INL/CON-23-74981-Revision-0

Are System Baselines within OT Environments Feasible?

October 2023

Gabriel Arthur Weaver, Scott Timothy Bowman

Changing the World's Energy Future

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/CON-23-74981-Revision-0

Are System Baselines within OT Environments Feasible?

Gabriel Arthur Weaver, Scott Timothy Bowman

October 2023

Idaho National Laboratory
Idaho Falls, Idaho 83415

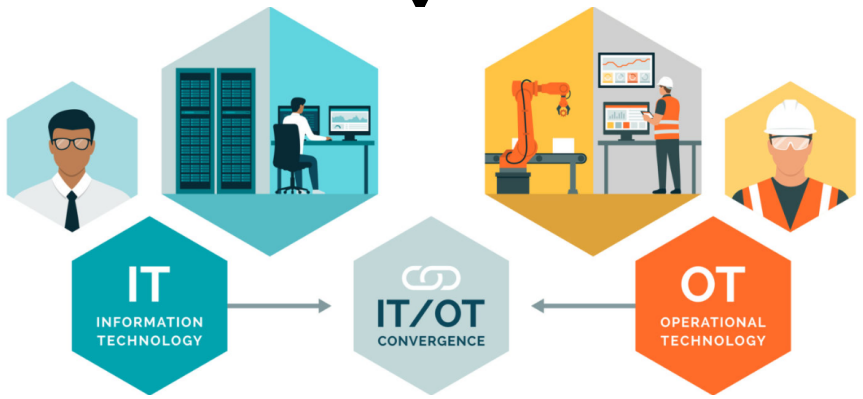
http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Are System Baselines within OT Environments Feasible?

