



Are System Baselines within OT Environments Feasible?

October 2023

Changing the World's Energy Future

Gabriel Arthur Weaver, Scott Timothy Bowman



DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

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>

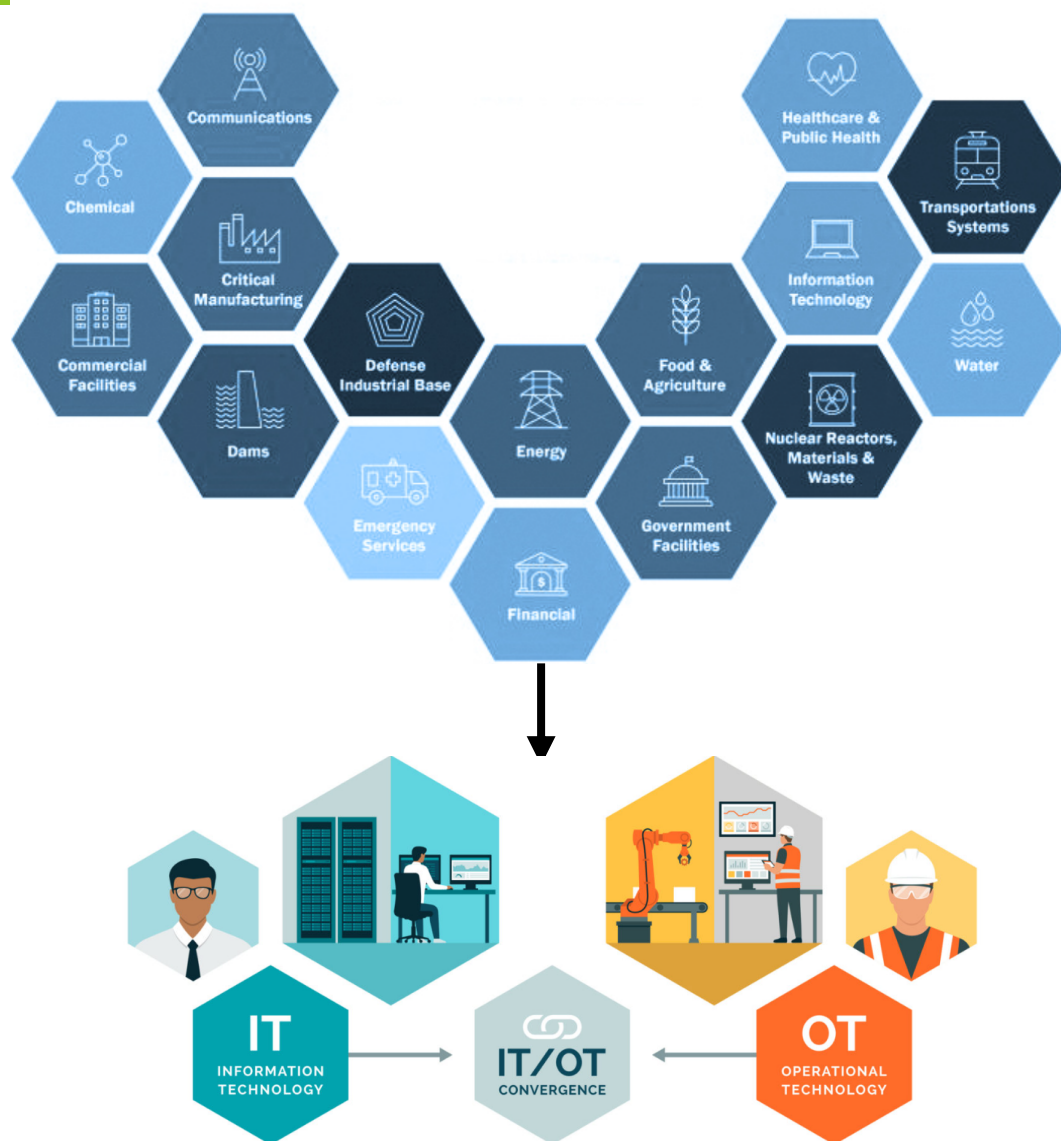
**Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517**

Are System Baselines within OT Environments Feasible?

