By the Numbers: Towards Standard Evaluation Metrics for Programmable Logic Controllers' Defenses

Efrén López-Morales, Jacob Hopkins,
Alvaro Cardenas, Ali Abbasi, and Carlos Rubio-Medrano

2nd International Workshop on Re-design Industrial Control Systems with Security (RICSS)

October 14th, 2024


DARKREADING
NEWSLETTER SIGN-UP
Cybersecurity Topics
World
The Edge
DR Technology
Events
Resources
Improved, Stuxnet-Like PLC Malware Aims to Disrupt Critical Infrastructure
A newly developed PLC malware does not require physical access to target an ICS environment, is mostly platform neutral, and is more resilient than traditional malware aimed at critical infrastructure.

DARKREADING

NEWSLETTER SIGN-UP

Cybersecurity Topics | World | The Edge | DR Technology | Events | Resources

Improved, Stuxnet-Like PLC Malware Aims to Disrupt Critical Infrastructure

A newly developed PLC malware does not require physical access to target an ICS environment, is mostly platform neutral, and is more resilient than traditional malware aimed at critical infrastructure.

‘Crash Override’: The Malware That Took Down a Power Grid

In Ukraine, researchers have found the first real-world malware that attacks physical infrastructure since Stuxnet.

DARKREADING

NEWSLETTER SIGN-UP

Cybersecurity Topics | World | The Edge | DR Technology | Events | Resources

Improved, Stuxnet-Like PLC Malware Aims to Disrupt Critical Infrastructure

A newly developed PLC malware does not require physical access to target an ICS environment, is mostly platform neutral, and is more resilient than traditional malware aimed at critical infrastructure.

‘Crash Override’: The Malware That Took Down a Power Grid

In Ukraine, researchers have found the first real-world malware that attacks physical infrastructure since Stuxnet.

Feds Uncover a ‘Swiss Army Knife’ for Hacking Industrial Control Systems

The malware toolkit, known as Pipedream, is perhaps the most versatile tool ever made to target critical infrastructure like power grids and oil refineries.

Background

Programmable Logic Controllers (PLC)

Programmable Logic Controllers (PLC)

- Control physical industrial equipment, e.g., pumps.

Programmable Logic Controllers (PLC)

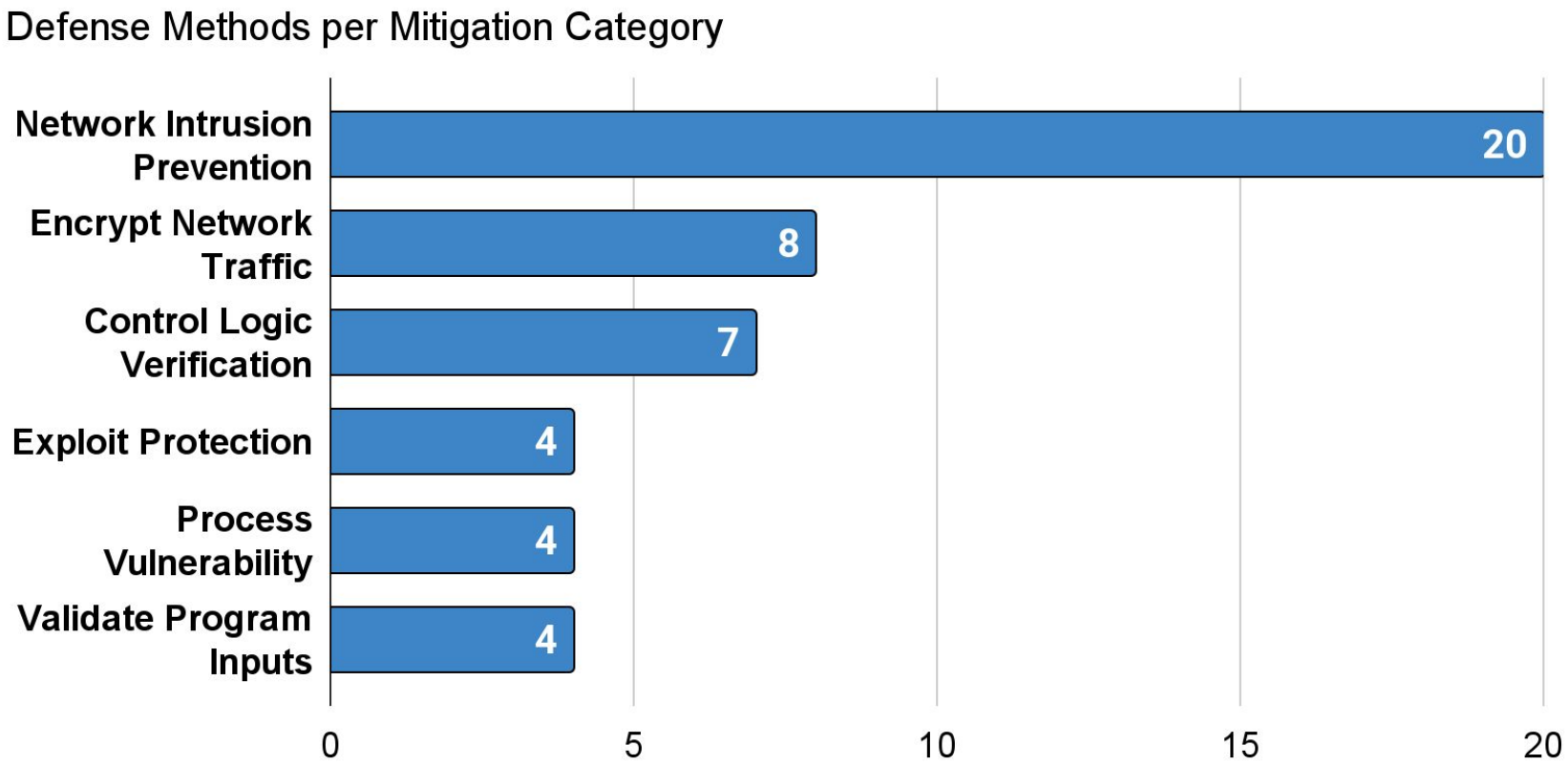
- Control physical industrial equipment, e.g., pumps.
- Varied software and hardware architectures.

