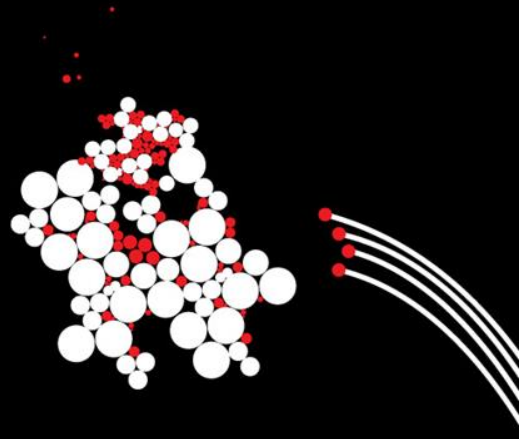
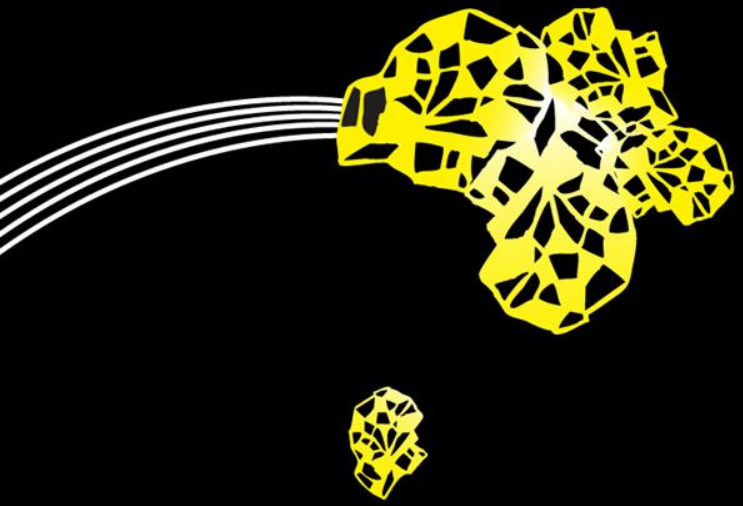
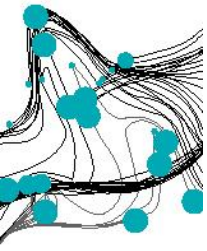
UNIVERSITY OF TWENTE.



SPECIFICATION MINING FOR INTRUSION DETECTION IN NETWORKED CONTROL SYSTEMS

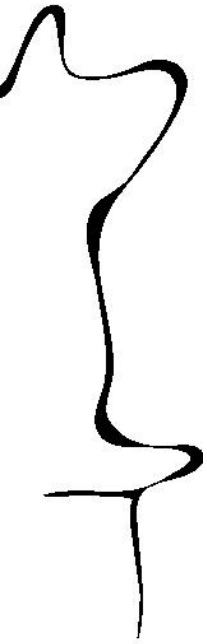
Marco Caselli, Emmanuele Zambon, Johanna Amann, Robin Sommer, Frank Kargl





Network Intrusion Detection in a Nutshell

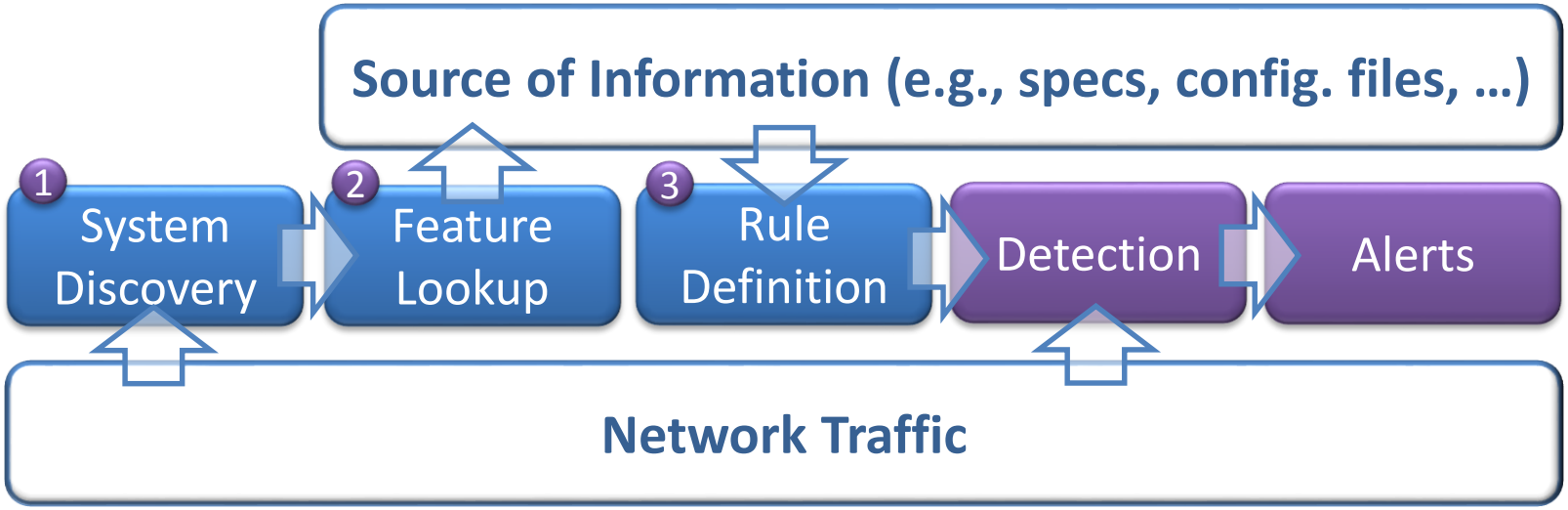
- From **anomaly**-based to **specification**-based
- Not all infrastructures come with specifications
- Deploying these IDSs requires substantial human effort



Our goal

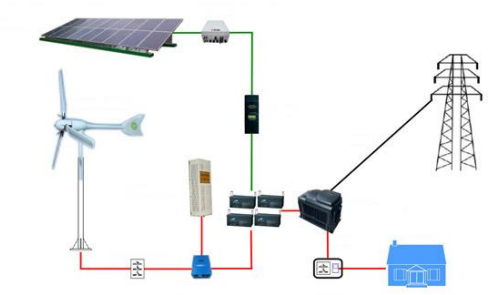
We aim to ease the deployment of a specification-based IDS by automating the creation of its specification rules

Specification Mining Approach



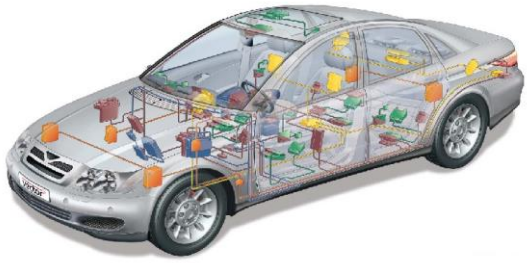
Networked Control Systems

"Systems whose constituents are **sensors**, **actuators**, and **controllers** distributed over a **network**"



