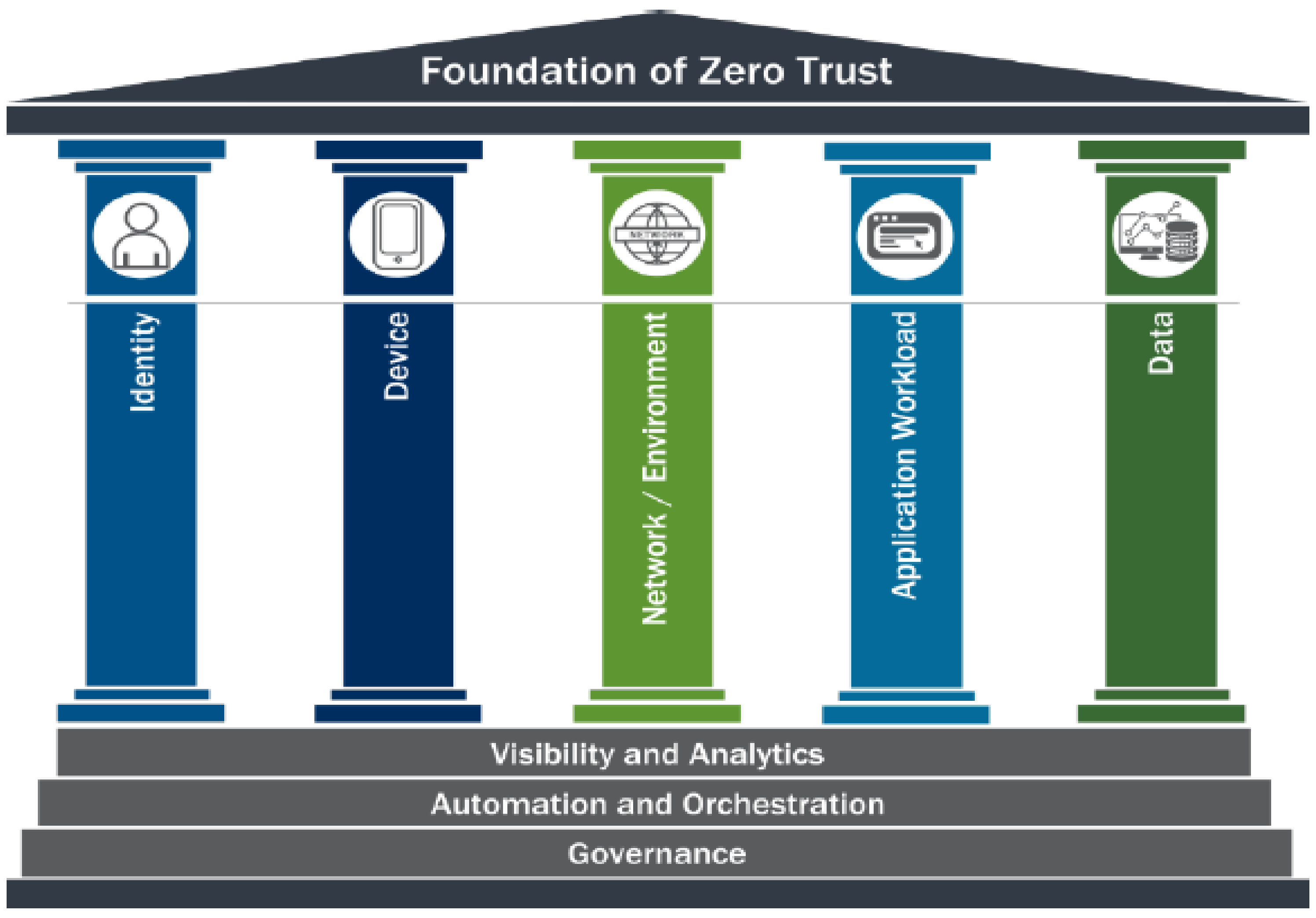
Zero Inherent Trust for Industrial Internet of Things

Summer 2022

Test beds, Data Analysis, & Everything in Between

Abstract

New-age industrial architectures for systems and processes require new-age security solutions. While advancements have been made in maintaining networks without inherently trusting agents, zero-trust architectures have yet to permeate industrial internet of things (IIoT) devices.

