ICS Testbed Tetris: Practical Building Blocks Towards a Cyber Security Resource

CSET ’20 - Long Preliminary Work Paper
13th USENIX Workshop on Cyber Security Experimentation and Test
August 10, 2020

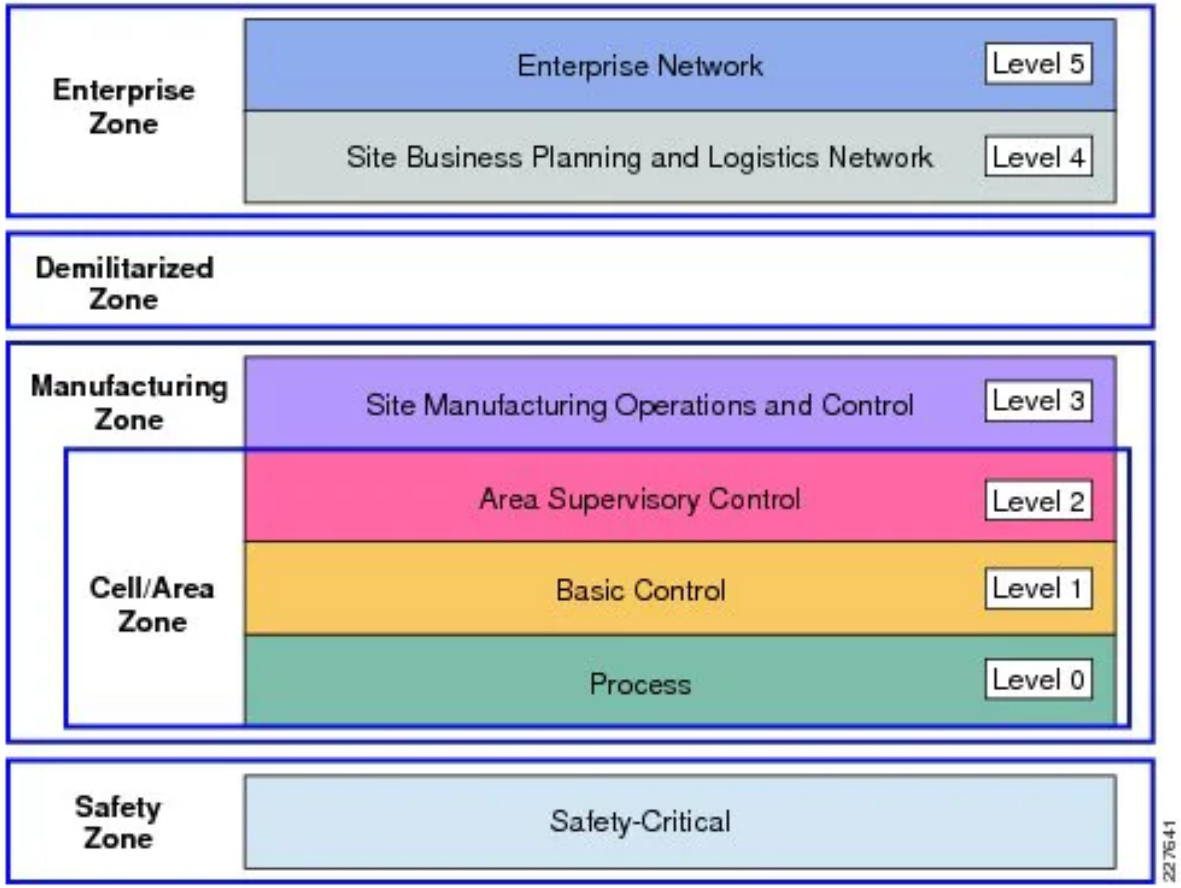
Benjamin Green
Richard Derbyshire
William Knowles
James Boorman
Pierre Ciholas
Daniel Prince
David Hutchison

https://www.lancaster.ac.uk/security-lancaster/

Introduction

- What are Industrial Control Systems (ICS)
- Our work to date/Related work
- Design considerations
- Experiment lifecycle
- High-Level Model
- Model breakdown
- Practical implementation
- Living resource
- TIDE-H and future work

What are Industrial Control Systems (ICS)