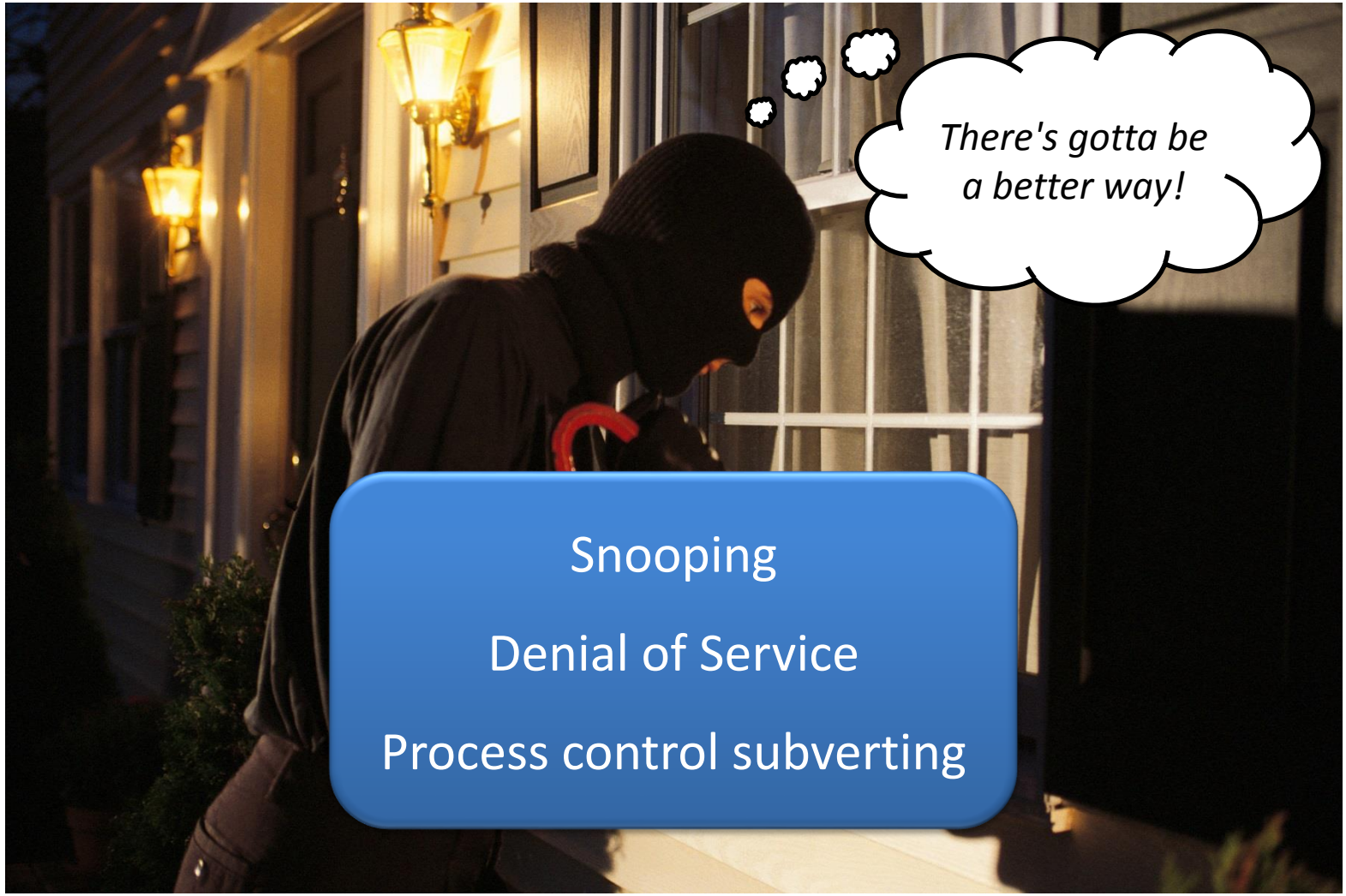
Industrial Control Systems

Building Automation Systems

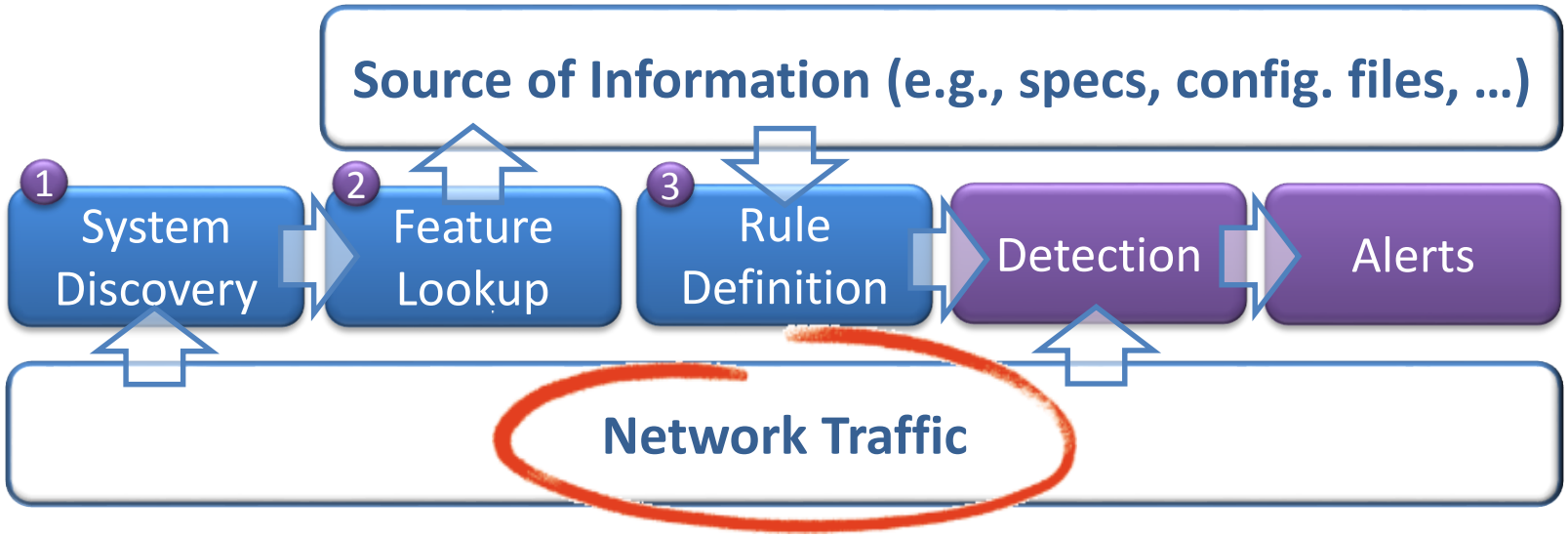


In-Vehicular Networks

Building Automation Threats

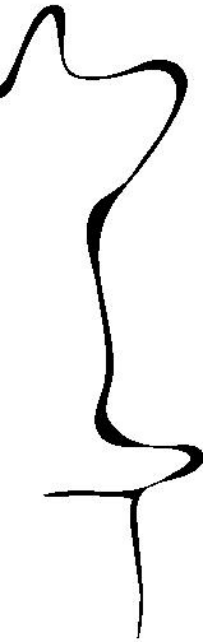


Specification Mining Approach



BACnet

Building **A**utomation and **C**ontrol **net**work

