Applying Agile to Large-Scale Safety-Critical, Cyber-Physical Systems

Using Industrial DevOps to Solve

Robin Yeman

Introduction

Carnegie Mellon University
Software Engineering Institute

Robin Yeman

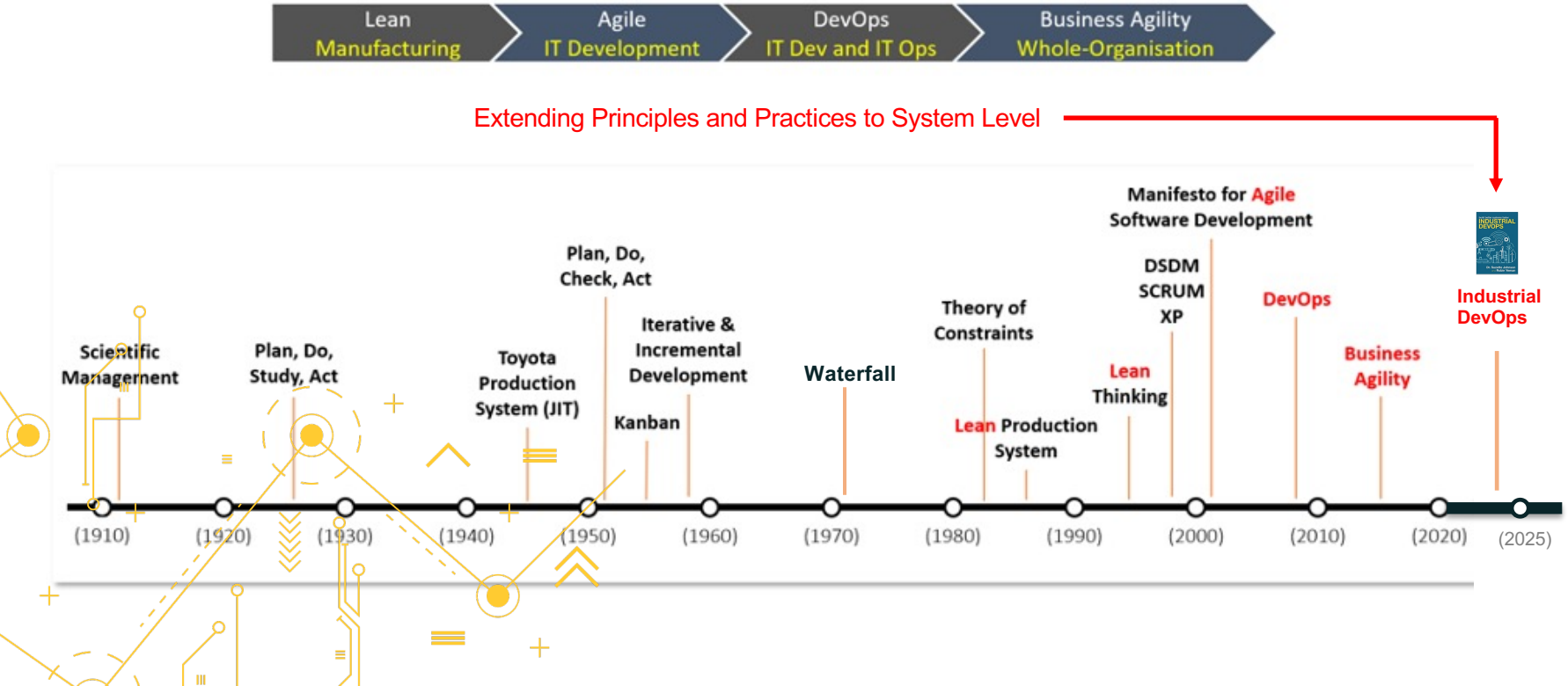
With a tenure of over twenty-eight years in the field of systems and software engineering, Robin Yeman has established herself as an expert, in the realm of the application of Agile, DevSecOps, and Digital Engineering applied across multiple domains from submarines to satellites.

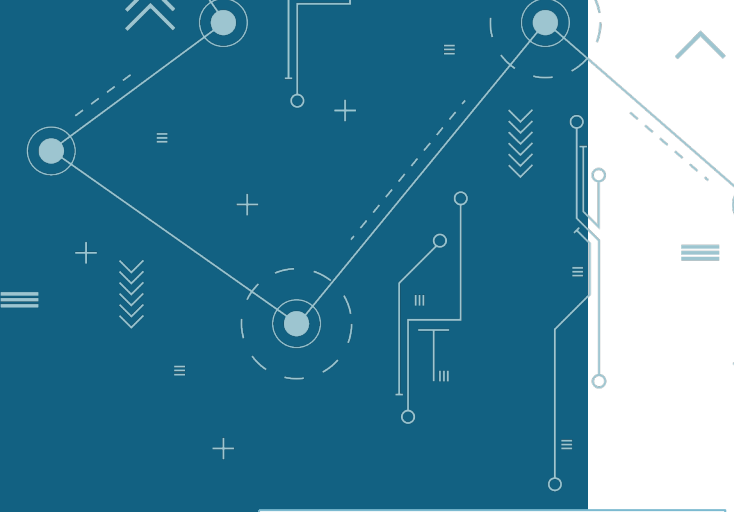
Her dedication to her craft have recently been channeled into the publication of a new book entitled "Industrial DevOps." This significant contribution to the field has been named Best DevOps book of 2023 by the DevOps Dozen community, affirming her position as a thought leader in the industry.

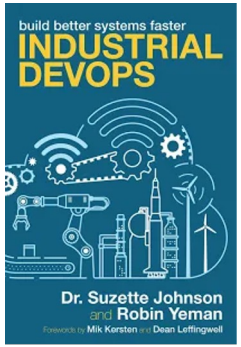
Her pioneering research is exploring the application of Agile to large-scale safety-critical cyber-physical systems to increase speed of delivery while ensuring safety and security in critical engineering systems.