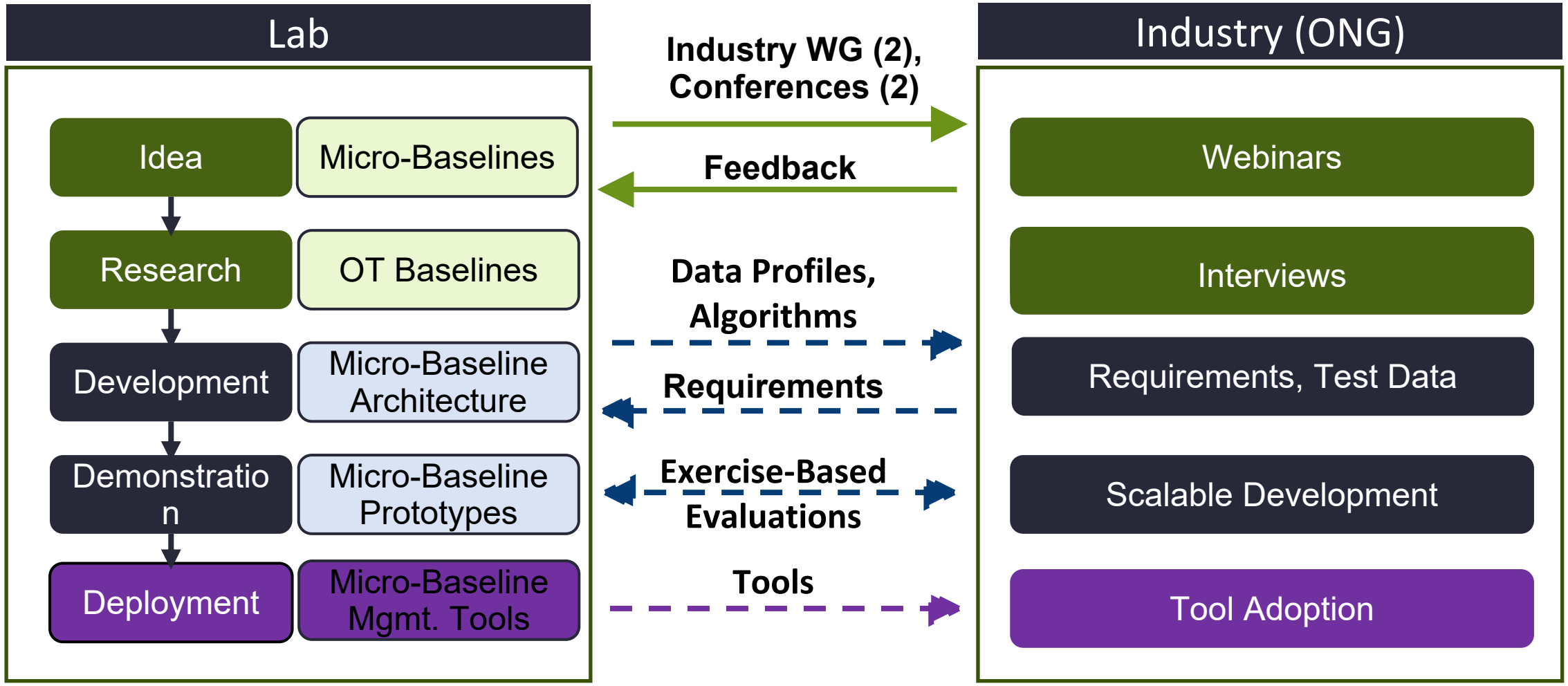
Scott Bowman & Gabe Weaver

Motivation: Why are Baselines Important?



