OAK RIDGE National Laboratory

Trust-but-Verify in Cyber-Physical Systems (CPS)*

Kalyan Perumalla

Distinguished R&D Staff Member, ORNL

ACM Workshop on Secure and Trustworthy Cyber-Physical Systems

ORNL is managed by UT-Battelle, LLC for the US Department of Energy

U.S. DEPARTMENT OF ENERGY

*Personal views of the author, not representing the author's employers

OAK RIDGE National Laboratory

Operational Technology (OT)

- Devices represent important cyber-physical interfaces
- Produced by many vendors
- Installed, configured, maintained by many integrators, contractors
- Devices becoming feature-rich over time

OT only recently began embracing IT principles, cybersecurity

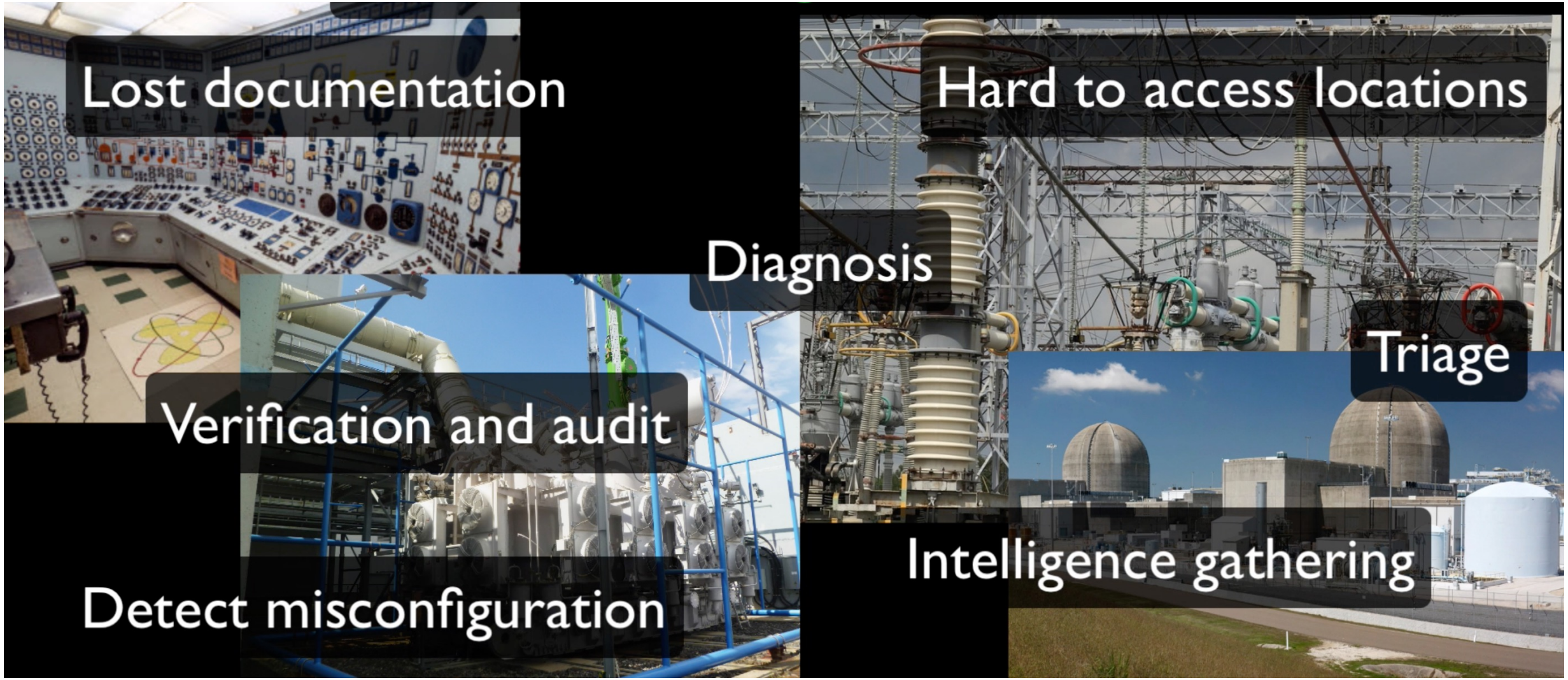
Trust by default, add verification

Ground Truth	Claims	Operation
• Add verification of ground truth	• Add verification of claims	• Add verification of operation

This seems to provide better overall value, as being seen in our current projects in energy and defense sectors

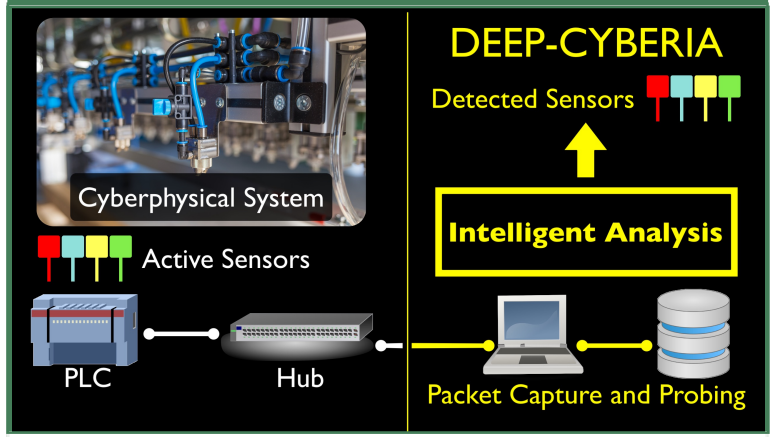
- Handles legacy well
- Lower up-front costs
- Can scale in complexity

"I **trust** you, but I need to **verify** what you have and how well you are"



