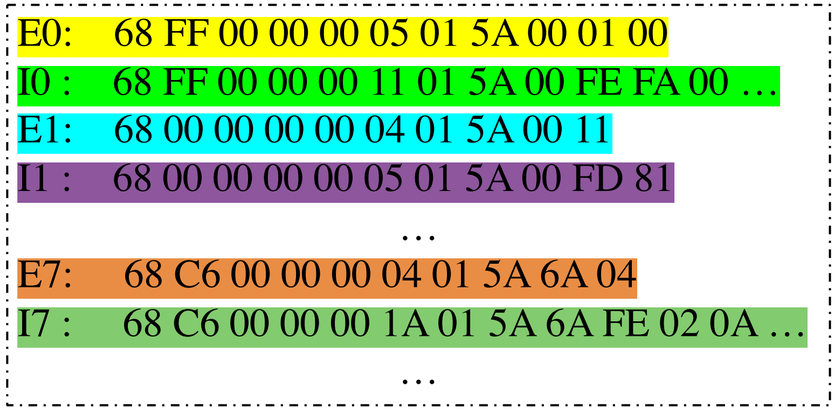
Connection 1

```
E0:   E7 4B 00 00 00 05 01 5A 00 01 00
I0 :  E7 4B 00 00 00 11 01 5A 00 FE FA 00 …
E1:   E7 4C 00 00 00 04 01 5A 00 11
I1 :  E7 4C 00 00 00 05 01 5A 00 FD 81
                        …
E7:   E7 52 00 00 00 04 01 5A D1 04
I7 :  E7 52 00 00 00 1A 01 5A D1 FE 03 0A ...
                        …
```

Connection 2

Analyze semantics of controller variable

- **Observation: network traffic between Engineering Software and PLC is starting-aligned**



Connection 1

Connection 2

Analyze semantics of controller variable

- **Observation: network traffic between Engineering Software and PLC is starting-aligned**

E0:	68 FF 00 00 00 05 01 5A 00 01 00
I0 :	68 FF 00 00 00 11 01 5A 00 FE FA 00 …
E1:	68 00 00 00 00 04 01 5A 00 11
I1 :	68 00 00 00 00 05 01 5A 00 FD 81
	…
E7:	68 C6 00 00 00 04 01 5A 6A 04
I7 :	68 C6 00 00 00 1A 01 5A 6A FE 02 0A …
	…

Connection 1

E0:	E7 4B 00 00 00 05 01 5A 00 01 00
I0 :	E7 4B 00 00 00 11 01 5A 00 FE FA 00 …
E1:	E7 4C 00 00 00 04 01 5A 00 11
I1 :	E7 4C 00 00 00 05 01 5A 00 FD 81
	…
E7:	E7 52 00 00 00 04 01 5A D1 04
I7 :	E7 52 00 00 00 1A 01 5A D1 FE 03 0A ...
	…

Connection 2

- **Base idea: multi-state comparing**

E0:	68 FF 00 00 00 05 01 5A 00 01 00
I0 :	68 FF 00 00 00 11 01 5A 00 FE FA 00 …
E1:	68 00 00 00 00 04 01 5A 00 11
I1 :	68 00 00 00 00 05 01 5A 00 FD 81
	…
E7:	68 C6 00 00 00 04 01 5A 6A 04
I7 :	68 C6 00 00 00 1A 01 5A 6A FE **02** 0A …
	…