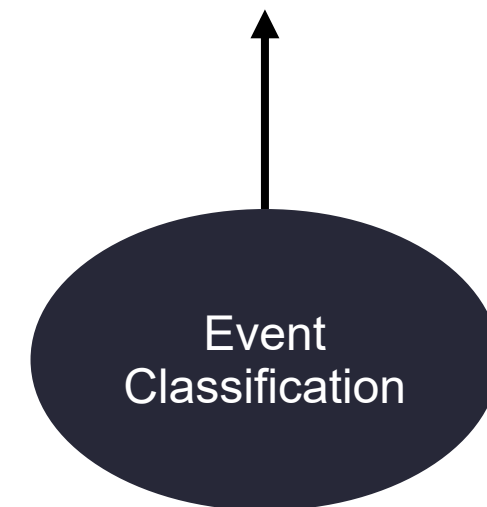
Scott Bowman & Gabe Weaver



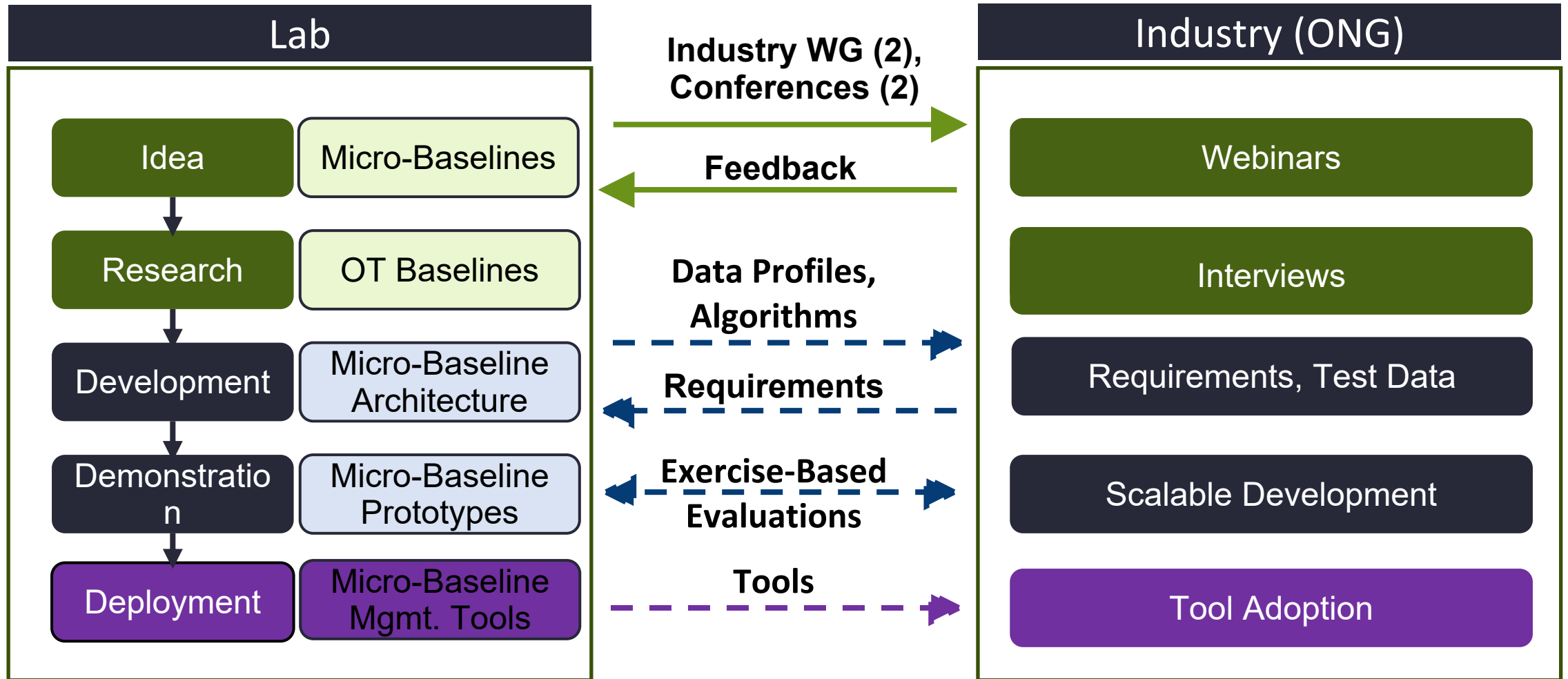
Motivation: Why are Baselines Important?