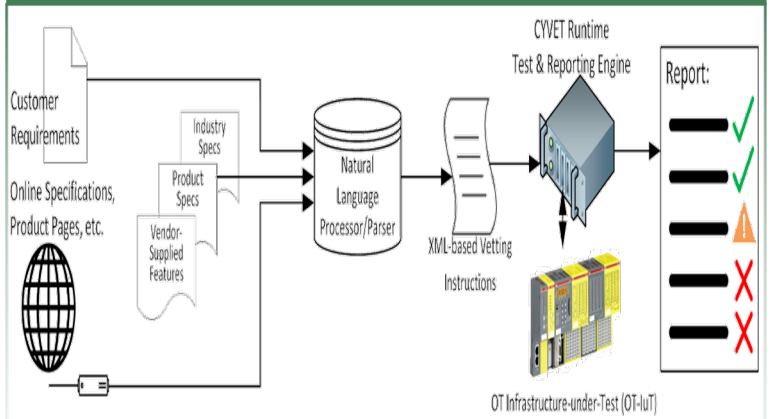
Trust-but-Verify: Illustration

OT Sensor Detection, Identification, Mapping



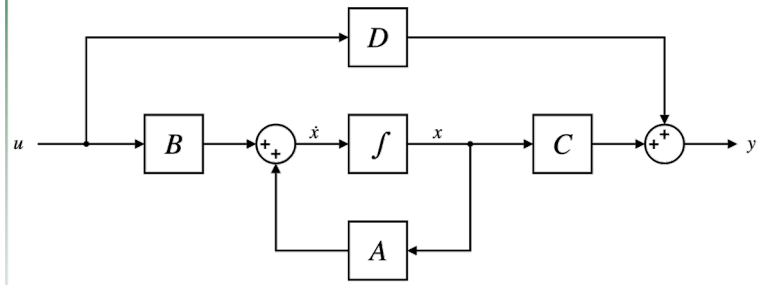
Deep CYBERIA

Semi-automated Vetting of OT Security Features



CYVET

Dynamic OT Monitoring via Digital Twins and Threads



DT

1. What's out there?

2. How robust is it?

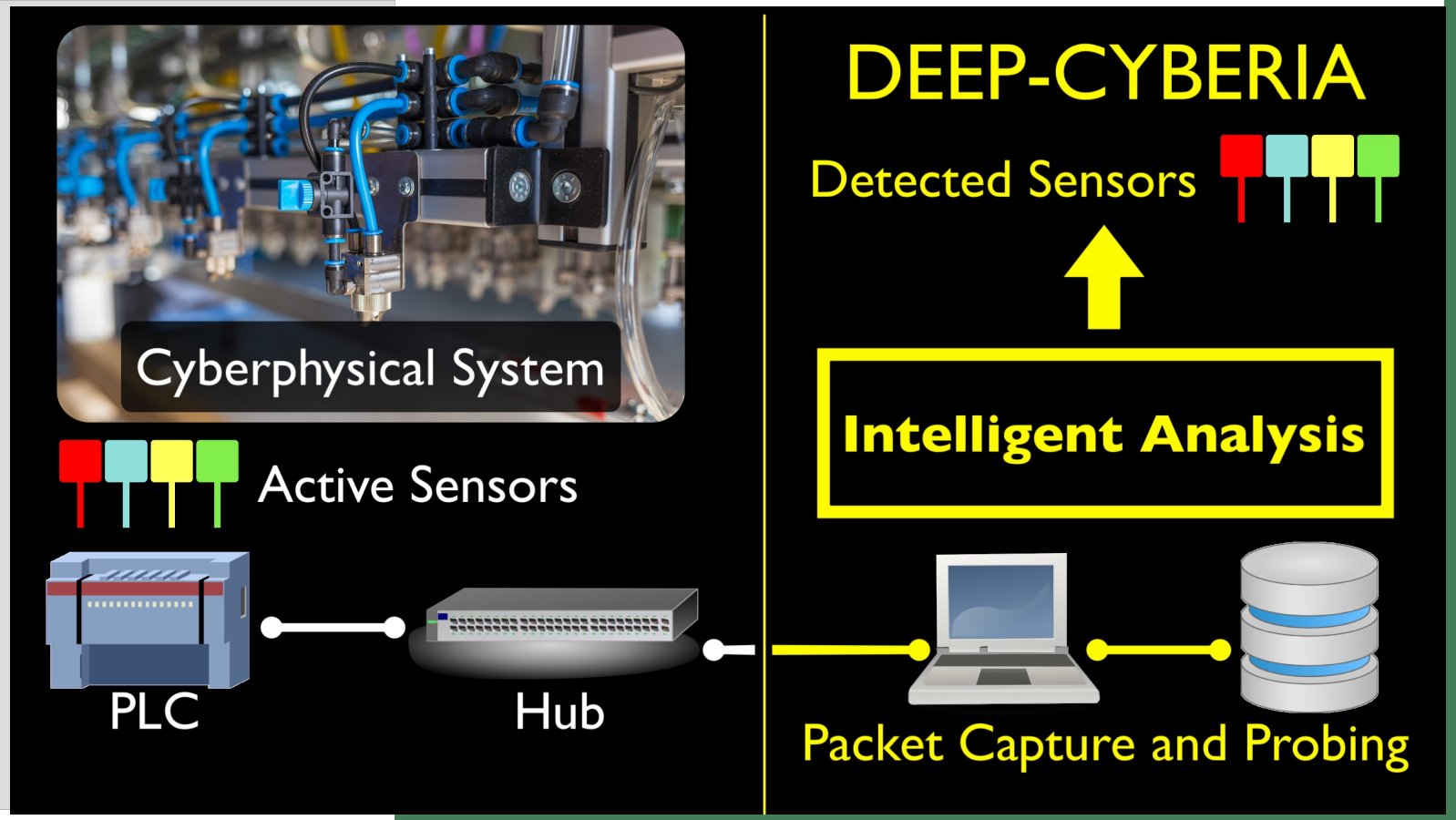
3. How well is it doing?

Question #1: What's there?

Deep CYBERIA

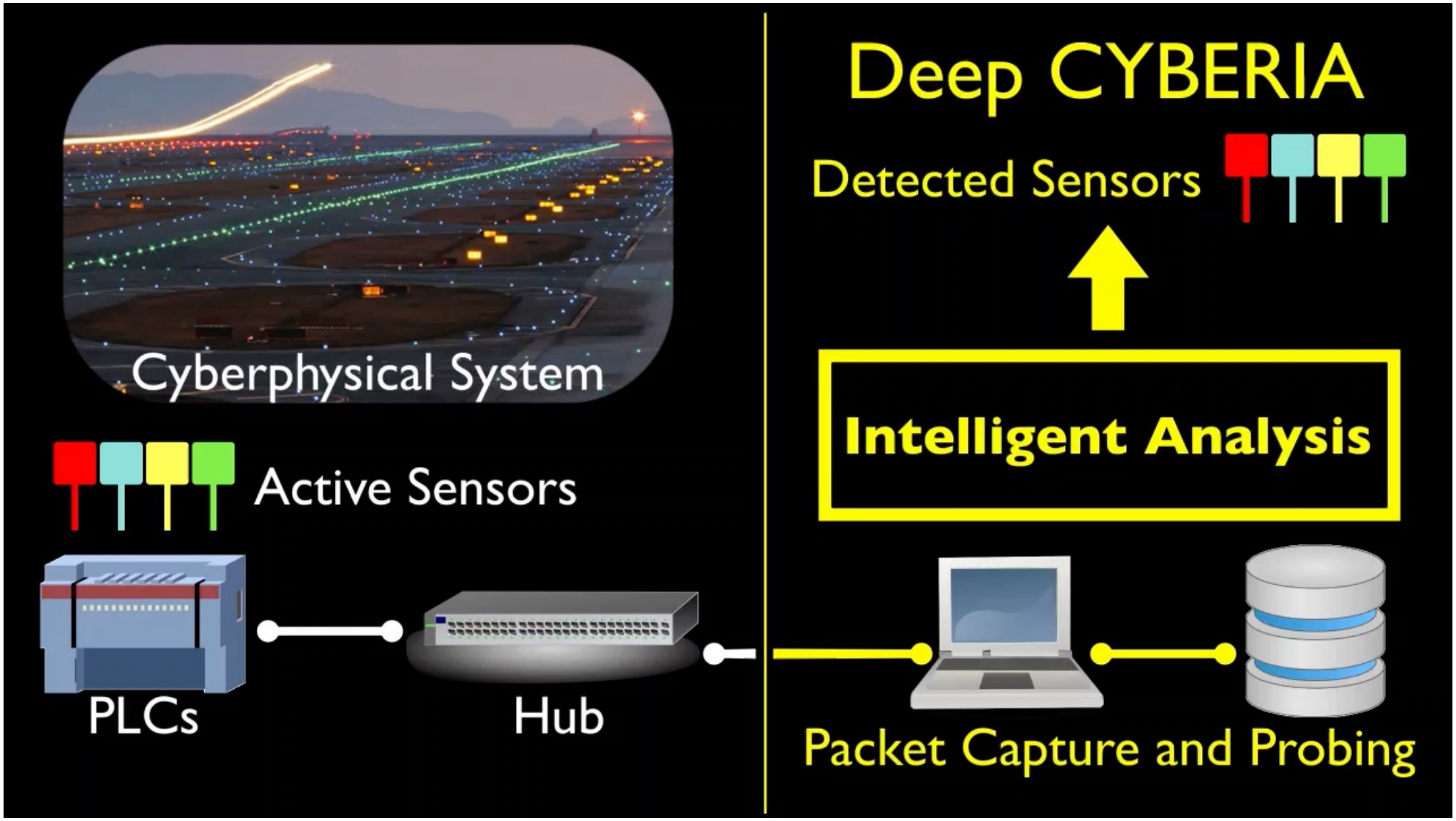
- Sensor Detection
- Sensor Identification
- Sensor Mapping
- Sensor Correlation