State: Stop

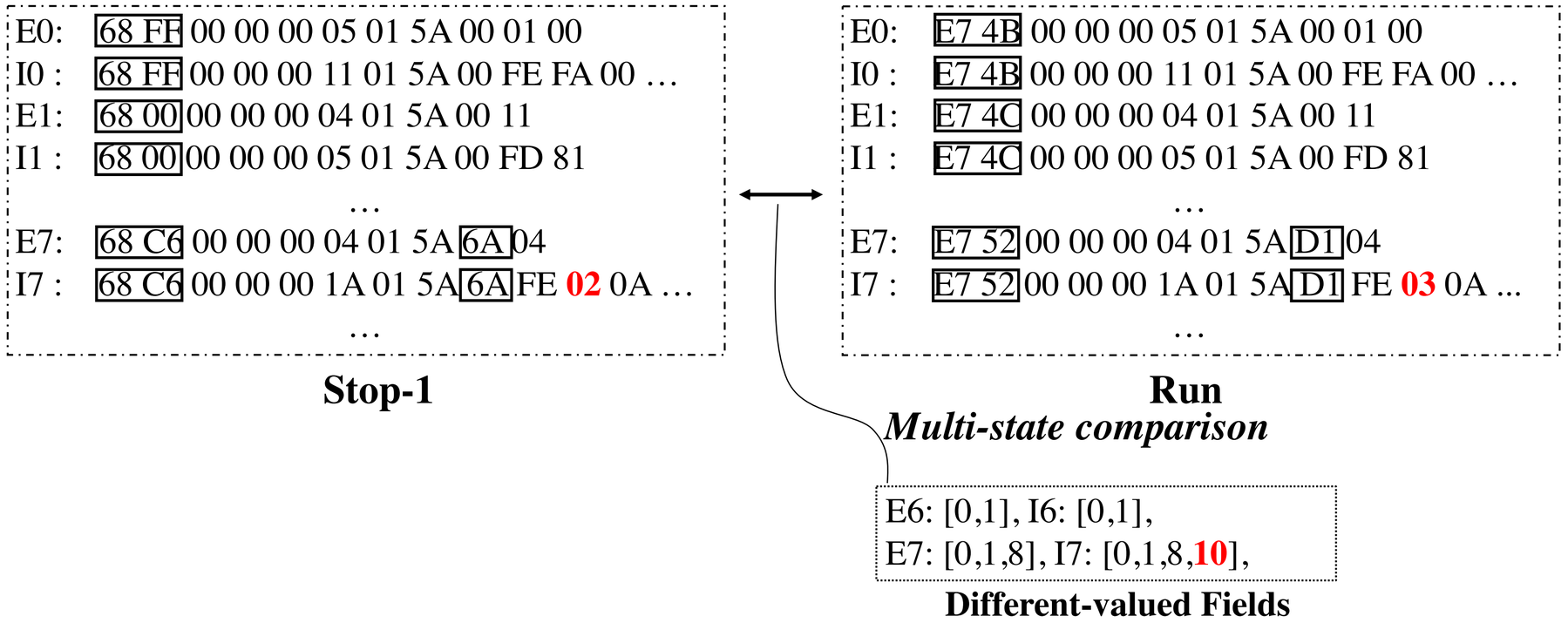
E0:	E7 4B 00 00 00 05 01 5A 00 01 00
I0 :	E7 4B 00 00 00 11 01 5A 00 FE FA 00 …
E1:	E7 4C 00 00 00 04 01 5A 00 11
I1 :	E7 4C 00 00 00 05 01 5A 00 FD 81
	…
E7:	E7 52 00 00 00 04 01 5A D1 04
I7 :	E7 52 00 00 00 1A 01 5A D1 FE **03** 0A ...
	…

