BUILDING INNOVATION
Emerging Technologies Series

Digital Twins and Cybersecurity for Public Facilities

Prof. Carrie Sturts Dossick, P.E.

University of Washington

Agenda

- Digital Twin for I-90 Bridge Monitoring
- Cybersecurity Roadmap

UW ACADEMIC TEAM

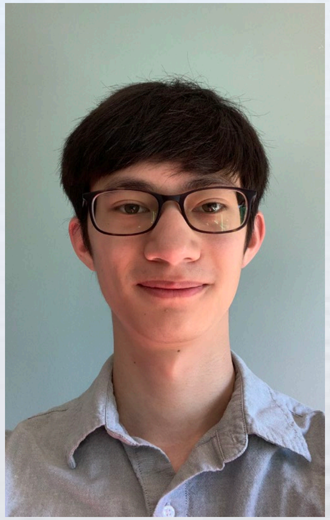
Dr. Travis Thonstad

Dr. Michael Motley

Dr. Carrie Sturts Dossick, P.E.

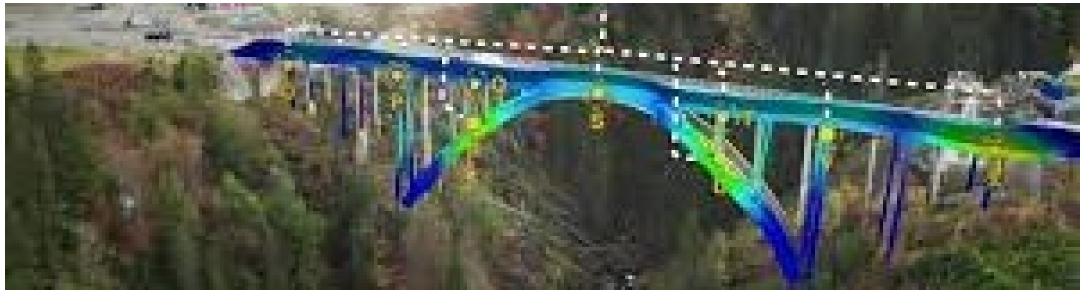
Bart Treece, PTP

Ori Borjigin, PhD Student



Timothy Bernard, MS Student

INNOVATION AND PARTNERSHIPS



WSDOT

CHALLENGE SEATTLE

Bentley®

Microsoft Azure

T Mobile®

SIERRA WIRELESS IS NOW SEMTECH®

WSP

CIVIL & ENVIRONMENTAL ENGINEERING
UNIVERSITY of WASHINGTON
College of Engineering

eScience Institute
ADVANCING DATA-INTENSIVE DISCOVERY IN ALL FIELDS

COLLEGE OF BUILT ENVIRONMENTS
UNIVERSITY of WASHINGTON

U.S. Department of Transportation
Federal Highway Administration

ABC UTC IBT

MOBILITY INNOVATION CENTER at the UNIVERSITY of WASHINGTON

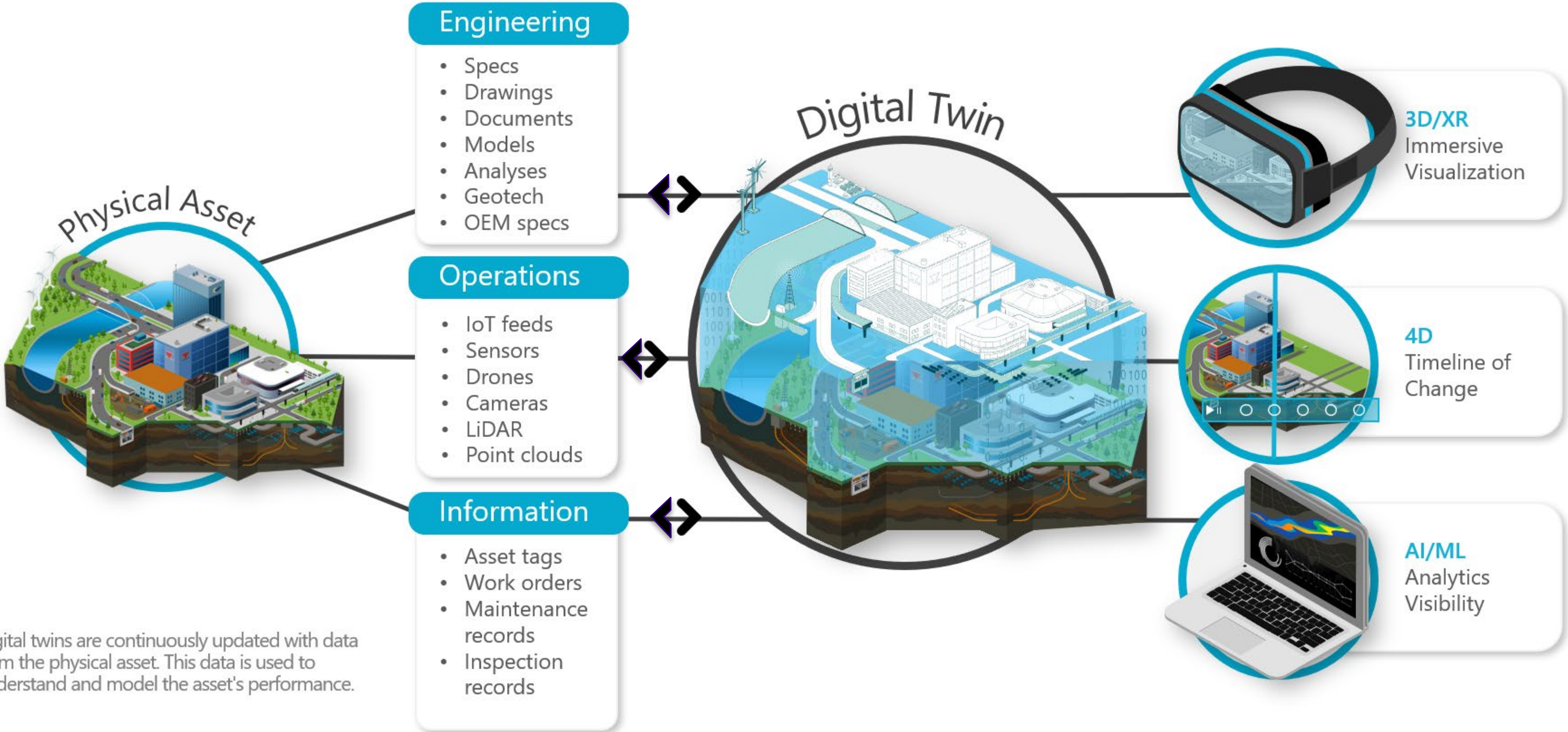
STIC
State Transportation Innovation Councils

What is a Digital Twin?

"digital equivalent to a physical product"

Landed on Mars August 5, 2012

Digital Twins for Buildings and Infrastructure



Digital twins are continuously updated with data from the physical asset. This data is used to understand and model the asset's performance.