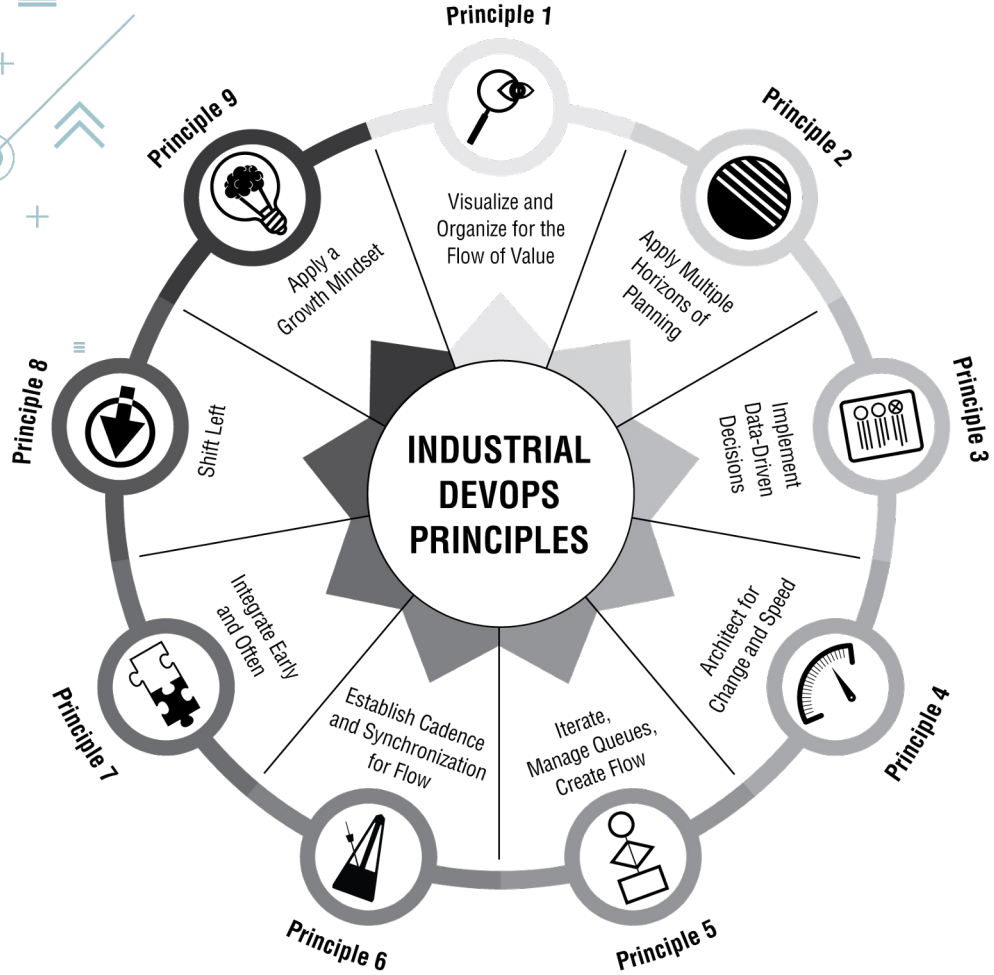
She holds multiple certifications that underscore her expertise including SAFe Fellow, SPCT (SAFe Program Consultant Trainer), CEC (Certified Enterprise Coach), PMP (Project Management Professional), PMI-ACP (PMI Agile Certified Practitioner), and CSEP (Certified Systems Engineering Professional).

Evolution


Lean
Manufacturing
Agile
IT Development
DevOps
IT Dev and IT Ops
Business Agility
Whole-Organisation
Extending Principles and Practices to System Level
Scientific Management
Plan, Do, Study, Act
Toyota Production System (JIT)
Plan, Do, Check, Act
Iterative & Incremental Development
Kanban
Waterfall
Theory of Constraints
Lean Production System
Lean Thinking
DSDM
SCRUM
XP
Manifesto for Agile Software Development
DevOps
Business Agility
Industrial DevOps
(1910)
(1920)
(1930)
(1940)
(1950)
(1960)
(1970)
(1980)
(1990)
(2000)
(2010)
(2020)
(2025)

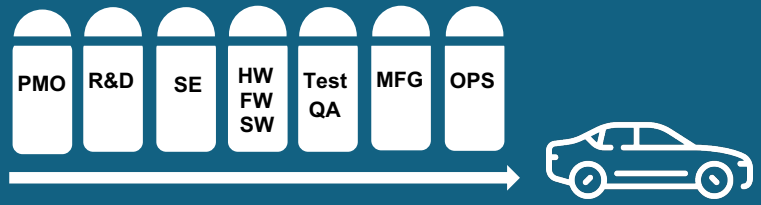



build better systems faster
INDUSTRIAL DEVOPS
Dr. Suzette Johnson
and Robin Yeman

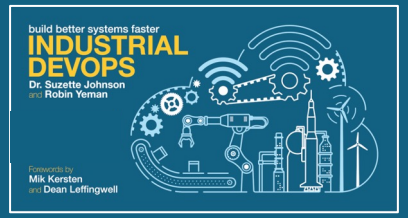

INDUSTRIAL DEVOPS PRINCIPLES
Principle 1
Visualize and Organize for the Flow of Value
Principle 2
Apply Multiple Horizons of Planning
Principle 3
Implement Data-Driven Decisions
Principle 4
Architect for Change and Speed
Principle 5
Iterate, Manage Queues, Create Flow
Principle 6
Establish Cadence and Synchronization for Flow
Principle 7
Integrate Early and Often
Principle 8
Shift Left
Principle 9
Apply a Growth Mindset

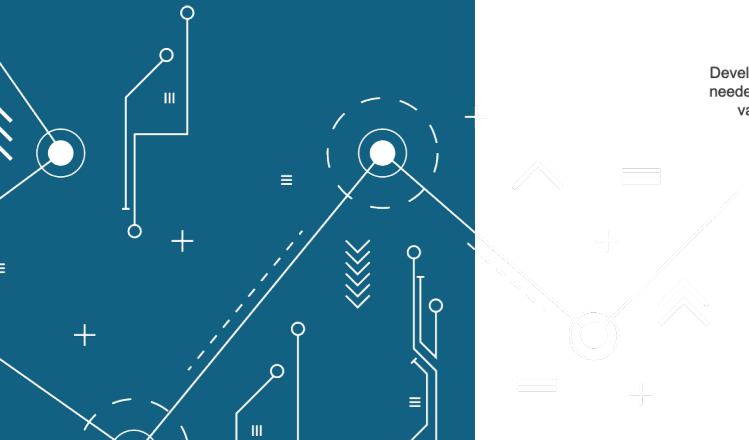
P1 Organize for the flow of value

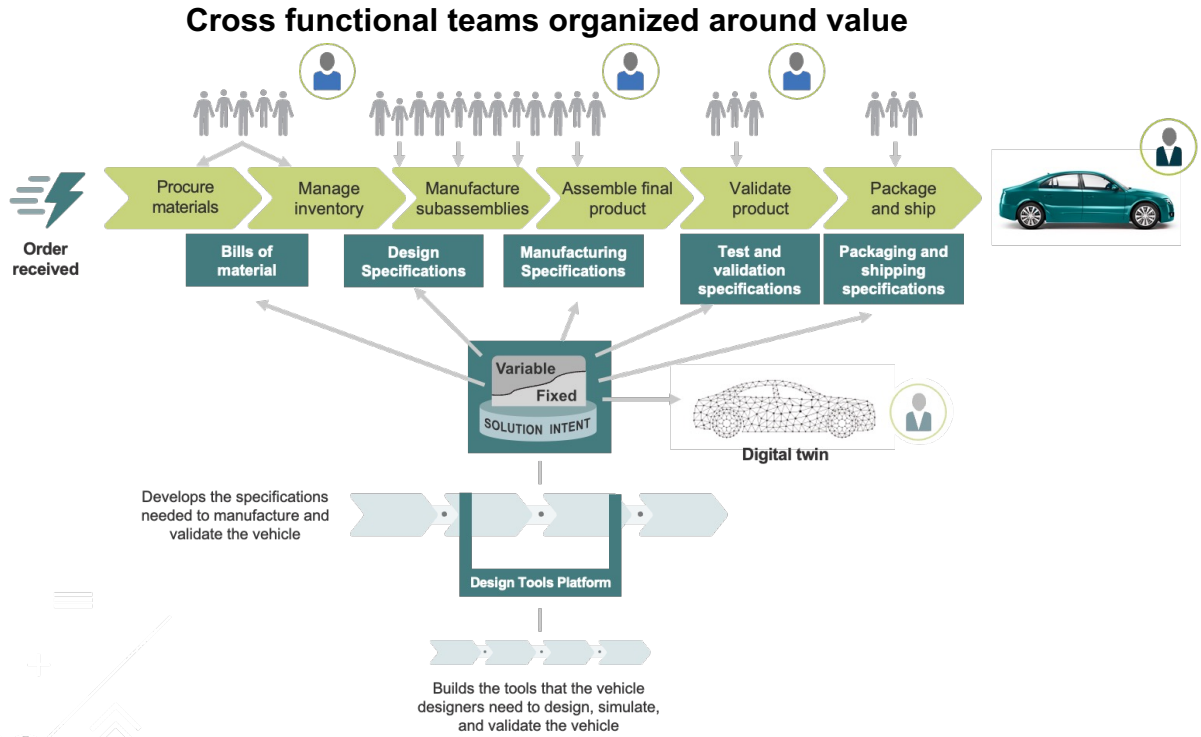
BMW plant structure is organized around a 5-finger structure to optimize flexibility, Organizing around the flow of value puts emphasis on outcomes, over outputs.