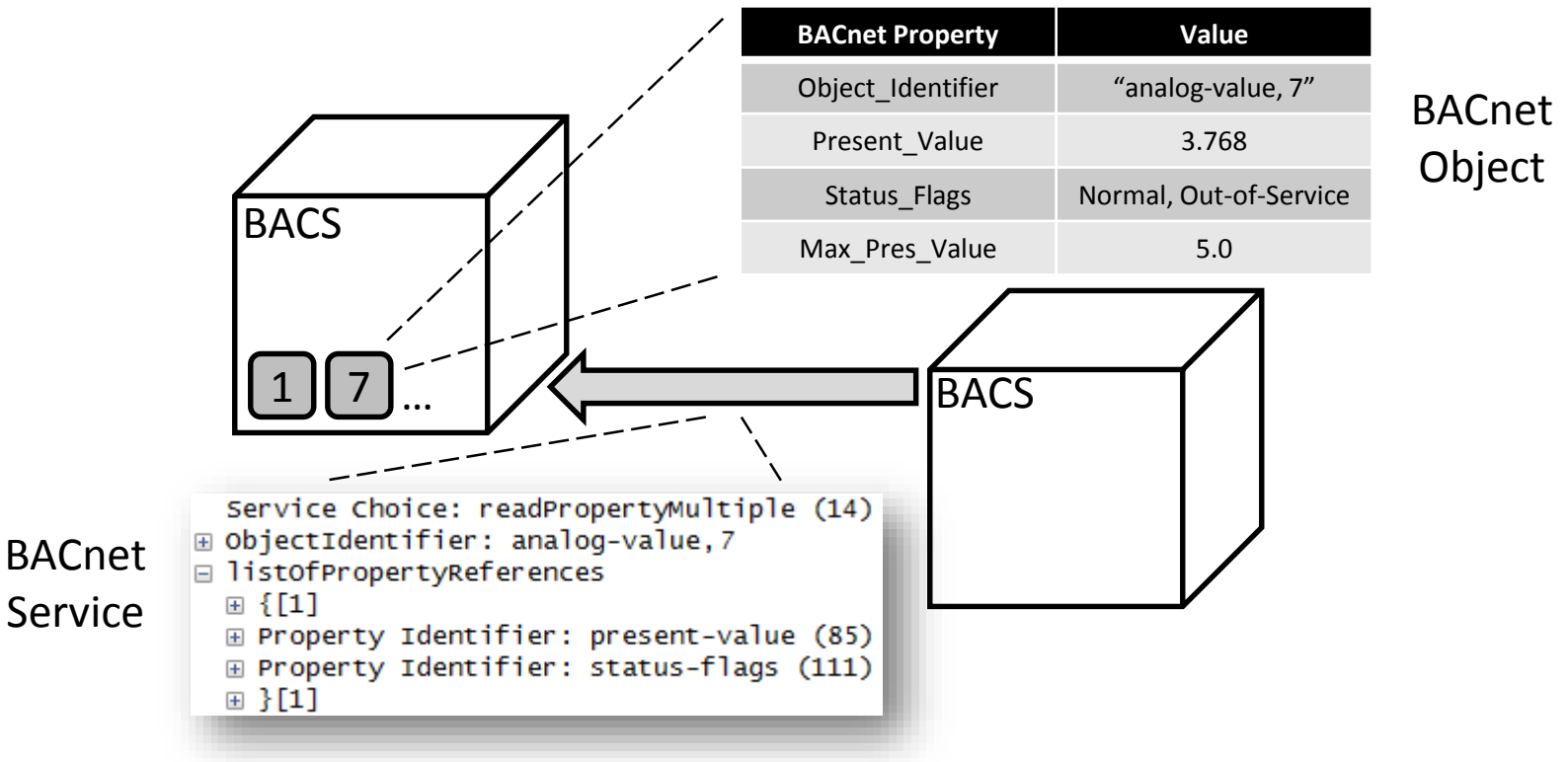


BACnet Application Layer						
BACnet Network Layer						
ISO 8802-2 (IEEE 802.2) Type 1		MS/TP	PTP	LonTalk	BVLL	BZLL
					UDP/IP	BP/GT
ISO 8802-3 Ethernet	ARCNET	EIA 485	EIA 232		IP Supporting Data link	Zigbee Stack

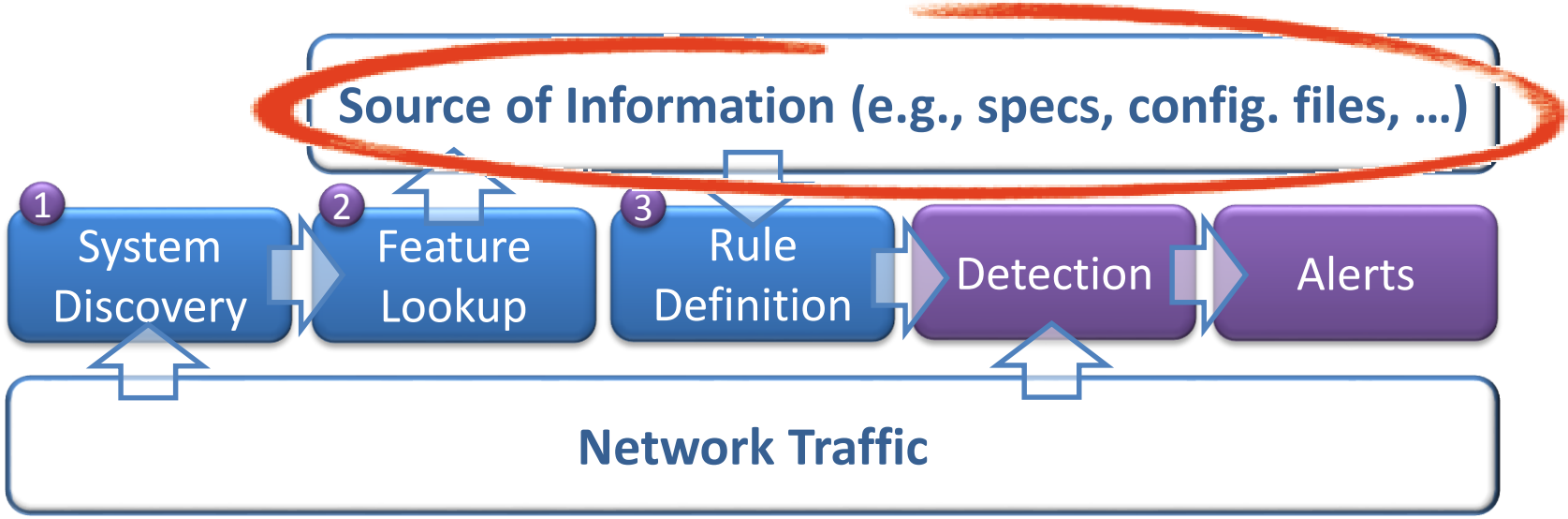
BACnet/IP

BACnet (Application Layer)