I-90 Project

"Proof-of-technology" project

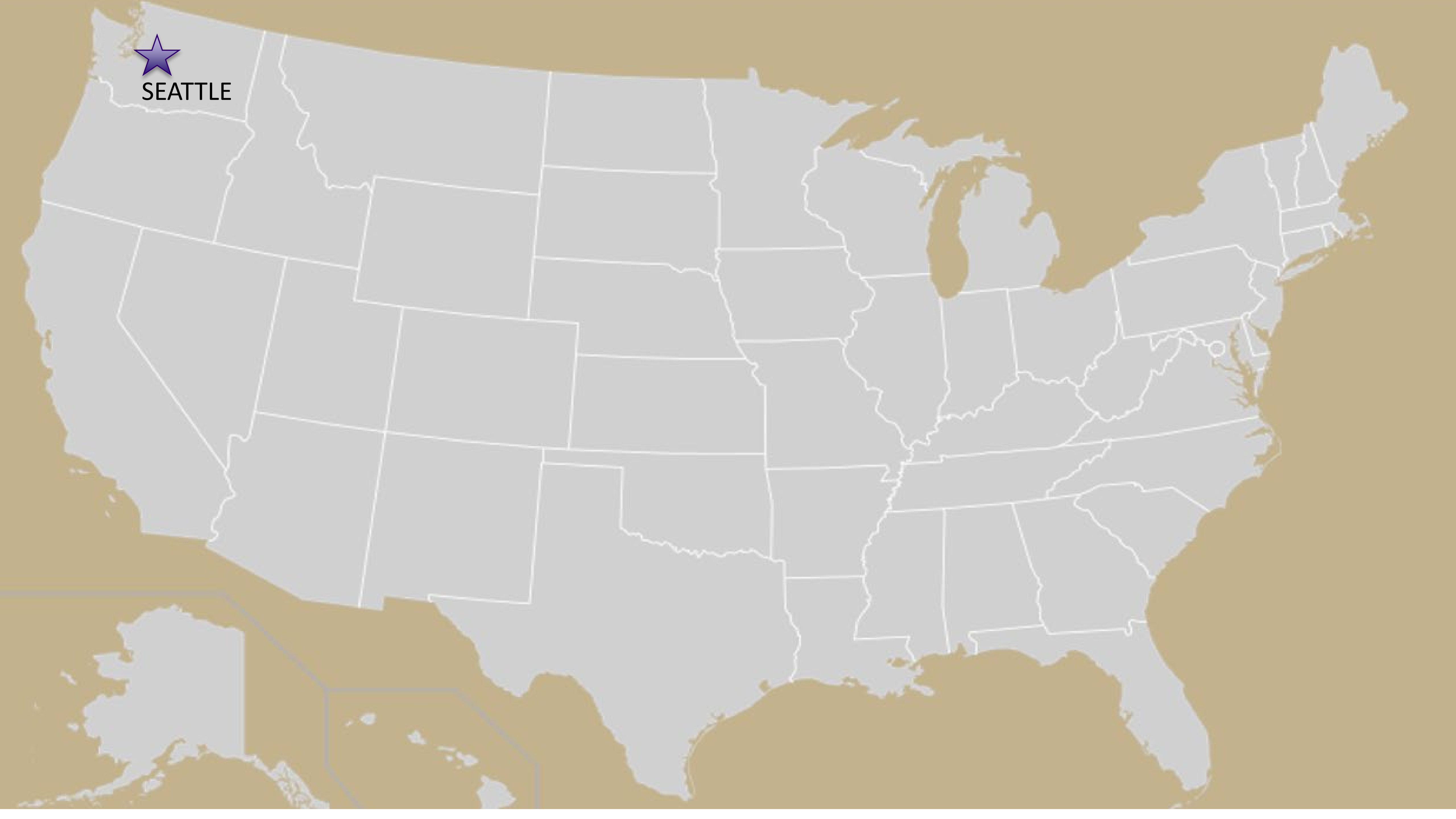
Evaluate the benefits, limitations, and tradeoffs that an agency or agencies could expect when using similar technologies for asset management, maintenance, and operations

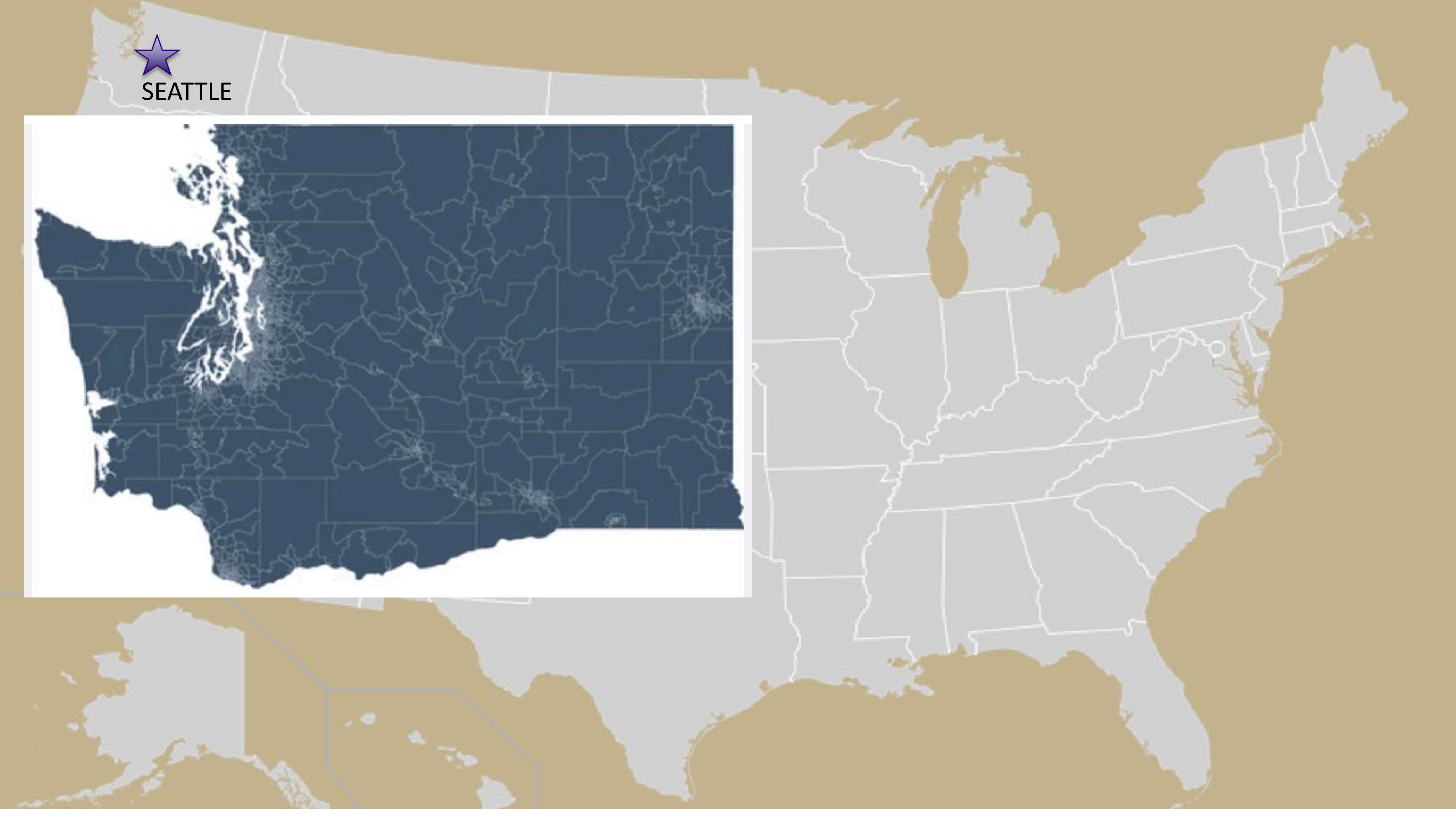
- Location and utility of IoT sensor types
- Ease of data retrieval and interpretation
- Integration of disparate data streams
- Ability to draw inferences for maintenance and operations decisions