State: Run

Semantic message: I7, Offset of semantic field: 10

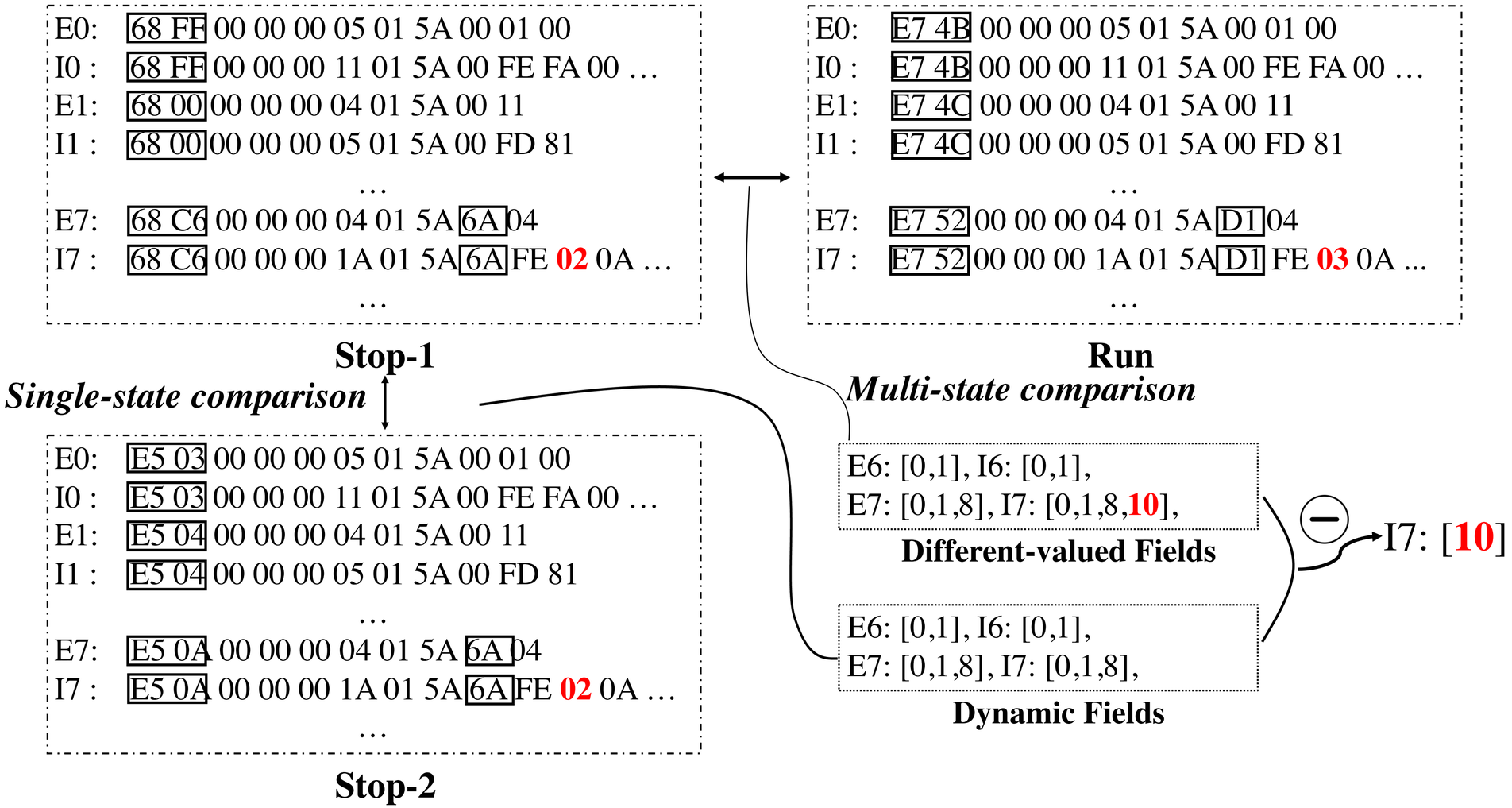
Analyze semantics of controller variable

- **Challenge 1: dynamic fields**



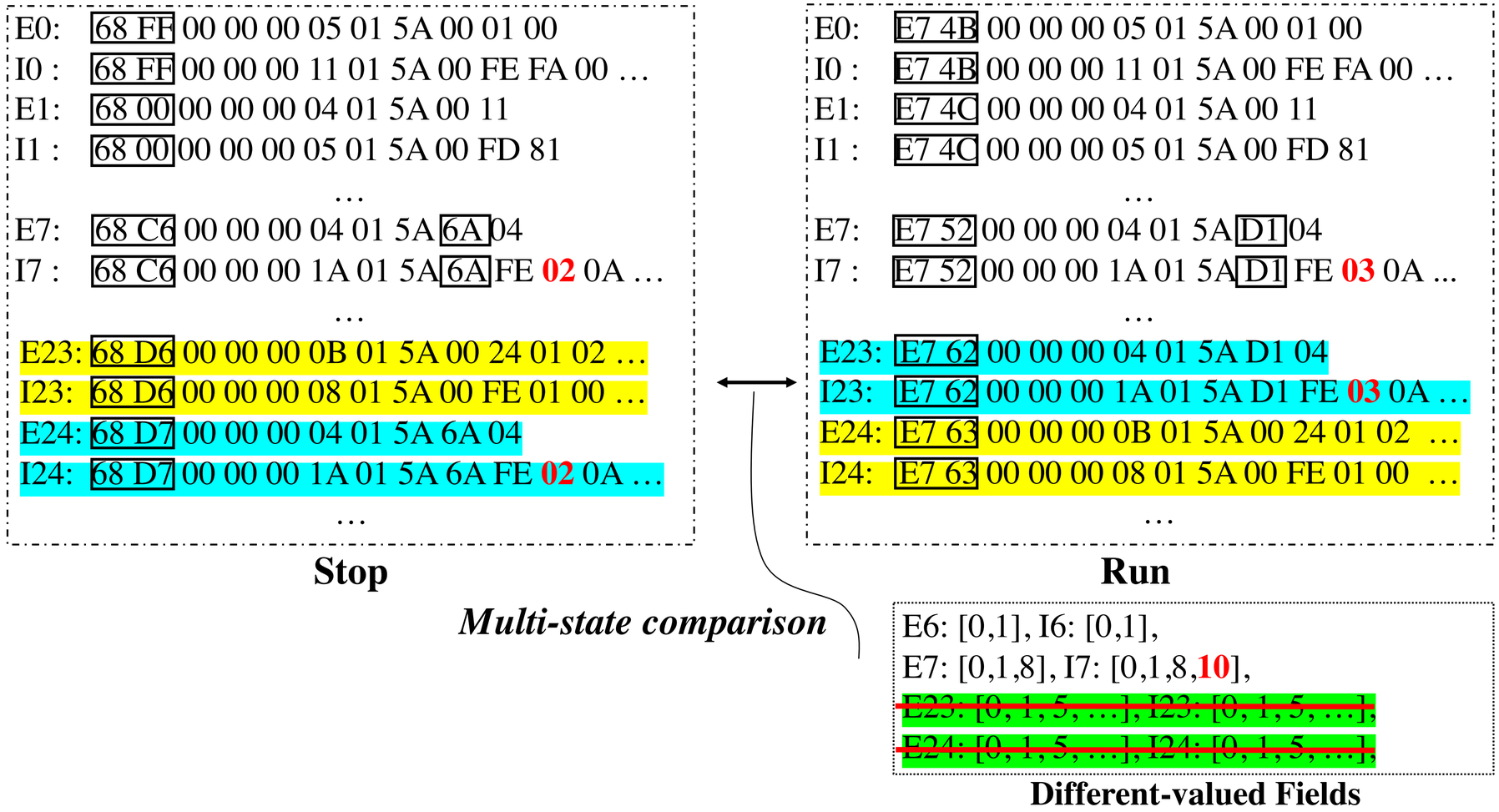
Analyze semantics of controller variable