CyOTE Cybersecurity for the Operational Technology Environment



Industry-Driven R&D: Baselineing 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

Data Sources

Device &
Network

Human
Operators

Sensors &
Gauges

Facility

Vertical Separator



Winter 2023

Data
Profile

Baselining
Algorithms

Compressor

Industrial Control Systems Depend on Context

Region: Texas, Louisiana

Facility: F1



Facility: F2



Version: April 2021

2021

Apr

May

'Jun

'Jul

'Aug

'Sep

'Oct

'Nov

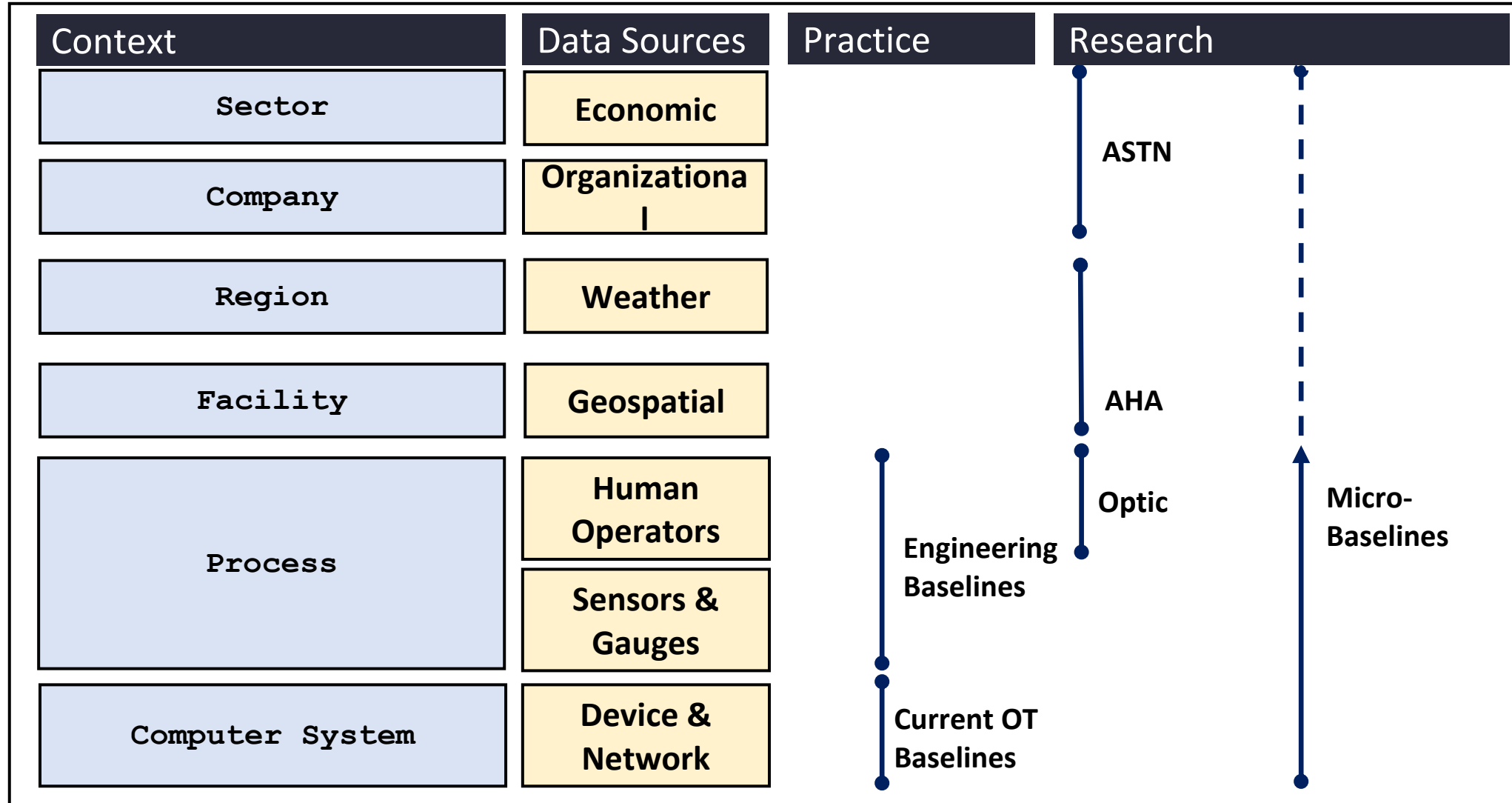
Operations process depend on context

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



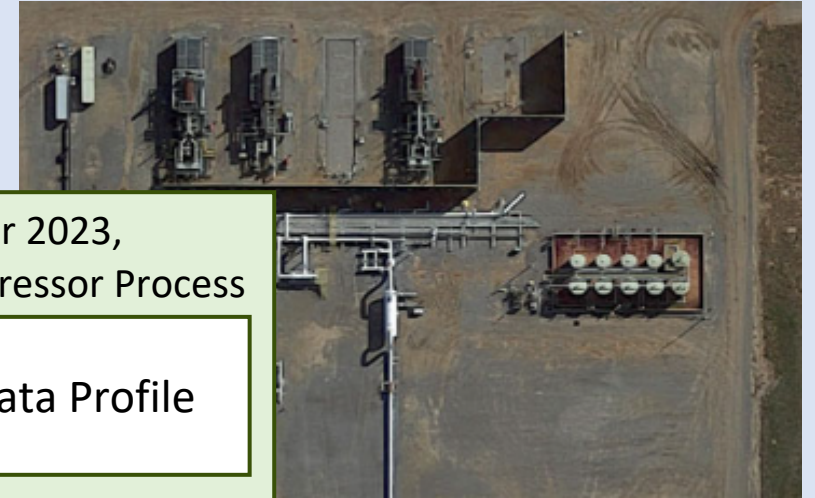
Unspecified,
Compressor Process

Data Profile

?

Comparable:
• Features?
• Values?

GasCo.Texas.F3



Winter 2023,
Compressor Process

Data Profile

Data Sources

Sensors &
Gauges

Device &
Network

Data
Features

Sensors &
Gauges

Human
Operators

Device &
Network

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

<i>Feature</i>	<i>...</i>	<i>Data Source</i>
Ambient Temperature		Sensors & Gauges
Protocol Function Codes		Device & Network
Communication Latency		Device & Network
<i>...</i>		
HMI Interactions		<i>Human Operators;</i> Device & Network