- Passive, Active, Hybrid



With Dr. Juan Lopez (ORNL) and team
[M. Alam, J. Asiamah, N. Guerra, R. Styles, L. Wetzel]

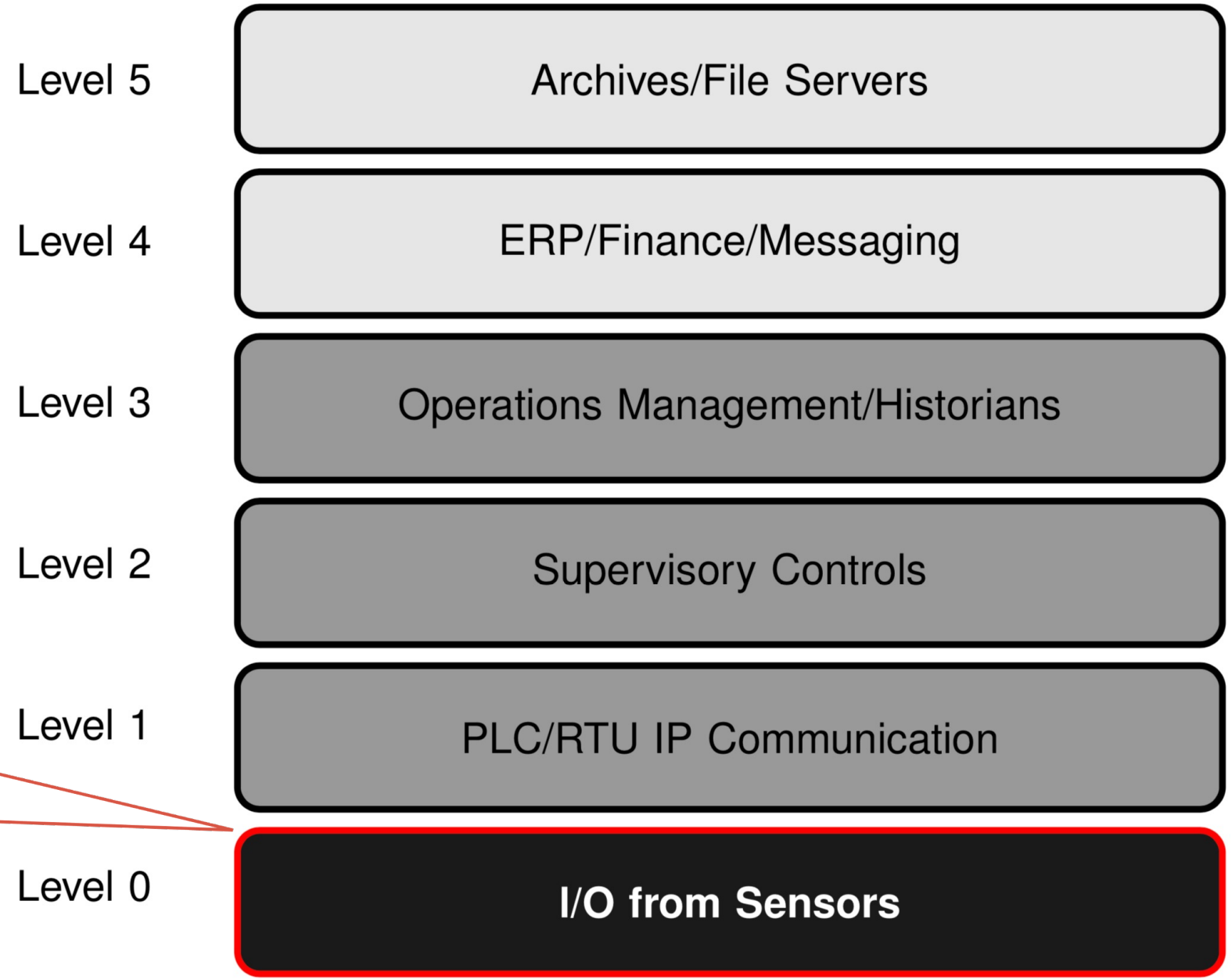
Detecting sensors for gaining Trust by verification



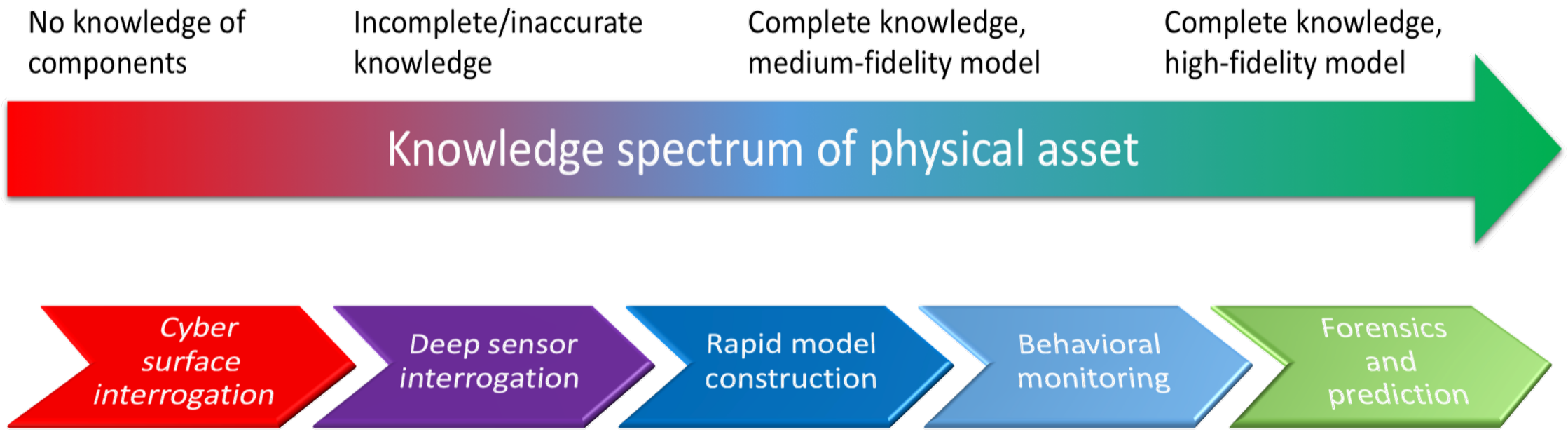
Trust-but-Verify at Lowest Cyber-Physical System Level

- **Levels 2-5**
  - Can use/reuse Information Technology (**IT**) solutions
- **Levels 0-1**
  - Specific to Operational Technology (**OT**)