Event Classification

Industry-Driven R&D: Baselining in OT Environments



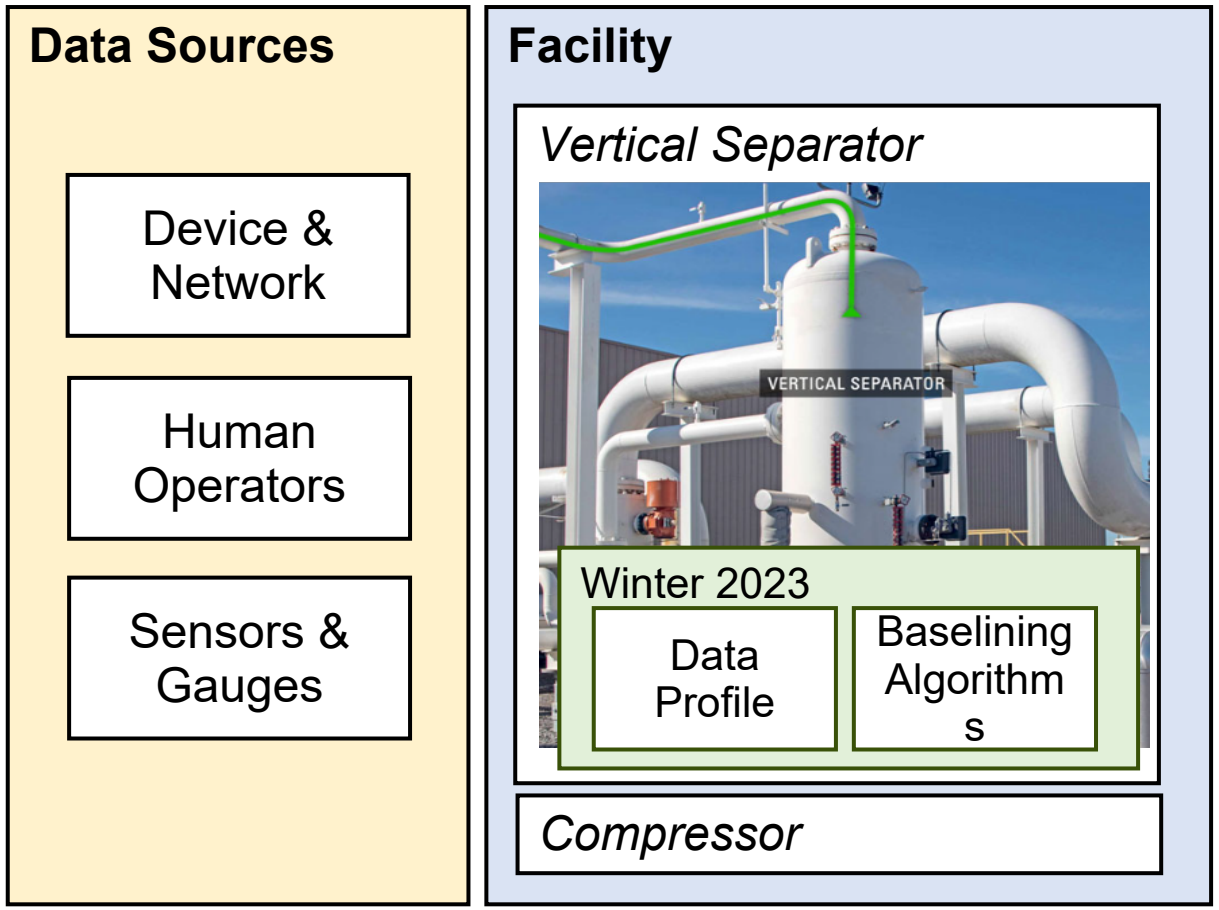
Micro-Baselines: Value to Industry

Micro-baselines profile expected behavior for a specific operational process

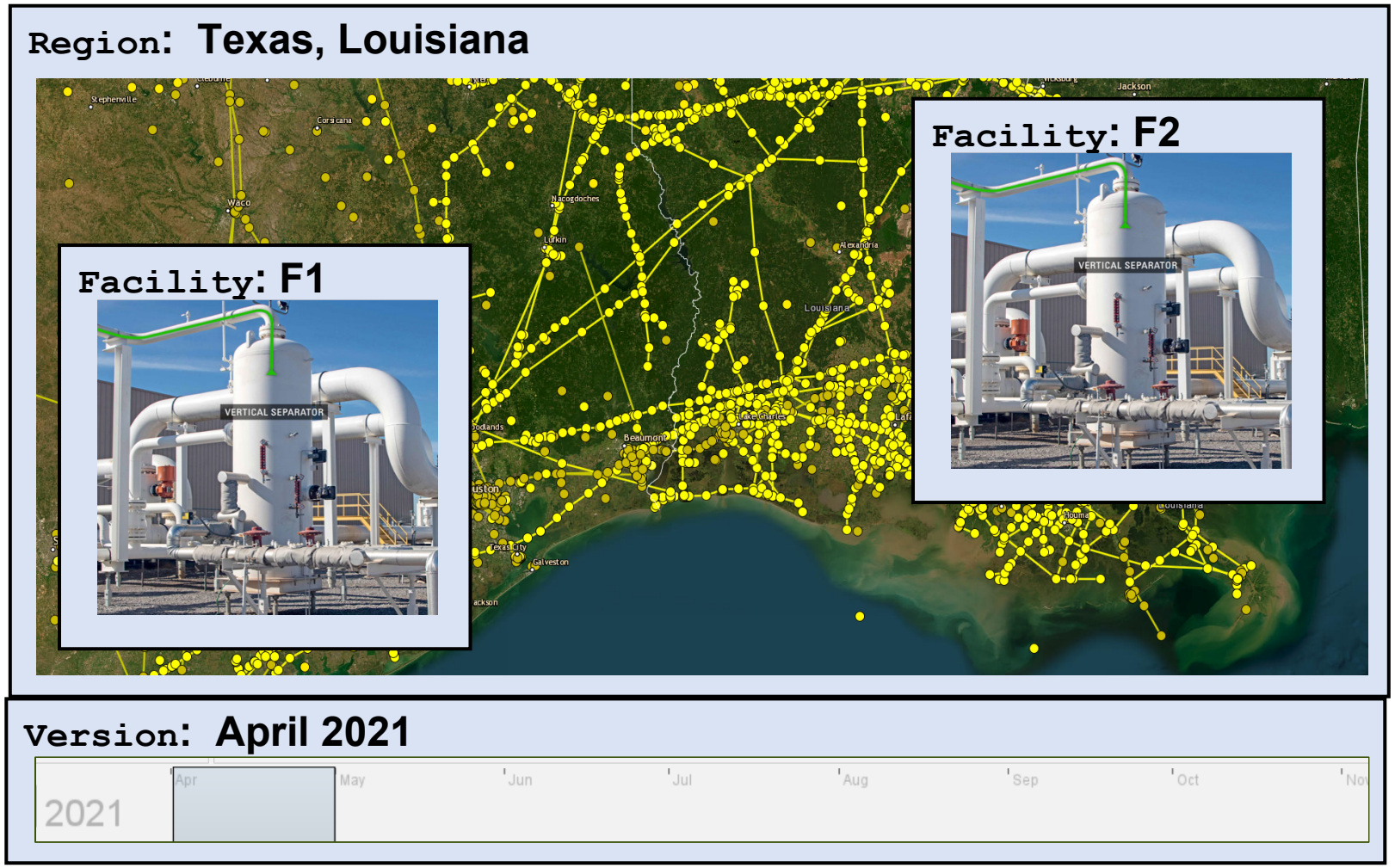
- **shift the focus from baselining *technology* to baselining *processes***
- **integrate data sources multiple organizational silos**

Micro-Baseline Management Tool:

- ***Inventory data source dependencies***
- ***Manage multi-versioned baselines* in an evolving operational context**
- **Detect anomalous behaviors sooner and reduce impact**