Industry Partnership: Algorithm Evaluations

Lab

INL.Idaho.CELR



Unspecified,
Compressor Process

Data Profile

Baselining
Algorithm

Comparable Features? Yes

Industry

GasCo.Texas.F3



Winter 2023,
Compressor Process

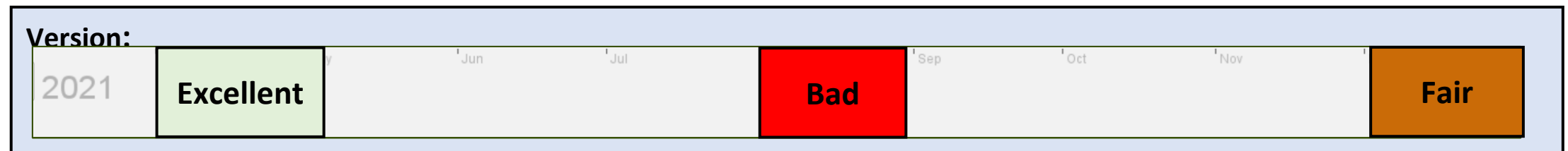
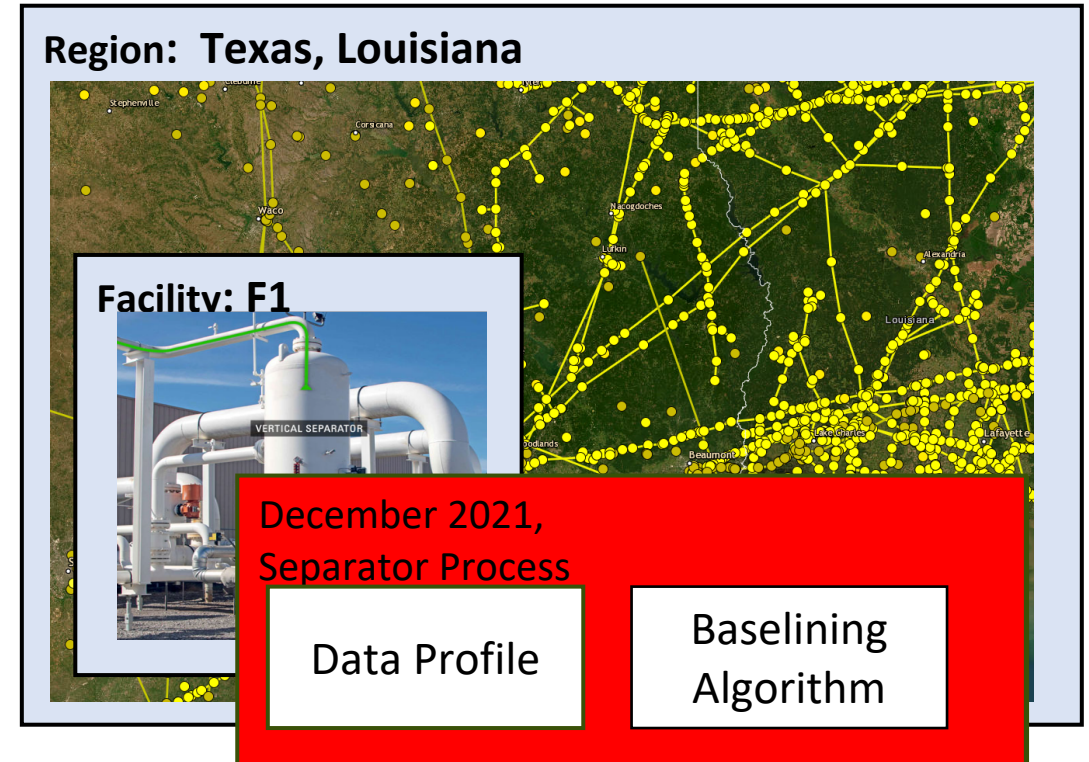
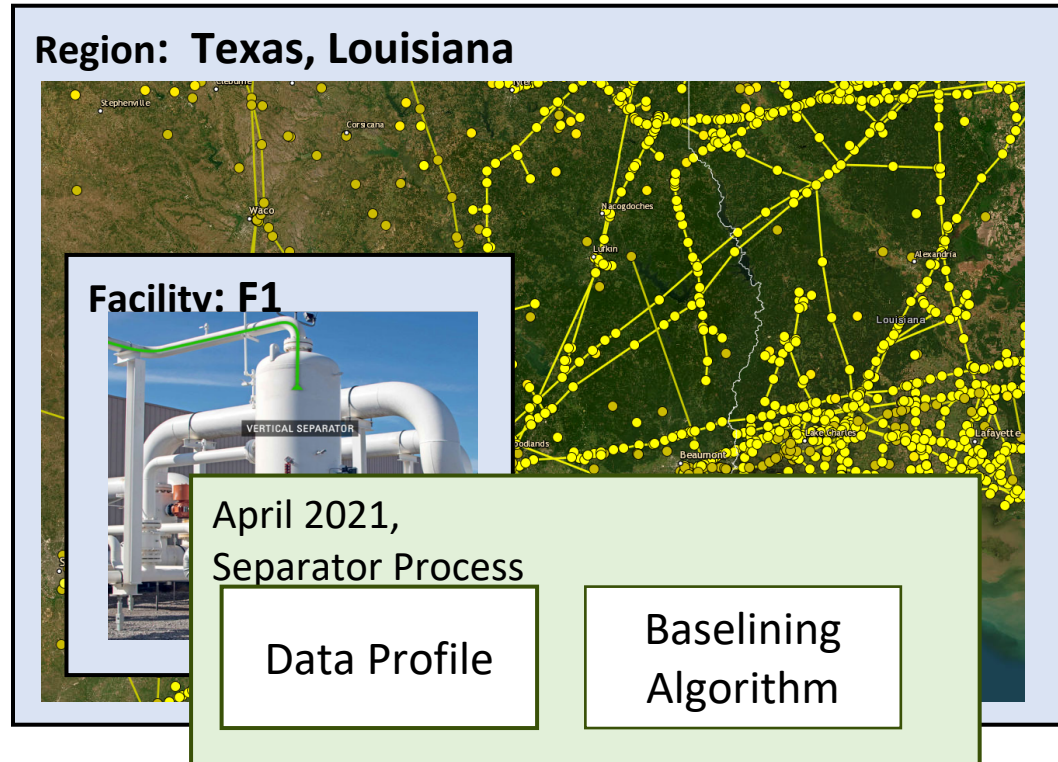
Data Profile