- **Solution 1: single-state comparison**



Analyze semantics of controller variable

- **Challenge 2: misordered packets**



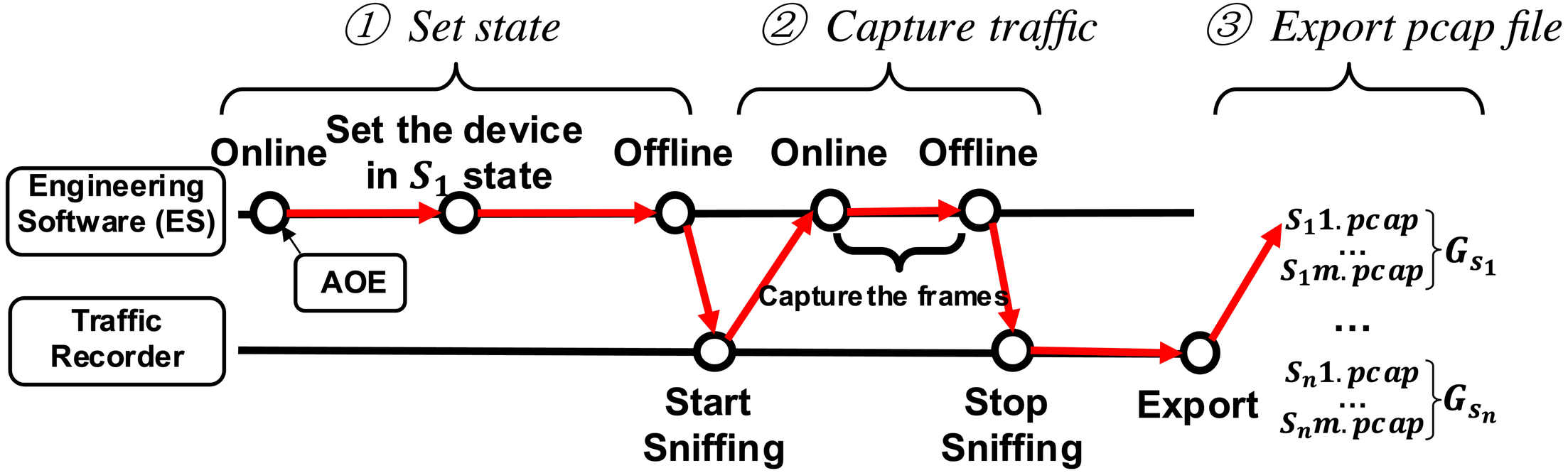
Solution 2: employ identification criteria to remove the misordered comparison