Enterprise Zone

Enterprise Network Level 5

Site Business Planning and Logistics Network Level 4

Demilitarized Zone

Manufacturing Zone

Site Manufacturing Operations and Control Level 3

Cell/Area Zone

Area Supervisory Control Level 2

Basic Control Level 1

Process Level 0

Safety Zone

Safety-Critical

227641

https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/DG/Industrial-AutomationDG/Industrial-AutomationDG.html

Related Work

- Our work
  - Over 6 years of ICS testbed development
  - Collaborative engagement
  - 5 Existing publications in this space
- Related work
  - Surveys
  - Theoretical concepts
  - Practical implementation

Green, B., Lee, A., Antrobus, R., Roedig, U., Hutchison, D. and Rashid, A., 2017. Pains, gains and PLCs: ten lessons from building an industrial control systems testbed for security research. In *10th {USENIX} Workshop on Cyber Security Experimentation and Test ({CSET} 17)*.

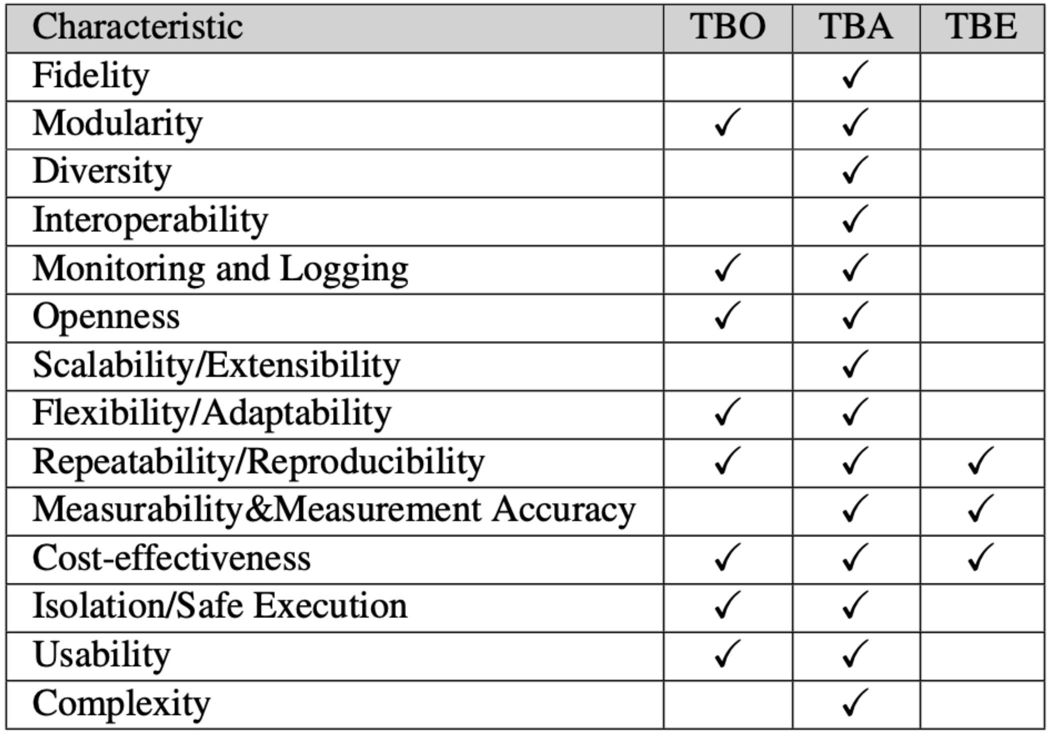
Green, B., Frey, S.A.F., Rashid, A. and Hutchison, D., 2016. Testbed diversity as a fundamental principle for effective ICS security research. *Serecin*.

Gardiner, J., Craggs, B., Green, B. and Rashid, A., 2019, November. Oops I did it again: further adventures in the land of ICS security testbeds. In *Proceedings of the ACM Workshop on Cyber-Physical Systems Security & Privacy* (pp. 75-86)

Ani, U.D., Watson, J.M., Green, B., Craggs, B. and Nurse, J., 2019. Design Considerations for Building Credible Security Testbeds: A Systematic Study of Industrial Control System Use Cases. *arXiv preprint arXiv:1911.01471.*

Green, B., Paske, B., Hutchison, D. and Prince, D., 2014. Design and construction of an industrial control system testbed. In *PG Net-The 15th Annual PostGraduate Symposium*