Baselining
Algorithm

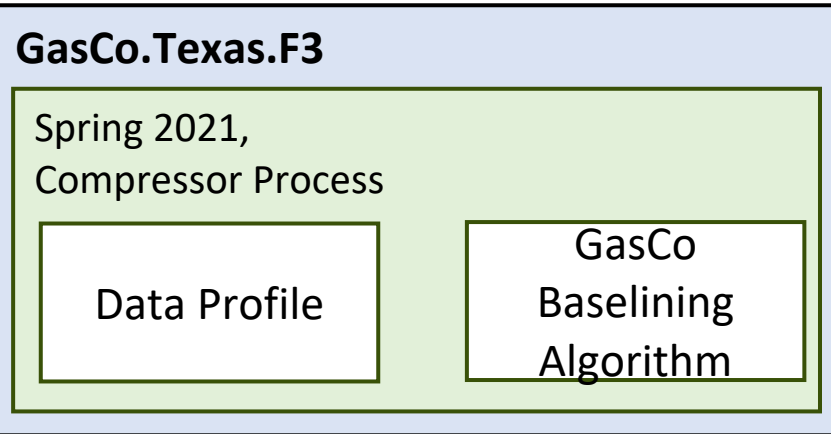
Comparable Performance? TBD

Micro-Baseline Lifecycle Management

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

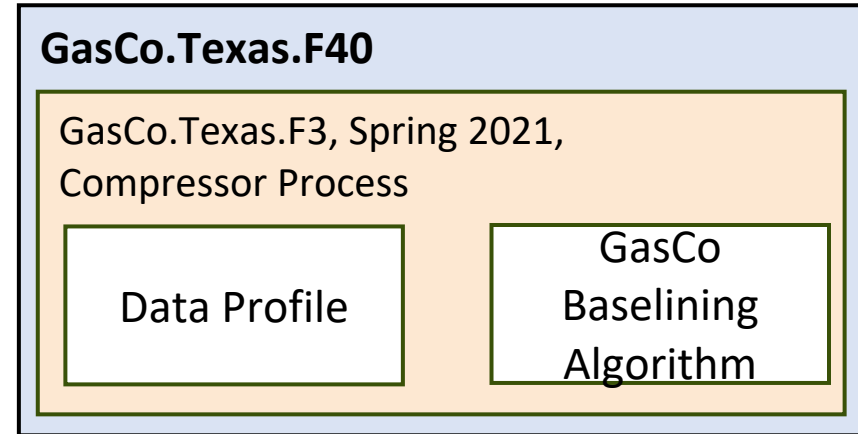


Micro-Baselining Information Sharing



Comparable

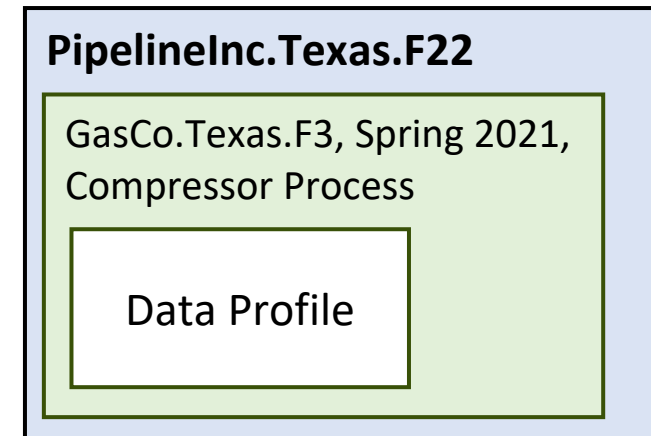
- *Features?*
Yes
- *Performance?*
Excellent > **Fair**



