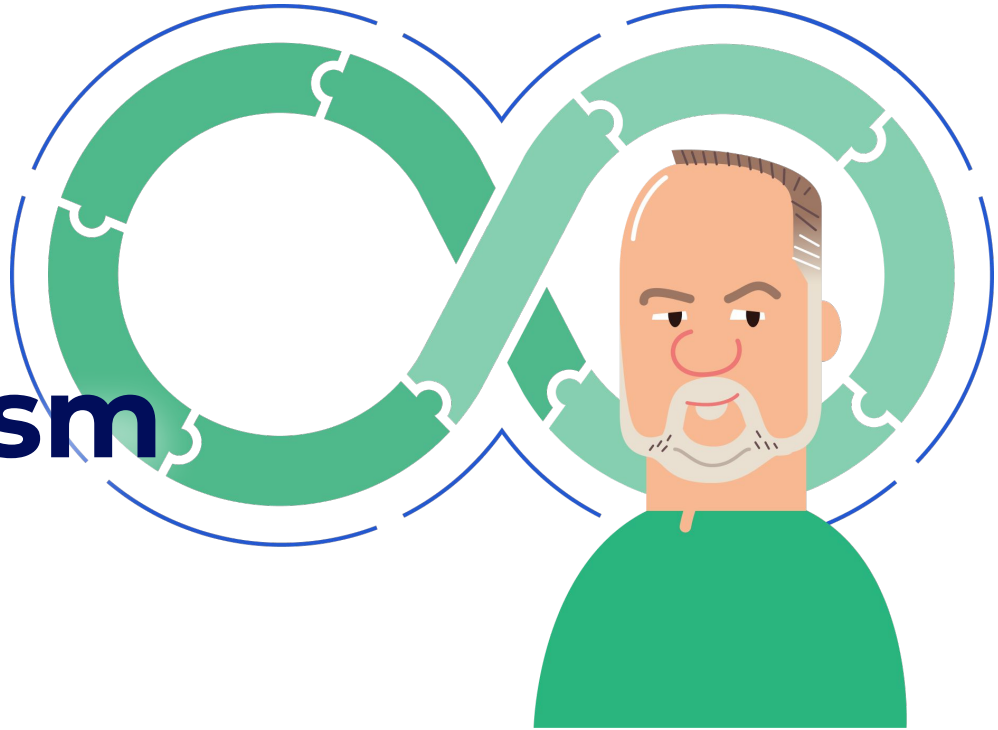
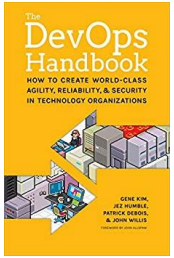
kosli