- 'Services' and 'Objects'
  - Every object has got a subset of 'Properties'



Specification Mining Approach



Building Automation Documentation

- Protocol Implementation Conformance Statement (PICS)

Product information	
Date	2013-07-23
Product name and model number	Blue ID S10 Controller
Application software version	1.0
Firmware revision	1.00
BACnet protocol revision	9
Product description	The Blue ID S10 Controller contains a powerful microprocessor. It can be easily programmed for building automation purposes. The processing speed and computing power mesh seamlessly with the requirements of modern and integrated systems. The controller uses a reliable operating system that ensures quality and operational security. It is fully controllable via BACnet including commissioning, writing, reading, alarm and event handling.
BACnet standardized device profile	BACnet Building Controller (B-BC)

Vendor information	
Vendor name	Priva
Vendor ID	105
Contact information	PO Box 18 2678 ZG The Netherlands www.priva.co.uk

Supported BIBBs	
DS-RP-A	Data Sharing - Read Property - A
DS-RP-B	Data Sharing - Read Property - B
DS-RPM-A	Data Sharing - Read Property Multiple - A

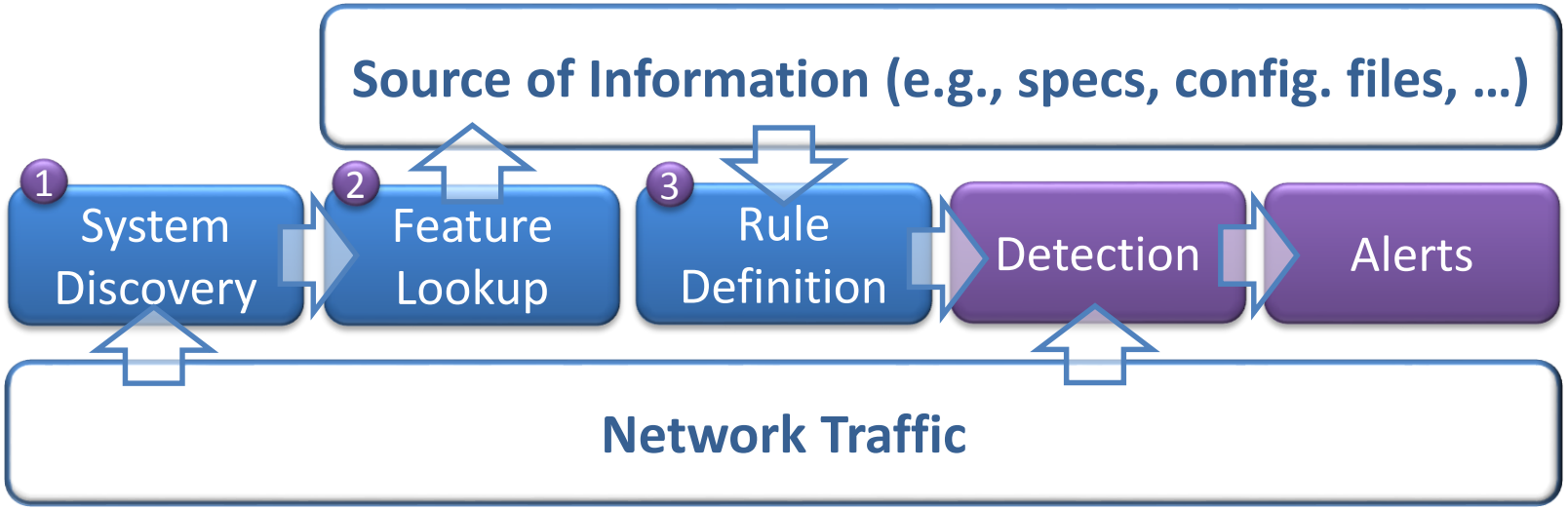
Building Automation Documentation

- Protocol Implementation Conformance Statement (PICS)

Standard object types supported[1]	Dynamically creatable and deletable
Accumulator	no
Analog Input	no
Analog Value	no
Binary Input	no
Binary Output	no
Binary Value	no
Calendar	yes
Device	no

Supported properties per object type	Required or optional	Readable (R) or readable/writeable (R/W)	Additional comments
Accumulator			
Object_Identifier	required	R	
Object_Name	required	R	
Object_Type	required	R	
Present_Value	required	R/W	
Description	optional	R	
Status_Flags	required	R	

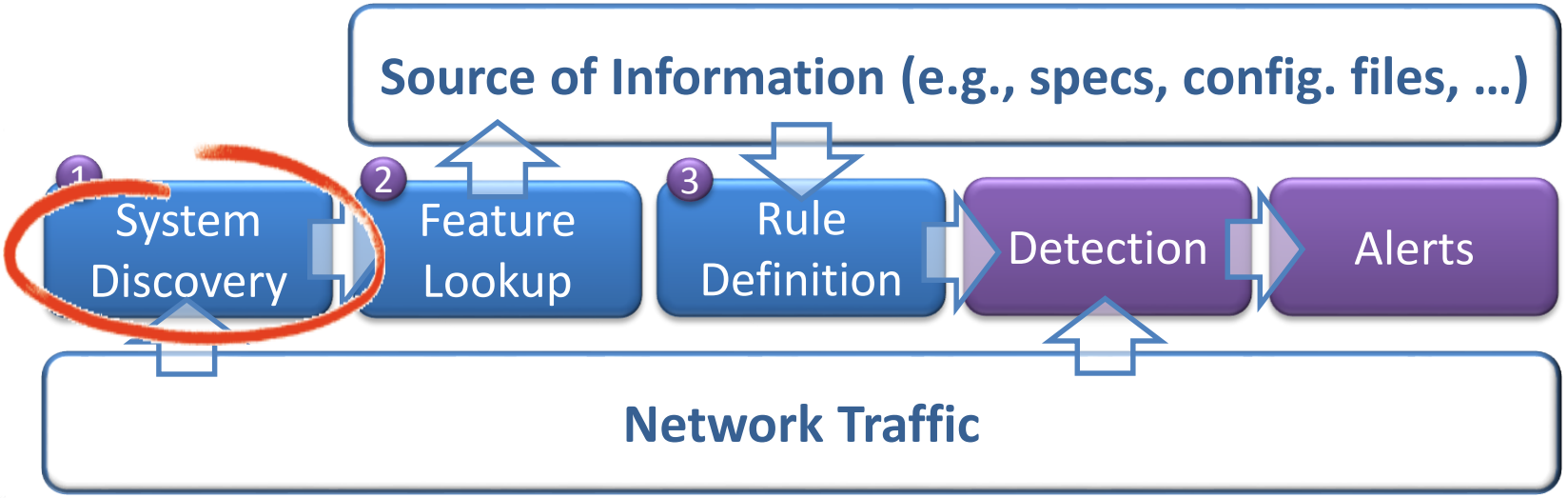
Specification Mining Approach



University of Twente (NL)