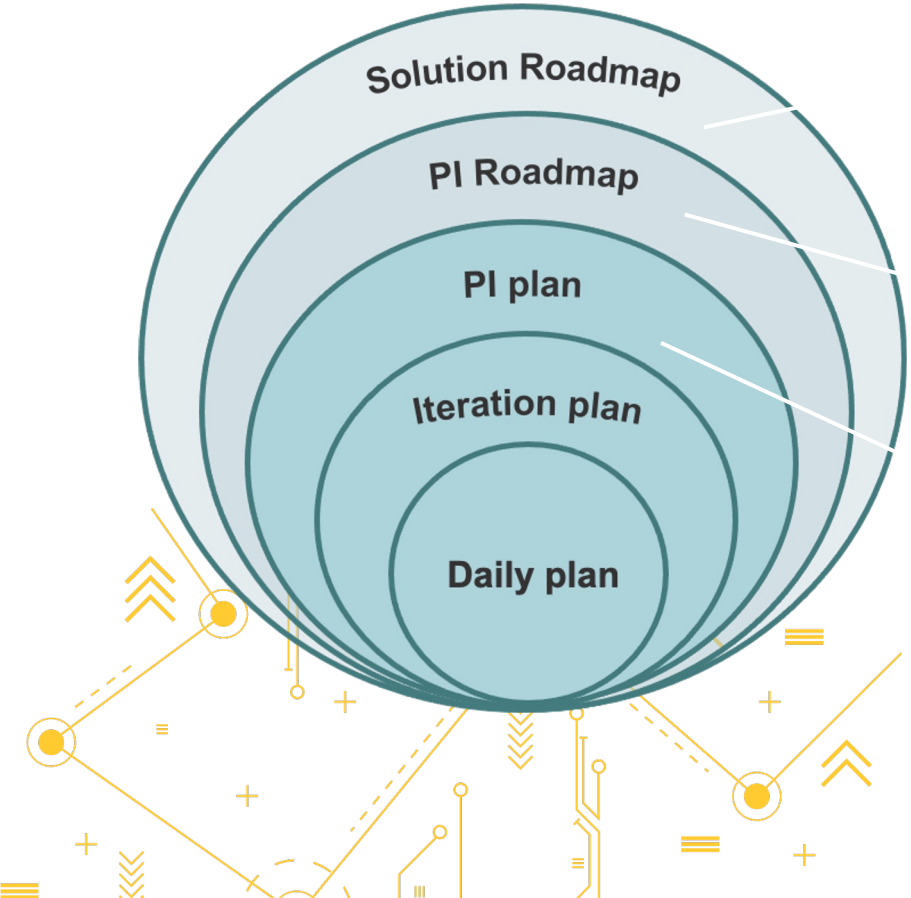
(P1) Organize Around the Flow of Value (example)



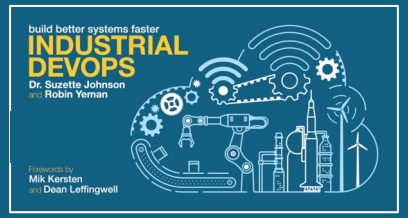




P2 Multiple Horizons of Planning

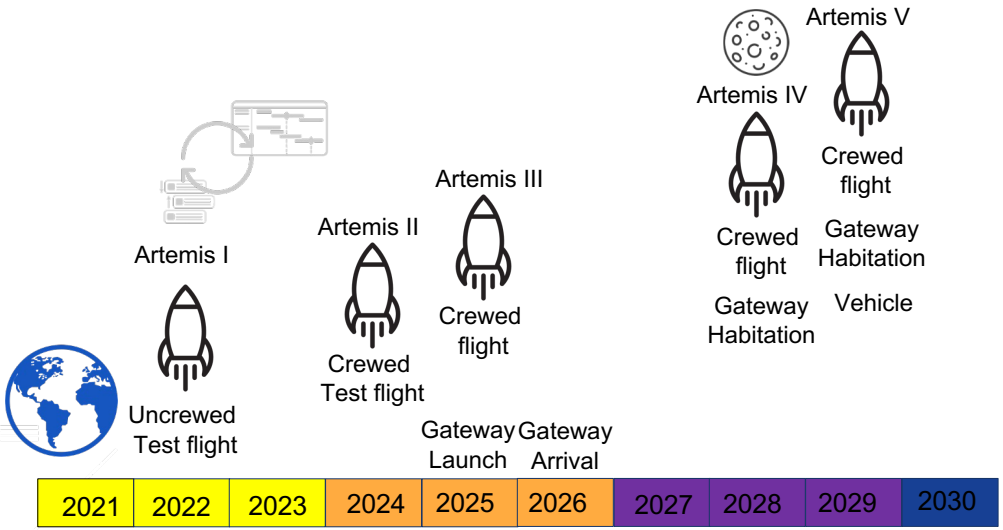


(P2) Multiple Horizons of planning (example)