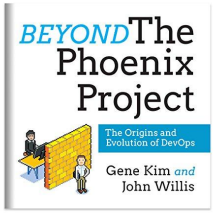
DevSecOps Operationalism

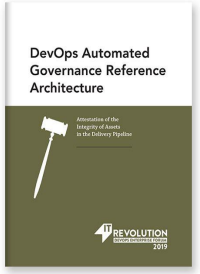


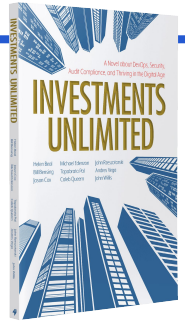
John Willis @botchagalupe

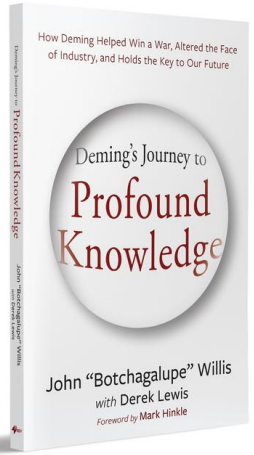
@botchagalupe











CANONICAL

CHEF

DELL

docker

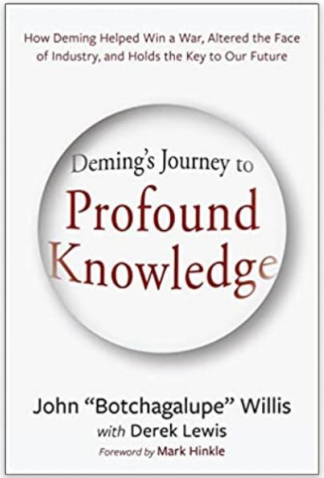
Red Hat

DEVOPS DAYS

DEVOPS ENTERPRISE SUMMIT

KeyBanc Capital Markets

kosli



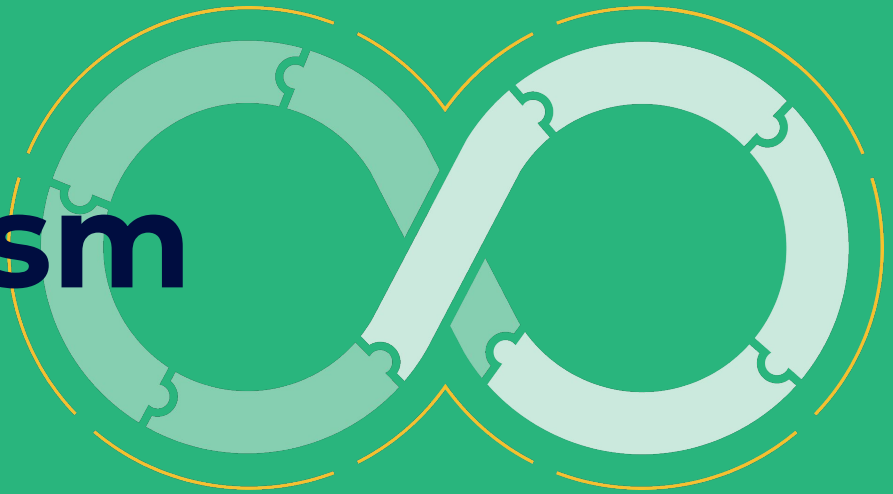
A thoroughly entertaining and educational look at Deming, a man whose insights are fundamental to modern software development. The book includes delightful stories of those around Deming who influenced his work and helped create the foundation for agile and DevOps"

Jim Whitehurst - President IBM, and CEO of RedHat

we work today, but also how we can continue to succeed in the future.

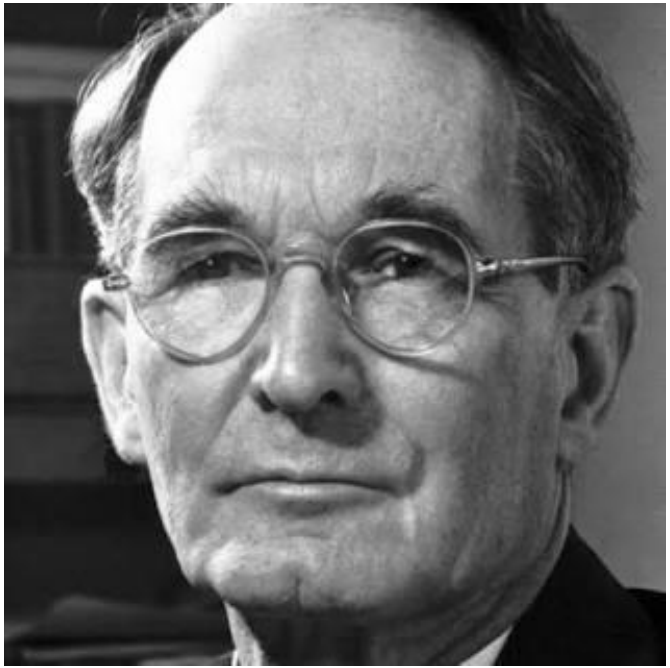
Part business history, part biography, part journey into deep business sense, bestselling author John Willis captures the full picture

Operationalism



John Willis @botchagalupe

Operationalism



"We do not know the meaning of a concept unless we have a **method** of measurement for it."