Programmable Logic Controllers (PLC)

- Control physical industrial equipment, e.g., pumps.
- Varied software and hardware architectures.
- Increasingly interconnected, e.g., cloud.

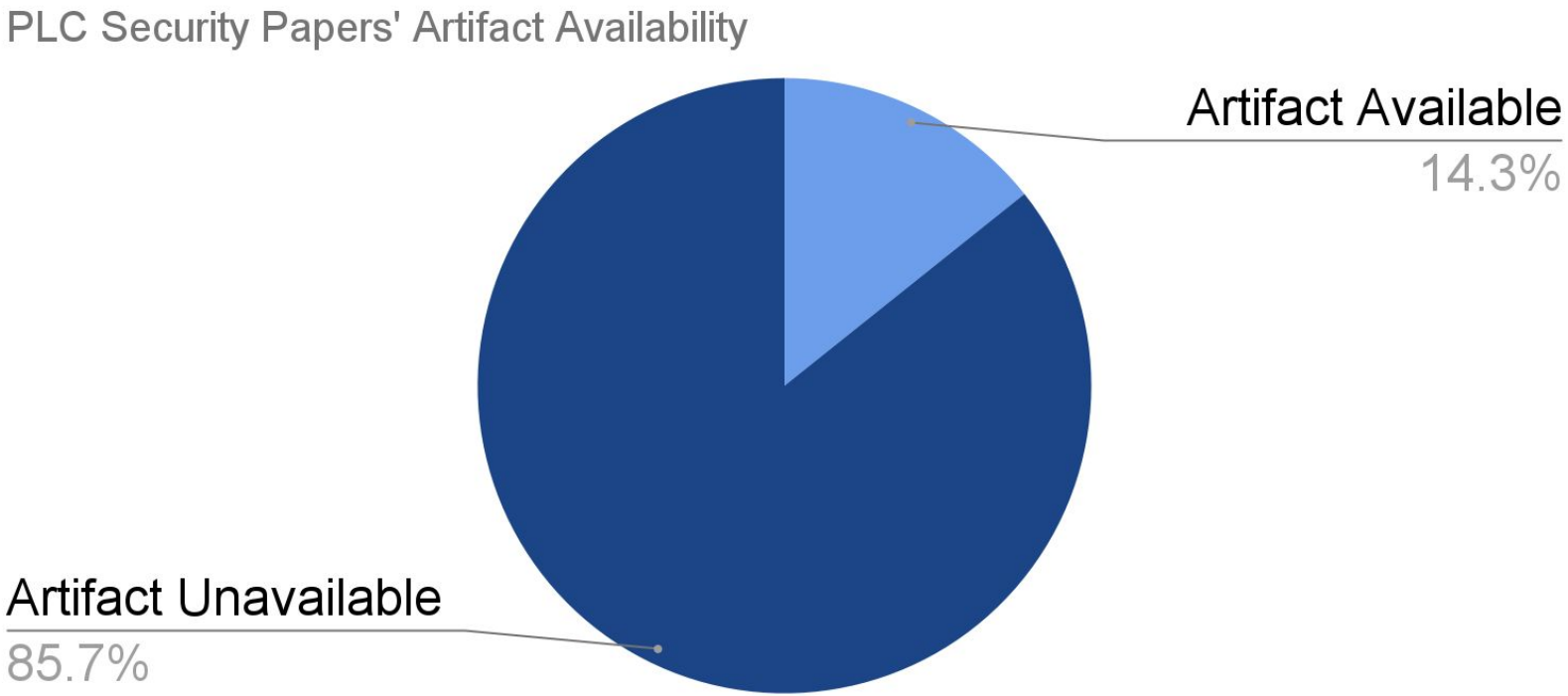
Programmable Logic Controllers (PLC)

- Control physical industrial equipment, e.g., pumps.
- Varied software and hardware architectures.
- Increasingly interconnected, e.g., cloud.
- Yet, little to no built-in security features.