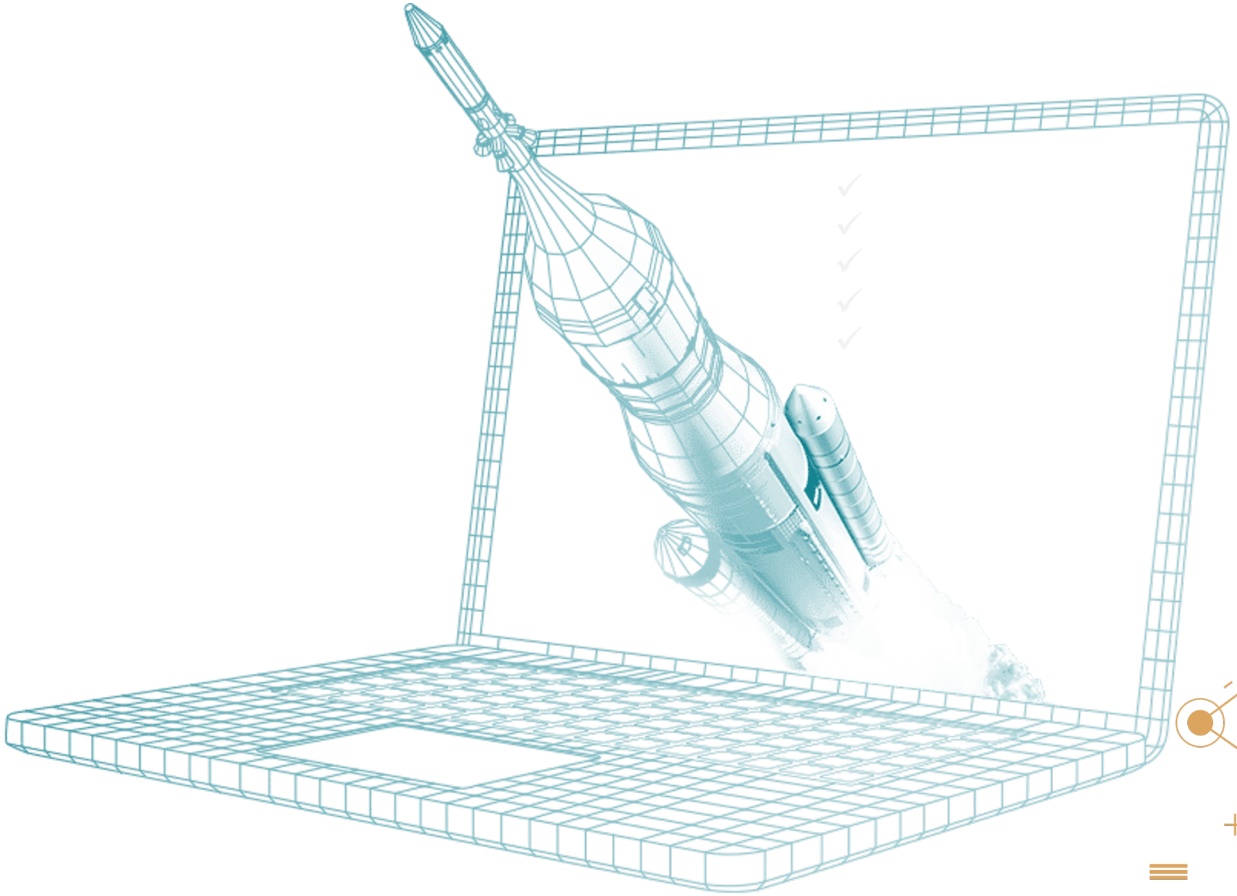


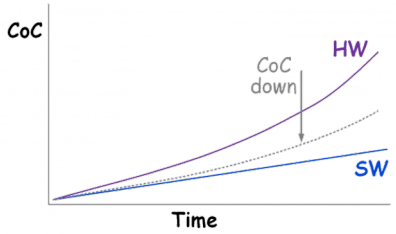
To deliver big hairy Audacious goals….

Moving from predictive planning to empirical planning requires multiple planning horizons that are regularly updated based on objective evidence.



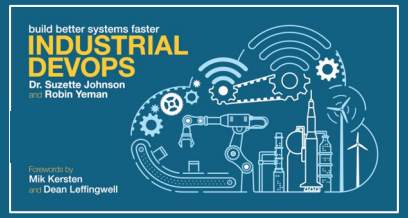
V, D. (2023, March 13). *NASA sets out new timeline for Moon and Mars missions - TLP news*. The Launch Pad. https://tlpnetwork.com/news/2023/03/nasa-sets-out-new-timeline-for-moon-and-mars-missions





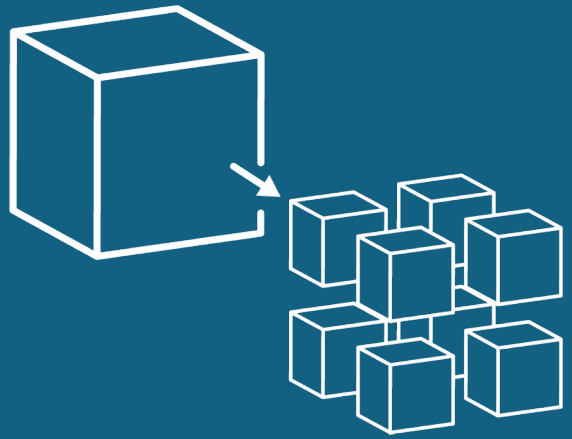
Hardware has multiple Options for fast feedback

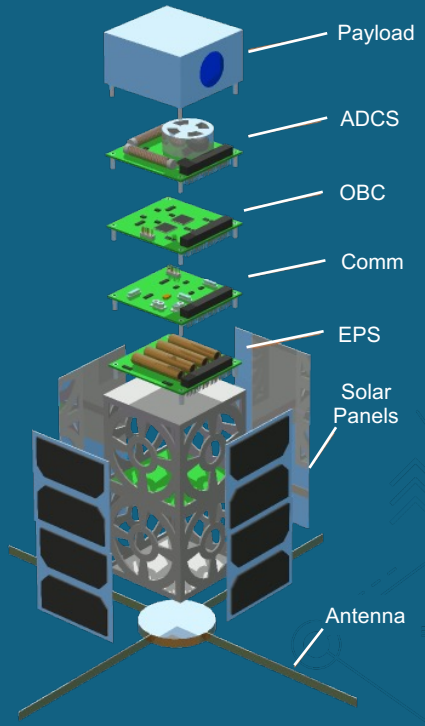
(P3) Implement Data Driven Decision (example)

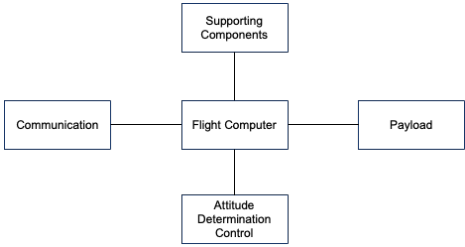


VC-25B program is now over two years behind schedule
(schedule variance for many reasons)

P4 Architect for Change and Speed

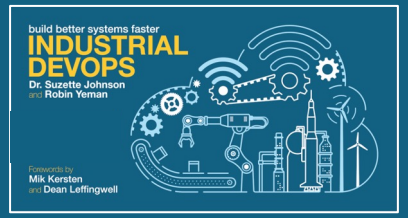




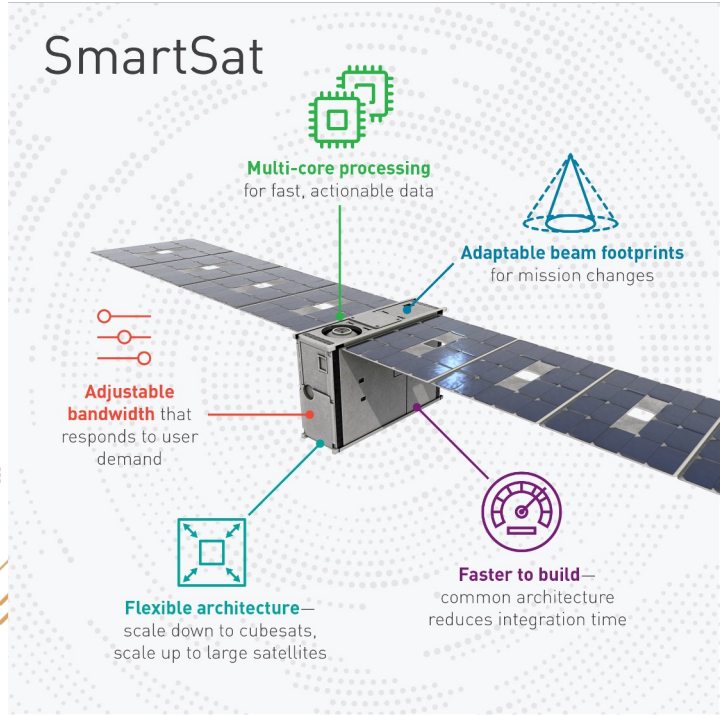


Cyber-physical systems need modular, open architecture with standardized interfaces for both software and hardware