Overview of SePanner

- Data collection module
- The message processing module
- Starting-aligned comparison module
- Semantics locating module

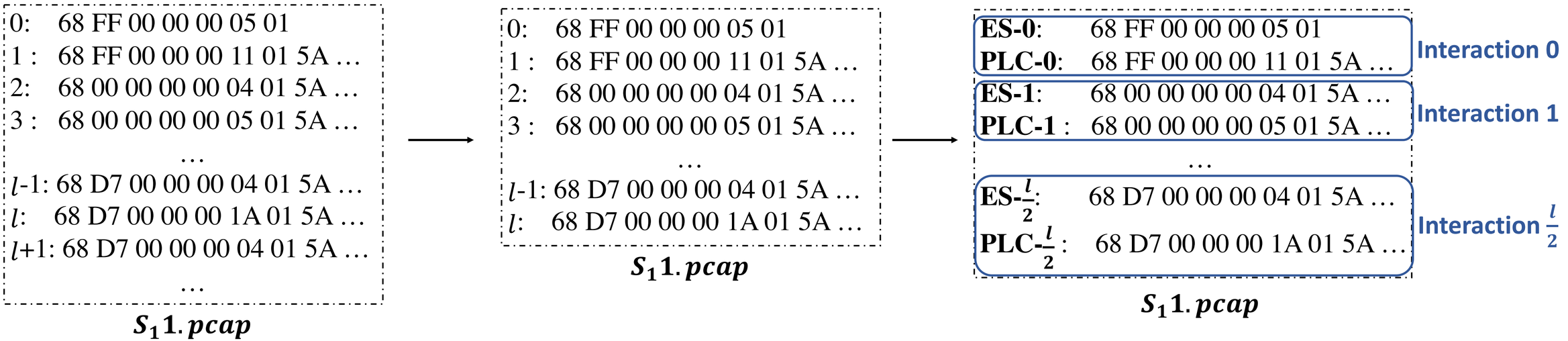
Data collection module

- Traffic Recorder: Wireshark
- Automatic operation Execution (AOE)



Message processing

- **Unify the Number of Messages**
- **Label Messages**
- **Identify Interactions**



Starting-aligned comparison

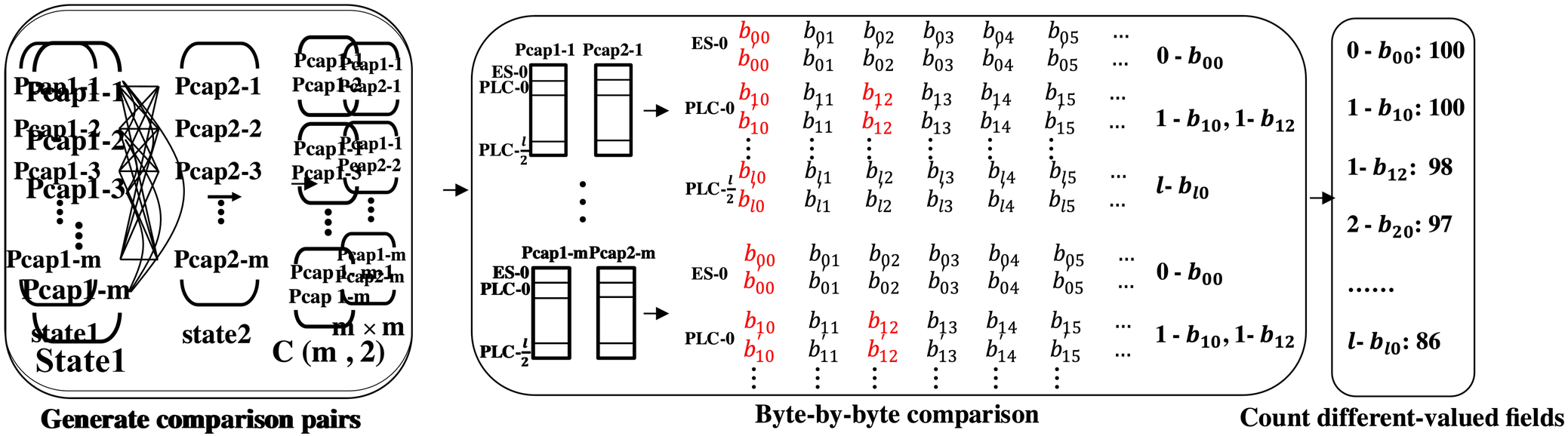
Generate comparison pairs

- Single-state: 1 group and **select random 2 files**
- Multi-state: 2 groups and **full-connect**