Industrial Control Systems Depend on Context



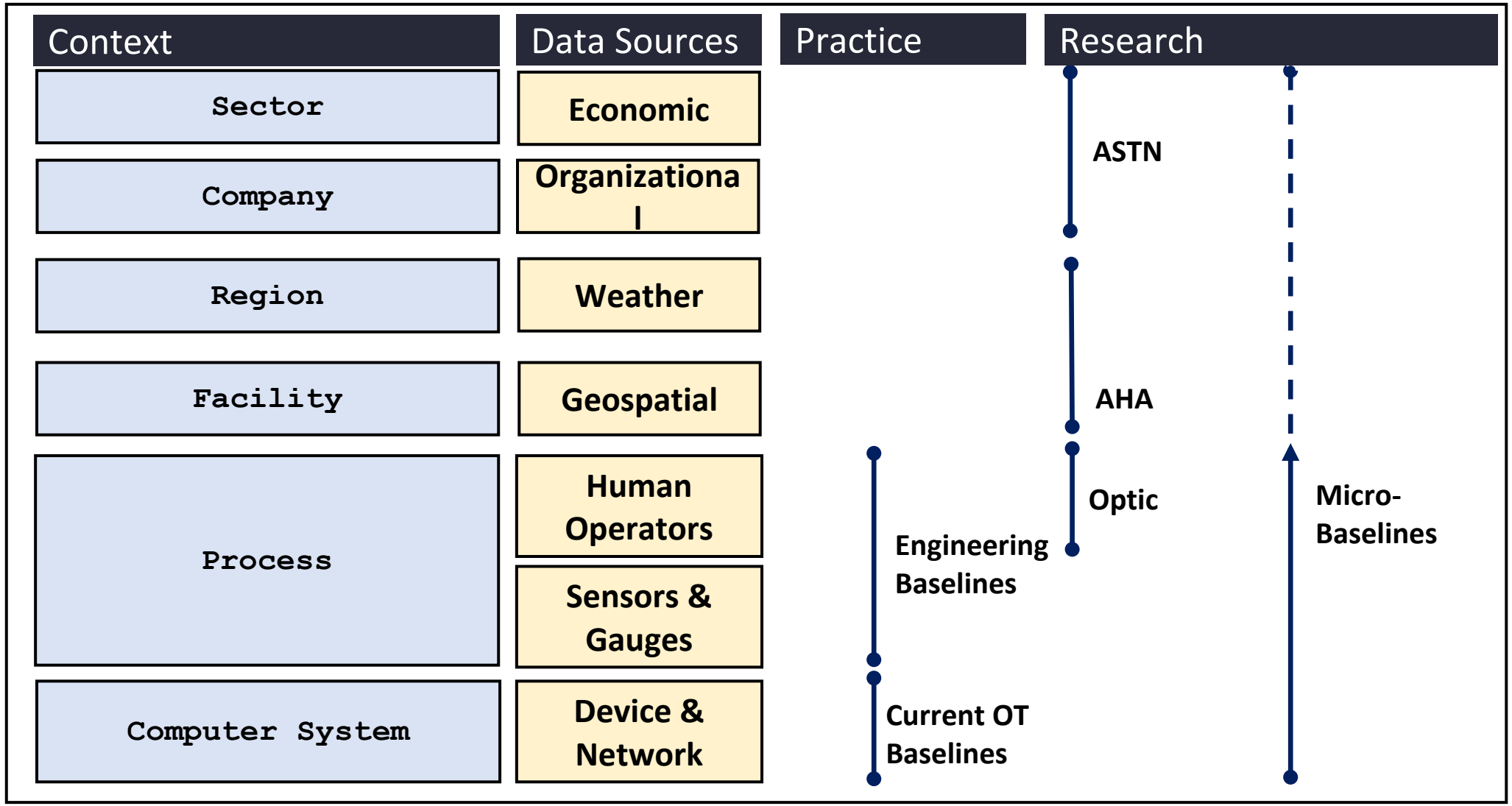
Operations process depend on context

Our tools represent this context as metadata for micro-baseline objects.