(P4) Architect for change and speed (example)

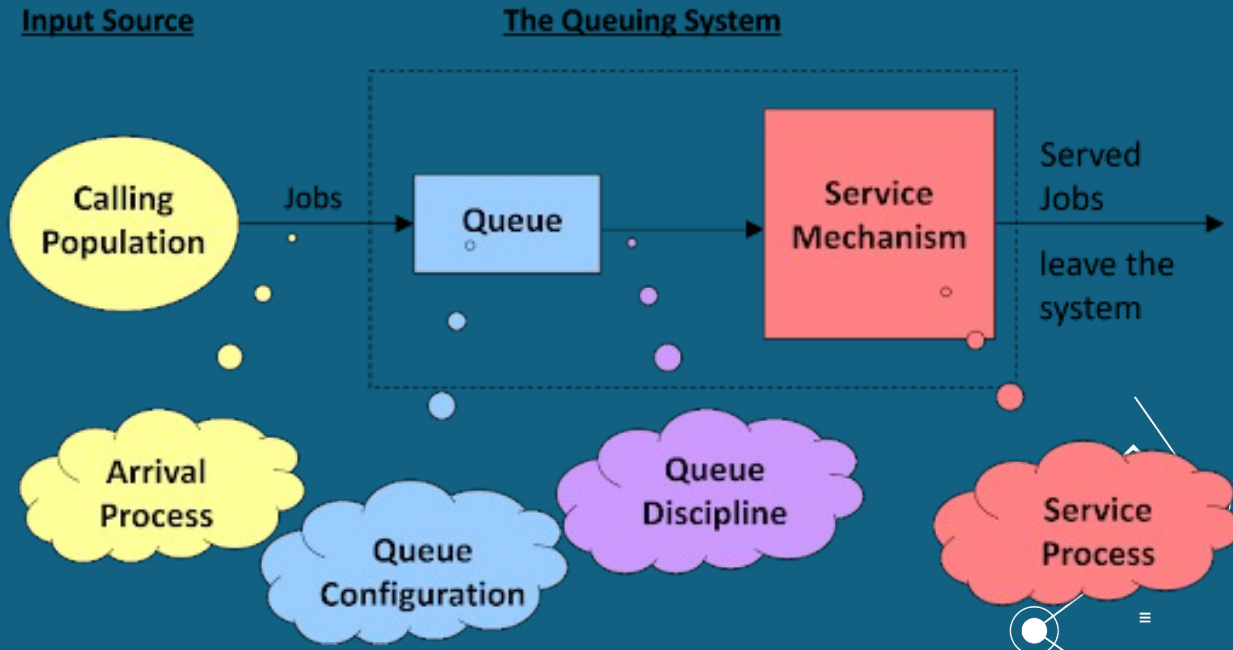


Modular, open architecture with standardized interfaces for both software and hardware



Software Defined Satellite can change its mission as easy as uploading a new mobile app!

P5 Iterate and manage queues for flow



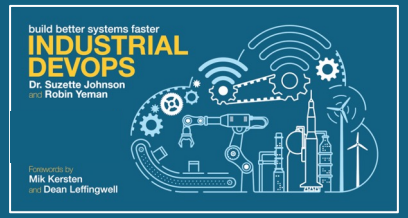
Littles Law

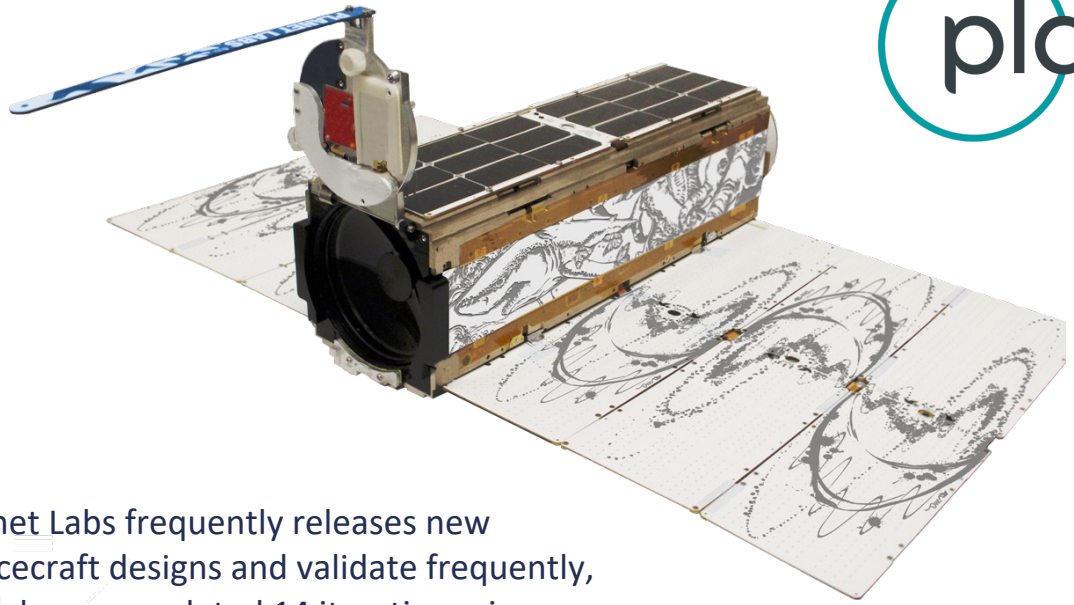
$$\text{Throughput} = \frac{\text{WIP}}{\text{Lead Time}}$$

$$\text{Lead Time} = \frac{\text{WIP}}{\text{Throughput}}$$

The more items we have in the queue, the longer it takes to deliver.

(P5) Iterate and manage queues (example)





planet.