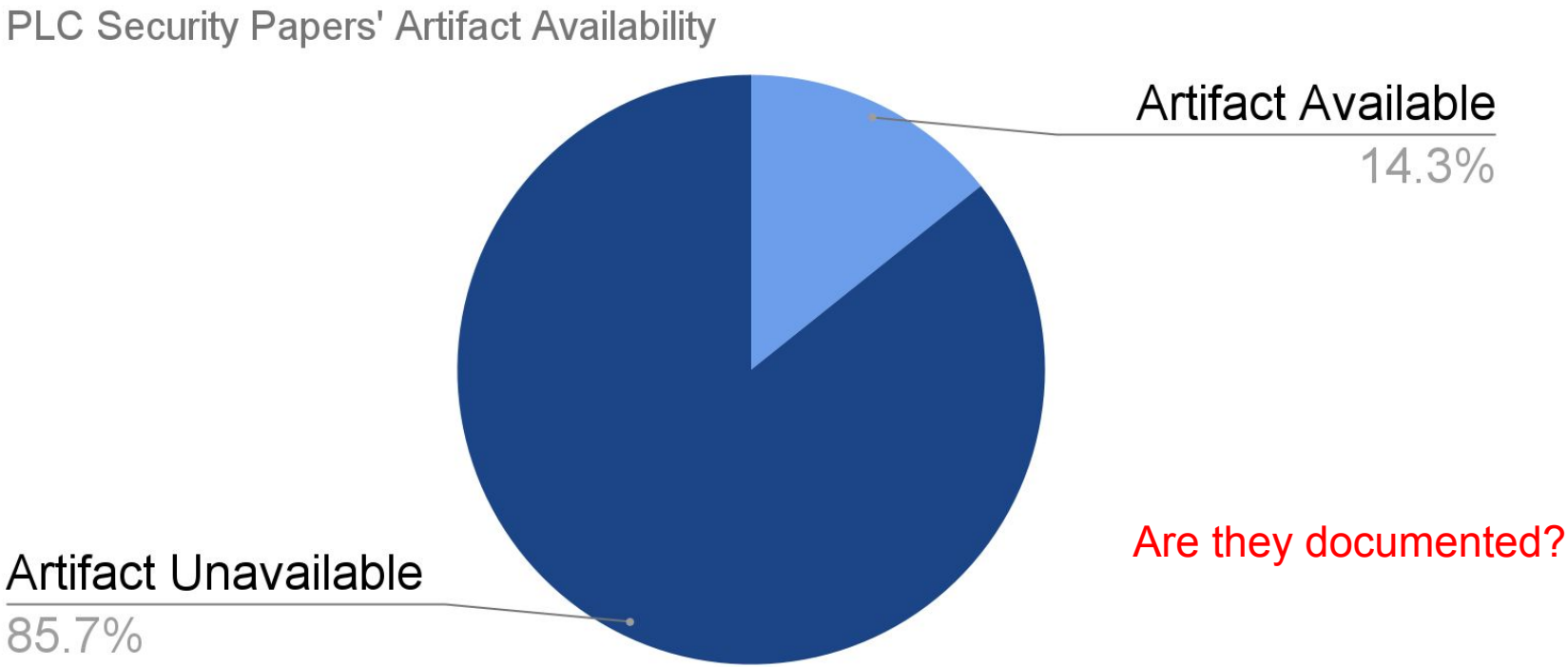


López-Morales, E., Planta, U., Rubio-Medrano, C., Abbasi, A., & Cardenas, A. A. (2024). SoK: Security of Programmable Logic Controllers. 33rd USENIX Security Symposium.

Cockburn, A., Dragicevic, P., Besançon, L., & Gutwin, C. (2020). Threats of a replication crisis in empirical computer science. *Communications of the ACM*, *63*(8), 70-79.