The Logic of Modern Physics 1927
- Percy Williams Bridgman

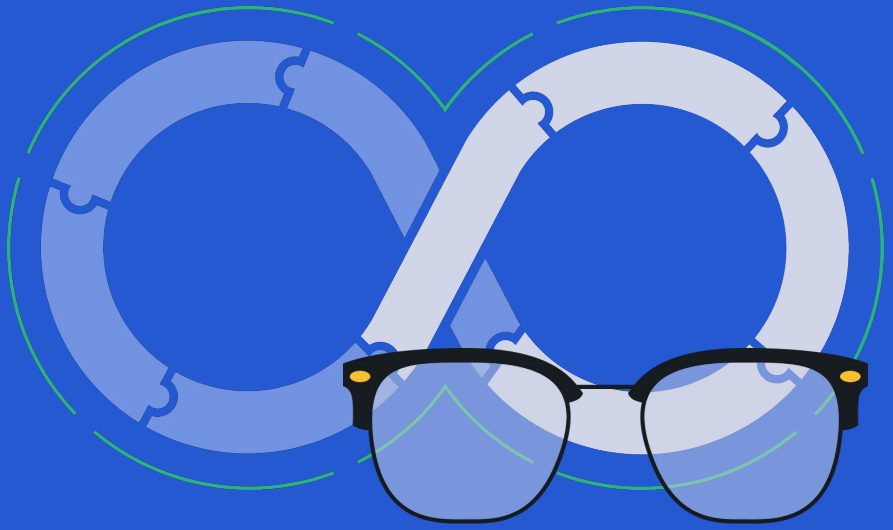
Percy Williams Bridgman

- Harvard physics professor
- Won a Nobel prize for physics of high pressures
- Synthetic diamonds (gauges kept breaking)
- Albert Einstein's special theory of relativity, where measurements used in time and space were different than conventional means of measurement.
- Length, Square Footage, Light Years

To find the length of an object, we have to perform certain physical operations. The concept of length is therefore fixed when the operations by which length is measured are fixed. The concept of length involves the set of operations by which length is determined.

Percy Williams Bridgman

Dr. Edwards Deming



John Willis @botchagalupe

Deming’s Influence

- Henri Fayol's 1916 General and Industrial Management
- Percy Bridgeman's 1927 The Logic of Modern Physics
- Clarence Irving Lewis' 1929, Mind and the World-Order
- Walter Shewhart’s 1924 Statistical Process Control

Deming Management Philosophy

- Operational Definitions
- Analytical Statistics
- Fourteen Points for Management
- System of Profound Knowledge

Operational Definition

An operational definition is a procedure agreed upon for translation of a concept into measurement of some kind

Count the Number of Horses, Elephants, and Pigs?

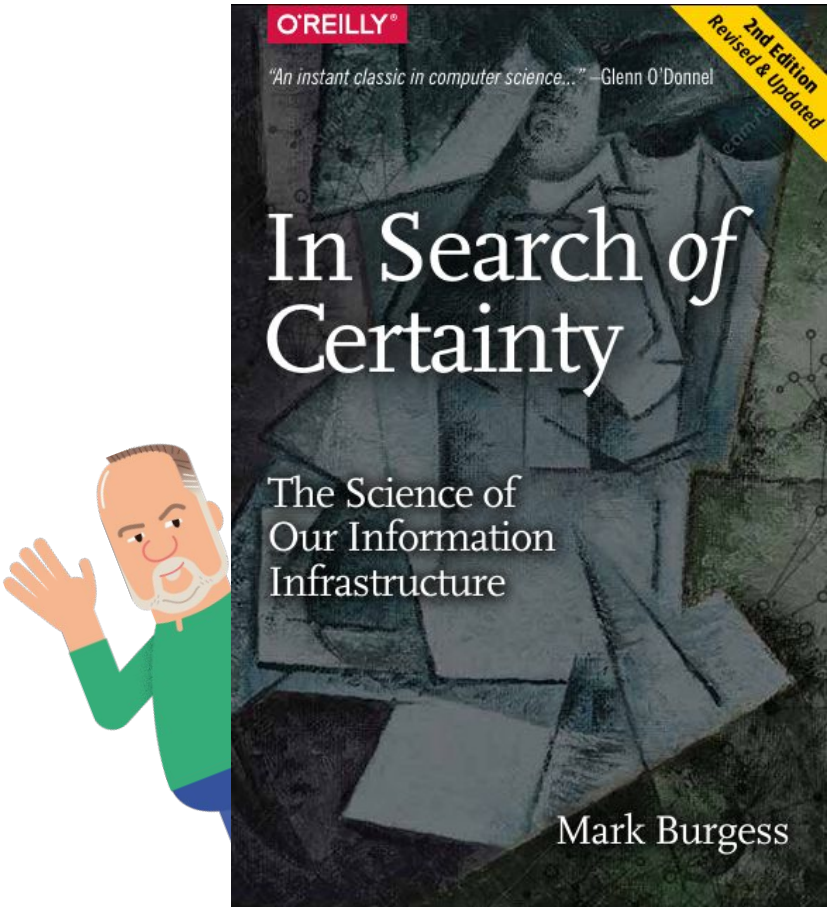
Count the Number People in a Restaurant?