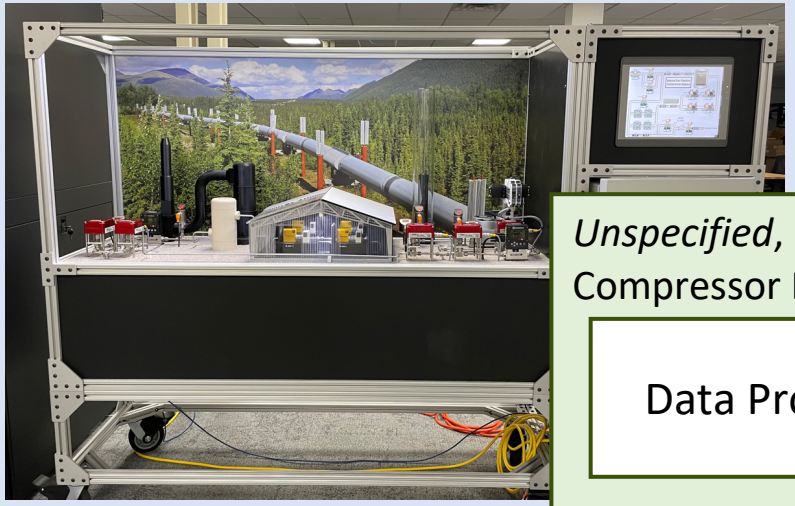
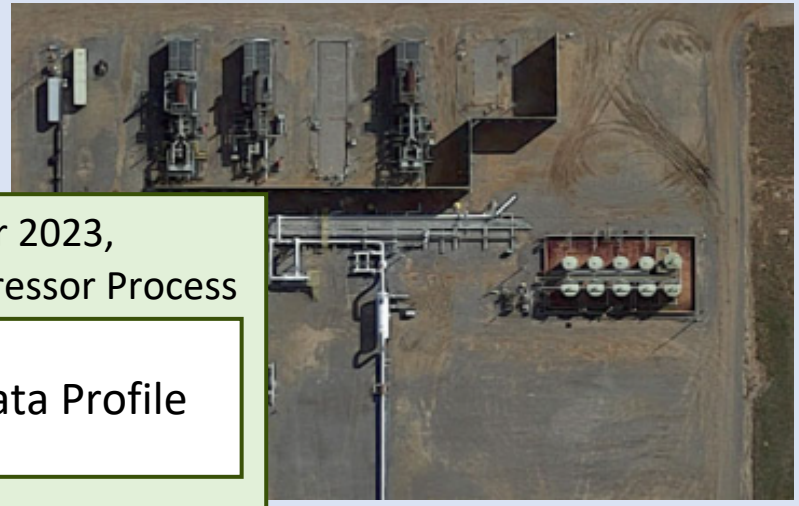
- Sector
- Company
- Region
- Facility
- Process
- Version

As a result, practitioners need tools to manage multi-versioned baselines

Micro-Baselines Depend on a Wide-Range of Context



Industry Partnership: Data Profile Exchanges

	Lab	Industry
Facility	**INL.Idaho.CELR**  *Unspecified*, Compressor Process Data Profile	**GasCo.Texas.F3**  Winter 2023, Compressor Process Data Profile
Data Sources	**Sensors & Gauges** **Device & Network**	**Sensors & Gauges** **Human Operators** **Device & Network**

Data Features

?

Comparable:

- ***Features?***
- ***Values?***

Micro-Baseline: Data Profile Construction

Industry Engagement

- Currently, baselines are heavily asset focused
- Need to integrate network and device data
- Desire to integrate application-layer semantics from ICS protocols [MITRE]
- Early exploration to integrate additional data sources from operations [OSISoft]

Micro-Baselining Data Profiles

- Use feature selection algorithms to augment SME intuition (PCA, shapelets)
- Fusion of different datasets via ontology and language grammars

Value

- Targeted threat hunts
- Identify informational single points of failure

INL.Idaho.CELR

***Unspecified,* Compressor Process**

Data Profile		
Feature	…	*Data Source*
Ambient Temperature		Sensors & Gauges
Protocol Function Codes		Device & Network
Communication Latency		Device & Network
…		
HMI Interactions		*Human Operators;* Device & Network