Planet Labs frequently releases new spacecraft designs and validate frequently, they have completed 14 iterations since 2012

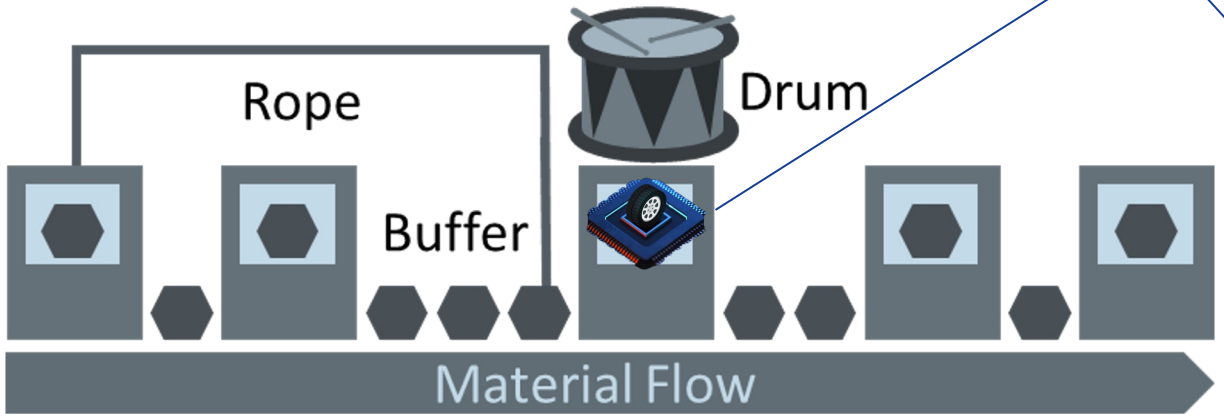
P6 Synchronization

Keeping activities in synchronized reduces waste and maximizes flow around the bottleneck.

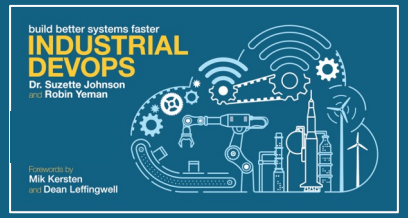
Automobile manufacturers drastically cut cadence of vehicle development to subordinate to the constraint of semi-conductor chips.

P6 Cadence

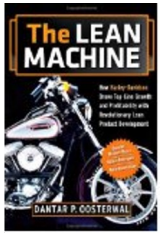
The rhythmic heartbeat lowers transaction cost and makes small batches economically feasible.

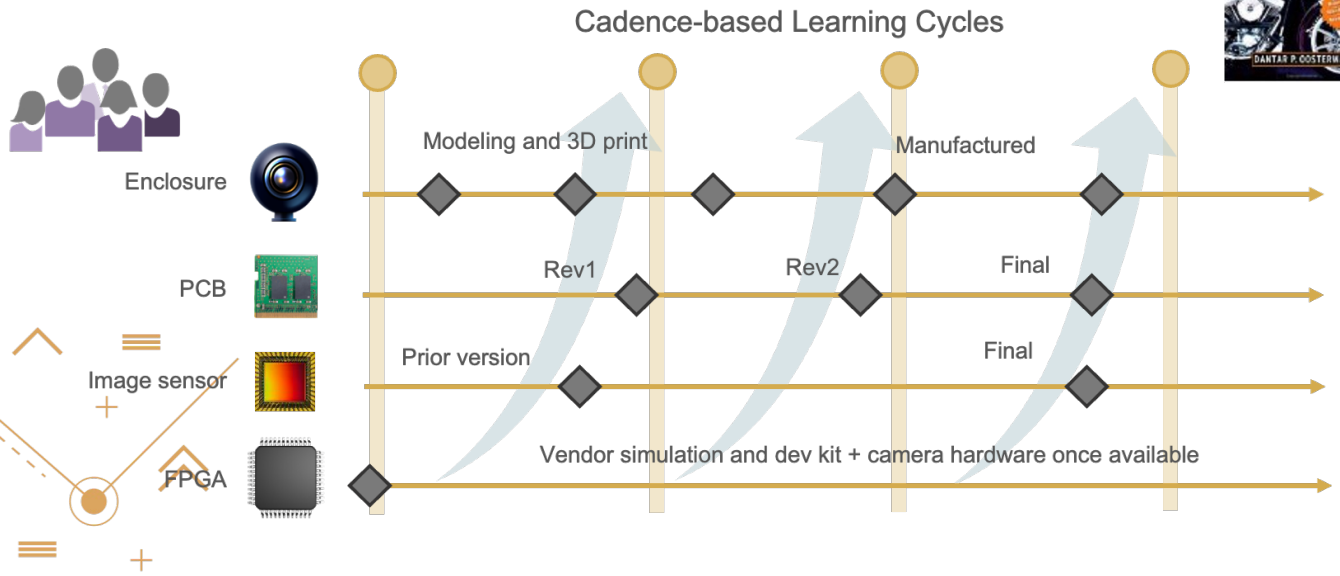


(P6) Cadence and Synchronization (example)

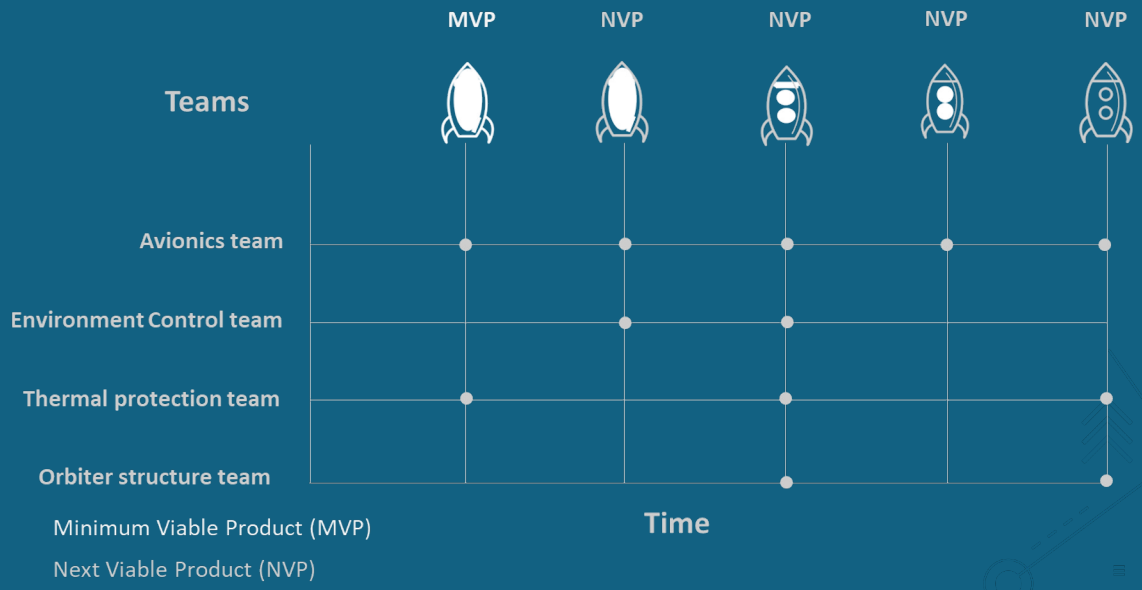


"Integration points control product development and are the leverage points to improve the system. When timing of integration points slips, the project is in trouble."
— *Dantar P. Oosterwal*



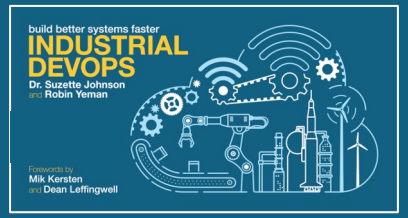


P7 Integrate early and often



Not all elements are going to be integrated at the time, but its critical to integrate as frequent as possible.