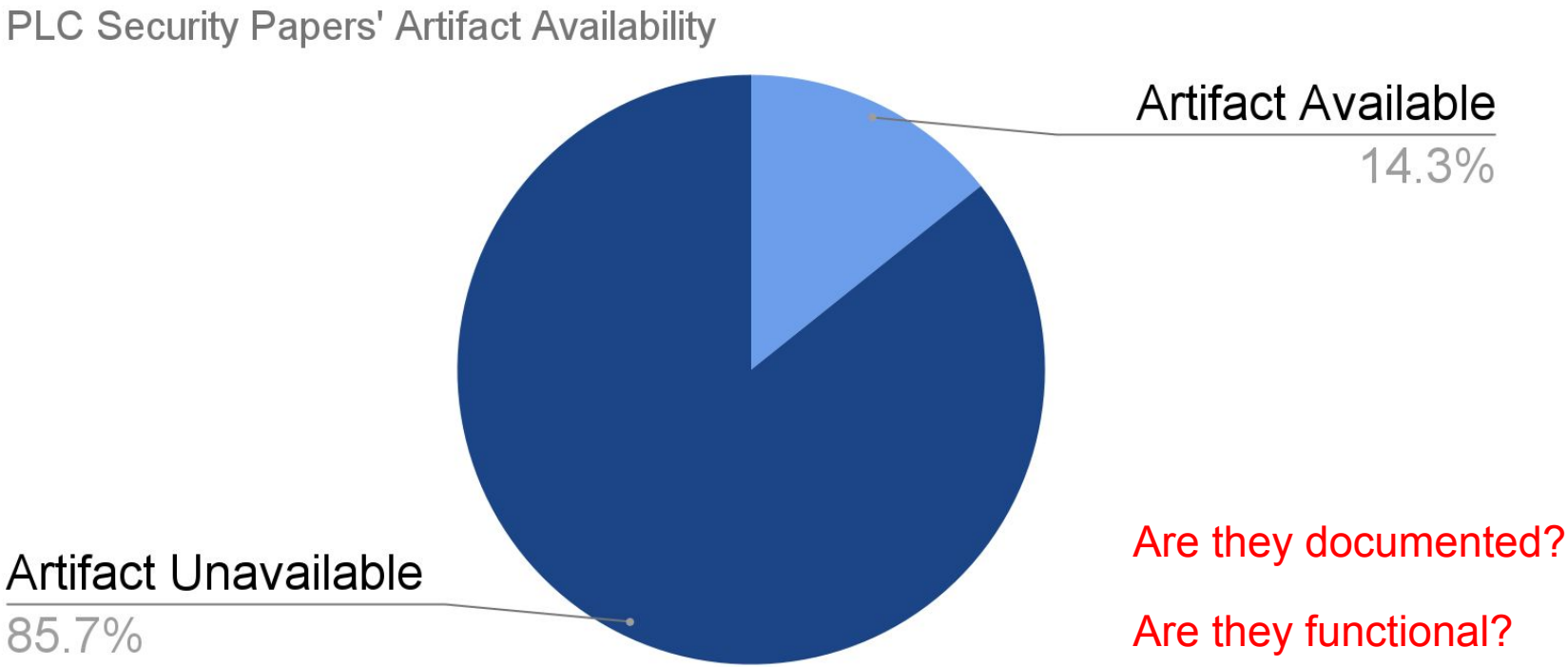


López-Morales, E., Planta, U., Rubio-Medrano, C., Abbasi, A., & Cardenas, A. A. (2024). SoK: Security of Programmable Logic Controllers. 33rd USENIX Security Symposium.



Are they documented?

López-Morales, E., Planta, U., Rubio-Medrano, C., Abbasi, A., & Cardenas, A. A. (2024). SoK: Security of Programmable Logic Controllers. 33rd USENIX Security Symposium.



Are they documented?

Are they functional?

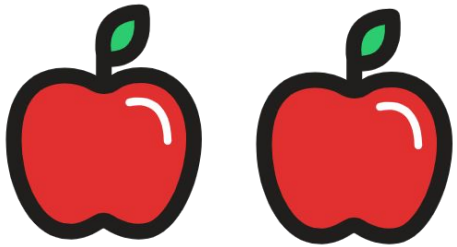
López-Morales, E., Planta, U., Rubio-Medrano, C., Abbasi, A., & Cardenas, A. A. (2024). SoK: Security of Programmable Logic Controllers. 33rd USENIX Security Symposium.

Is there an **alternative** to research artifacts to **improve** PLC security research **reproducibility**?

Evaluation Metrics

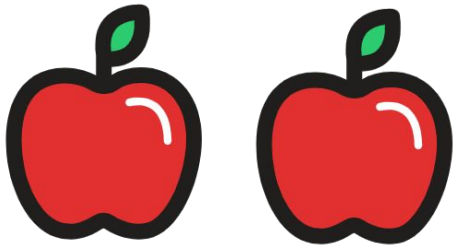
Evaluation Metrics

- Provide the **standards** by which different algorithms, systems, or artifacts are **compared**.



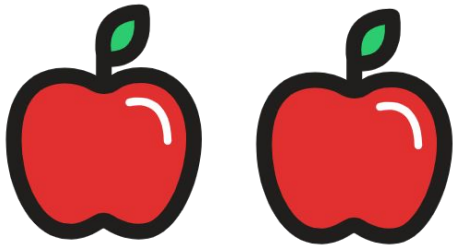
Evaluation Metrics

- Provide the **standards** by which different algorithms, systems, or artifacts are **compared**.
- Provide **quantitative** measures to assess the **performance** of the artifact.



Evaluation Metrics

- Provide the **standards** by which different algorithms, systems, or artifacts are **compared**.
- Provide **quantitative** measures to assess the **performance** of the artifact.
- Do not require access to artifacts.