Byte by byte comparison

- Compare each byte of the packets with the same label

Count the different-valued fields

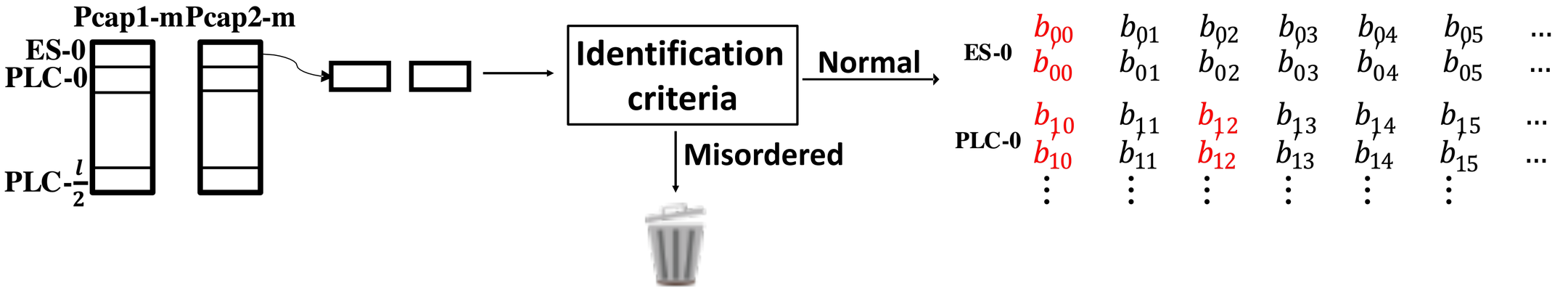


Misorder Filtering

- **Identification criteria:**
  - Message length
  - Proportion of different-valued bytes

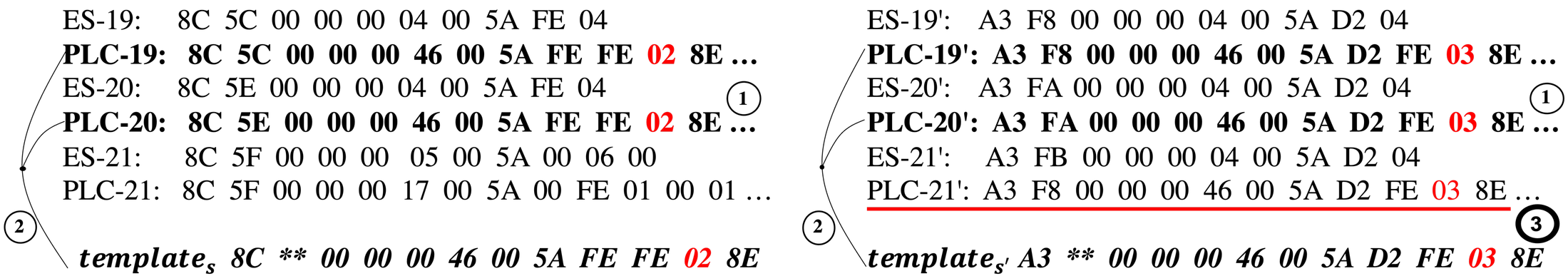
$$p_r = \frac{\text{the num of different-valued bytes}}{\text{the num of all bytes in the message}}$$

  - Interaction relevance



Generate the template of semantic message

- Find the semantic messages
- Generate the semantic template
- Locate semantic messages



$$template \quad ** \; ** \; 00 \; 00 \; 00 \; 46 \; 00 \; 5A \; ** \; FE \; ** \; 8E$$

Evaluation

- **Testbed (7 PLCs, 5 industrial control protocols)**
- **Metrics**
  - Accuracy
  - Correlation (protocol without ground truth)