Our focus of Trust-but-Verify



Broader Trust-but-Verify with Deep-CYBERIA



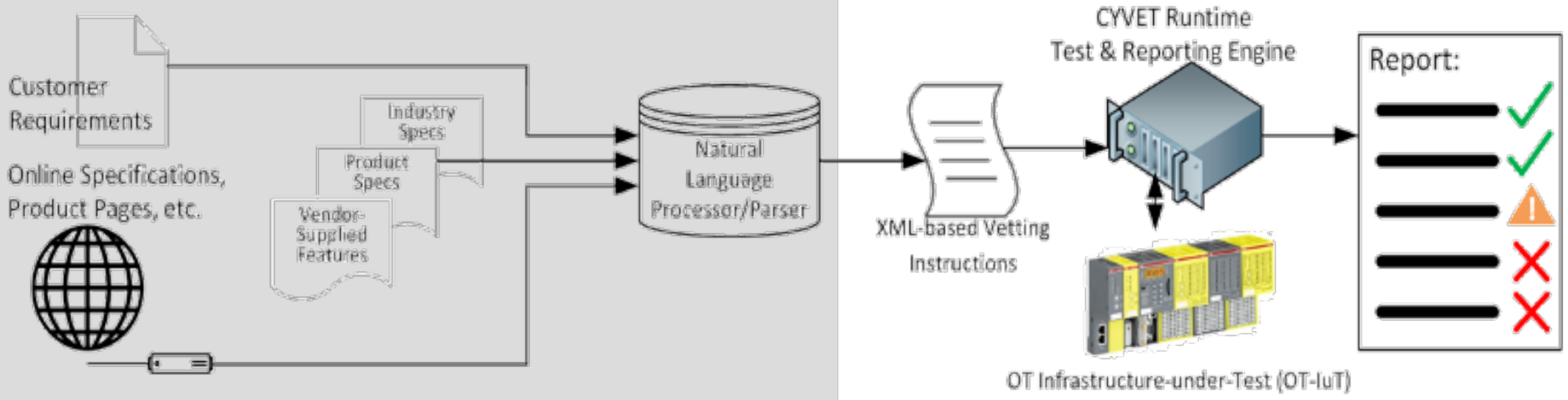
Deep Cyber-Physical System **I**nterrogation and **A**nalysis

K. Perumalla, S. Yoginath, and J. Lopez, "Detecting Sensors and Inferring their Relations at Level-0 in Industrial Cyber-Physical Systems" In 2019 IEEE International Symposium on Technologies for Homeland Security (HST)

Question #2: How robust is it?

CYVET

A Cyber-Physical Security Assurance Framework Based on a Semi-Supervised Vetting



With Dr. Juan Lopez (ORNL) and team

Vendor-Supplied Features (VSF)

FieldGuide

Enhance Operations

Write Protection

▪ Introduction

Transmitters used in Safety Systems, Custody Transfer, or critical processes need to be able to be secure from tampering or inadvertent changes to their setup.

▪ Yokogawa Solution

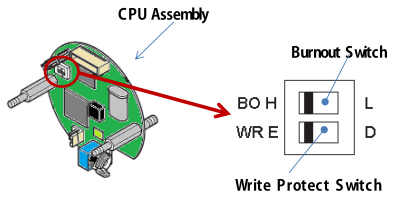
Yokogawa's EJA-E and EJX-A series of pressure transmitters have the security of a Software Write Protection (Password) and a Hardware Write Protection (Switch). These can be used independently or together to build the level of security desired.

▪ Applicable Models

⇒ **EJA-E Series:** All models
⇒ **EJX-A Series:** All models

▪ Hardware Write Protection (Switch)

The HART communication EJA-E and EJX-A transmitters have a Write Protection (WR) switch located on the CPU Assembly Board next to the Burn Out (BO) switch. When the WR switch is in the "D" (Disabled) position, the transmitter will not allow parameter changes through the use of a handheld communicator, FieldMate, or range setting switch on the transmitter indicator (if equipped). When the WR switch is in the "E" (Enable) position, parameter changes will be allowed.



Hardware Write Protection Switch (WR)		
Write Protection Switch Position	H L E D	H L E D
Write Protection	*Write Enabled*	*Write Disabled*

FGP 110-01.a

Refer to the exploded view of the transmitter in the Instruction Manual (IM) for the location of the CPU Assembly Board within the transmitter.

▪ Software Write Protection (Password)

The EJA-E and EJX-A transmitters with HART communication have a Password that can be set to protect the configured parameters. The Hardware Write Protect switch takes precedence over the Password Protection.

Using FieldMate, the Password function can be Enabled or Disabled. When the Password function is Enabled, a 8-digit password will need to be entered to make any setting changes. This Password can be any 8-digit password the customer wants.

Once the password is set-up, anytime a change needs to be made, the unit will need to be un-locked using the chosen password. When the password in entered, the technician will have 10 minutes to make the changes needed. Once the time limit has expired, the password will need to be re-entered for another 10-minute time block.

FieldMate™

Hart 5

DTM Works
> Write Protect

Hart 7

DTM Works HART 7
> Detailed Setup
> Device Information
> Field Device Info
> Wrt Protect Menu

FGP 110-02.a

Once on the write protect screen, the current status of the write protect function is displayed. There will also be instructions to Enable or Disable the password function and how to assign the password.

Although FieldMate is highlighted here, any Hart Communicator has access to these functions. Refer to the User's Manual for the HART programming tree.

What if I forget the Password?
The transmitter has a temporary recovery password pre-programmed. Once this recovery password in entered, the technician is given 10 minutes to reset the password only. No other parameters can be changed during this 10-minute block. Refer to the Instruction Manual or contact Technical Service for the Recovery Password. The recovery password is the same for all Yokogawa pressure transmitters.

Besides FieldMate, is there any way to know the Write Protect status of the transmitter?
Transmitters with integral indicators will display a key symbol when the Write Protect is enabled. (*See* **Figure 1**)

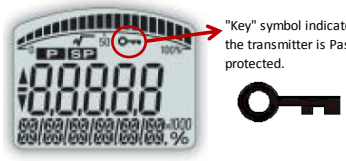
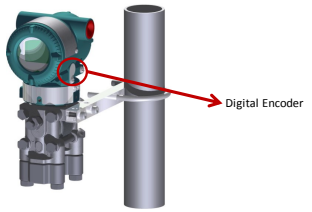


Figure 1: *EJA-E and EJX-A display*

▪ Zero-Adjustment Digital Encoder

The zero-adjustment digital encoder (Standard on all Yokogawa Transmitters), allows for simple adjustments to the LRL and URL. The functionality of this Encoder is un-affected by the Hardware or Software Write Protect settings. Using FieldMate, the technician can disable the Encoder.

There is no indication on the integral display whether this feature is Enabled or Disabled.