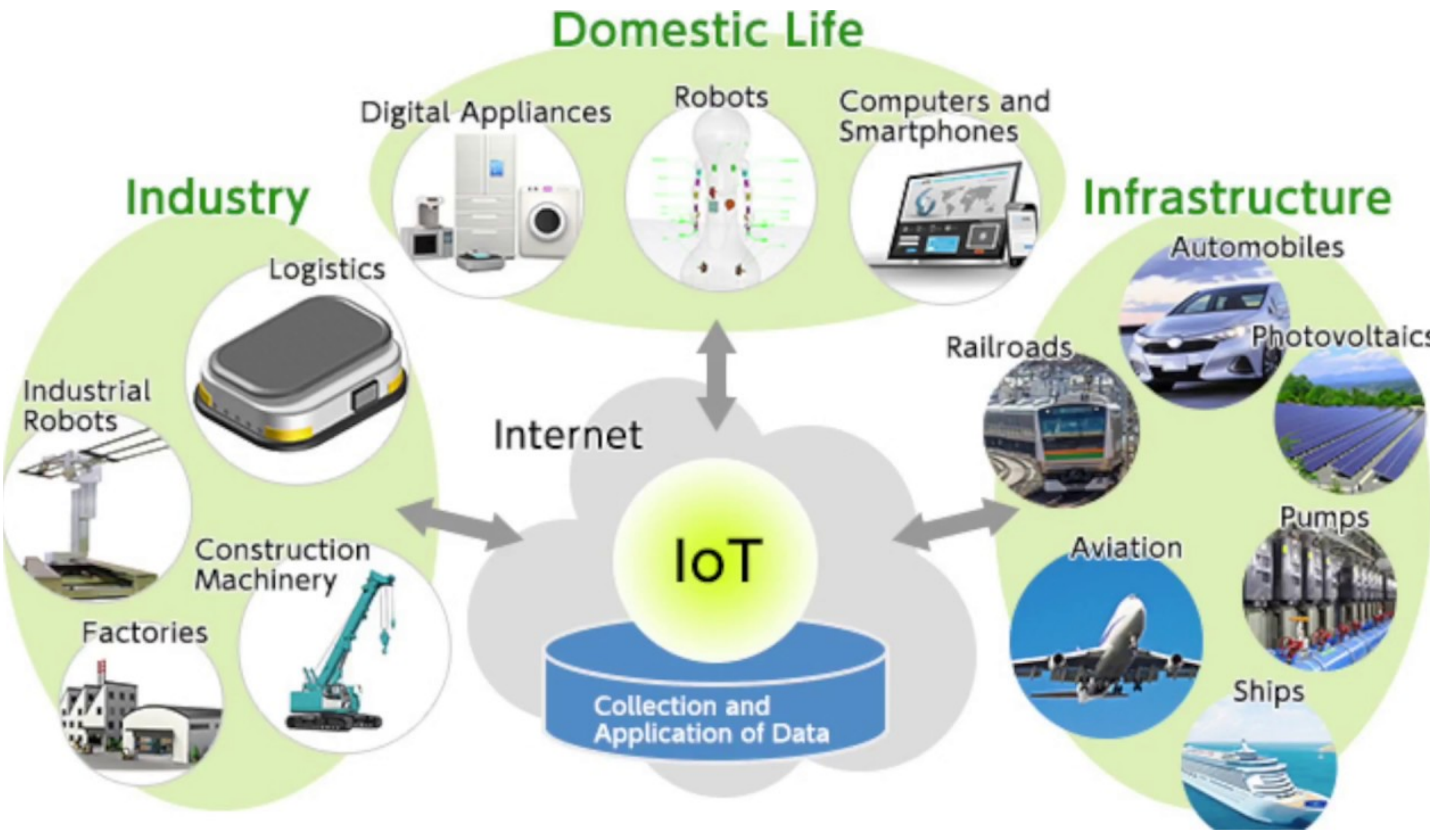


[1]

Methods

This project entails:

- Building a test bed from low-cost IIoT devices with various processes
- Codifying system characteristics
- Creating trust metrics based on resilience and system measures
- Visualizing large amounts of data and making descriptive evidence-based system security determinations