Lawrence Berkeley National Laboratory (US)

Specification Mining Approach

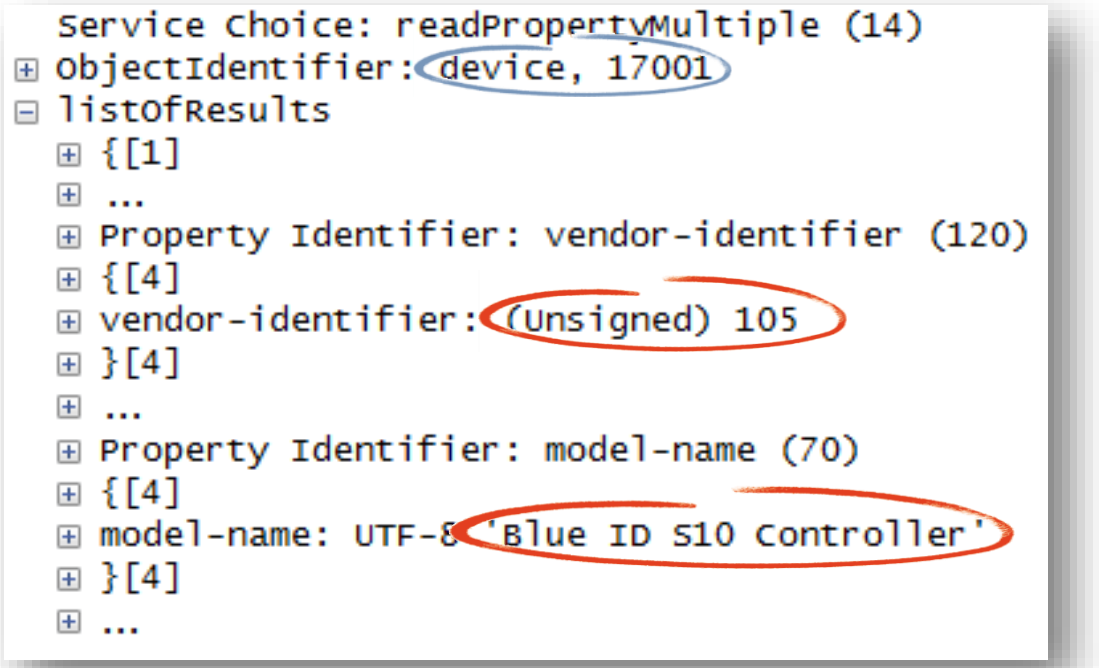


1) Identify devices communicating on the network

2) Determine role and purpose of each identified device

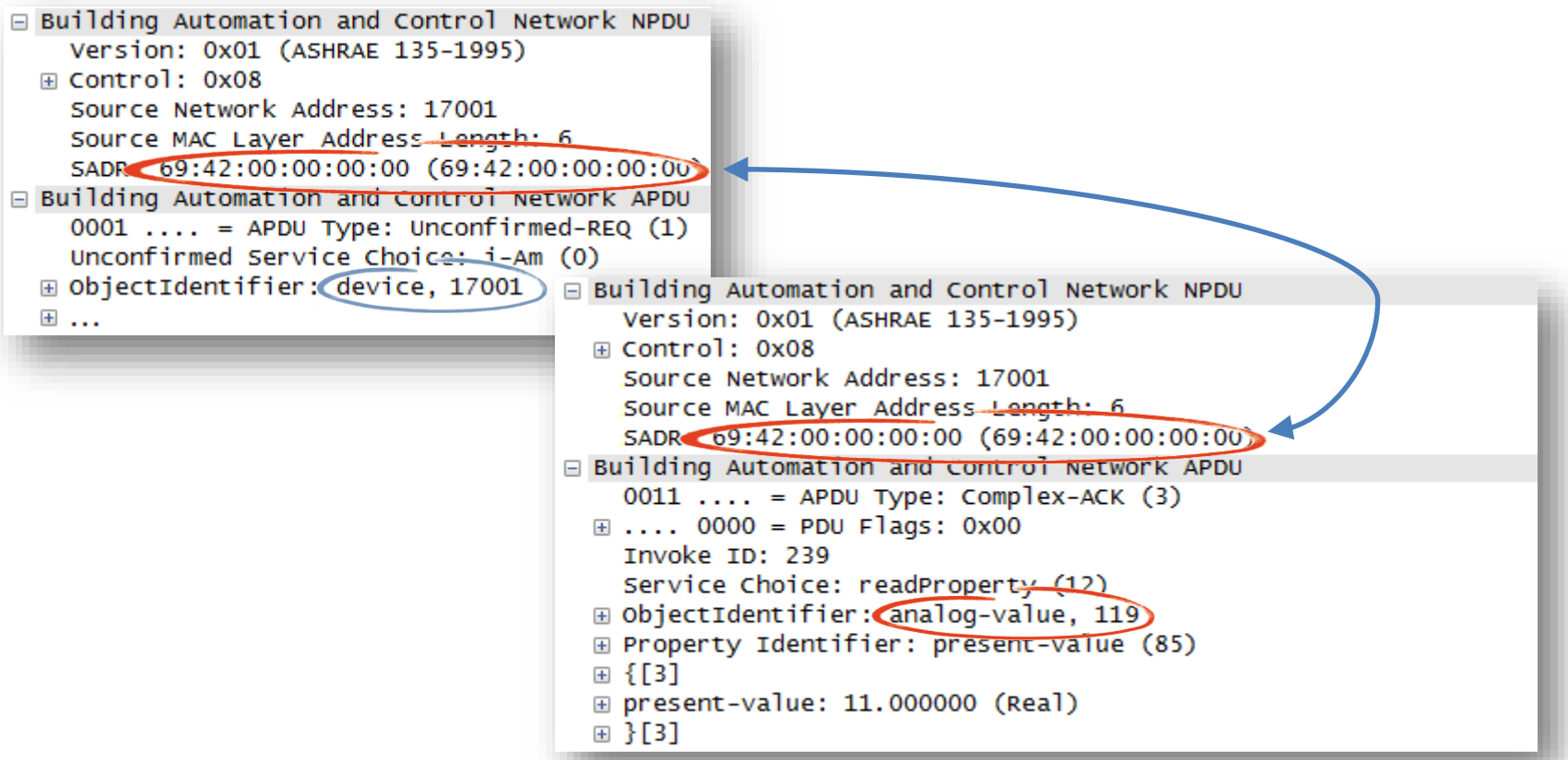
System Discovery

- "BACnet Device Object analysis"



System Discovery

- "BACnet Device Object analysis"
- "BACnet Address linking"