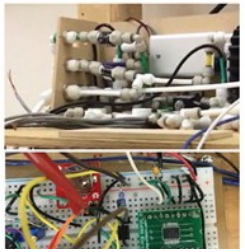
(P7) Integrate early and often (example)



https://www.alten.com/mechanical-electrical-engineering-agile-method/

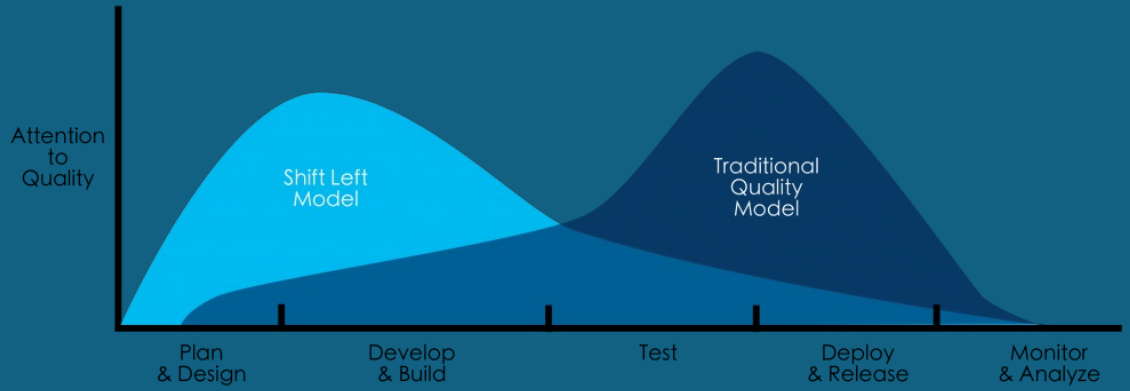
Plywood Prototype	Hydraulic Prototype	"Alpha" Near-Final Prototype	"Beta" Fully-Functional Verification Ready

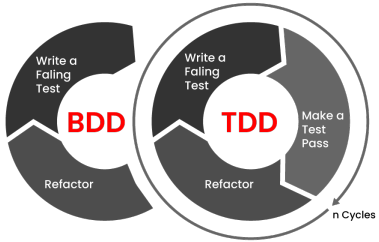
• Wooden support frame
• Power-on
• Installation features
• Time-based filter replacement
	• Functional hydraulics
	• In-line sensors installed
	• Read sensors
	• Flow-based filter expiration
		• 'Rev 1' hardware
		  • PCBA
		  • Sheet metal
		  • Cables
		• Internet connection
		• Logging
		• Secondary GUI screens
			• 'Rev A' hardware
			• Service screens
			• Reliability improvements
			• Final GUI improvements
			• Bug fixes



Rapid Prototyping and Agile allow Alten to learn fast

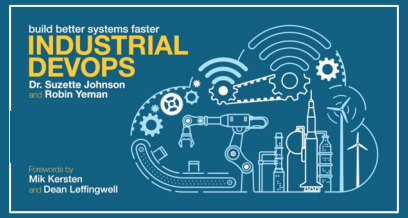
P8 Shift Left

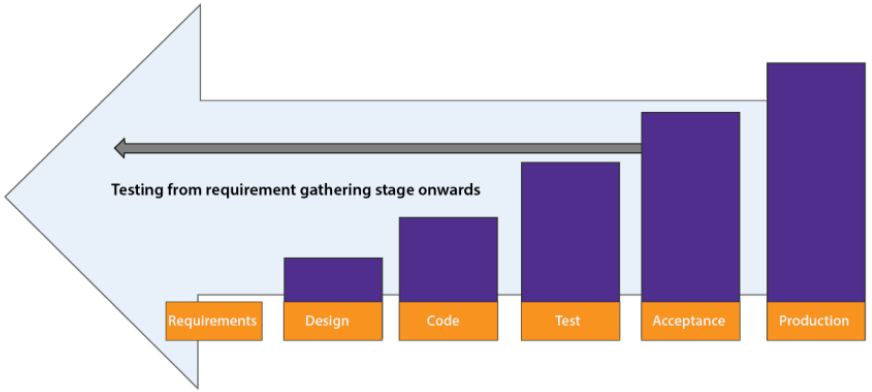




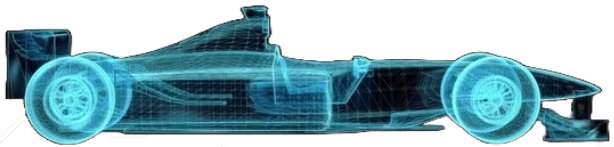
Shift Left everything :
Test, Data Sets, Security, Safety

(P8) Shift Left (example)





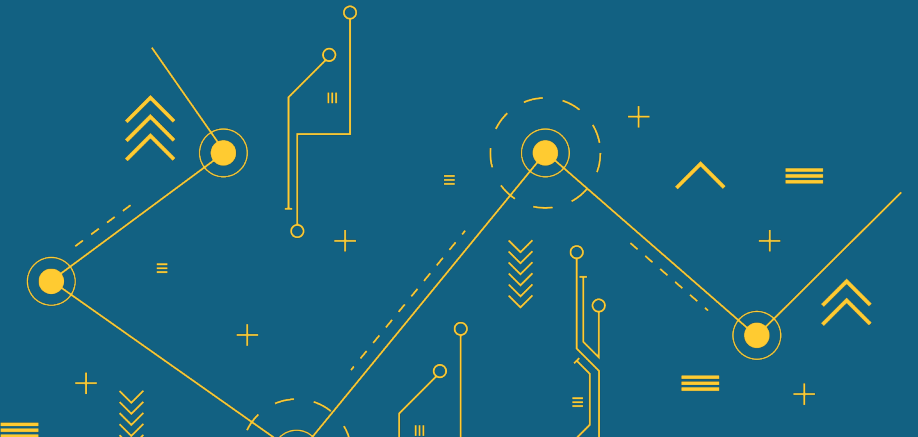
Shifting towards "LEFT"

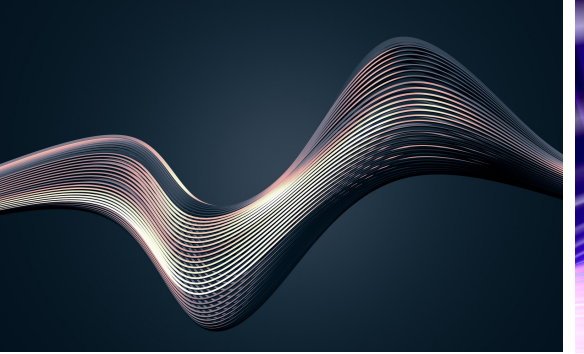


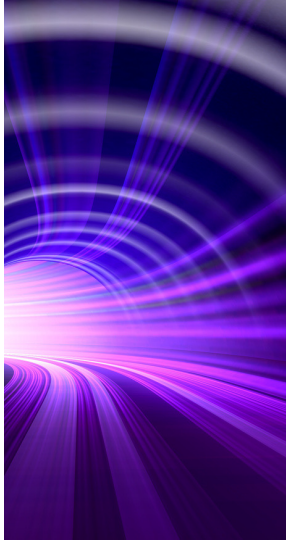
McLaren commercial technology head Edward Green stressed the importance of maximizing digital twins to succeed under a budget cap.