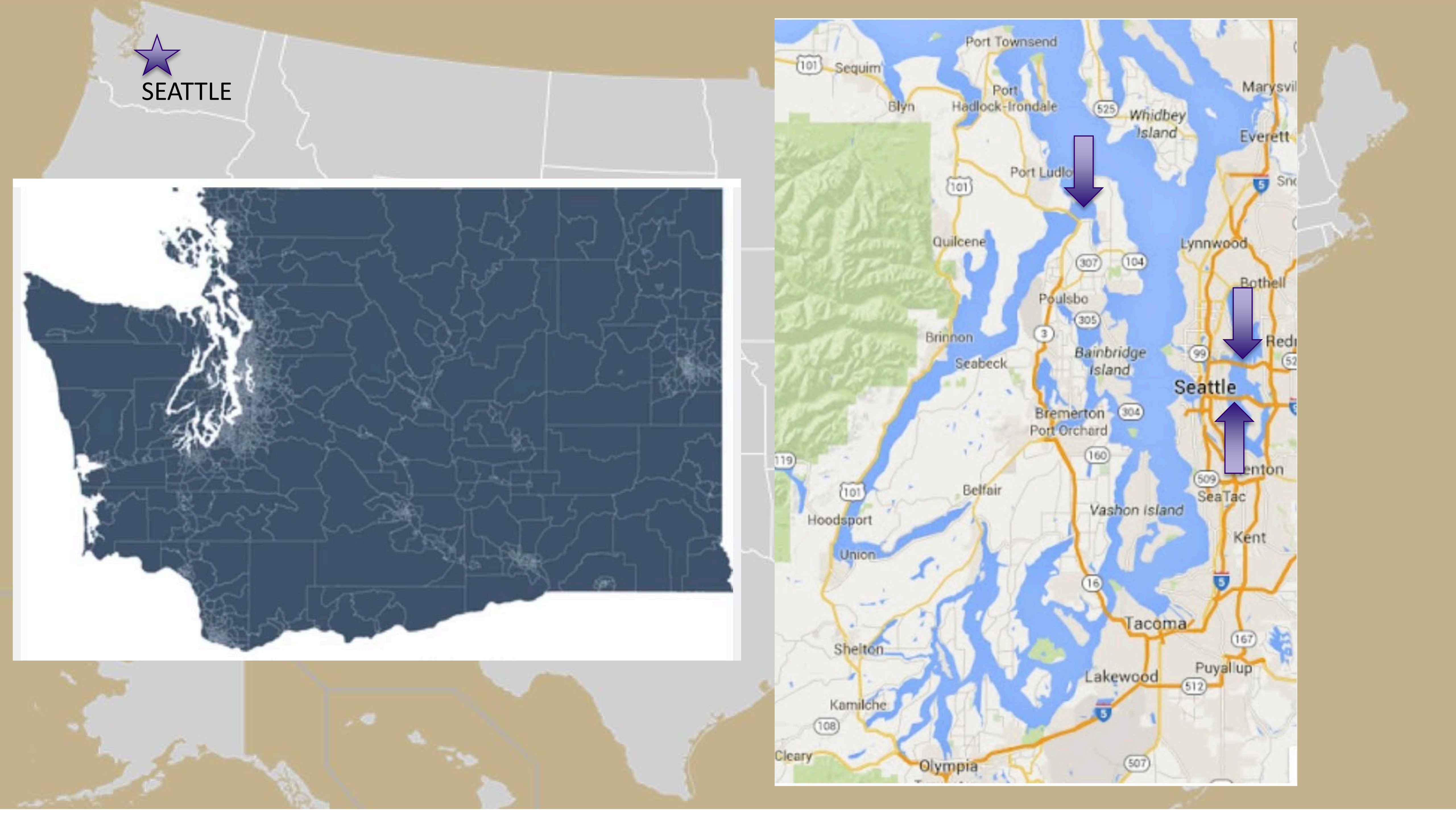
100 YEARS OF PIONEERING INNOVATION IN WASHINGTON STATE (4 of 20 floating bridges)

- **1921** – Idea for a concrete pontoon bridge first proposed, ridiculed as "Hadleys' Folly"
- **1940** – Lacey V. Murrow Floating Bridge (rebuilt in 1993)
- **1961** – Hood Canal Floating Bridge (rebuilt in 1982)
- **1963** – Evergreen Point Floating Bridge (SR520)
- **1989** – Homer M. Hadley Floating Bridge (I-90)
- **2016** – New Evergreen Point Floating Bridge (SR520)

Homer Hadley (1885-1967)
Mercer Island Historical Society
© 2001


SEATTLE

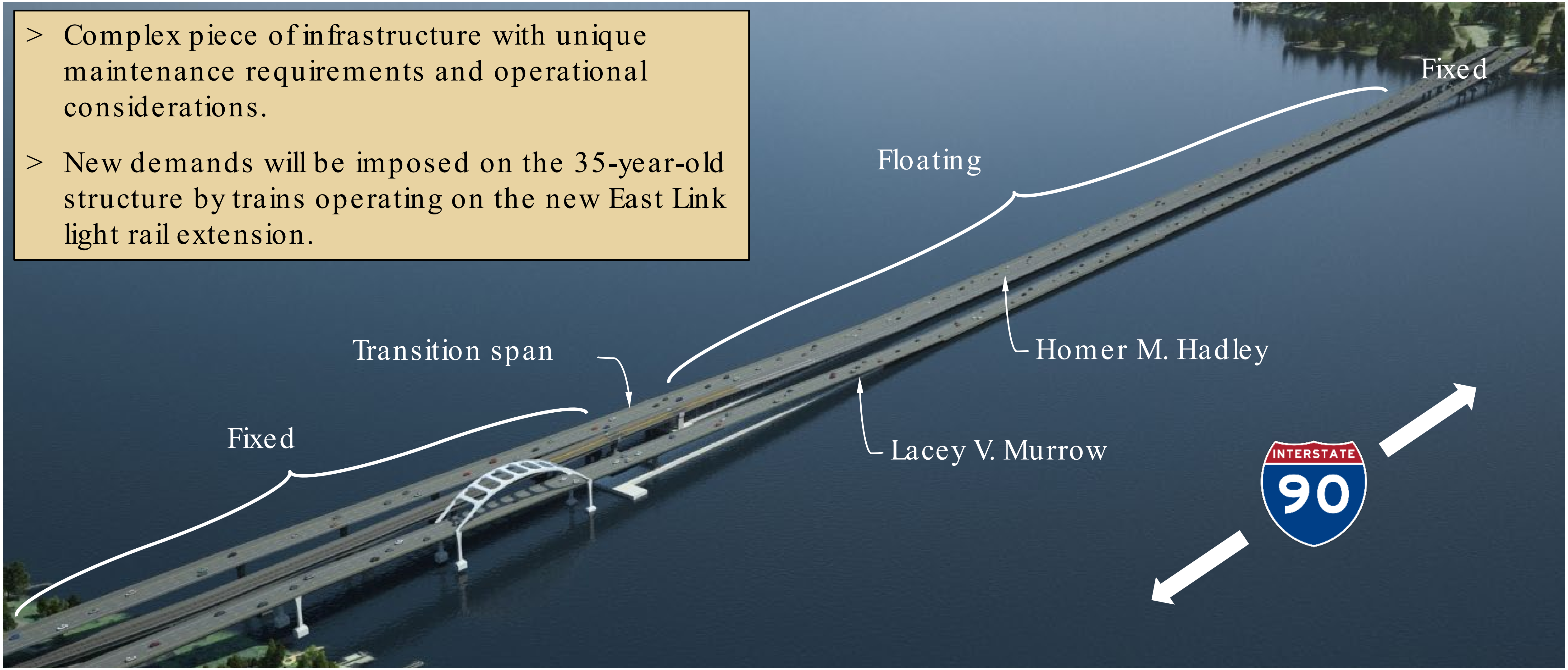

SEATTLE


SEATTLE
Port Townsend
Sequim
Port Hadlock-Irondale
Blyn
Whidbey Island
Marysvil
Everett
Port Ludlo
Quilcene
Lynnwood
Bothell
Poulsbo
Brinnon
Seabeck
Bainbridge Island
Redr
Seattle
Bremerton
Port Orchard
Renton
SeaTac
Belfair
Vashon Island
Hoodsport
Kent
Union
Tacoma
Shelton
Lakewood
Puyallup
Kamilche
Cleary
Olympia