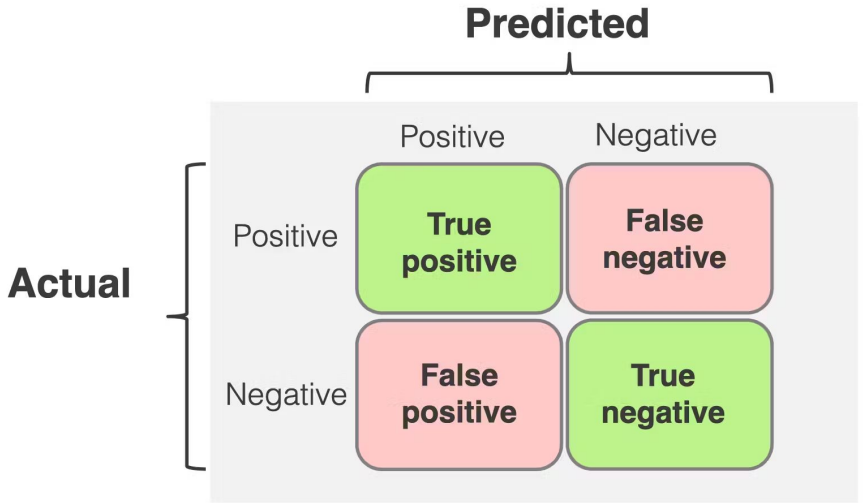
Existing Evaluation Metrics for PLCs

Overhead

Existing Evaluation Metrics for PLCs

Overhead

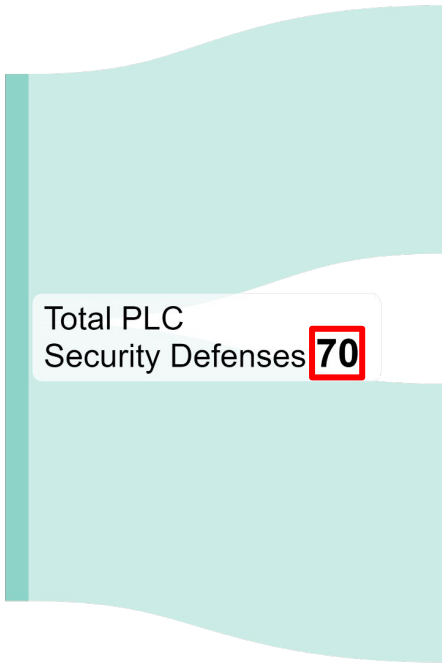
Effectiveness



Existing Evaluation Metrics for PLCs

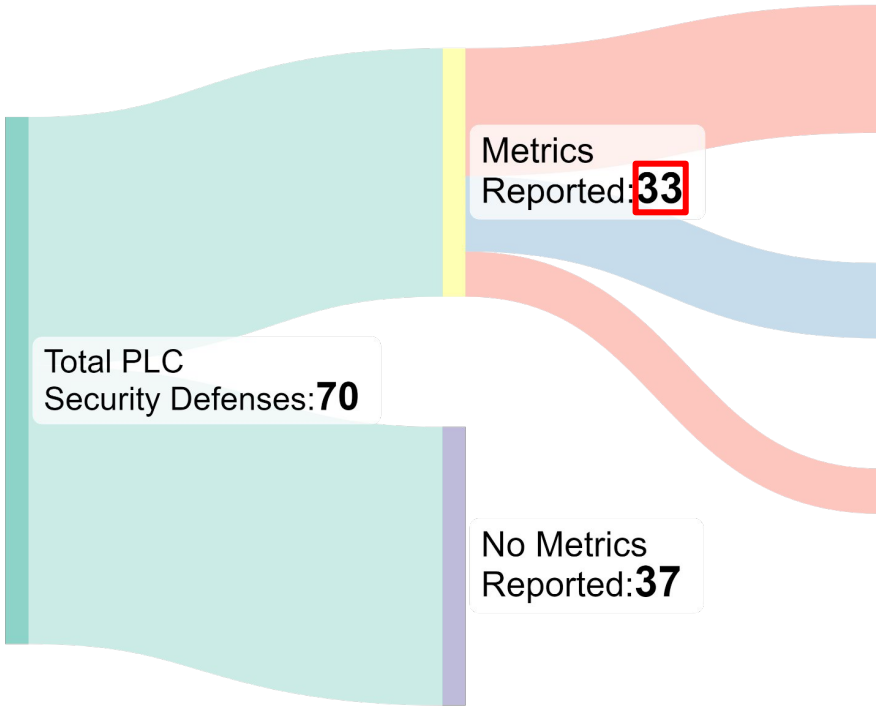
No security metrics

PLC Defenses Reported Metrics (2007-2023)



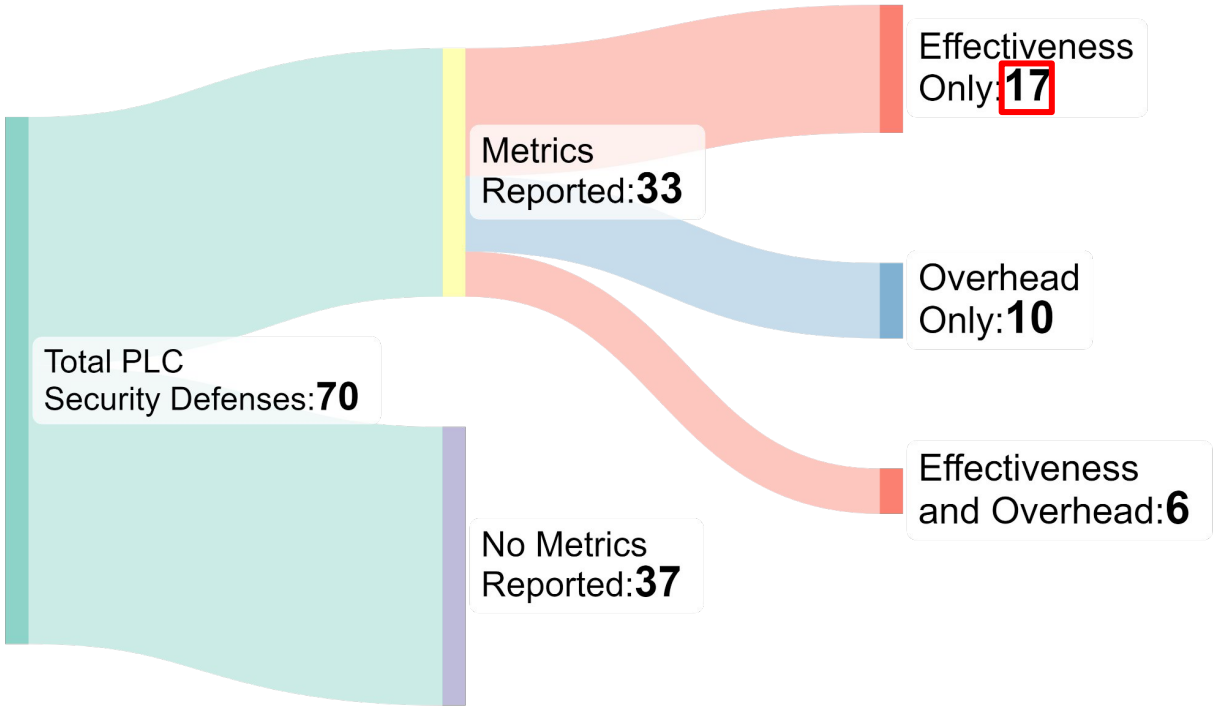
López-Morales, E., Planta, U., Rubio-Medrano, C., Abbasi, A., & Cardenas, A. A. (2024). SoK: Security of Programmable Logic Controllers. 33rd USENIX Security Symposium.