Design Considerations



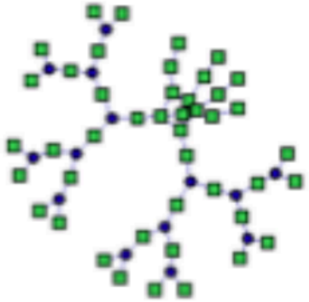
Characteristic	TBO	TBA	TBE
Fidelity		✓	
Modularity	✓	✓	
Diversity		✓	
Interoperability		✓	
Monitoring and Logging	✓	✓	
Openness	✓	✓	
Scalability/Extensibility		✓	
Flexibility/Adaptability	✓	✓	
Repeatability/Reproducibility	✓	✓	✓
Measurability&Measurement Accuracy		✓	✓
Cost-effectiveness	✓	✓	✓
Isolation/Safe Execution	✓	✓	
Usability	✓	✓	
Complexity		✓	

Ani, U.D., Watson, J.M., Green, B., Craggs, B. and Nurse, J., 2019. Design Considerations for Building Credible Security Testbeds: A Systematic Study of Industrial Control System Use Cases. *arXiv preprint arXiv:1911.01471.*

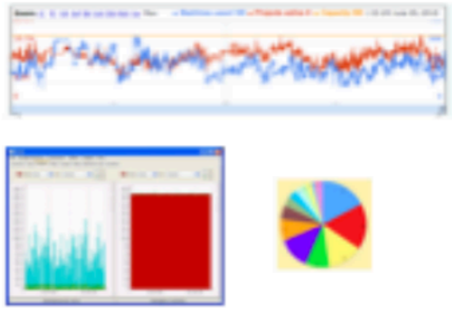
Cyber Security Experiment Lifecycle

Design ⇄ Instantiation ⇄ Execution ⇄ Analysis

cache
True resource
Fake resource
2. Access
4. Ask for rare location
3. Attacker poisons cache (question + gratuitous info)
1. Ask for rare location
5. Access
attacker
leg. client