Inter-Facility Micro-Baseline Evaluation

Comparable

- *Features?*
Yes
- *Performance?*
n/a



Inter-Organizational Micro-Baseline Information Sharing

Industry Partnerships: Engagement Levels

Lab Capabilities



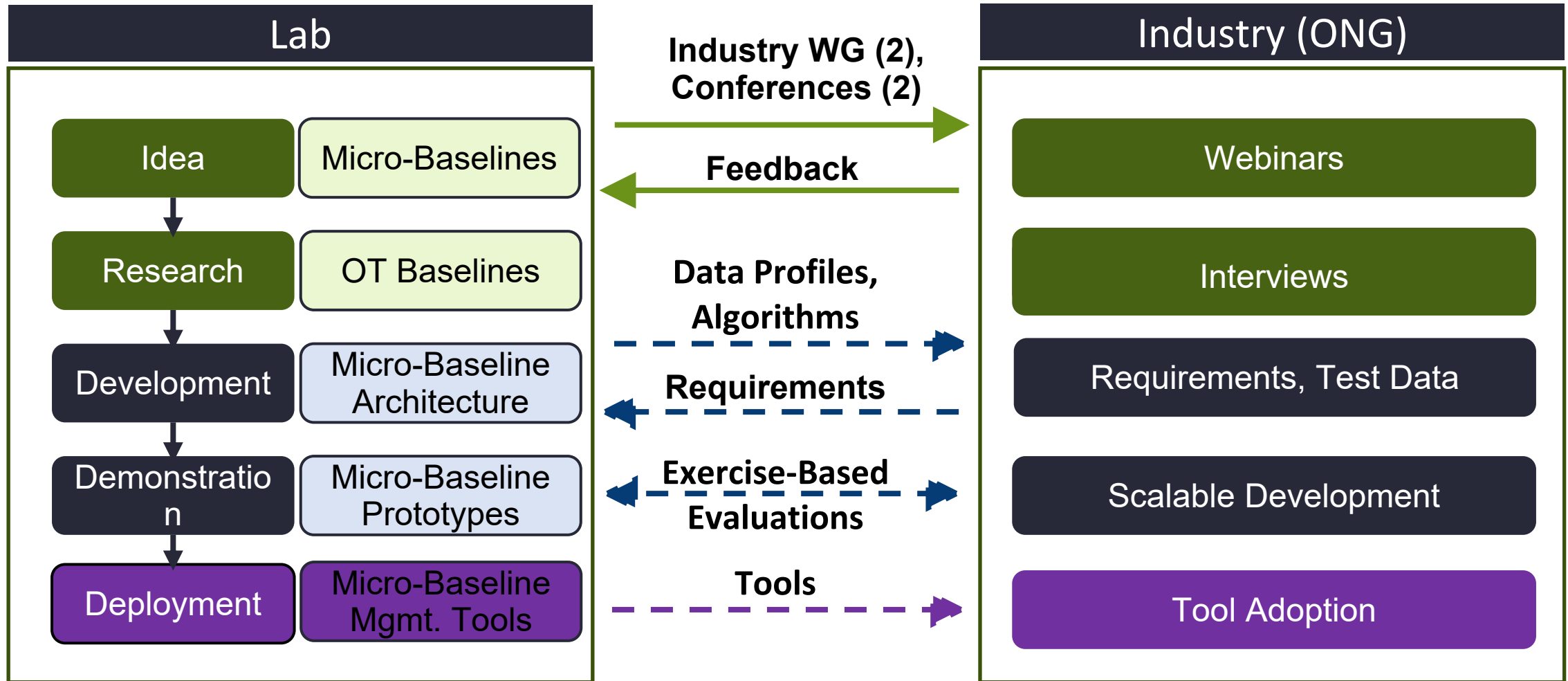
Micro-Baseline Partnerships

- 1 Data Profile Exchanges
- 2 Algorithm Evaluations
(Test Environments)
- 3 Exercise-Based Evaluations

Industry Capabilities



Industry-Driven R&D: Baselineing in OT Environments



Join our R&D Efforts!