Industry Partnership: Algorithm Evaluations

Lab

INL.Idaho.CELR

Unspecified,
Compressor Process

Data Profile	Baselining Algorithm

Industry

GasCo.Texas.F3

Winter 2023,
Compressor Process

Data Profile	Baselining Algorithm

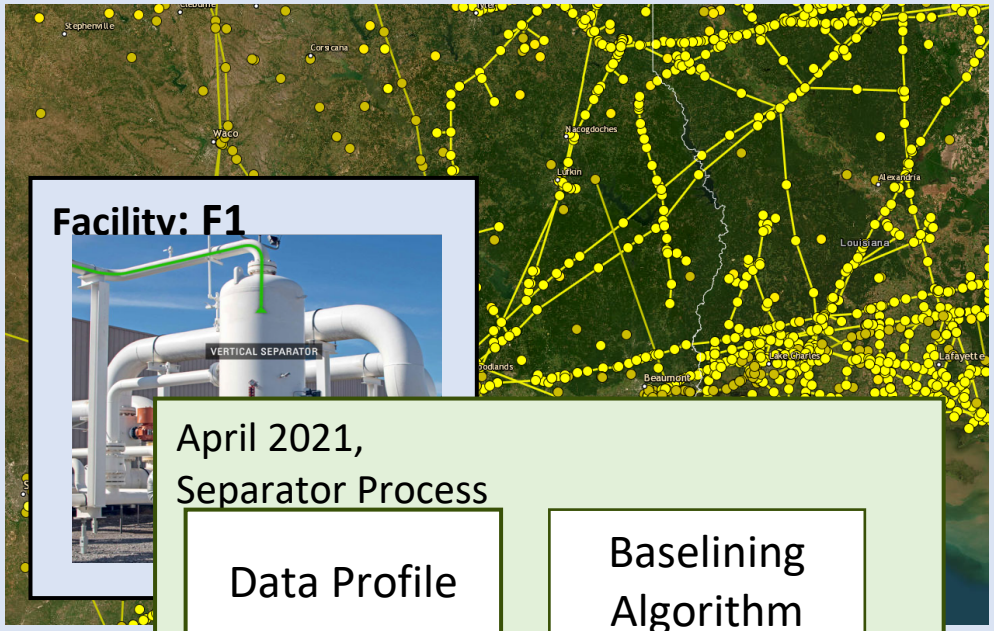
Comparable Features? Yes

Comparable Performance? TBD

Micro-Baseline Lifecycle Management

Micro-baselining management tools should reflect the asset and operations lifecycles.