HOMER M. HADLEY MEMORIAL BRIDGE

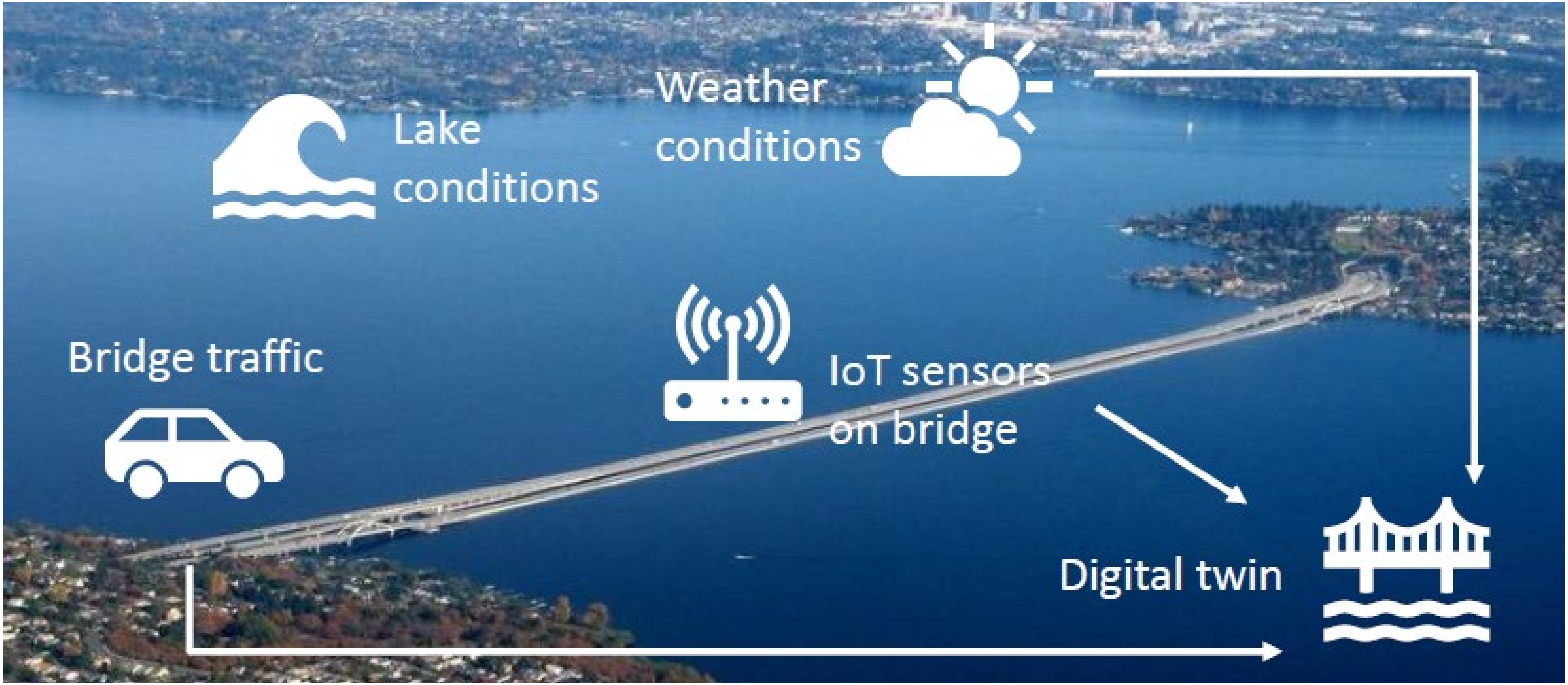
> Complex piece of infrastructure with unique maintenance requirements and operational considerations.

> New demands will be imposed on the 35-year-old structure by trains operating on the new East Link light rail extension.