PLC	Firmware	Manufacturer	Protocol	ES
M340	2.8	Schneider	UMAS-2	Control Expert Classic
M221	1.12.00	Schneider	UMAS-1	Machine Expert Basic
M200	1.12.00	Schneider	UMAS-1	Machine Expert Basic
S7300	3.1.0	Siemens	S7COMM	TIA/Snap7
1400	21.00	Rockwell	PCCC	RSlogix 500
1100	16.00	Rockwell	PCCC	RSlogix 500
H3U	24314.0	Huichuan	Huichuan	AutoShop

$$H(S) = \sum_{s \in S} p(s) \log\left(p(s)\right)$$

$$H(V) = \sum_{v \in V} p(v) \log\left(p(v)\right)$$

$$I(V;S) = \sum_{v \in V} \sum_{s \in S} p(v,s) \log\left(\frac{p(v,s)}{p(v)p(s)}\right)$$

$$correlation = \frac{2I(V;S)}{H(V) + H(S)}$$

Evaluation via parsed protocol

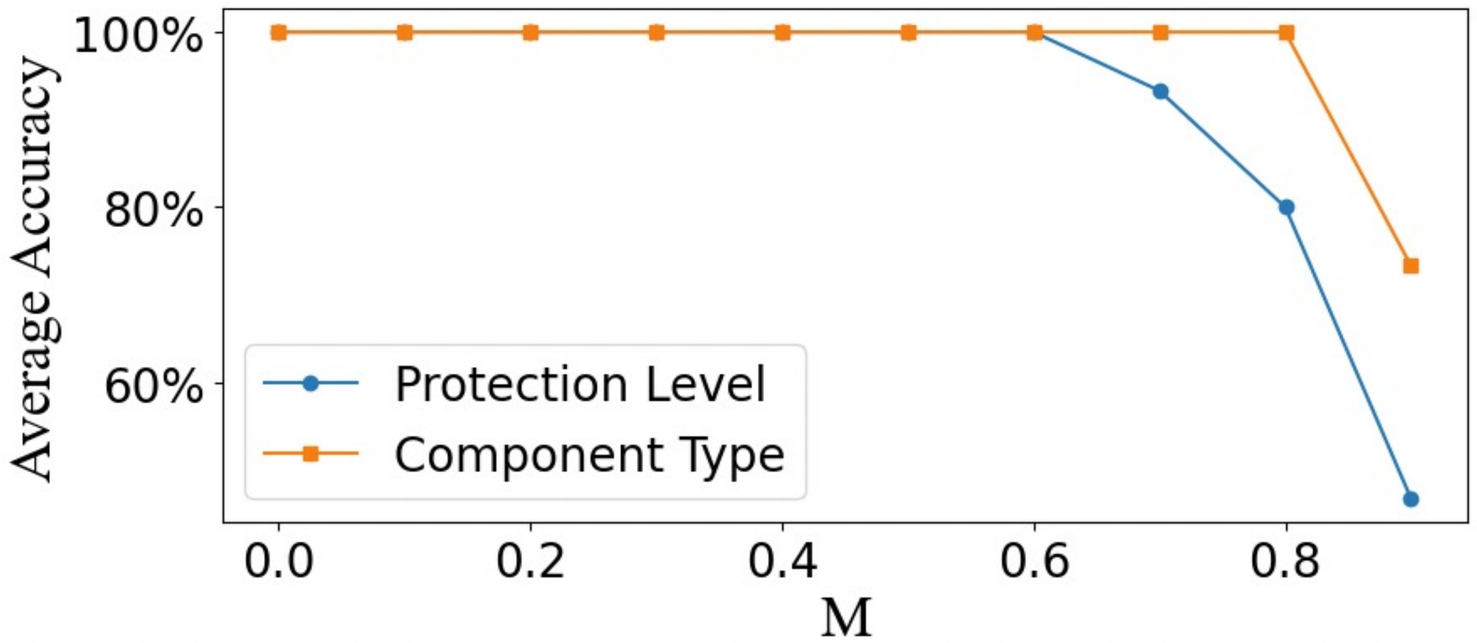
- **Analyzing the semantics of controller variables of the S7COMM protocol**