Region: Texas, Louisiana

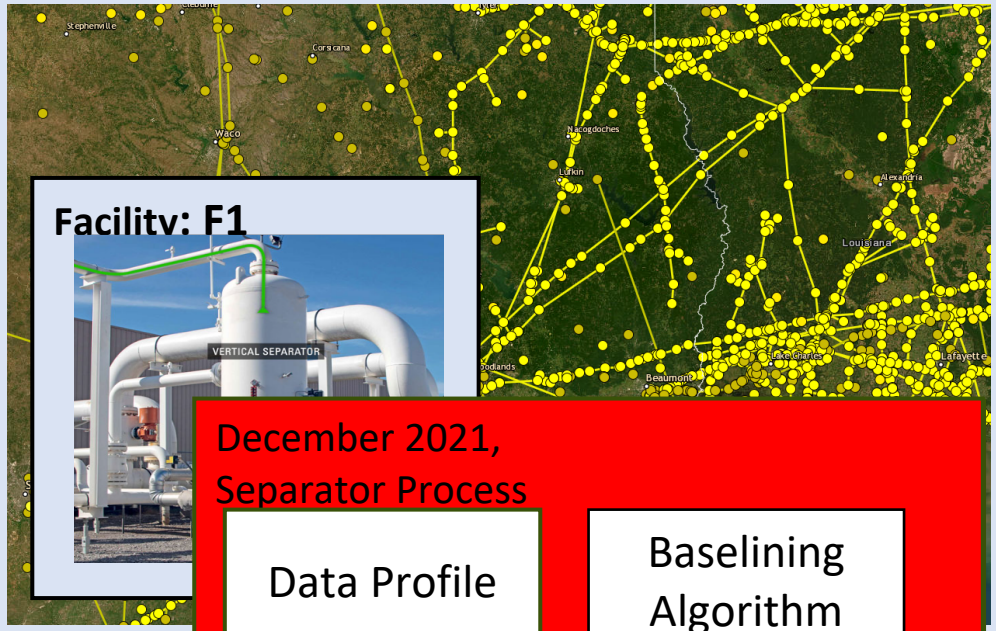


April 2021,
Separator Process

Data Profile

Baselining Algorithm

Region: Texas, Louisiana



December 2021,
Separator Process

Data Profile

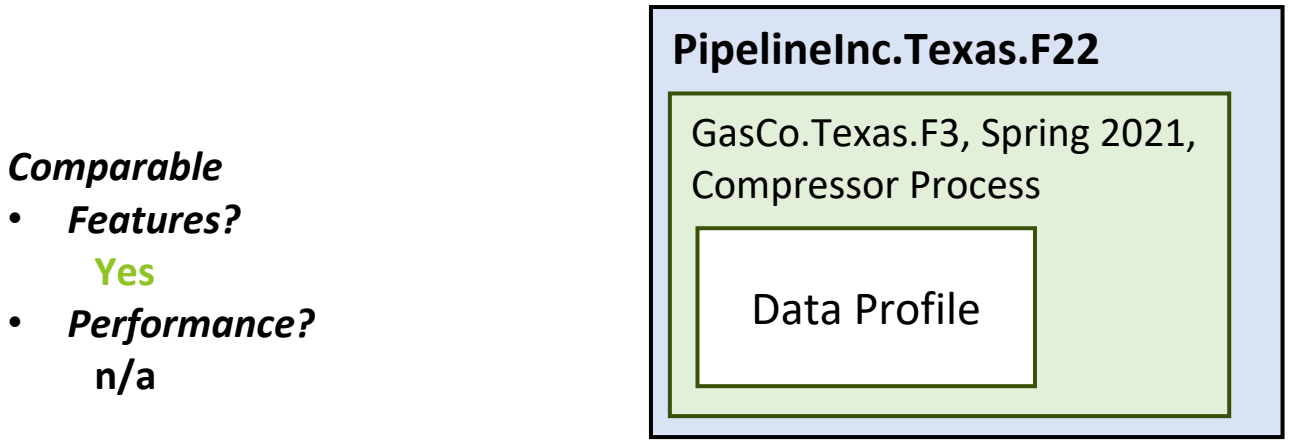
Baselining Algorithm

Version:

2021 | **Excellent** | Jun | Jul | **Bad** | Sep | Oct | Nov | **Fair**

Micro-Baselining Information Sharing

***Inter-Facility* Micro-Baseline Evaluation**

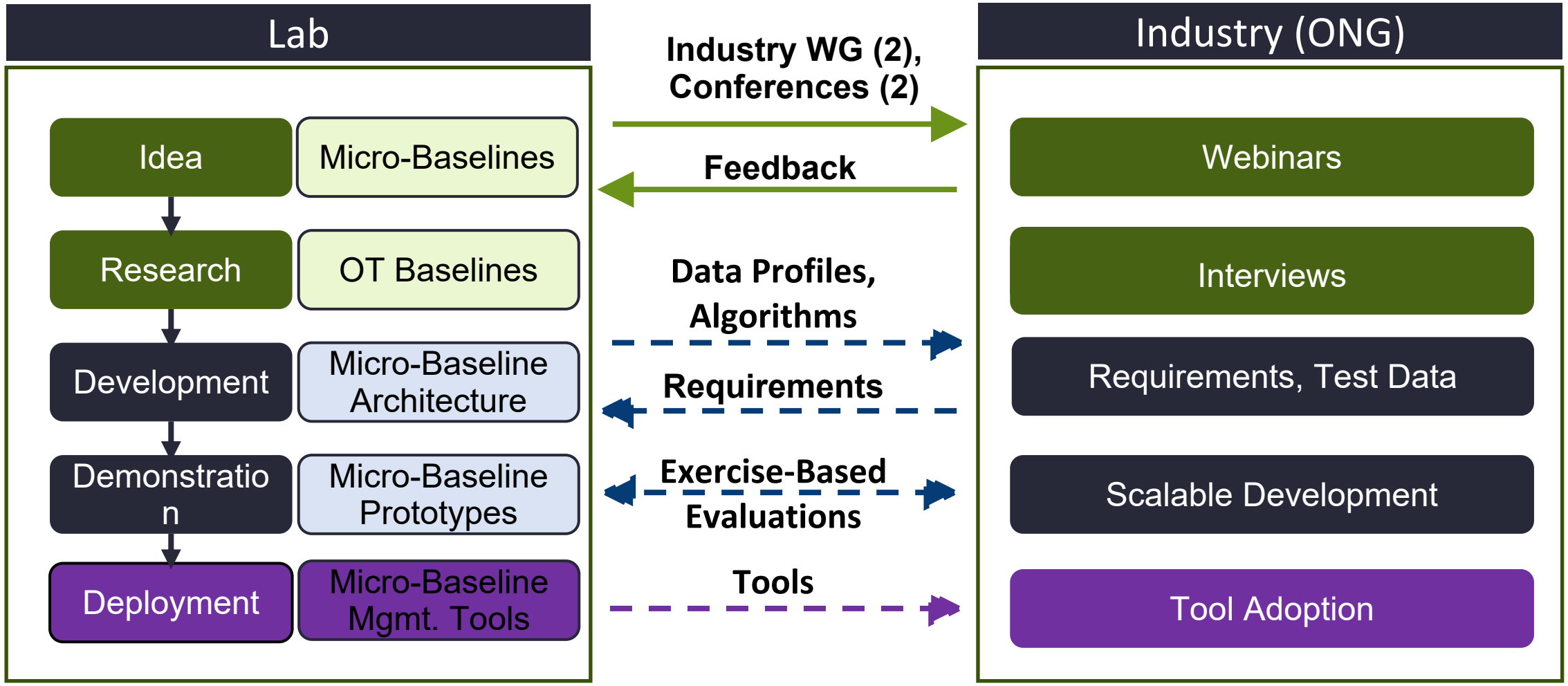


***Inter-Organizational* Micro-Baseline Information Sharing**

Industry Partnerships: Engagement Levels

Lab Capabilities	Micro-Baseline Partnerships	Industry Capabilities
	1 **Data Profile Exchanges** 2 **Algorithm Evaluations** ***(Test Environments)*** 3 **Exercise-Based Evaluations**	