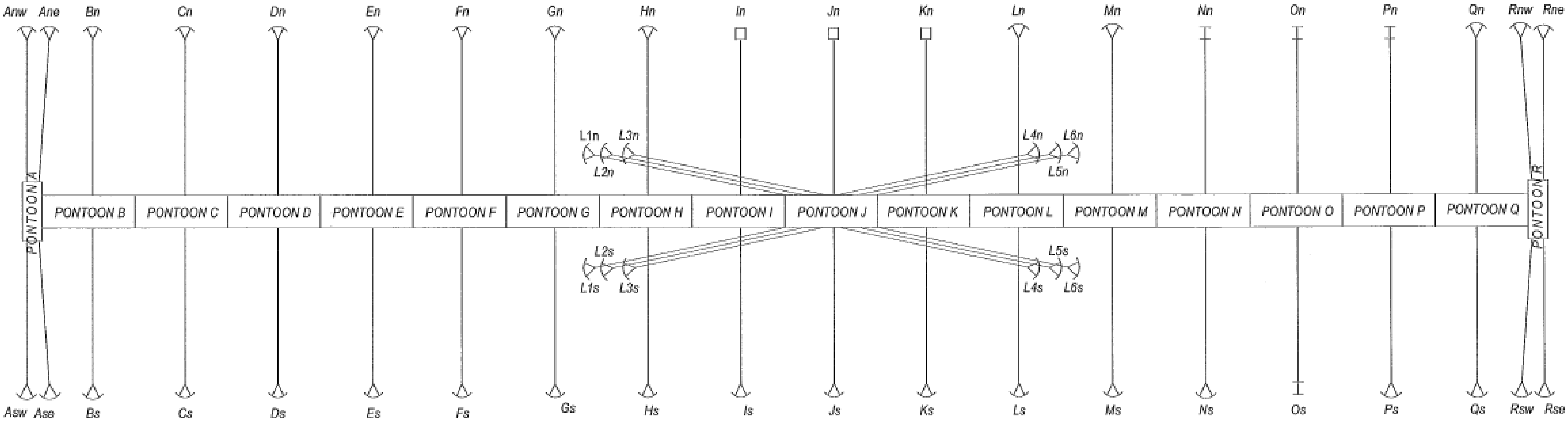
Courtesy: WSP USA

DIGITAL TWIN TECHNOLOGY



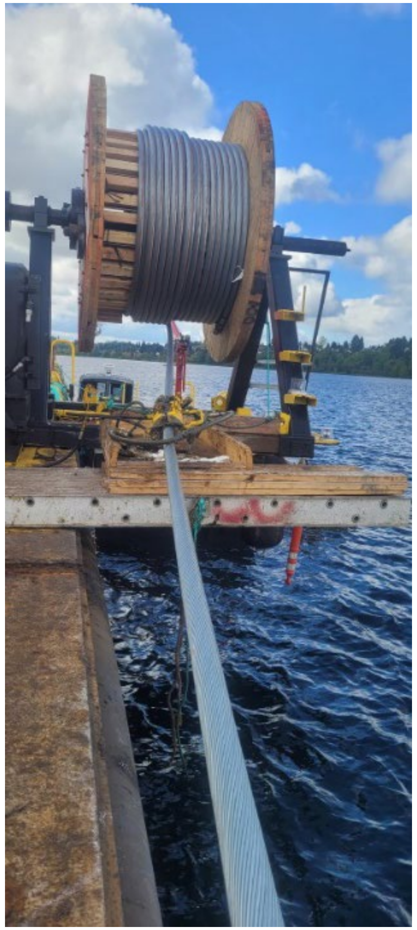
HOMER M. HADLEY MEMORIAL BRIDGE

Floating portion of bridge restrained by 52 anchor cables



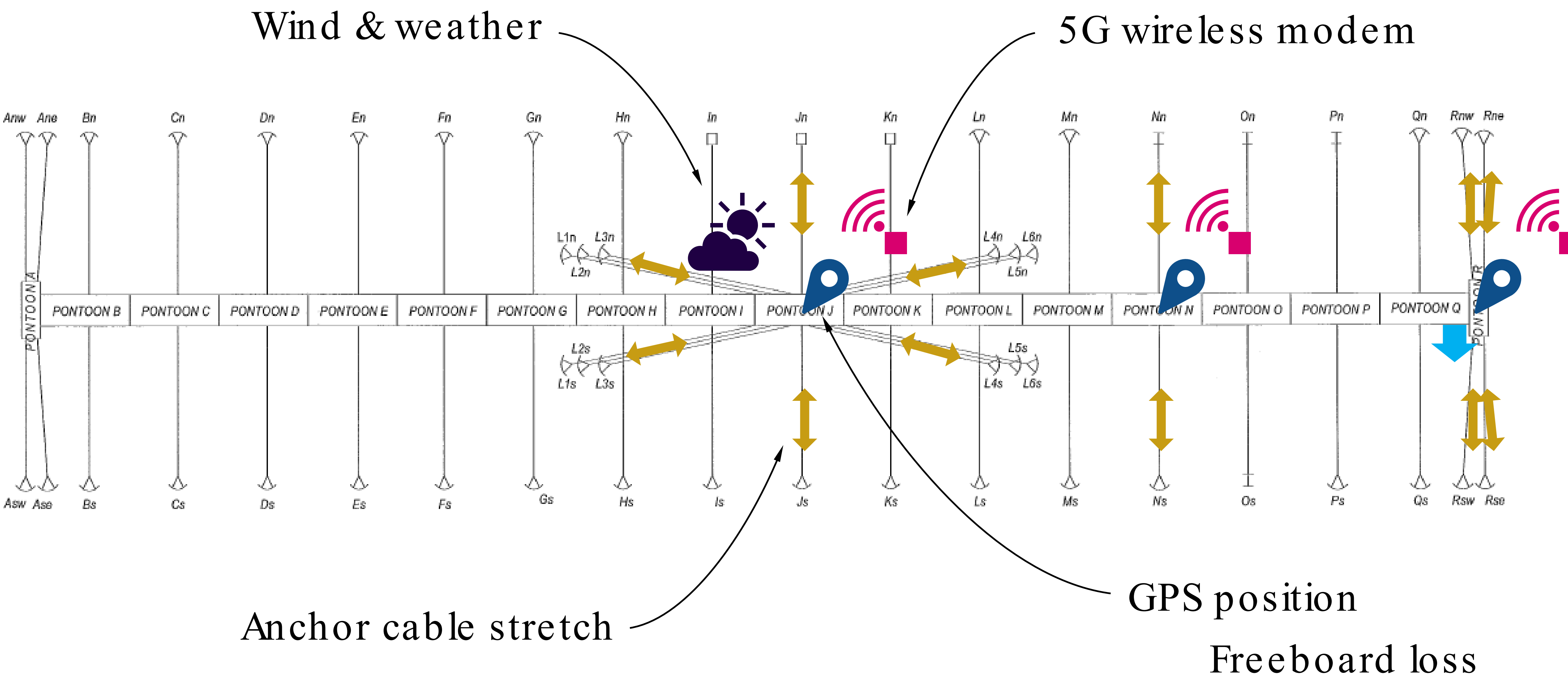
ASSET MANAGEMENT – ANCHOR CABLE REPLACEMENT