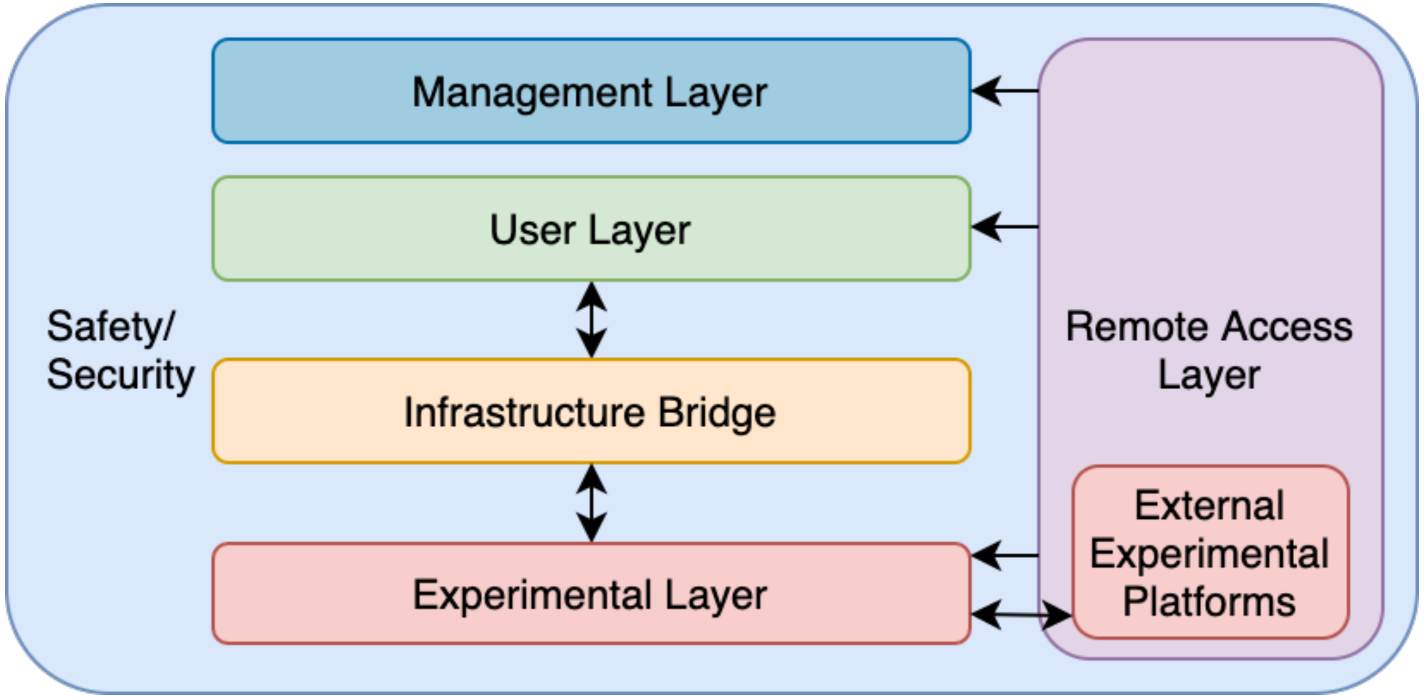


File Experiment Build View
Controls Topology Graphs Debug
V
A2
A1
control
Attached to Floo... calling local.getg... get Status: 0 queu

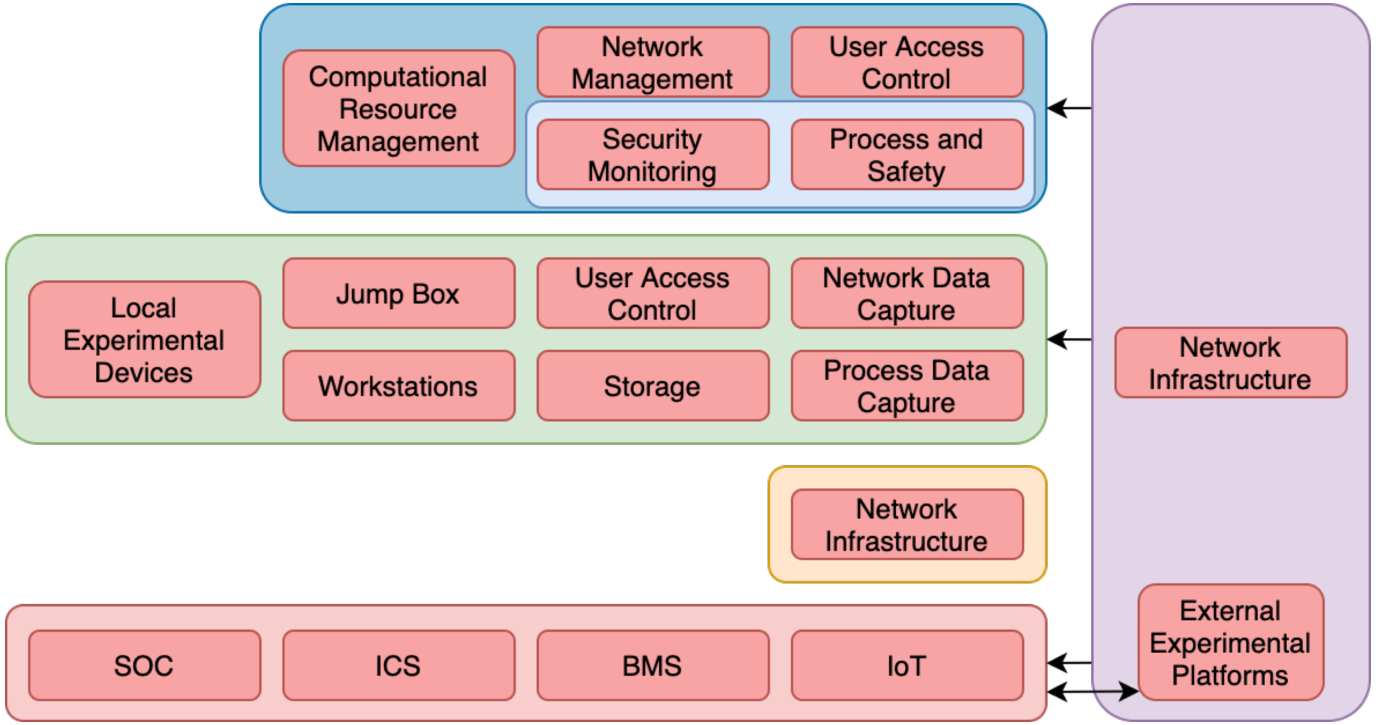


Mirkovic, J., Benzel, T.V., Faber, T., Braden, R., Wroclawski, J.T. and Schwab, S., 2010, November. The DETER project: Advancing the science of cyber security experimentation and test. In *2010 IEEE International Conference on Technologies for Homeland Security (HST)* (pp. 1-7). IEEE.