Semantics Type	Controller Variable	State	Semantics	Accuracy	Correlation
Device Status	Operating Mode	Run	TGS = (8,4,1), SSL-ID = 04240000,offset = 44, value = 08,	100%	100%
		Stop	TGS = (8,4,1), SSL-ID = 04240000,offset = 44, value = 04,	100%	100%
	LED State	ON	TGS = (8,4,1), SSL-ID = 00190000,offset = 55, value = 01,	100%	100%
		OFF	TGS = (8,4,1), SSL-ID = 00190000,offset = 55, value = 00,	100%	100%
	Protection Level	None	TGS = (8,4,1), SSL-ID = 01320004,offset = 46, value = 00 TGS = (8,4,1), SSL-ID = 01320004,offset = 48, value = 01	100%	100%
		Write	TGS = (8,4,1), SSL-ID = 01320004,offset = 46, value = 02 TGS = (8,4,1), SSL-ID = 01320004,offset = 48, value = 02	100%	100%
		Read & Write	TGS = (8,4,1), SSL-ID = 01320004,offset = 46, value = 03 TGS = (8,4,1), SSL-ID = 01320004,offset = 48, value = 03	100%	100%
Program Component	Component Type	I	TGS = (4,1,2), offset = 59, value = 11	100%	100%
		Q	TGS = (4,1,2), offset = 59, value = 21	100%	100%
		M	TGS = (4,1,2), offset = 59, value = 01	100%	100%
	Component Number	0-255	TGS = (4,1,2), offset = 64, value = 0-ff	100%	100%
	Component Value	OFF	TGS = (0,1,2), offset = 47, value = 00	100%	100%
		ON	TGS = (0,1,2), offset = 47, value = 01	100%	100%

SePanner extracts semantics of 6 controller variables with 100% accuracy and correlation

Evaluation via parsed protocol

- **Robustness of SePanner**
  - Variation of SePanner's average accuracy when removing M ×100 % messages



SePanner remains robust when removing 60% of ICP messages from network traffic

Evaluation via unanalyzed protocols

- Analyzing the semantics of controller variables of the 4 proprietary protocol

Protocol	Device Status (States)	Program Components (States)	Correlation
UMAS-1	2(4)	9(18)	100%
UMAS-2	2(5)	9(18)	100%
PCCC	5(10)	10(28)	100%
H3U	2(4)	6(8)	100%
ALL	11(23)	34(72)	100%

- Verifying the correctness of semantics by constructing simulators

PLC	Protocol	Controller Variables	Semantics	Correctness
M221	UMAS-1	Read/Write Protect	MS=****0000, offset = 31	✓
M340	UMAS-1	Operating Mode	MS=****fa00, offset = 10	✓
H3U	Huichuan	Force Y0 Value	MS=**0301**,offset = 19,24	✓
1400	PCCC	Test Mode	MS=****fc01, offset = 73	✓

SePanner successfully extracts semantics of 45 controller variables from 4 unanalyzed protocols

Applications: monitoring and detection

- **ICSMonitor: Monitor real-time state of PLCs**
- **Detect offensive messages targeting controller variables**

```
Scaning the IP: 192.168.1.118
Model: 1766-L32BWA C/21.00
Firmware: 21.00
*Operating State: Run
*Remote State: Remote
*Force Install: None
*Force Enable: Enable
*Protection Level: Access Protect
```

```
Scaning the IP: 84.32.54.68
Model: BMX P34 20302
Firmware: v2.8
Memory Card: BMXRMS008MP
*Operating State: Run
*Protection Level: Access Protect
*Connection: Connected
```

```
Scaning the IP: 192.168.0.35
Model: 6ES7 317-2EK14-0AB0
Firmware: 3.1.0
*Operating State: Run
*Protection Level: None
*Connection: Connected
```

```
Scaning the IP: 192.168.1.21
Model: TM221CE24T
Firmware: 1.12.0.0
*Operating State: Run
*Protection Level: Read&Write
*Connection: Disconnected
```

PLC	Functions	Offensive Messages
M221	Start device	5a**ff00
	Change the value of Q0.0	5a00**01
	Read the value of Q0.0	5a00**00
	Initialize the device	5a**0000
M340	Start device	5a**ff00
	Read the value of I0	5a00**00
	Stop device	5a**ff00
1400	Change into Remote Run mode	0f**8006
	Change into Remote Program mode	0f**8001

Extensions: in-vehicle protocols

- **Analyzing the semantics of in-vehicle protocols**

Protocol	CAR	ID	Num
IBUS	BMW e46/e53	Module ID in SRC	24
		Module ID in DST	36
		Command ID of message	74
CANBUS	BMW e65	Arbitraion ID	7
		Semantics in Data Fields	23
	BMW e60	Arbitraion ID	9
		Semantics in Data Fields	16
	Lexus RX350	Arbitraion ID	3
		Semantics in Data Fields	30
ALL			222

SePanner can infer the semantic information of in-vehicle protocols

Thank You!

jie_meng@zju.edu.cn