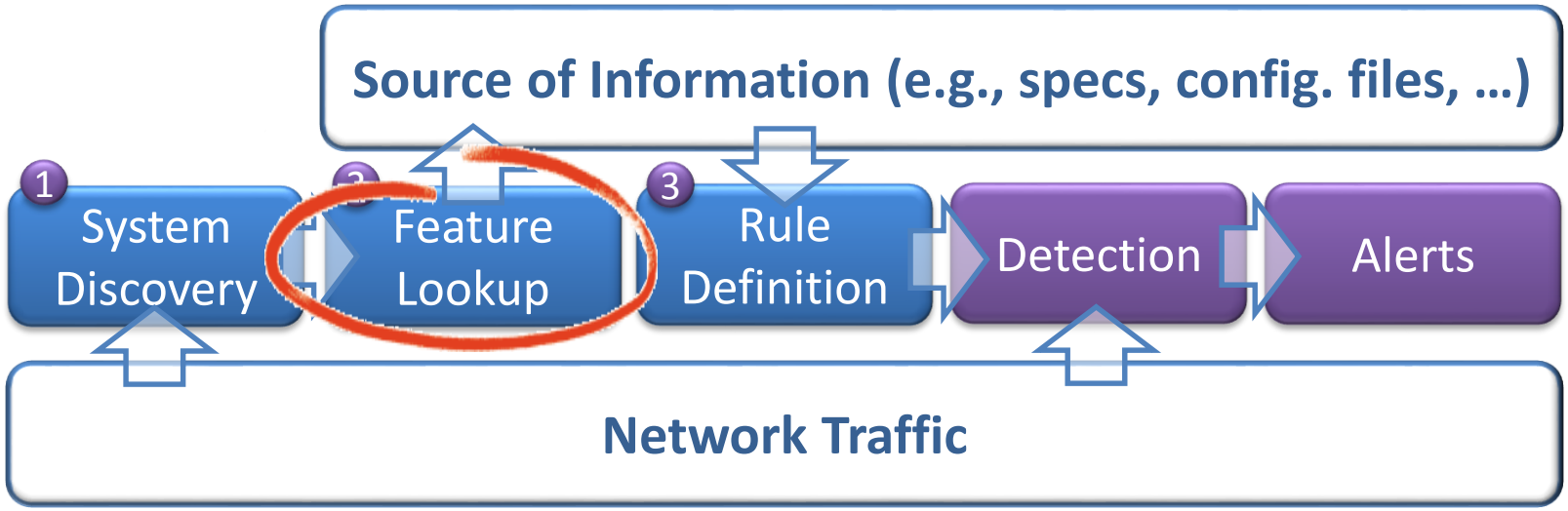


System Discovery

- Results at the University of Twente:

# of devices	Vendor	Model	Role
5	Kieback&Peter	DDC4000	DCS
15	Priva	HX 80E	Router
7	Priva	Compri HX	Controller
25	Priva	Compri HX 3	Controller
36	Priva	Compri HX 4	Controller
12	Priva	Compri HX 6E	Controller
85	Priva	Compri HX 8E	Controller
2	Priva	Blue ID S10	Controller
16	Priva	Comforte CX	HMI
2	Delta Controls	eBCON	Controller
3	Siemens	PXG80-N	Controller
3	Siemens	PXC64-U	Controller
3	Siemens	PXC128-U	Controller
3	Siemens	PXR11	Controller
3	Siemens	PXC00-U + PXA30-RS	Controller
1	Unknown	Unknown	-