FGP 110-04.a

Figure 2: *External Digital Encoder location*

FieldMate™

Hart 5

DTM Works
> Configuration
> Device Information1
EXT SW Enabled / Disabled

Hart 7

DTM Works HART 7
> Detailed Setup
> Device information
> Field Device info
> EXT SW Enabled / Disabled

▪ Settings when Shipped

Hardware Write Protect (Switch)	Enabled (Parameters can be changed)
Software Write Protect (Password)	Disabled (Parameters can be changed)
Zero-adjustment Digital Encoder	Enabled (Encoder is active)

FGP 110-06.a

▪ BRAIN Protocol

The features described in this FieldGuide are also available for EJA-E and EJX-A transmitters with BRAIN Protocol communication. Please refer to the Instruction Manual for details.

https://web-material3.yokogawa.com/2/28456/files/FGP-110%20_06_.pdf

Cyber-security Requirements (CR)

CONTENTS

Trust: Matching OT Device Security Feature Claims

Vendor-Supplied Features (VSF)

- Created by OT device vendors
- Example:

Yokogawa EJA-E Series Field Guide – Write Protection (pages 1-2)

Hardware Write Protection Switch (WR)
The HART communication EJA-E and EJX-A transmitters have a Write Protection (WR) switch located on the CPU Assembly Board next to the Burn Out (BO) switch. When the WR switch is in the "D" (Disabled) position, the transmitter will not allow parameter changes through the use of a handheld communicator, FieldMate, or range setting switch on the transmitter indicator (if equipped). When the WR switch is in the "E" (Enable) position, parameter changes will be allowed.
Software Write Protection (Password)
The EJA-E and EJX-A transmitters with HART communication have a Password that can be set to protect the configured parameters. The Hardware Write Protect switch takes precedence over the Password Protection.
Using FieldMate, the Password function can be Enabled or Disabled. When the Password function is Enabled, a 8-digit password will need to be entered to make any setting changes. This Password can be any 8-digit password the customer wants.
Once the password is set-up, anytime a change needs to be made, the unit will need to be un-locked using the chosen password. When the password is entered, the technician will have 10 minutes to make the changes needed.

Cybersecurity Requirements (CR)

- Created by standards bodies
- Example:

IACS Standard (pages 27-28)

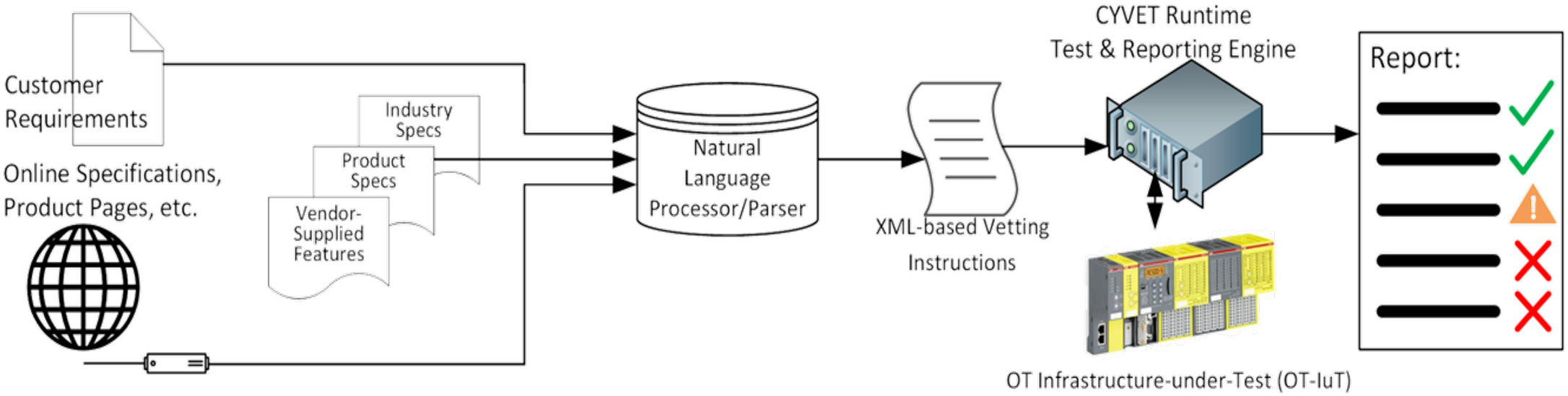
5.7 CR 1.5 – Authenticator management
5.7.1 Requirement
Components shall provide the capability to:

- **(a) Support the use of initial authenticator content;**
- **(b) Support the recognition of changes to default authenticators made at installation time;**
- **(c) Function properly with periodic authenticator change/refresh operation; and**
- **(d) Protect authenticators from unauthorized disclosure and modification when stored, used and transmitted.**

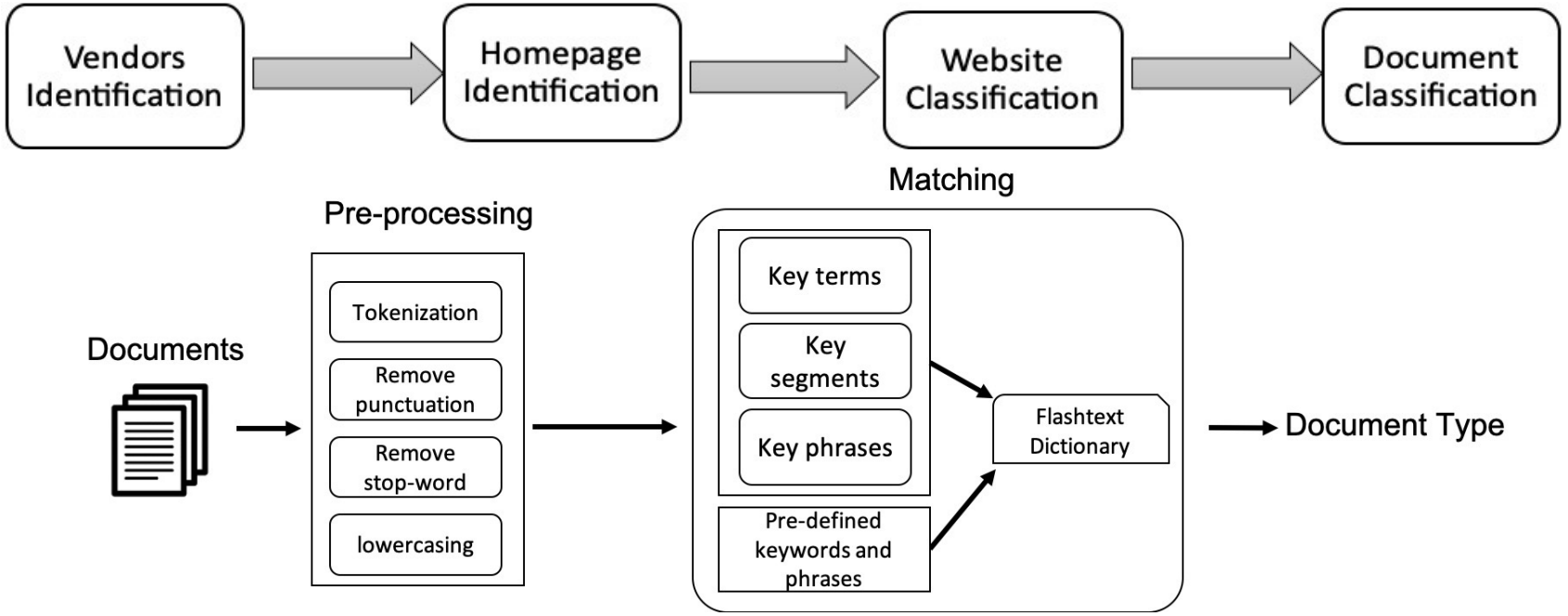
Trust-but-Verify with **CYVET**

Goal: To develop verification and validation (V&V) capabilities to test deployed systems against cybersecurity requirements

- **Verification**: Synthesis and reconciliation of cybersecurity requirements (CR) and vendor supplied features (VSF)
- **Validation**: Generation, execution, and presentation of testing scripts of verified security features
- **Application**: Apply the developed technology capabilities for verification and validation at relevant end-user facilities in the energy sector.