PLC Defenses Reported Metrics (2007-2023)



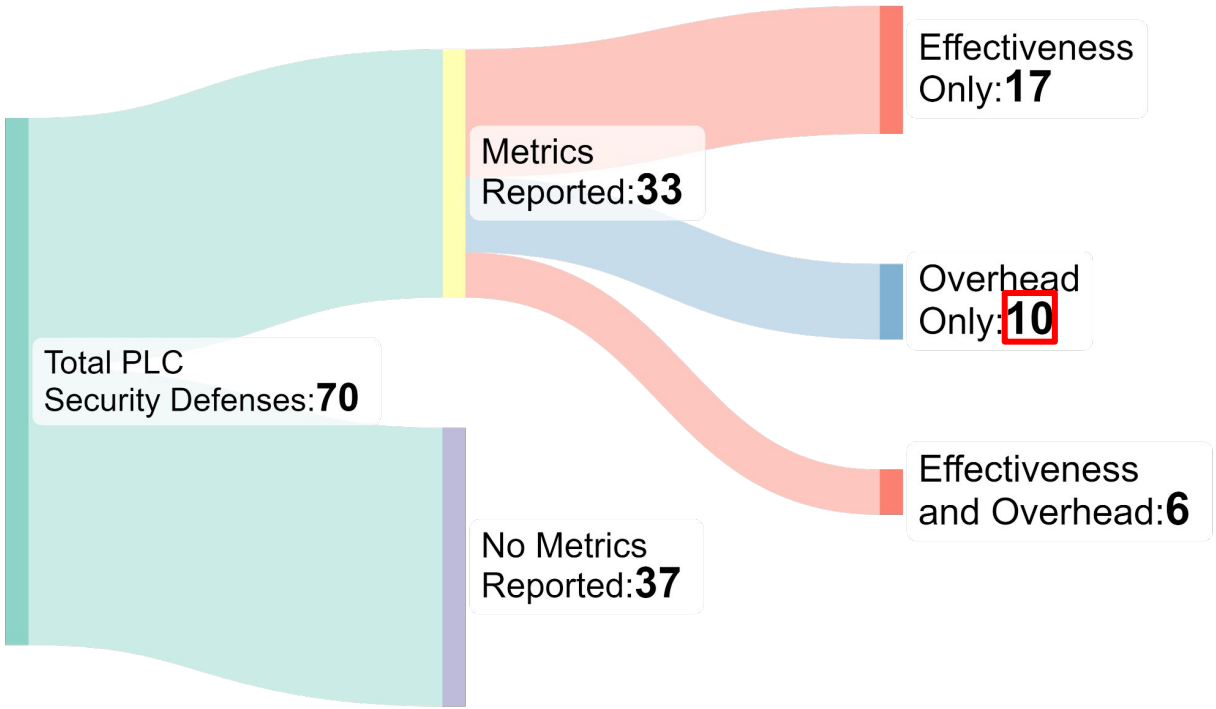
López-Morales, E., Planta, U., Rubio-Medrano, C., Abbasi, A., & Cardenas, A. A. (2024). SoK: Security of Programmable Logic Controllers. 33rd USENIX Security Symposium.

PLC Defenses Reported Metrics (2007-2023)



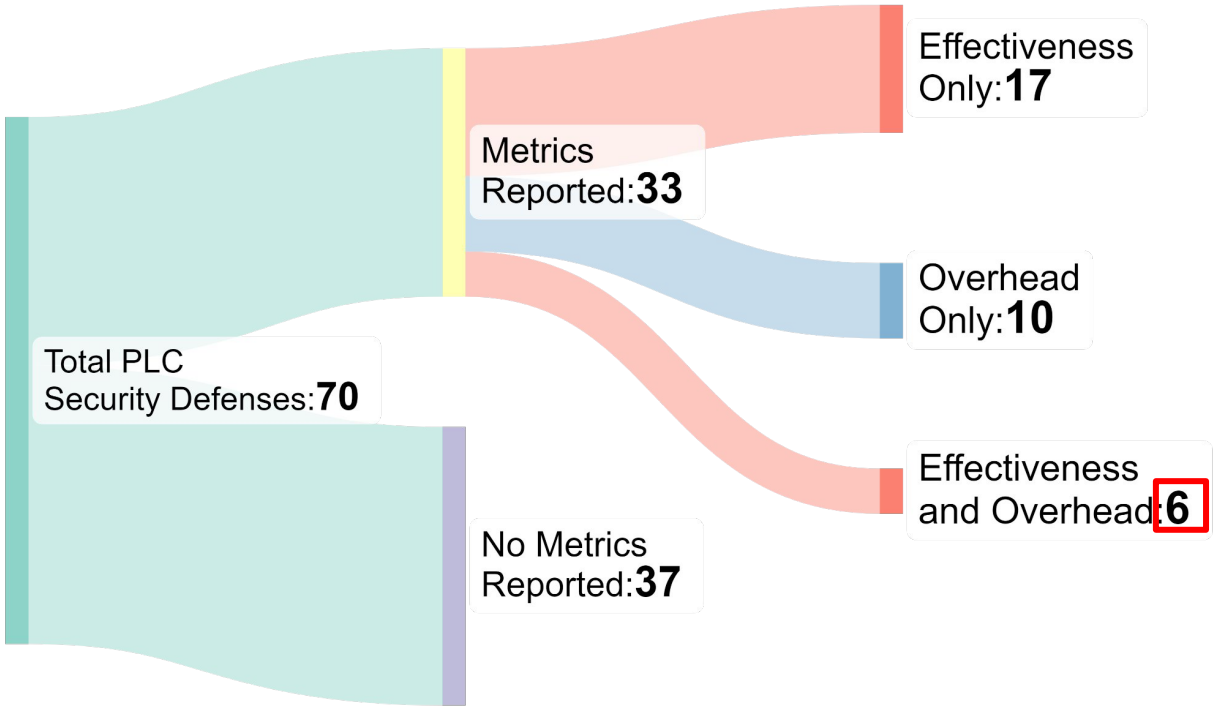
López-Morales, E., Planta, U., Rubio-Medrano, C., Abbasi, A., & Cardenas, A. A. (2024). SoK: Security of Programmable Logic Controllers. 33rd USENIX Security Symposium.