Specification Mining Approach

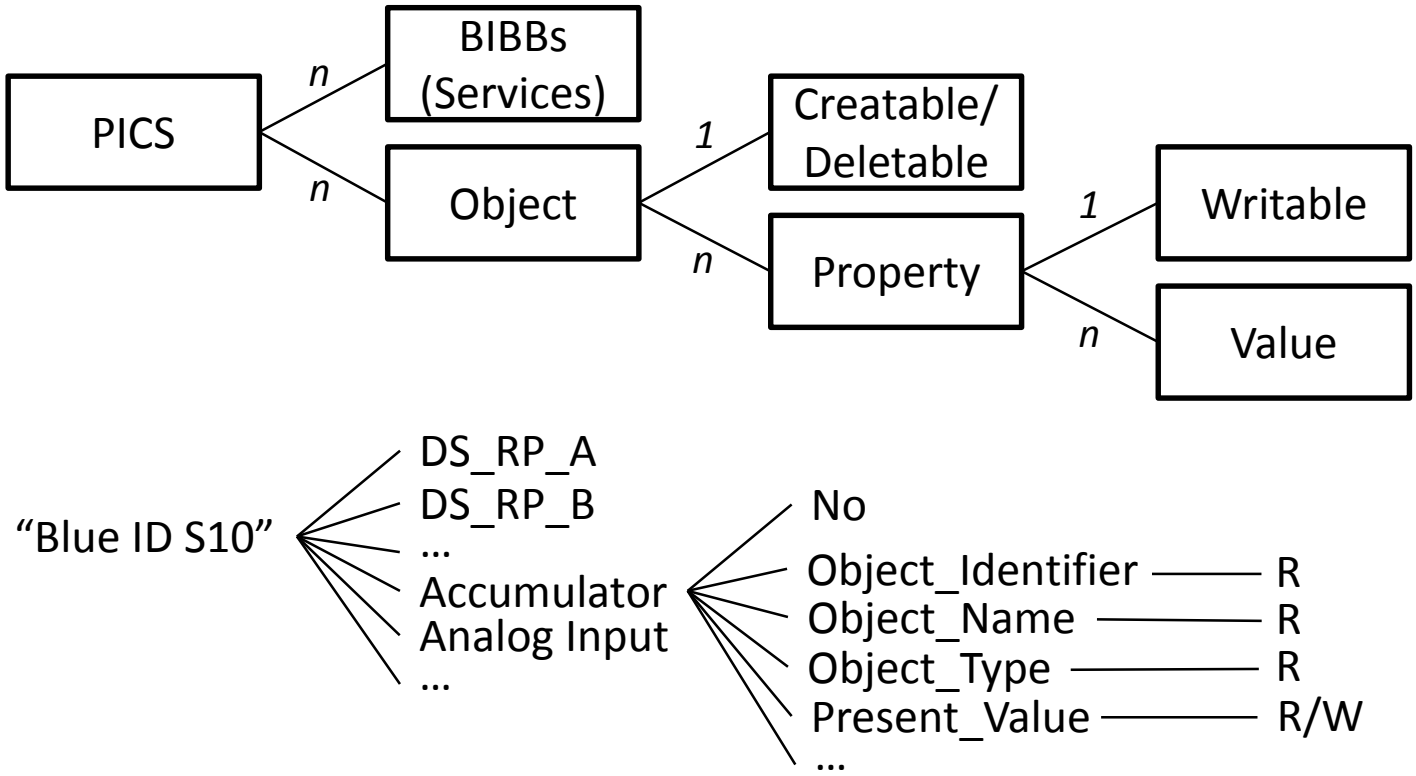


1) Find verified information about the infrastructure's devices

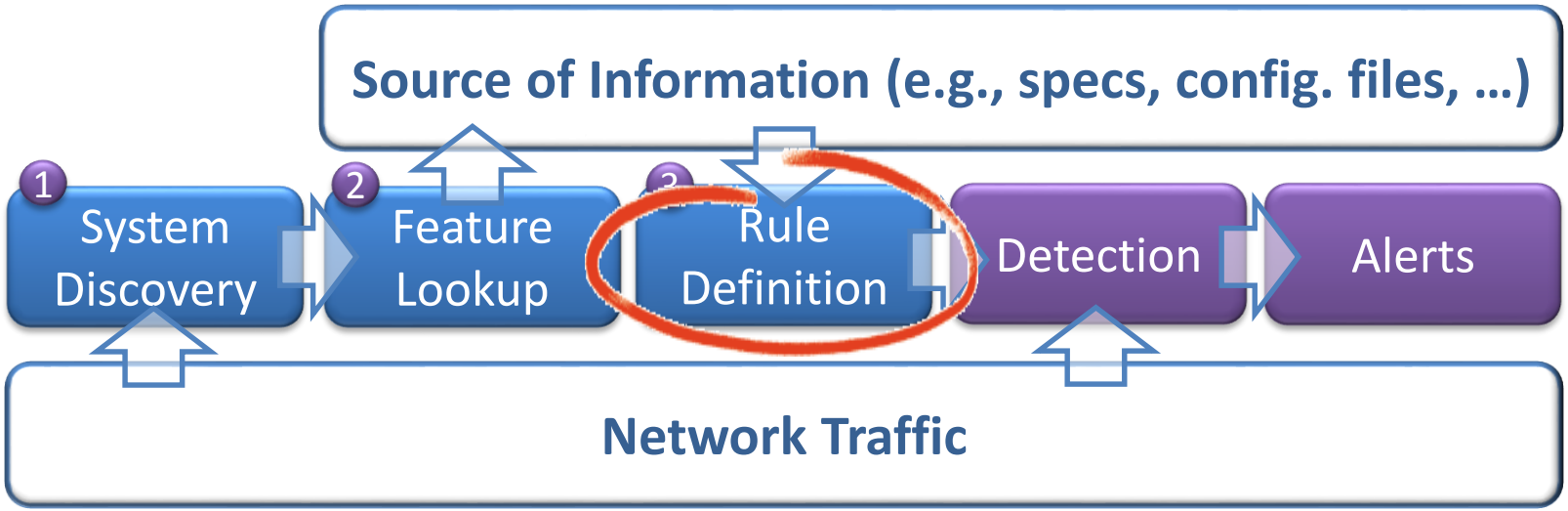
2) Select features and constraints from the retrieved documents and arrange results in a structured form

Feature Lookup

- PICS



Specification Mining Approach



1) Select identified information from Feature Lookup

2) Translate this information to specification rules

Rule Definition

- NCS components (e.g., controllers) share some properties:
  - Employing a limited set of variables to fulfill their functions
  - These variables often have predetermined types
  - There limited set of methods to access and manipulate variables

- Three different abstract rules:
  1) "**Type**" rule checks if a variable of a specific type is allowed
  2) "**Value**" rule checks which values a variable may assume
  3) "**Method**" rule checks which methods can be used to access a specific variable

Rule Definition

Algorithm 1 Abstract "Type" rule

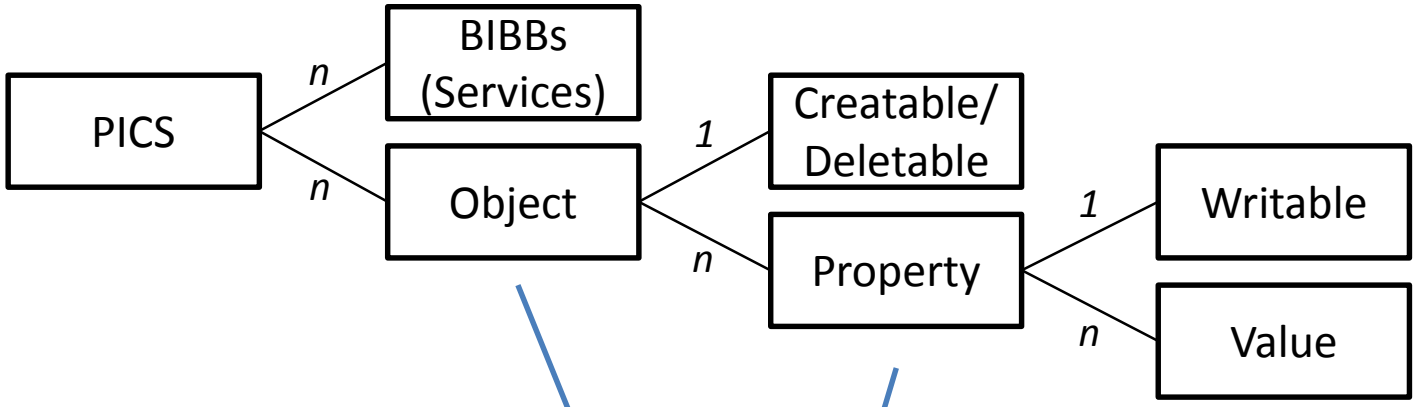
```
1: if Variable_type ∉ Controller_AllowedVariableTypes then
2:     Alert("Variable type not permitted")
3: end if
```

Algorithm 2 BACnet "Type" rules

```
1: if BACnet Object ∉ Controller_AllowedObjectTypes then
2:     Alert("Forbidden Object")
3: end if

1: if BACnet Property ∉ Controller_ObjectAllowedPropertyTypes then
2:     Alert("Forbidden Property")
3: end if
```