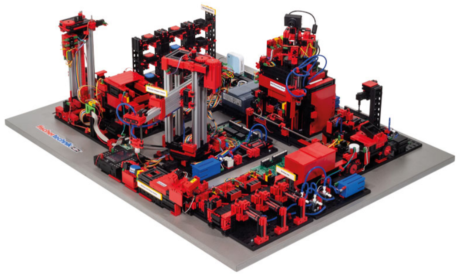
High-Level Model



Model Breakdown



Baseline Implementation Guide



https://www.gunt.de/en/products/process-engineering/water-treatment/multistage-water-treatment/water-treatment-plant-1/083.58100/ce581/glct-1:pa-148:ca-255:pr-57

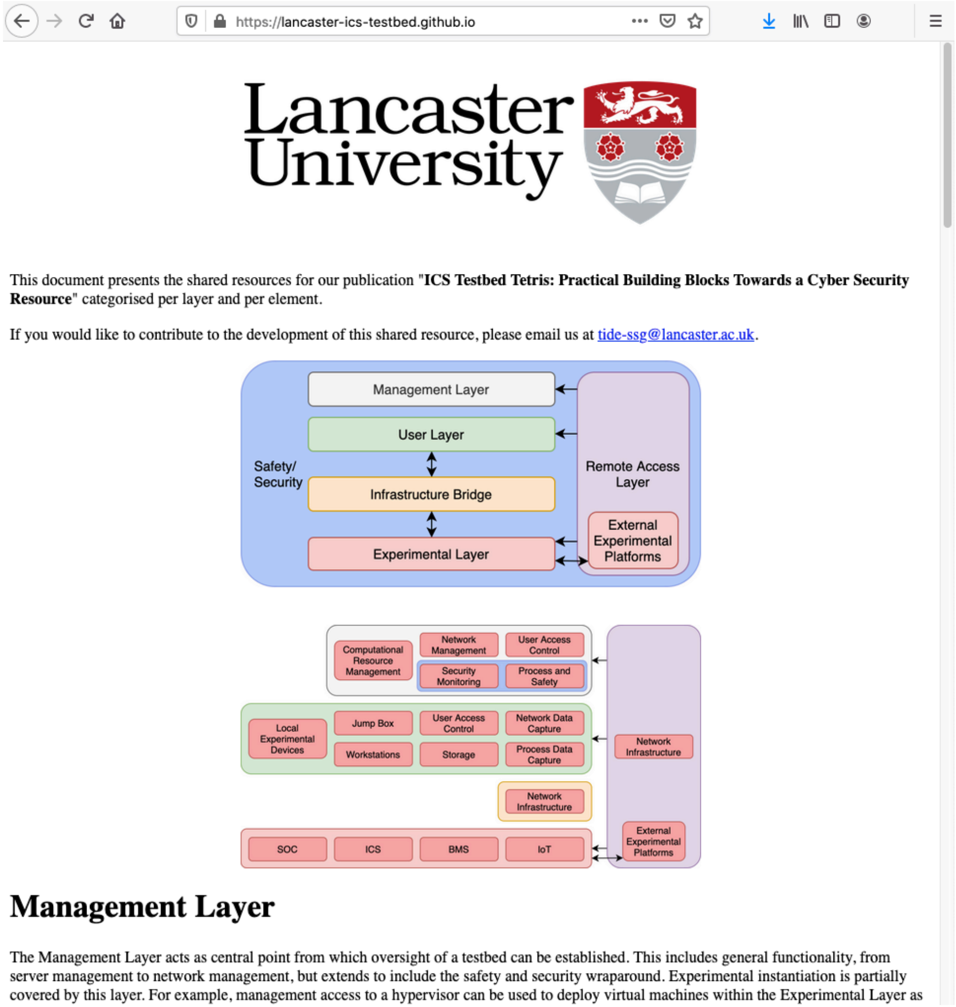
https://www.fischertechnik.de/en/products/teaching/training-models/554868-edu-training-factory-industry-4-0-24v-education

https://factoryio.com/features

http://snap7.sourceforge.net/

Living Resource

- Online resource
  - www.ics-testbed.co.uk
  - Transcends static nature of paper
  - Community contribution
  - tide-ssg@lancaster.ac.uk