PLC Defenses Reported Metrics (2007-2023)



López-Morales, E., Planta, U., Rubio-Medrano, C., Abbasi, A., & Cardenas, A. A. (2024). SoK: Security of Programmable Logic Controllers. 33rd USENIX Security Symposium.

PLC Defenses Reported Metrics (2007-2023)



López-Morales, E., Planta, U., Rubio-Medrano, C., Abbasi, A., & Cardenas, A. A. (2024). SoK: Security of Programmable Logic Controllers. 33rd USENIX Security Symposium.

Main Problem:

Metrics are not being reported and are not standardized

Our contribution:

Set of Standard Evaluation Metrics for PLC Defenses

Research Questions

1. What are the key evaluation metrics for PLC Defenses?

Research Questions

1. What are the key evaluation metrics for PLC Defenses?

2. What are the challenges in obtaining these evaluation metrics?

Research Questions

1. What are the key evaluation metrics for PLC Defenses?

2. What are the challenges in obtaining these evaluation metrics?

3. How can these challenges be addressed?

How did we select our standard metrics?

Multiple PLC Architectures

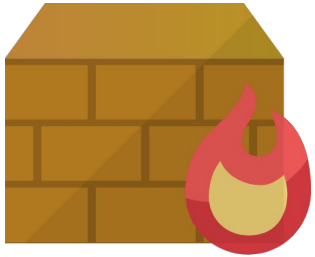
CODESYS

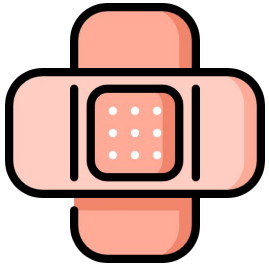
How did we select our standard metrics?

Multiple PLC Architectures

CODESYS

Multiple PLC Defenses



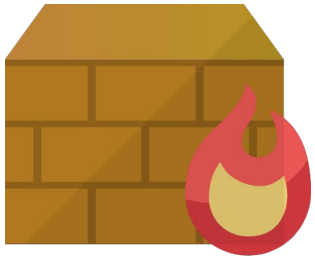


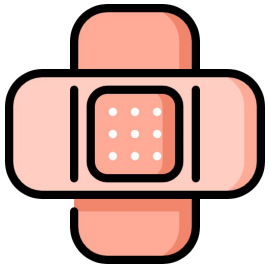
How did we select our standard metrics?

Multiple PLC Architectures

CODESYS

Multiple PLC Defenses





Straightforward

Our Standard Evaluation Metrics

Overhead

Our Standard Evaluation Metrics

Overhead

Security

Our Standard Evaluation Metrics

Overhead

Security

Effectiveness

Our Standard Evaluation Metrics: Overhead

Metric	Unit
Scan Cycle	milliseconds (ms)
Total Runtime Cycles	milliseconds (ms)
CPU Cycles	milliseconds (ms)
Total RAM Usage	Kilobytes (KiB)

Our Standard Evaluation Metrics: Security

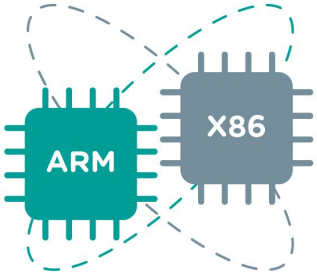
Metric	Unit
ROP Gadgets	Integer
Memory Region Ratio (MRR)	Kilobytes (KiB)
Privileged Cycles	milliseconds (ms)

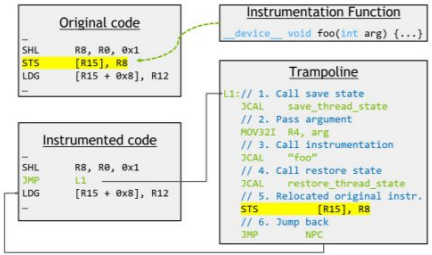
Our Standard Evaluation Metrics: Effectiveness

Metric	Unit
True Positive	Integer
True Negative	Integer
False Positive	Integer
False Negative	Integer
Accuracy	Float

What are the challenges obtaining our evaluation metrics?

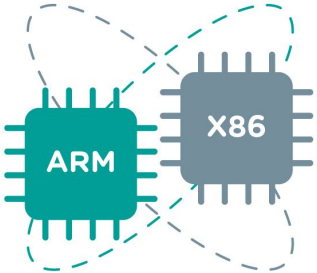
No standard benchmarking tool

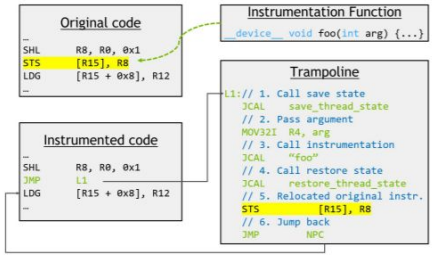




What are the challenges obtaining our evaluation metrics?