Rule Definition

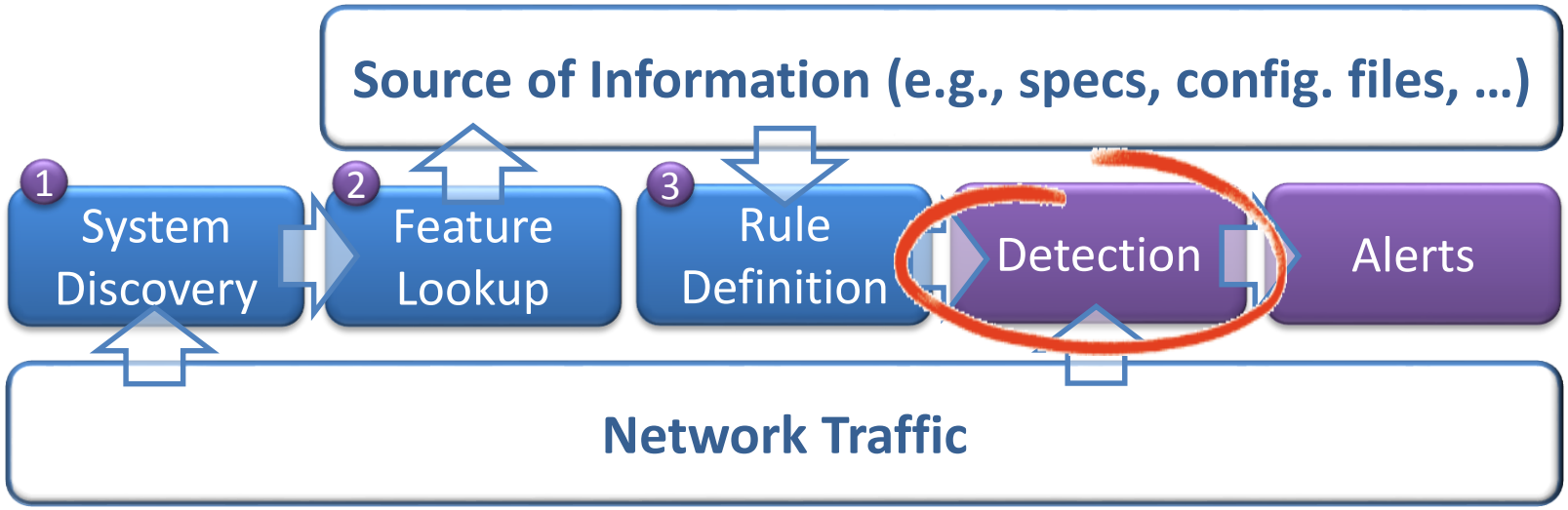


Algorithm 2 BACnet "Type" rules

```
1: if BACnet Object ∉ Controller_AllowedObjectTypes then
2:     Alert("Forbidden Object")
3: end if

1: if BACnet Property ∉ Controller_ObjectAllowedPropertyTypes then
2:     Alert("Forbidden Property")
3: end if
```

Specification Mining Approach

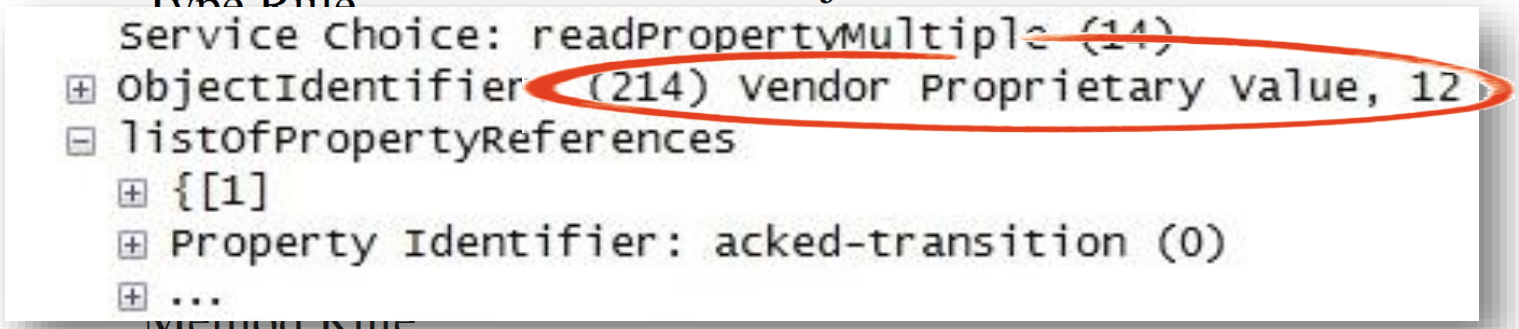


Detection Results

Abstract Rule	Specification Rule	# Alerts
Type Rule	Forbidden object	2
	Forbidden property	234
Value Rule	Forbidden value	0
Method Rule	Forbidden service	0
	Forbidden object creation	0
	Forbidden object deletion	0
	Forbidden property writing	1

Detection Results

Abstract Rule	Specification Rule	# Alerts
Type Rule	Forbidden object	2
Method Rule	Forbidden object deletion	0
	Forbidden property writing	1



Detection Results

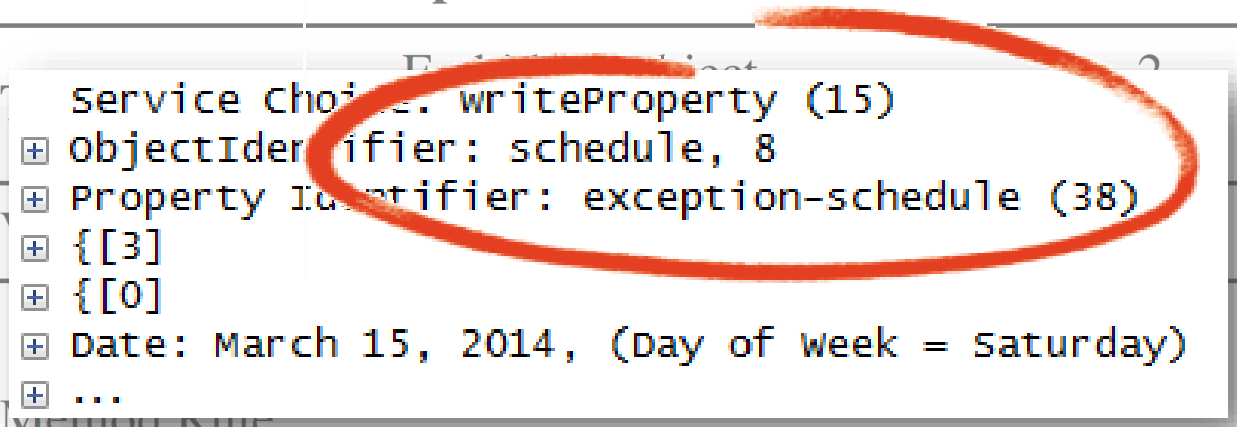
```
Service Choice: readPropertyMultiple (14)
⊞ ObjectIdentifier: device, 1050634
⊟ listOfPropertyReferences
  ⊞ {[1]
  ⊞ Property Identifier: max-segments-accepted (167)
  ⊞ ...
```

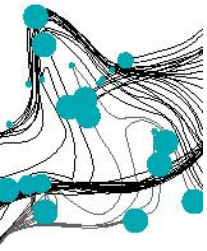
Type Rule Forbidden property 234

```
Service Choice: readPropertyMultiple (14)
⊞ ObjectIdentifier: device, 1050634
⊟ listOfResults
  ⊞ {[1]
  ⊞ Property Identifier: max-segments-accepted (167)
  ⊟ propertyAccessError
    ⊞ {[5]
    ⊞ error Class:  property
    ⊞ error Code:  unknown-property
  ⊞ ...
```

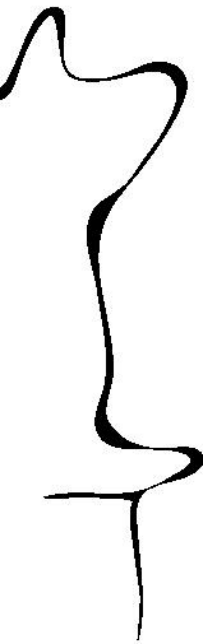
Detection Results

Abstract Rule	Specification Rule	# Alerts
	Forbidden object deletion	0
	Forbidden property writing	1





Discussion



- **Configuration mismatches** vs. **Security relevant events**
- **Attack Coverage**
- **Generalization** beyond BACnet-based BASs

Conclusions

Networked control technologies are rapidly spreading

We need security solutions that can quickly scale up to a multitude of heterogeneous devices

Automated specification mining and rule description:

- More efficient deployment of specification-based IDSs
- Automated adaptation to the environment

Q&A

Thanks

Marco Caselli
m.caselli@utwente.nl