In 2022, 38 anchor cables were replaced at a cost of ~$9 million

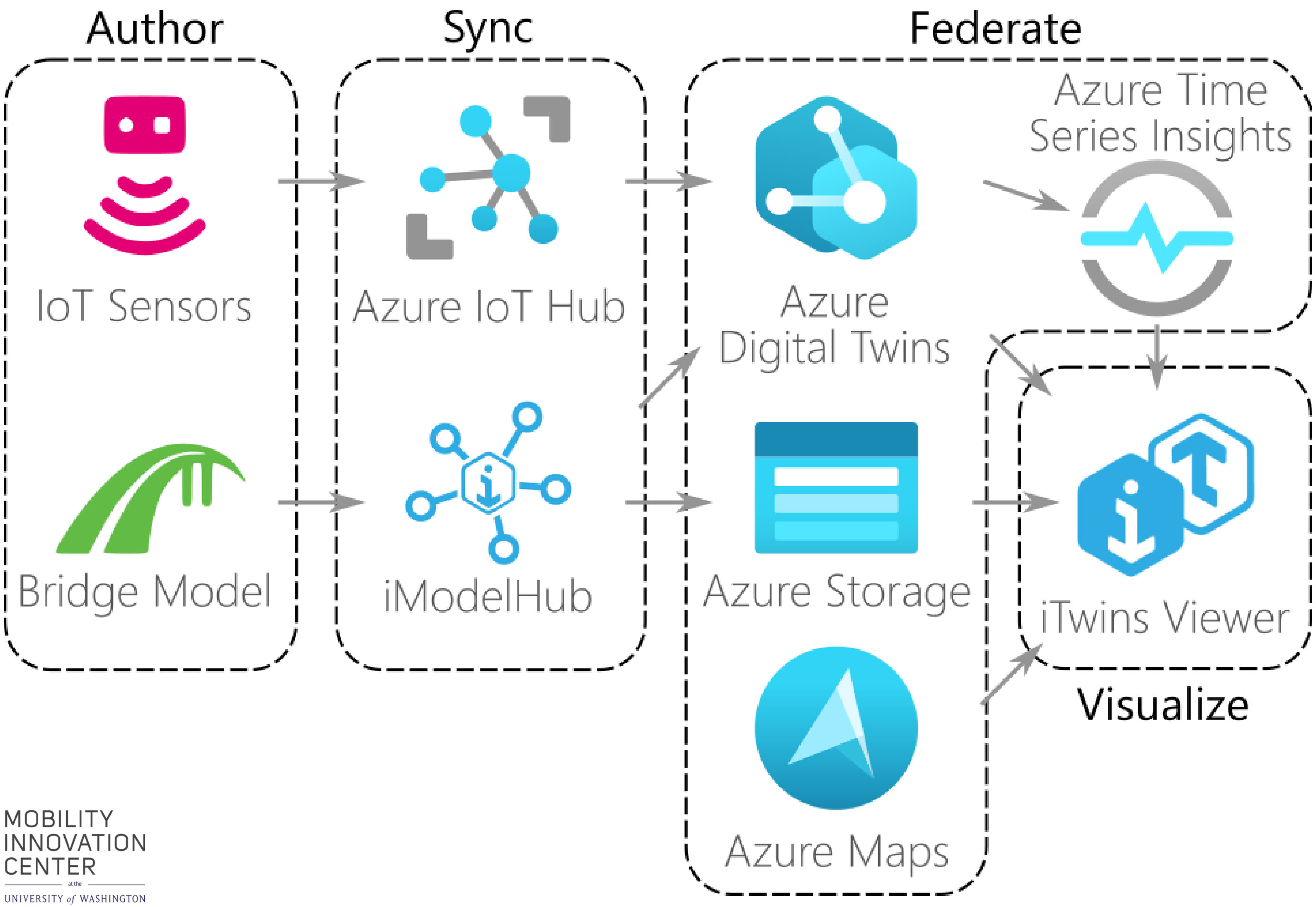


Photos courtesy of WSDOT

MEASUREMENT LOCATIONS



I-90 Twin Preliminary Project Architecture



MOBILITY INNOVATION CENTER at the UNIVERSITY of WASHINGTON

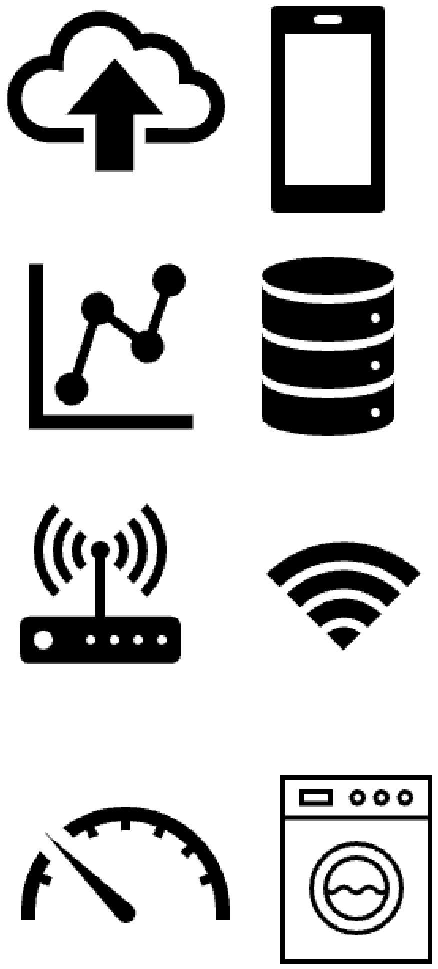
Digital Twin Architecture, Cybersecurity Risks & Attack Surfaces

Application layer
- Cloud/server, smart application, analytics management, archive

Data processing layer
- Edge IT, data pre-processing, analytics

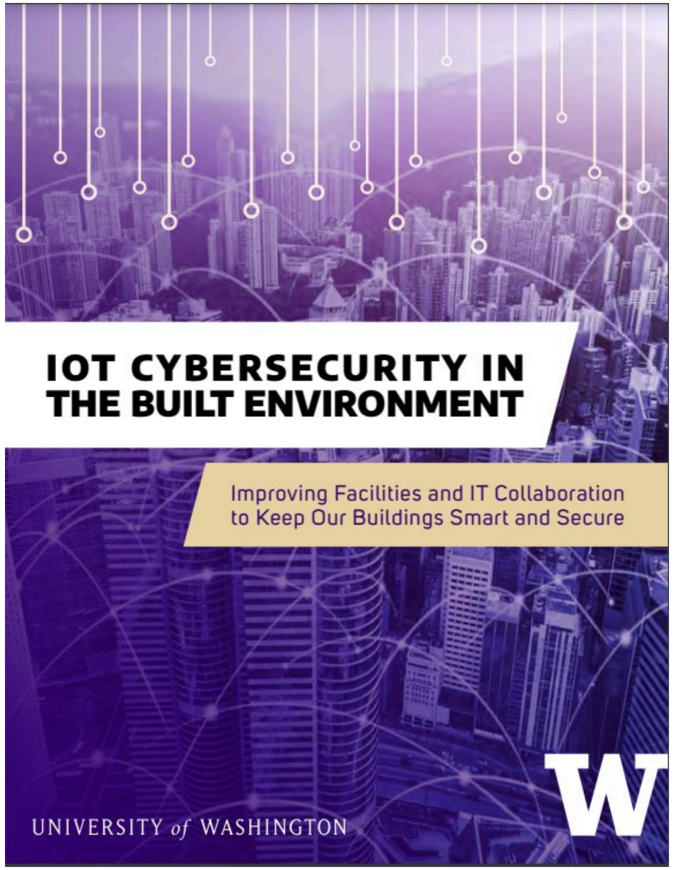
Network layer
- Routers/gateways/data acquisition