P9 Apply a growth mindset

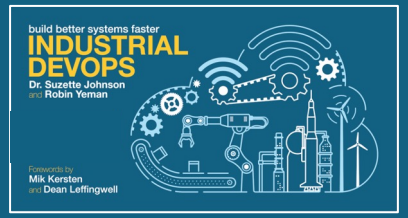
- Champion Learning
- Create a feedback culture
- Rethink Failure
- Be comfortable with uncomfortable
- Ask stupid questions







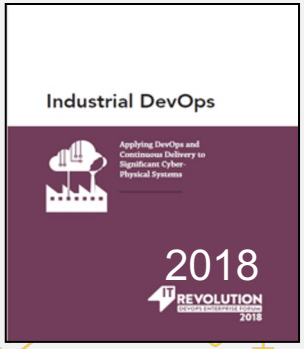
(P9) Growth Mindset (example)

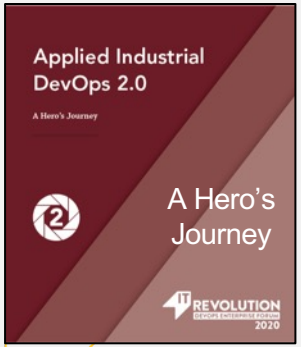


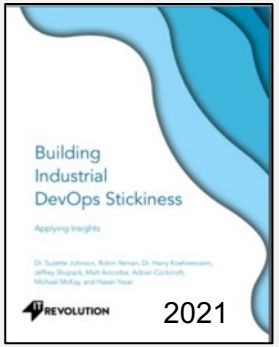
SPACEX

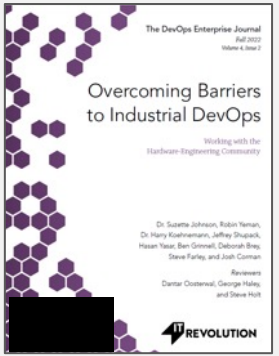
Industrial DevOps: Lean-Agile for Cyber-Physical Systems

Published through IT Revolution, Industrial DevOps expands the definition of DevOps beyond software to enable significant cyber-physical systems development programs to be more responsive to changing needs while reducing lead times. It is the application of continuous delivery and DevOps principles to the development, manufacturing, deployment, and serviceability of significant cyber-physical systems.

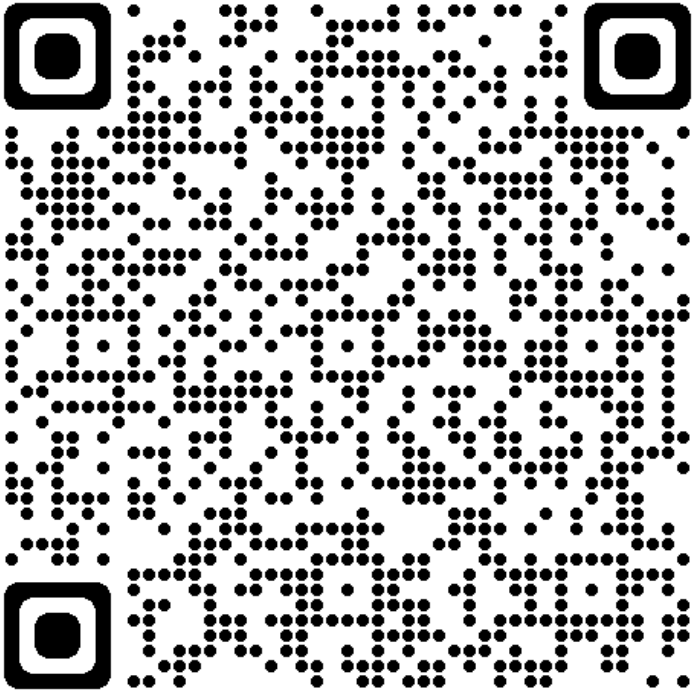


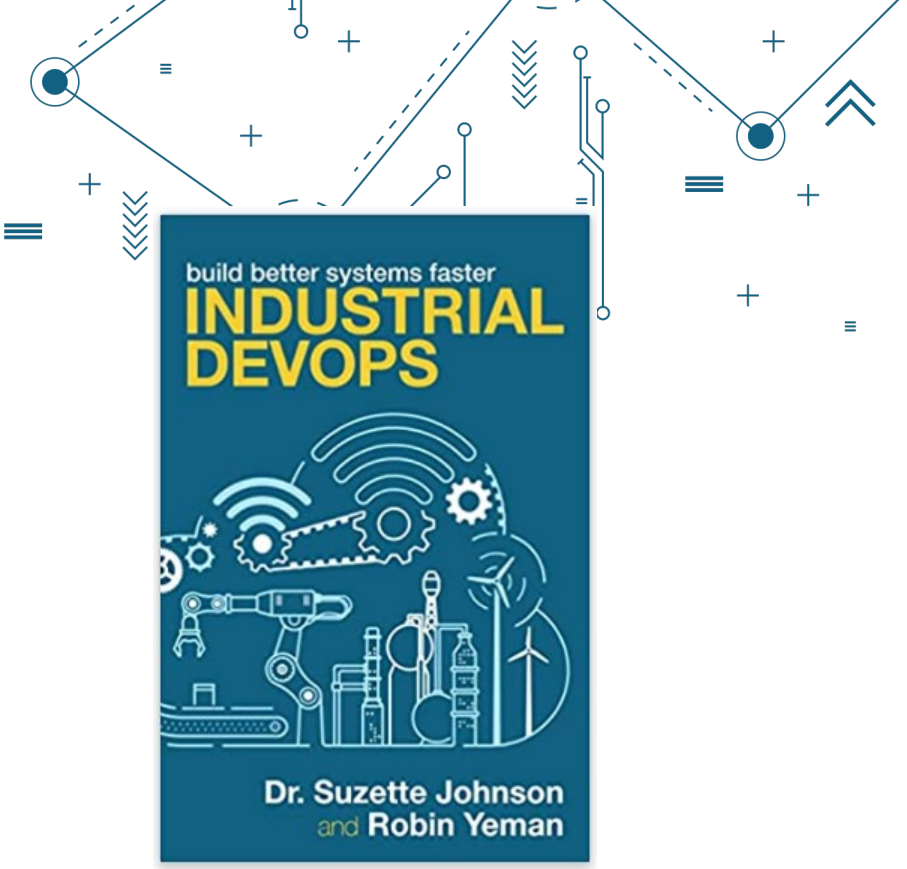






https://itrevolution.com/book/industrial-devops//
https://itrevolution.com/book/applied-industrial-devops/
Building Industrial DevOps Stickiness (itrevolution.com)




build better systems faster
INDUSTRIAL DEVOPS
Dr. Suzette Johnson
and Robin Yeman


Q & A
ASK AWAY!