Vendor Device Document Collection & Classification

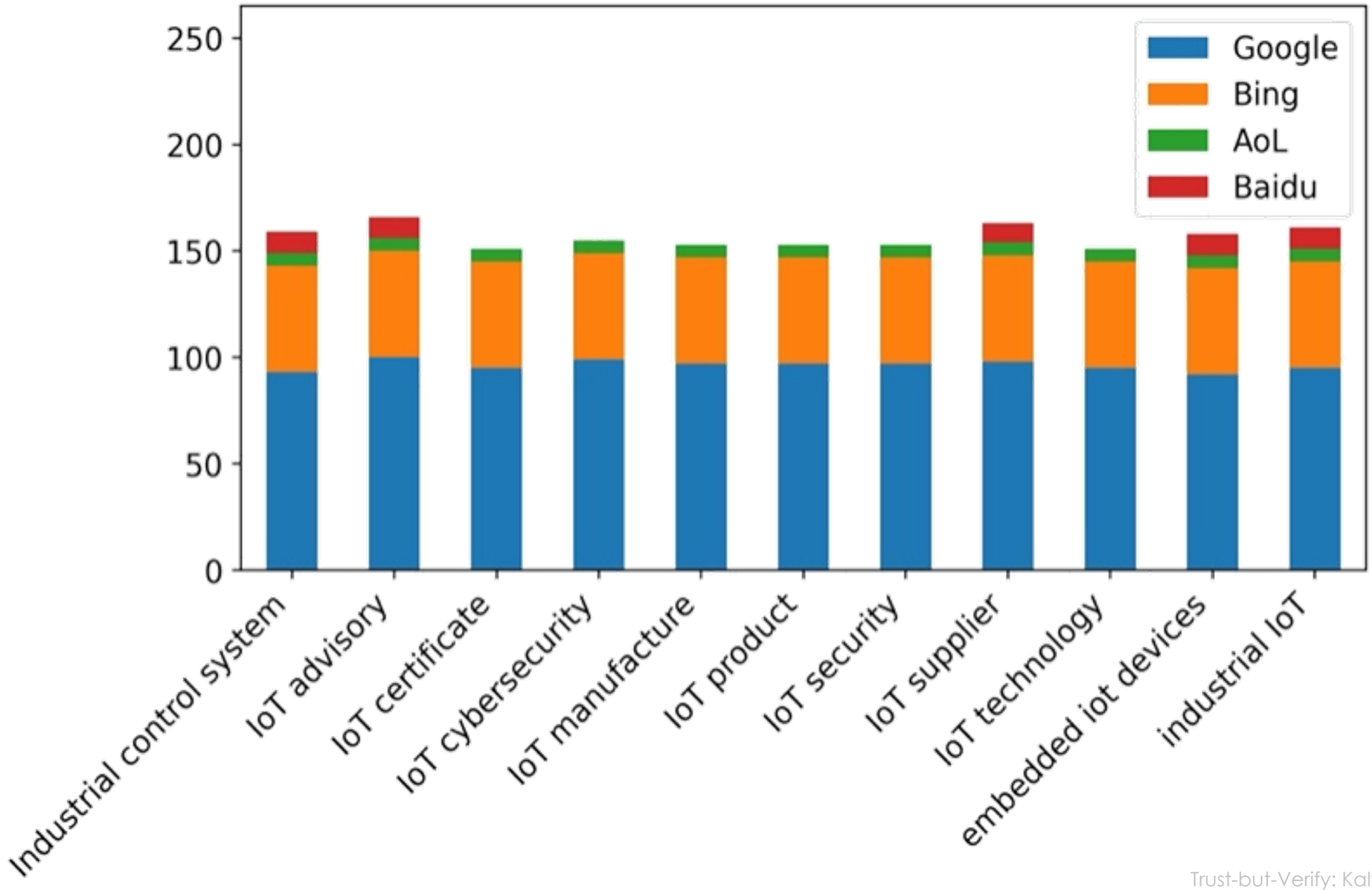


		Precision	Recall	F1-score	Accuracy
Training Phase	ICS vendor sites	0.98	1.00	0.99	0.99
	Non-ICS vendor sites	1.00	0.98	0.99	
Test Phase	ICS vendor sites	0.90	0.90	0.89	0.88
	Non-ICS vendor sites	0.93	0.89	0.90	

Total number of documents	19,793
ICS product-related documents	12,581
Manuals	2248
Brochures	9326
Catalogs	1007
Non-product-related documents	7,212

Vendor Identification Results

Number of matches for 11 keywords, by search engine



OAK RIDGE National Laboratory

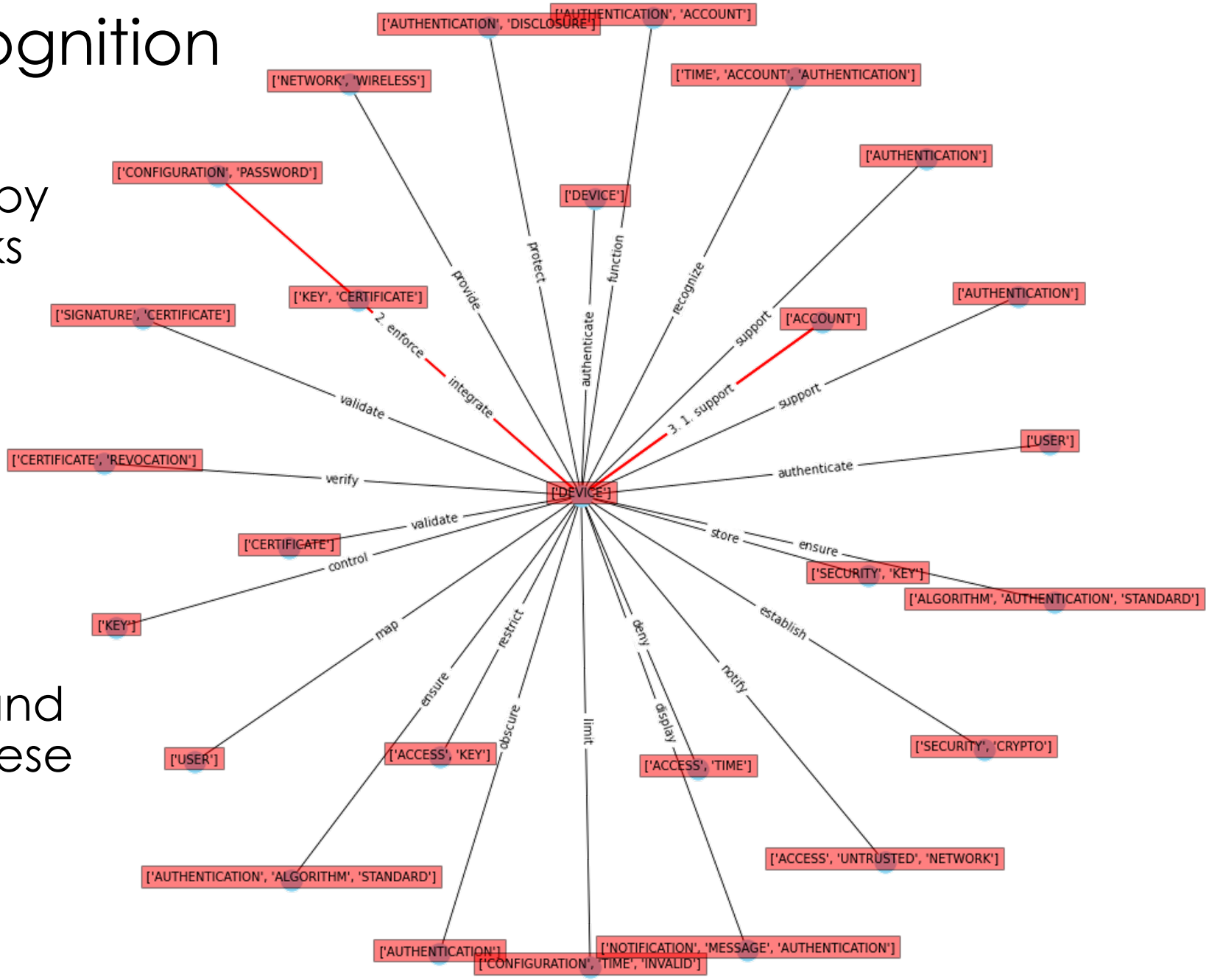
CR and VSF sentences with Simplified Structures for Natural Language Processing (NLP)