Industry-Driven R&D: Baselining in OT Environments

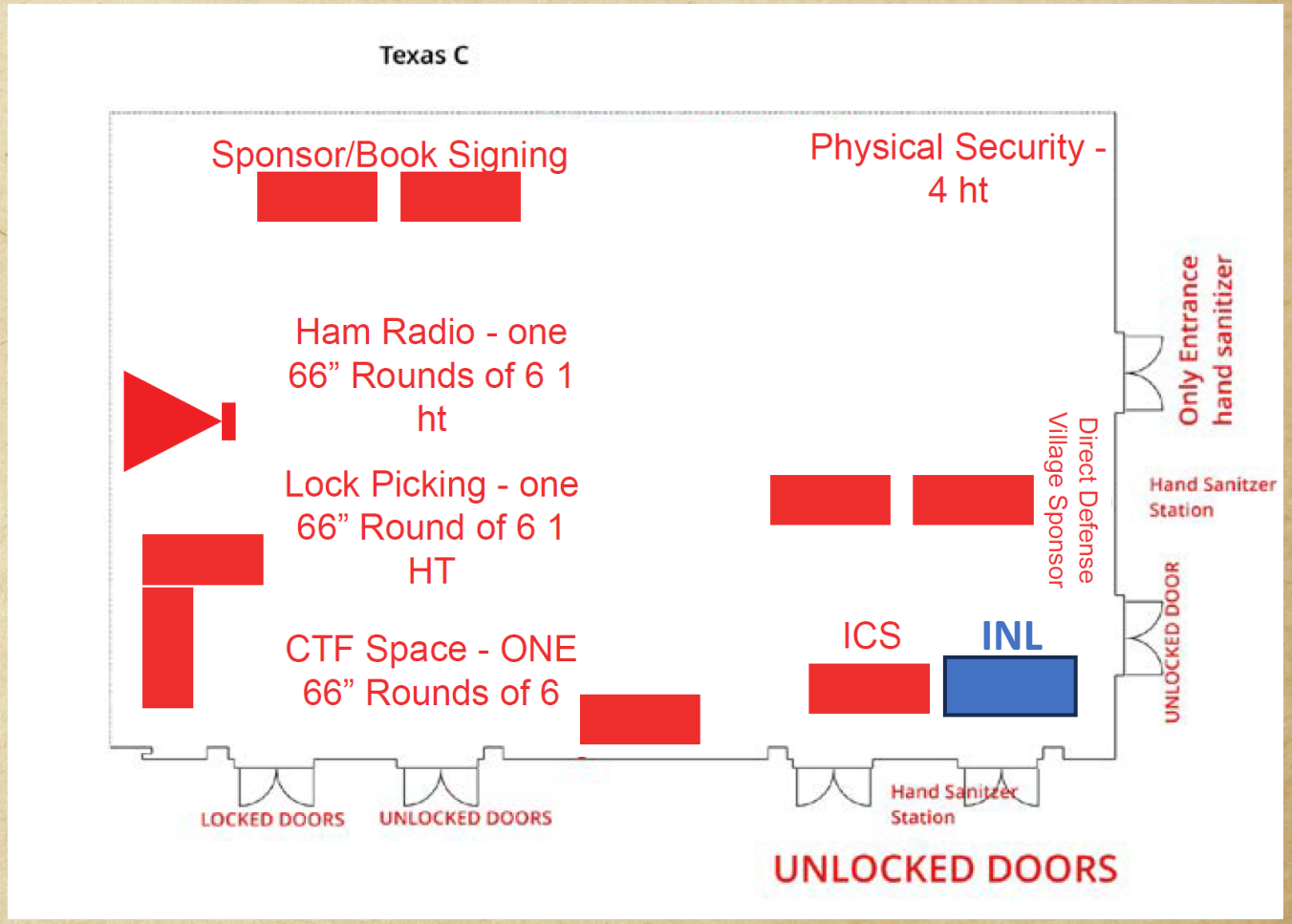


Join our R&D Efforts!

Questions?

- Stop by the **INL booth**
- Contact us at:

cyote@inl.gov



Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.