Perception layer
- Sensors/actuators on devices, machines, people, tools

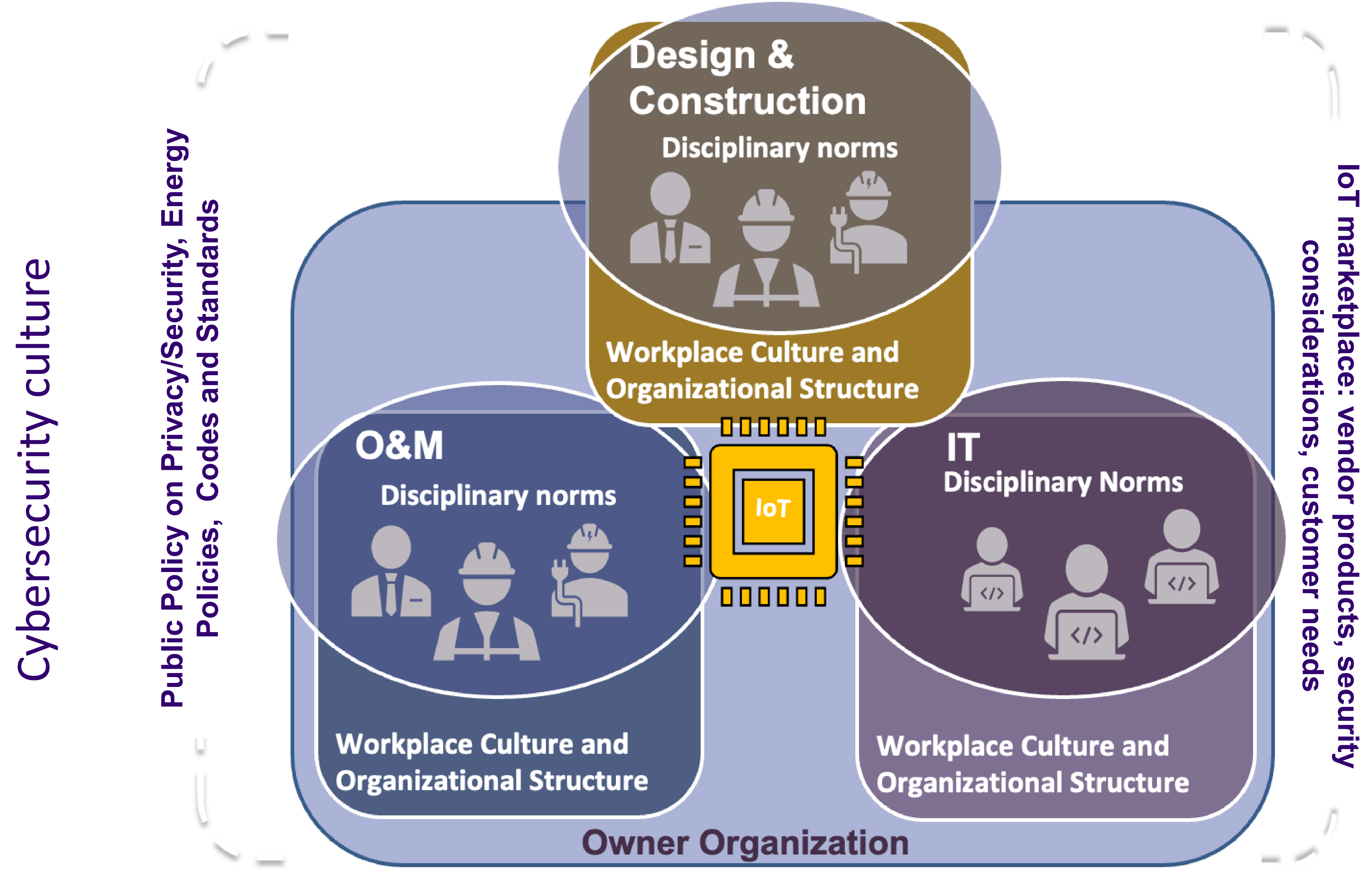


Roadmap for Infrastructure

Need for a Washington State Transportation Cybersecurity Roadmap



http://cyber.be.uw.edu

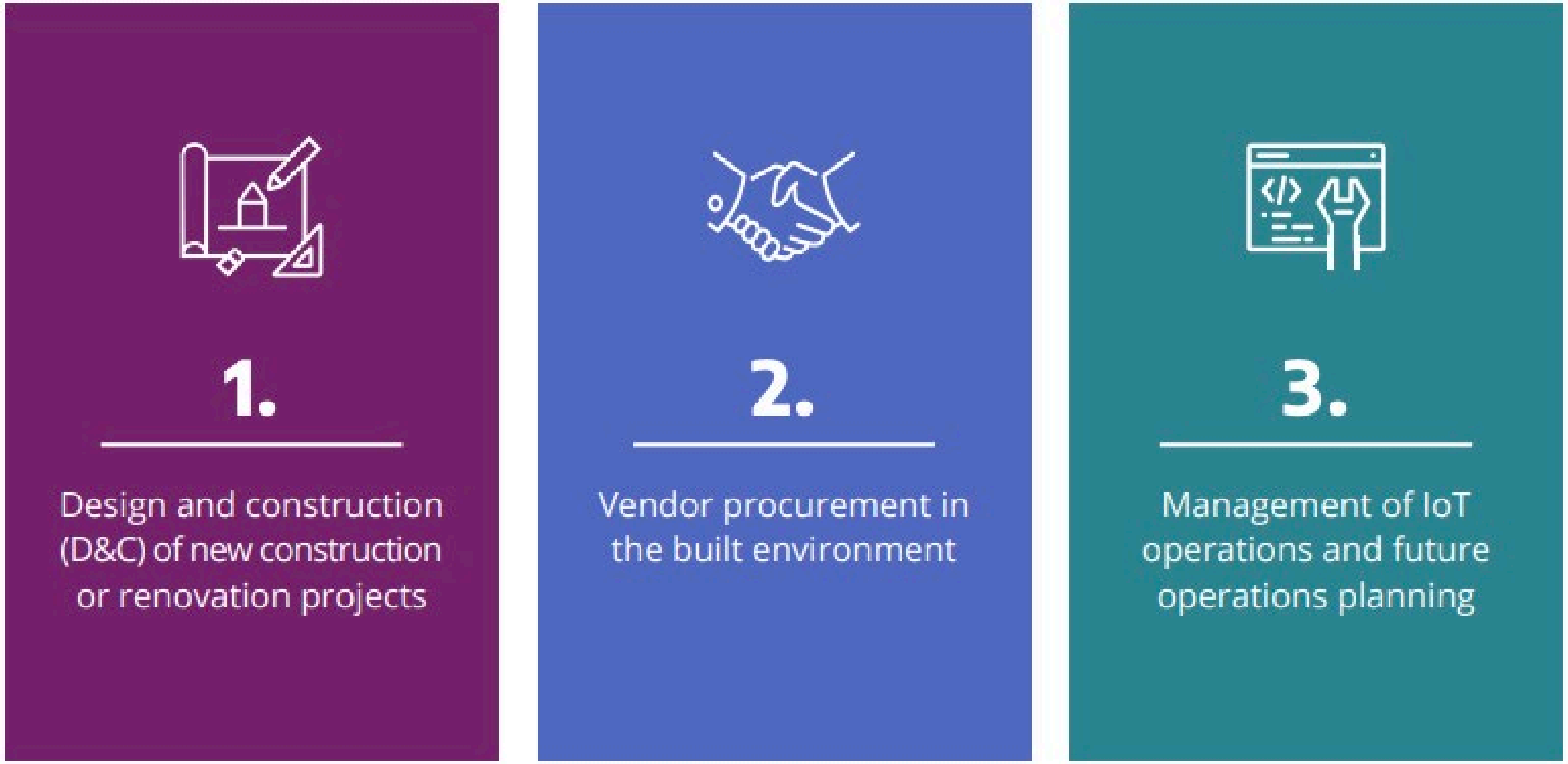

Cybersecurity culture
Public Policy on Privacy/Security, Energy Policies, Codes and Standards
Design & Construction
Disciplinary norms
Workplace Culture and Organizational Structure
O&M
Disciplinary norms
Workplace Culture and Organizational Structure
IoT
IT
Disciplinary Norms
</>
Workplace Culture and Organizational Structure
Owner Organization
IoT marketplace: vendor products, security considerations, customer needs

Cybersecurity Risks

		OT	IoT Risks	IT
Technological	Purpose	Control/manage physical devices	Potential disruptions; data vulnerabilities	Manage information
Technological	Connectivity	Often stand-alone applications	Connectivity creates risk that can disrupt OT and IT	Interconnected (applications)
Technological	Architecture	Often closed, proprietary, task specific	Bad actors can reprogram many devices	Frequently more open, standards based
Technological	Life Span	Long (10 - 20 years)	May not be patched; disruptive upgrades	Frequent, systematic patches and upgrades
	Discipline	Engineering, skilled trades	Different terminologies and siloed practices	Computer science
	Governance	O&M, engineers, technicians	Unclear responsibility when systems overlap	IT department
Organizational	Technical Knowledge	Many workers only know older technology	Few have IT and O&M skillsets needed for IoT	Emphasis on keeping up with latest technology
Organizational	Practice	Interventions not required daily	Different views on how and when to support IoT	Needs daily human and automated support
Organizational	Culture	Maintaining/managing physical processes	Difficulties aligning agendas/needs for IoT	Maintaining and securing information
Organizational	Policy Expertise	Building codes and standards	Lack of expertise on laws that impact IoT	Data security and privacy laws

Table 1: How technological and organizational differences in IT and OT systems impact IoT risk

ROADMAP NEEDS TO ADDRESS CHALLENGES, STRATEGIES, AND RECOMMENDATIONS



Note: this research was funded by the National Science Foundation (NSF #1932769) SaTC: CORE: Medium: Knowledge Work and Coordination to Improve O&M and IT Collaboration to keep our Buildings Smart AND Secure.

Roadmap needs to address

1.

Design and construction (D&C) of new construction or renovation projects

CHALLENGES

IT AND FACILITIES MANAGEMENT COLLABORATION

Roadmap needs to address

1.

Design and construction (D&C) of new construction or renovation projects

CHALLENGES

IT AND FACILITIES MANAGEMENT COLLABORATION

STRATEGIES

CONSULT CYBERSECURITY AND FACILITIES PROFESSIONALS IN DESIGN REVIEW AND DECISION-MAKING

ESTABLISH PROCUREMENT VETTING COMMITTEES

Roadmap needs to address

1.

Design and construction (D&C) of new construction or renovation projects

CHALLENGES

IT AND FACILITIES MANAGEMENT COLLABORATION

STRATEGIES

CONSULT CYBERSECURITY AND FACILITIES PROFESSIONALS IN DESIGN REVIEW AND DECISION-MAKING

ESTABLISH PROCUREMENT VETTING COMMITTEES

RECOMMENDATIONS

IDENIFY IOT STAKEHOLDERS ACROSS THE LIFE CYCLE

UNDERSTAND IOT STAKEHOLDERS' NEEDS AND VALUES

ESTABLISH PROCESSES FOR STAKEHOLDER INPUT

Roadmap needs to address

2.