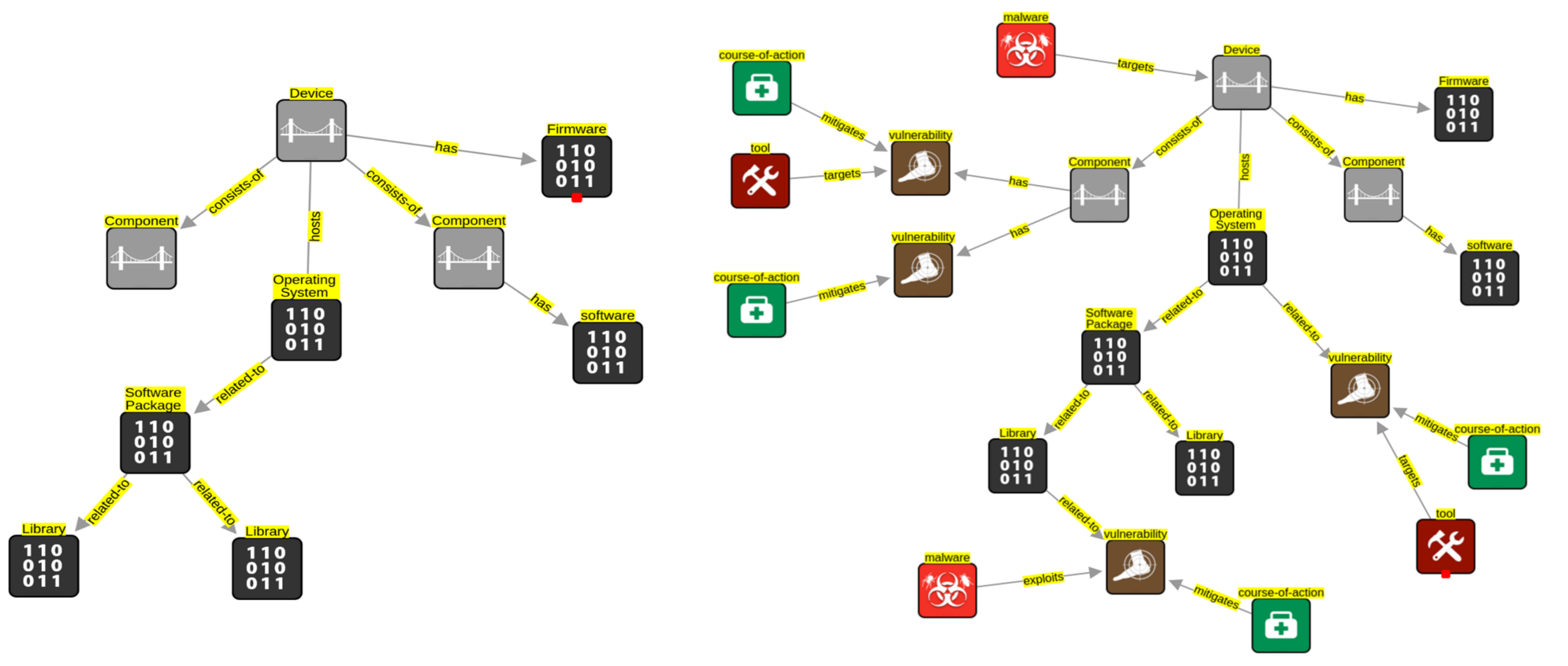
[2]

Preliminary Results

Results are backed by Idaho National Laboratory research including:

- Codified attack surfaces
- Firmware analysis at scale
- Data analysis tool sets

Research will build on various projects. A Wyoming student will therefore draw on a breadth of knowledge to fuel their research while controlling how their work will augment this three-year project.



[3]

Challenges & Future Work

We are looking for a senior looking to master in cybersecurity. This is a funded project giving the opportunity to explore zero-trust IIoT systems while partnering with Idaho National Laboratory.

This multidisciplinary project will give such a student the opportunity to:

- Work with experts in the field
- Collaborate with students from Boise State University, and
- Work with CEDAR alumni.

University of Wyoming [4] Idaho National Laboratory [5] Boise State University [6]

Advisor: Dr. Mike Borowczak

Group Members:

- INL Team of Experts
- A Boise State University Senior-to-Master Student

University of Wyoming

CEDAR
Cybersecurity Education And Research Center

[1] https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf
[2] https://empoweringpumps.com/wp-content/uploads/2017/08/maxresdefault-2.jpg
[3] Rita Foster, Zach Priest, Michael Cutshaw, Infrastructure eXpression for Codified Cyber Attack Surfaces and Automated Applicability, https://ieeexplore.ieee.org/document/9611807
[4] https://www.drought.gov/sites/default/files/hero/partners/UW_Signature_stacked_brown_0.png
[5] https://inl-gov.imgix.net/2021/03/INL-Logo_Centered-Two-Color.png?auto=compressformat&ixlib=php-1.2.1,
[6] https://d28htnjz2elwuj.cloudfront.net/wp-content/uploads/2019/03/14143644/Boise-State-University.jpg

UW School of Computing | UW College of Engineering and Physical Sciences | UW College of Engineering and Physical Sciences Electrical Engineering and Computer Science | UW Cybersecurity Education and Research Center