No standard benchmarking tool





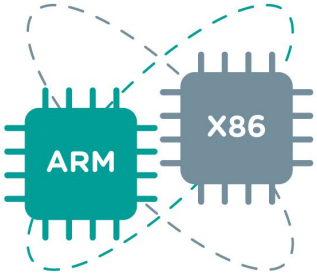
Proprietary Software and Hardware

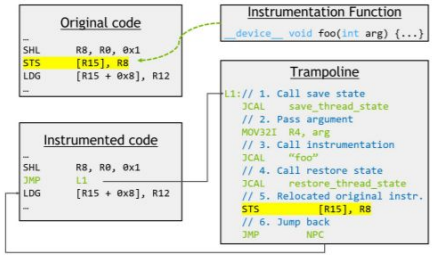
SIEMENS

Rockwell Automation

What are the challenges obtaining our evaluation metrics?

No standard benchmarking tool





Proprietary Software and Hardware

SIEMENS

Rockwell Automation

Different Environmental Conditions

Recommendation 1: Leverage existing tools

Benchmarking

Recommendation 1: Leverage existing tools

Benchmarking

arm Developer

OPENPLC

TO A MORE
OPEN FUTURE

Profiling

SIMATIC Controller
Profiling

TIA Portal

CODESYS Profiler

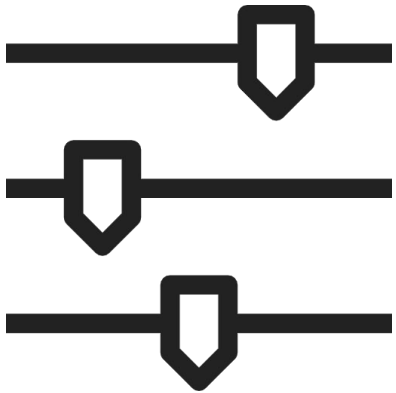
The CODESYS Profiler enables
level.
The CODESYS Profiler is part of

Aktuelle Version: 2.2.0.0
Article no.: 2101000004

Download

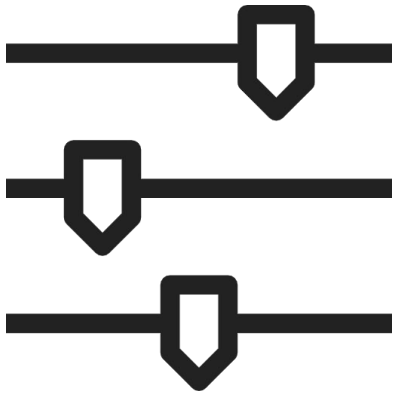
Recommendation 2: Normalize Environment Configuration

Track configuration

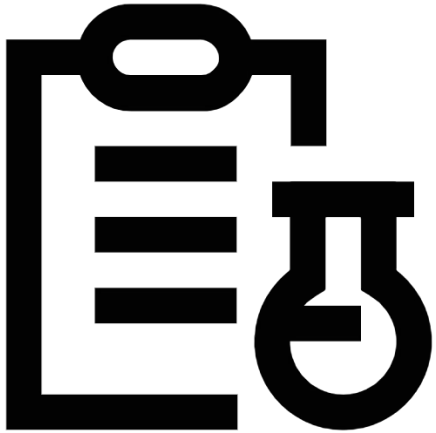


Recommendation 2: Normalize Environment Configuration

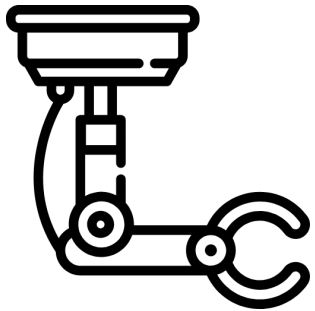
Track configuration



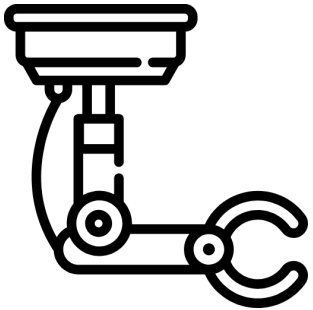
Report in paper



Recommendation 3: Worst-Case Execution Time (WCET)



Recommendation 3: Worst-Case Execution Time (WCET)



WCET over Average

Future Work

- Develop a PLC defenses **benchmark framework**.

Future Work

- Develop a PLC defenses **benchmark framework**.
  - How to **automate** it?

Future Work

- Develop a PLC defenses **benchmark framework**.
  - How to **automate** it?
  - How many **sub-benchmarks** will such a framework require?

Future Work

- Develop a PLC defenses **benchmark framework**.
  - How to **automate** it?
  - How many **sub-benchmarks** will such a framework require?
  - What **PLCs** will be **supported**?

Conclusion

- We provided evidence to show that **current evaluation metrics are lacking.**

Conclusion

- We provided evidence to show that **current evaluation metrics are lacking.**
- We proposed a **set of standard evaluation metrics**.

Conclusion

- We provided evidence to show that **current evaluation metrics are lacking.**
- We proposed a **set of standard evaluation metrics**.
- We **provided recommendations** on how to measure and report these metrics.

Conclusion

- We provided evidence to show that **current evaluation metrics are lacking.**
- We proposed a **set of standard evaluation metrics**.
- We **provided recommendations** on how to measure and report these metrics.
- We hope this work will **serve as a starting point** to improve the current state of evaluation metrics for PLC security.

Thank you!

Efrén López-Morales
efrenlopez.org
@efren_lopezm

TEXAS A&M UNIVERSITY
CORPUS CHRISTI