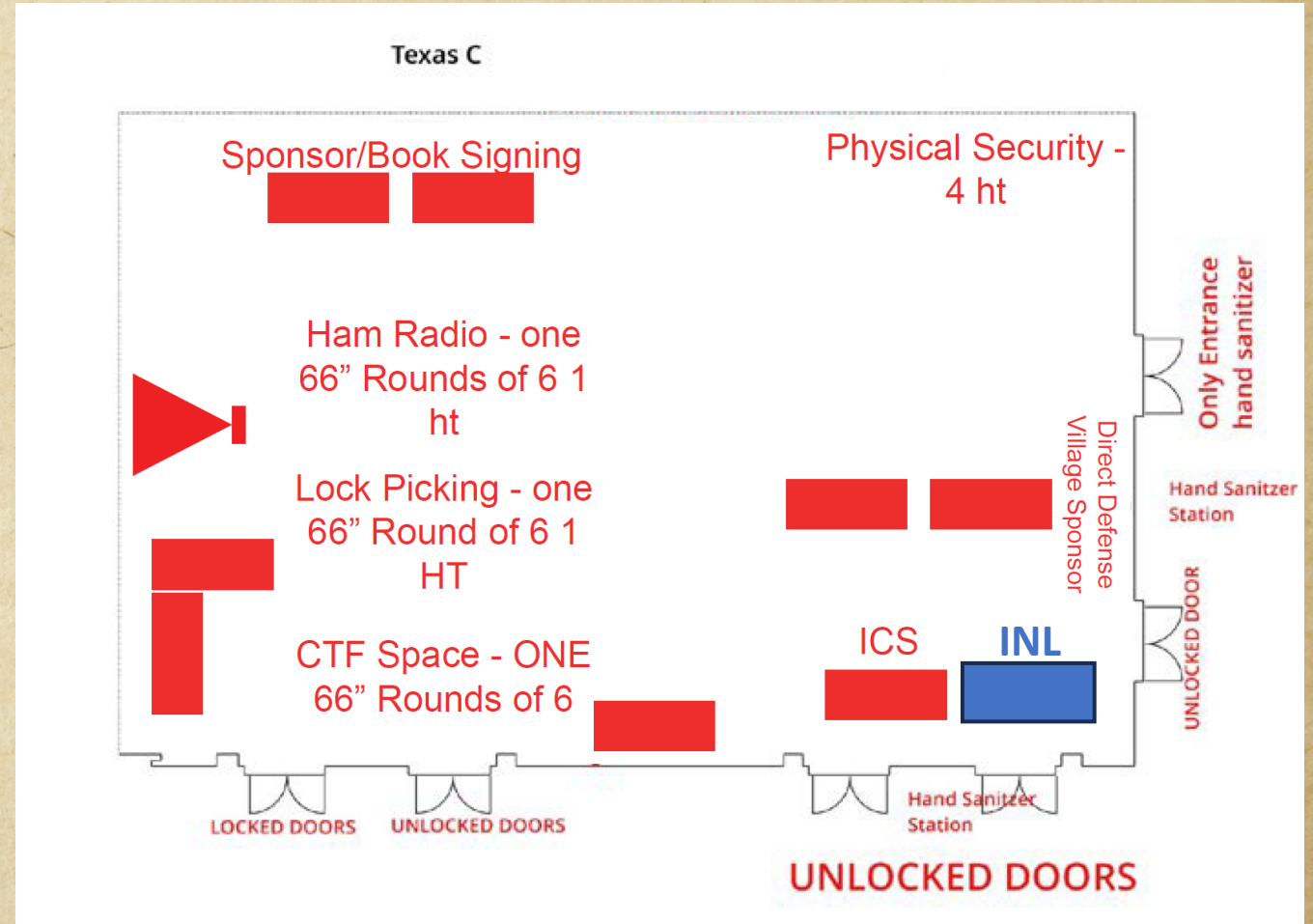


Questions?

- Stop by the INL booth

- Contact us at:

cycote@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.

WWW.INL.GOV