	original_sentence	simplified_sentence	subject_pattern_chopped	verb_pattern_chopped	object_pattern_chopped
0	Components shall provide the capability to identify and authenticate all human users according t...	Components shall authenticate human users.	Components shall	authenticate	human users.
1	Components shall provide the capability to identify itself and authenticate to any other compone...	Components shall authenticate to other components.	Components shall	authenticate	to other components.
2	Components shall provide the capability to support the management of all accounts directly or in...	Components shall support the management of accounts.	Components shall	support	the management of accounts.
3	Components shall provide the capability to integrate into a system that supports the management ...	Components shall support the management of identifiers.	Components shall	support	the management of identifiers.
4	support the use of initial authenticator content.	Components shall support initial authentication.	Components shall	support	initial authentication.
5	support the recognition of changes to default authenticators made at installation time.	Components shall recognize at instalation time changes to default authenticators.	Components shall	recognize	at instalation time changes to default authenticators.
6	function properly with periodic authenticator change/refresh operation.	Components shall function with periodic authentication changes.	Components shall	function	with periodic authentication changes.
7	protect authenticators from unauthorized disclosure and modification when stored, used and trans...	Components shall protect authenticators from anauthorized disclosure.	Components shall	protect	authenticators from anauthorized disclosure.
8	The wireless access management requirements are network-component-specific and can be located as...	Components shall provide network-specific wireless requirements.	Components shall	provide	network-specific wireless requirements.
9	For components that utilize password-based authentication, those components shall provide or int...	Components shall enforce configurable password strength.	Components shall	enforce	configurable password strength.

Named Entity Recognition

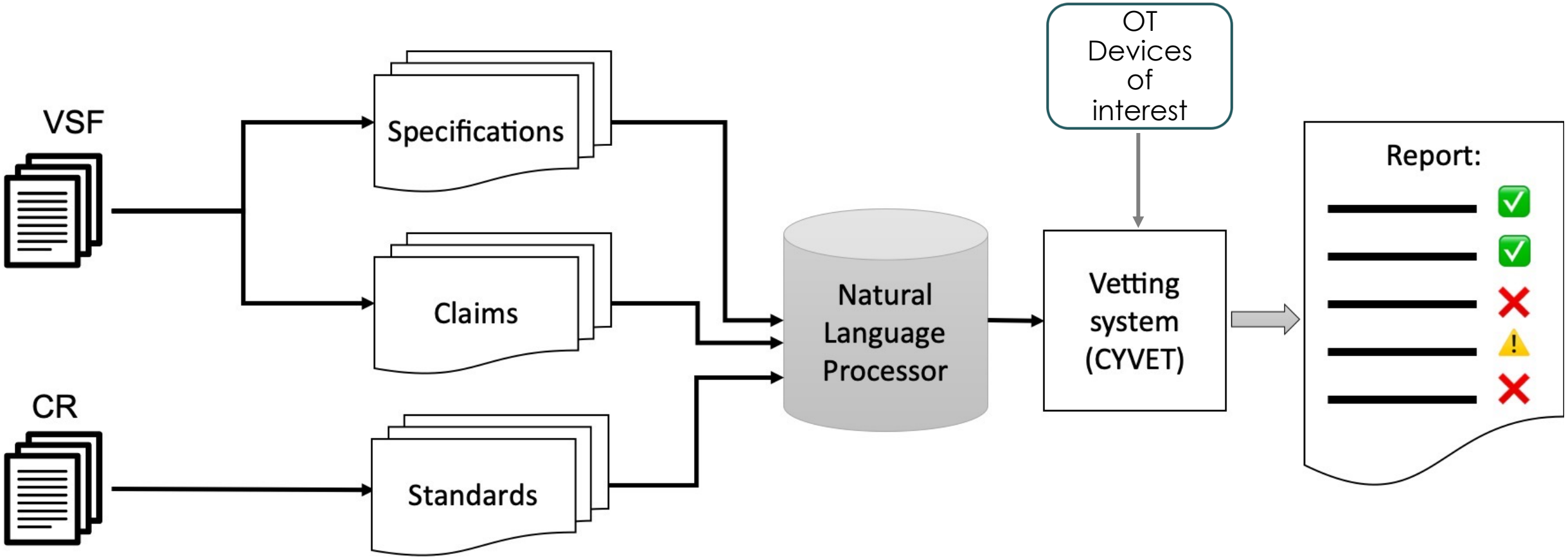
- Concepts are defined by subject-verb-object links