Vendor procurement in the built environment

CHALLENGES

LACK OF CLEAR OWNER CYBERSECURITY CRITERIA AND STANDARDS FOR PROCUREMENT PROCESSES, DATA GOVERNMENT, AND ROLES AND RESPONSIBILITIES

Roadmap needs to address

2.

Vendor procurement in the built environment

CHALLENGES

LACK OF CLEAR OWNER CYBERSECURITY CRITERIA AND STANDARDS FOR PROCUREMENT PROCESSES, DATA GOVERNMENT, AND ROLES AND RESPONSIBILITIES

STRATEGIES

CREATE CLEAR OWNER CYBERSECURITY CRITERIA AND STANDARDS

INTEGRATE IT EXPERTS INTO PROCUREMENT TEAMS

Roadmap needs to address

2.

Vendor procurement in the built environment

CHALLENGES

LACK OF CLEAR OWNER CYBERSECURITY CRITERIA AND STANDARDS FOR PROCUREMENT PROCESSES, DATA GOVERNMENT, AND ROLES AND RESPONSIBILITIES

STRATEGIES

CREATE CLEAR OWNER CYBERSECURITY CRITERIA AND STANDARDS

INTEGRATE IT EXPERTS INTO PROCUREMENT TEAMS

RECOMMENDATIONS

INVEST IN MANUFACTURERS WITH HIGH CYBERSECURITY STANDARDS

INTEGRATE SECURITY AND GOVERNANCE INTO CONTRACTS AND DESIGN GUIDELINES

CONDUCT CYBERSECURITY REVIEWS DURING PROCUREMENT PROCESSES

Roadmap needs to address

3.

Management of IoT operations and future operations planning

CHALLENGES

UNCLEAR NETWORK GOVERNANCE

CONFLICTS BETWEEN IT AND FACILITIES

Roadmap needs to address

3.

Management of IoT operations and future operations planning

CHALLENGES

UNCLEAR NETWORK GOVERNANCE

CONFLICTS BETWEEN IT AND FACILITIES

STRATEGIES

IT AND FACILITIES COLLABORATE TO DEFINE GOVERNANCE

ROUTINE COLLABORATION BETWEEN IT AND FACILITIES

Roadmap needs to address

3.

Management of IoT operations and future operations planning

CHALLENGES

UNCLEAR NETWORK GOVERNANCE

CONFLICTS BETWEEN IT AND FACILITIES

STRATEGIES

IT AND FACILITIES COLLABORATE TO DEFINE GOVERNANCE

ROUTINE COLLABORATION BETWEEN IT AND FACILITIES

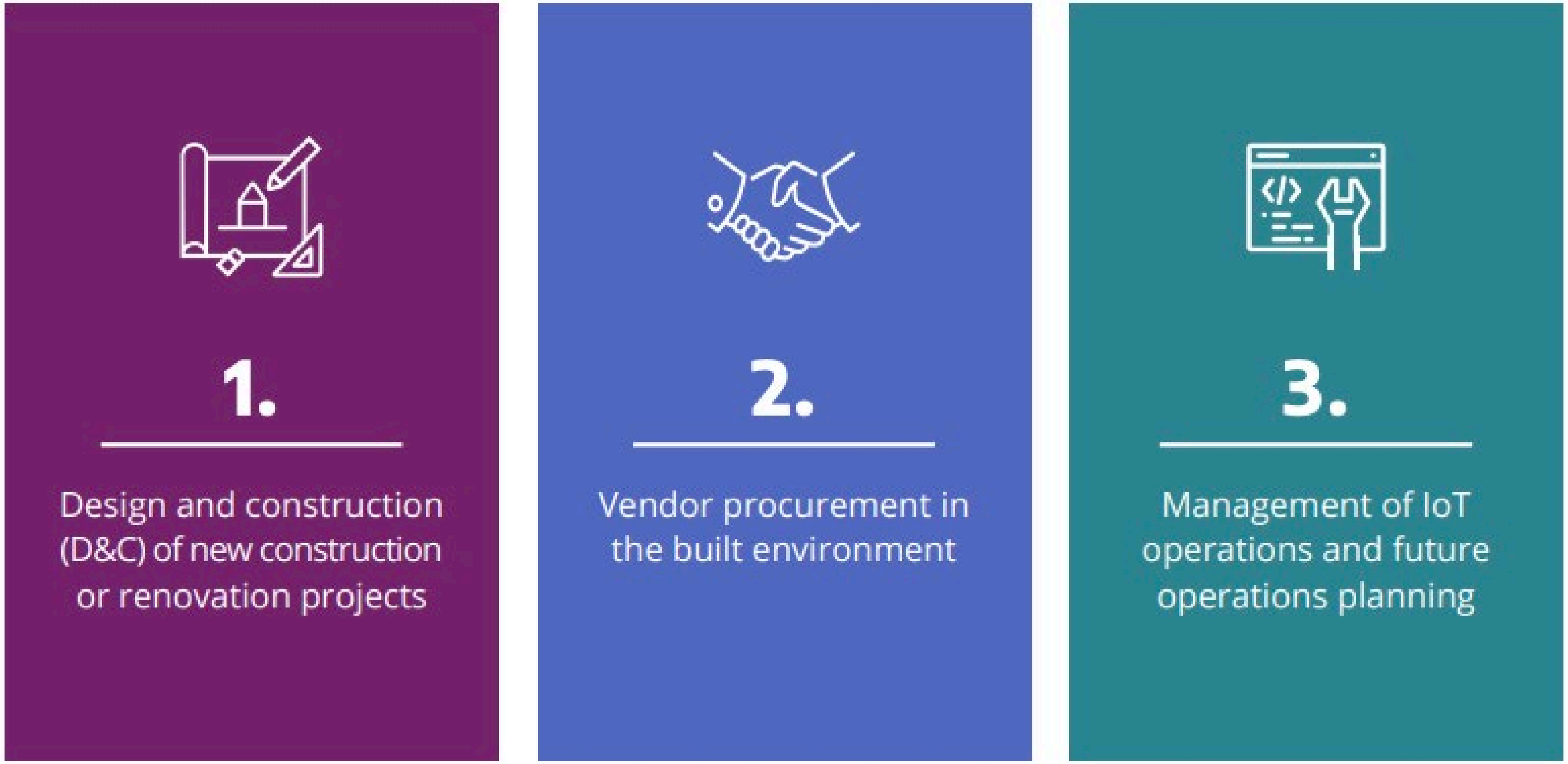
RECOMMENDATIONS

ADDRESS DISCIPLINARY DIFFERENCES BETWEEN IT AND FACILITIES MANAGEMENT

CREATE SHARED GOVERNANCE BETWEEN IT AND FACILITIES MANAGEMENT

CLARIFY ROLES AND RESPOSIBILITIES IN IOT AND DIGITAL TWIN MANAGEMENT

Roadmap needs to address
Challenges, Strategies, and Recommendations



Note: this research was funded by the National Science Foundation (NSF #1932769) SaTC: CORE: Medium: Knowledge Work and Coordination to Improve O&M and IT Collaboration to keep our Buildings Smart AND Secure.

Thank you!

PROJECT LEAD

Bart Treece

Btreece@uw.edu

Carrie Sturts Dossick

Cdossick@uw.edu

MOBILITY INNOVATION CENTER at the UNIVERSITY of WASHINGTON

Department of Construction Management, College of Built Environment