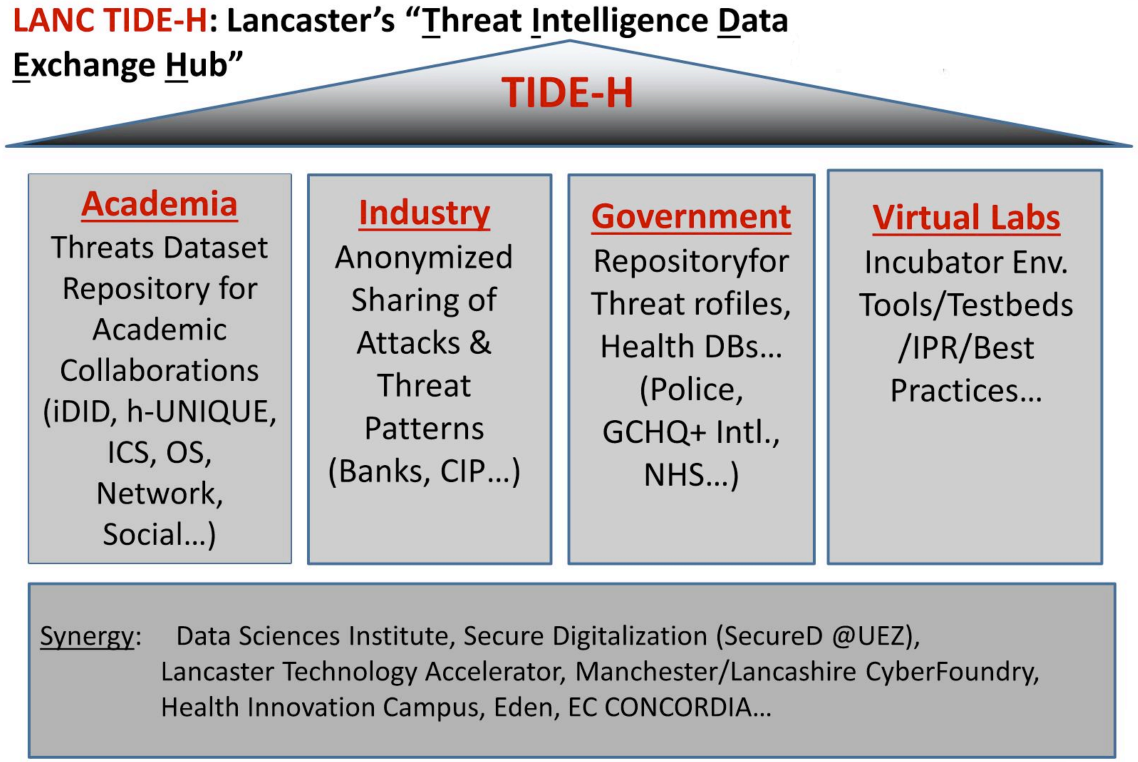
This document presents the shared resources for our publication "**ICS Testbed Tetris: Practical Building Blocks Towards a Cyber Security Resource**" categorised per layer and per element.

If you would like to contribute to the development of this shared resource, please email us at tide-ssg@lancaster.ac.uk.

Management Layer

The Management Layer acts as central point from which oversight of a testbed can be established. This includes general functionality, from server management to network management, but extends to include the safety and security wraparound. Experimental instantiation is partially covered by this layer. For example, management access to a hypervisor can be used to deploy virtual machines within the Experimental Layer as

Security Lancaster’s TIDE-H & Future Work



LANC TIDE-H: Lancaster’s “Threat Intelligence Data Exchange Hub”

TIDE-H

Academia
Threats Dataset Repository for Academic Collaborations (iDID, h-UNIQUE, ICS, OS, Network, Social…)

Industry
Anonymized Sharing of Attacks & Threat Patterns (Banks, CIP…)

Government
Repositoryfor Threat rofiles, Health DBs… (Police, GCHQ+ Intl., NHS…)

Virtual Labs
Incubator Env. Tools/Testbeds /IPR/Best Practices…

Synergy: Data Sciences Institute, Secure Digitalization (SecureD @UEZ), Lancaster Technology Accelerator, Manchester/Lancashire CyberFoundry, Health Innovation Campus, Eden, EC CONCORDIA…

Thank You for Watching!