- Sentences across VSF and CR are matched via these conceptual matches



OAK RIDGE National Laboratory

CYVET Verification: Putting it all together

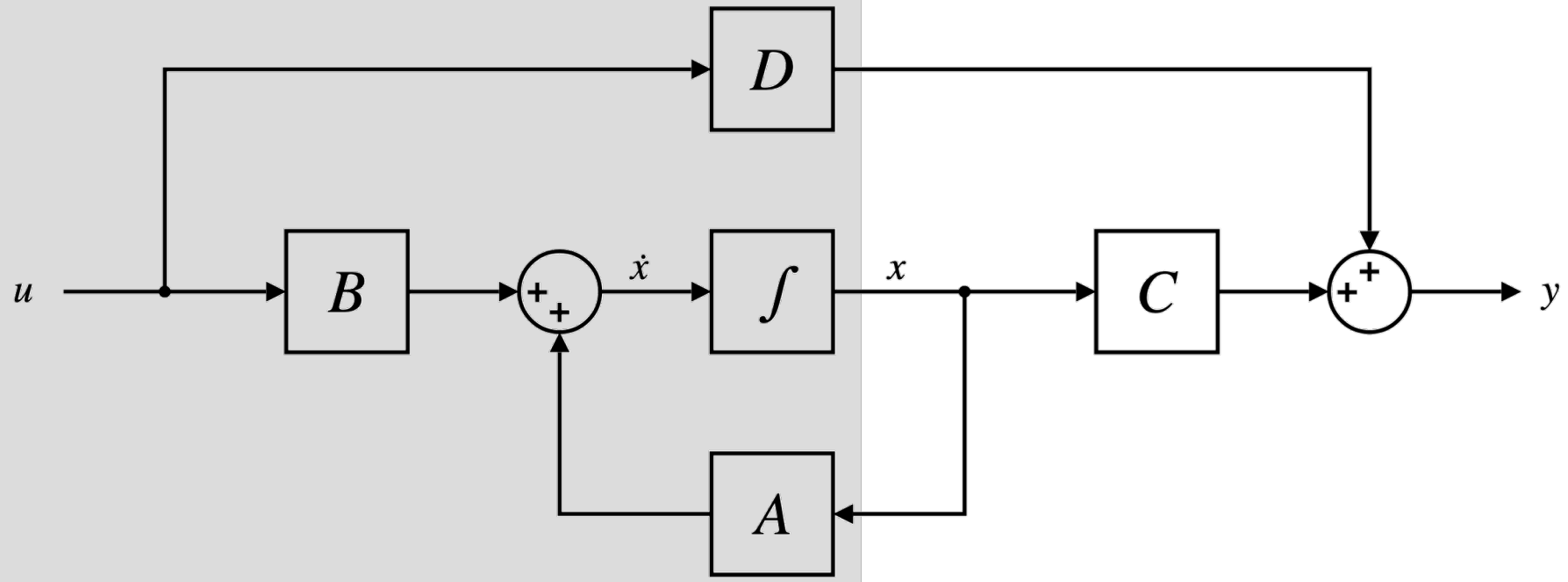


- K. Perumalla, J. Lopez, M. Alam, O. Kotevska, M. Hempel, and H. Sharif, "A Novel Vetting Approach to Cybersecurity Verification in Energy Grid Systems" IEEE Kansas Power and Energy Conference (KPEC)
- K.Ameri, H.Sharif, J.Lopez, and K.Perumalla, "Smart Semi-Supervised Accumulation of Large Repositories for ICS Device Information" Intl Conference on Cyber Warfare and Security (ICCWS)

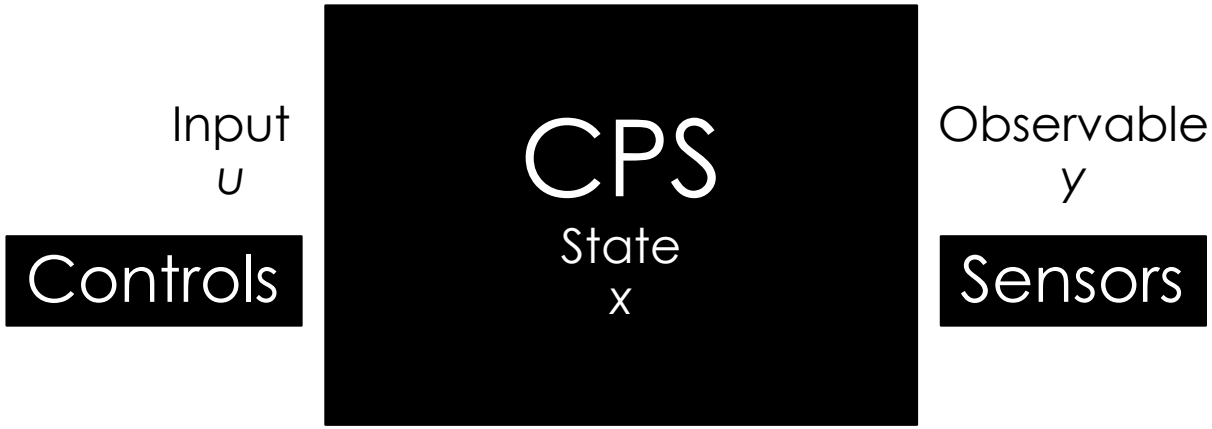
Question #3: How well is it doing?

DT

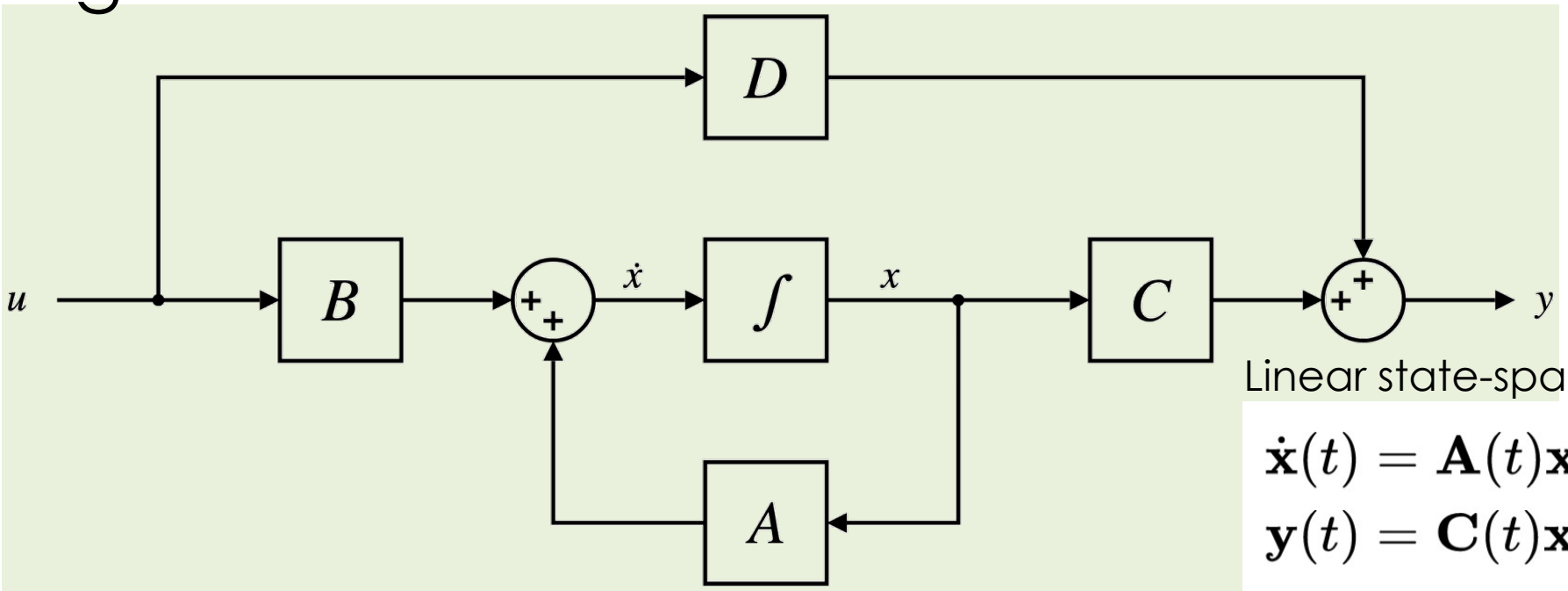
Digital Twins for Dynamic Monitoring for Trust-but-Verify



Trust-but-Verify Dynamically with Online Digital Twins



Digital Twin



Linear state-space representation

$$\dot{\mathbf{x}}(t) = \mathbf{A}(t)\mathbf{x}(t) + \mathbf{B}(t)\mathbf{u}(t)$$
$$\mathbf{y}(t) = \mathbf{C}(t)\mathbf{x}(t) + \mathbf{D}(t)\mathbf{u}(t)$$

Summary

- OT is clearly gaining increasing degree of attention
- Overall business value is a key metric guiding Trust and security
- **Trust-but-Verify** appears to be a good paradigm forward
  - Accommodates legacy
  - Operator or asset owner adoption
  - Business value
  - Increasing complexity

OAK RIDGE National Laboratory

Thank you

Q&A

Kalyan Perumalla, Ph.D.

Distinguished R&D Staff, **Oak Ridge National Lab**

perumallaks@ornl.gov | 865-241-1315

www.ornl.gov/staff-profile/kalyan-s-perumalla