There is no true value of any characteristic, state, or condition that is defined in terms of measurement or observation

The New Economics
Deming, W. Edwards

In Complex Systems, Definitions Matter

- Time
- Root
- Zero
- Hermetic
- Service


O'REILLY®
"An instant classic in computer science..." —Glenn O'Donnel
2nd Edition
Revised & Updated
In Search of Certainty
The Science of Our Information Infrastructure
Mark Burgess

What is Lead Time, or Time to Restore?

- **Criteria:** Why are we asking? What is good or bad,or standard? Are all the teams in an org aligned on the same operational definition? Industry?
- **Test:** What's the measurement? Delivery or deployment, branch, master branch or pull request? Dark launch, feature flag. Mean, mode, standard deviation?
- **Decision:** Did it meet the criteria? What action do we take? Are we continuously improving?

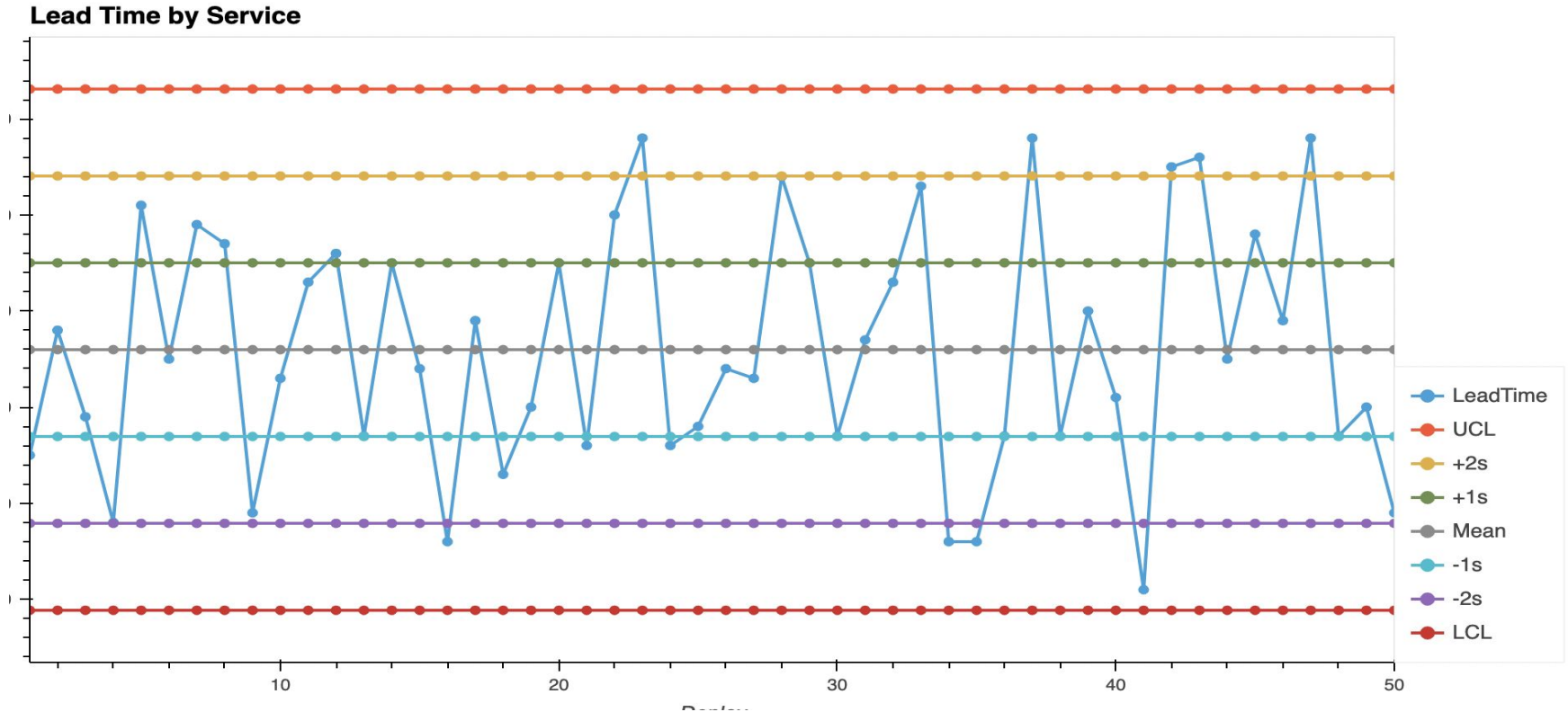
Dr. Donald Wheeler

- **Criteria:** A measurement system “is consistent if and only if repeated measurements of the same items result in a sequence of values that are homogeneous.”

- **Test:** An individuals control chart is used to determine if the values are homogeneous, i.e., in statistical control.

- **Decision:** The determination as to whether the test results show that the characteristic meets the criteria. The measurement process is inconsistent if there are points beyond the control limits or there are patterns present.

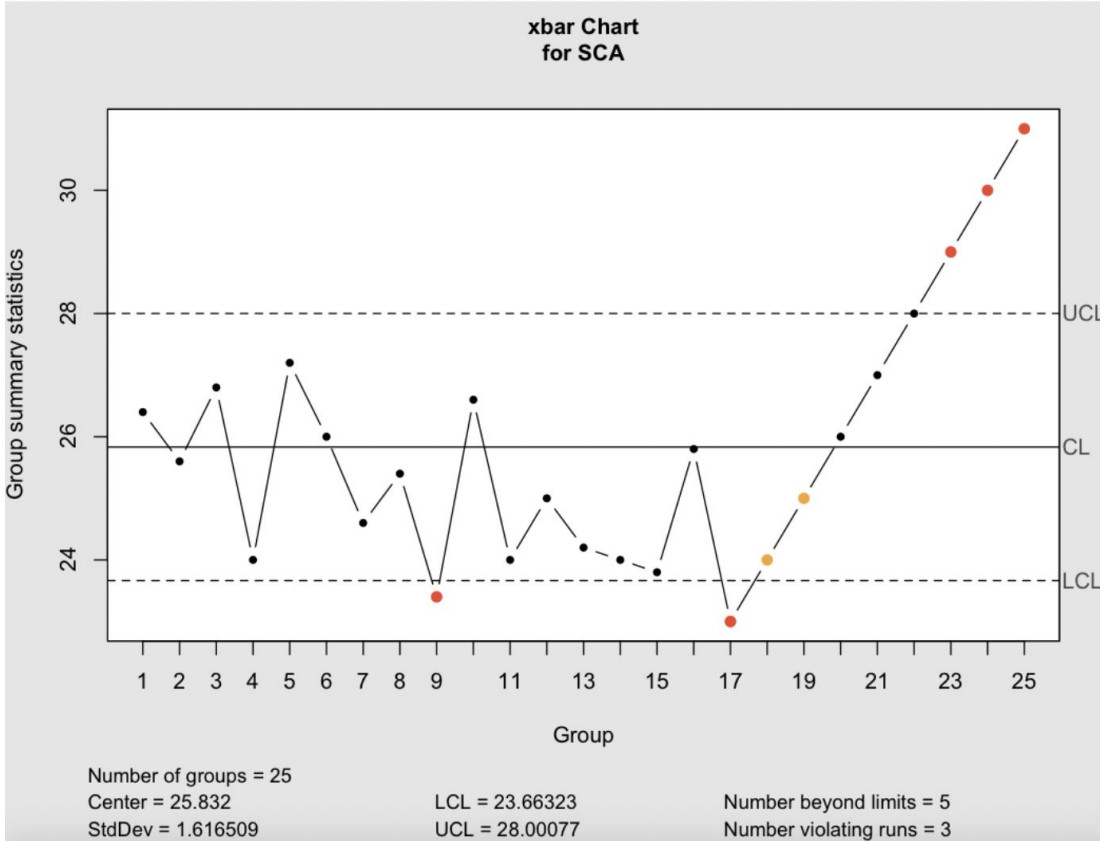
Analytical Statistics (Variation - No True Value)



Operationalization & Risk

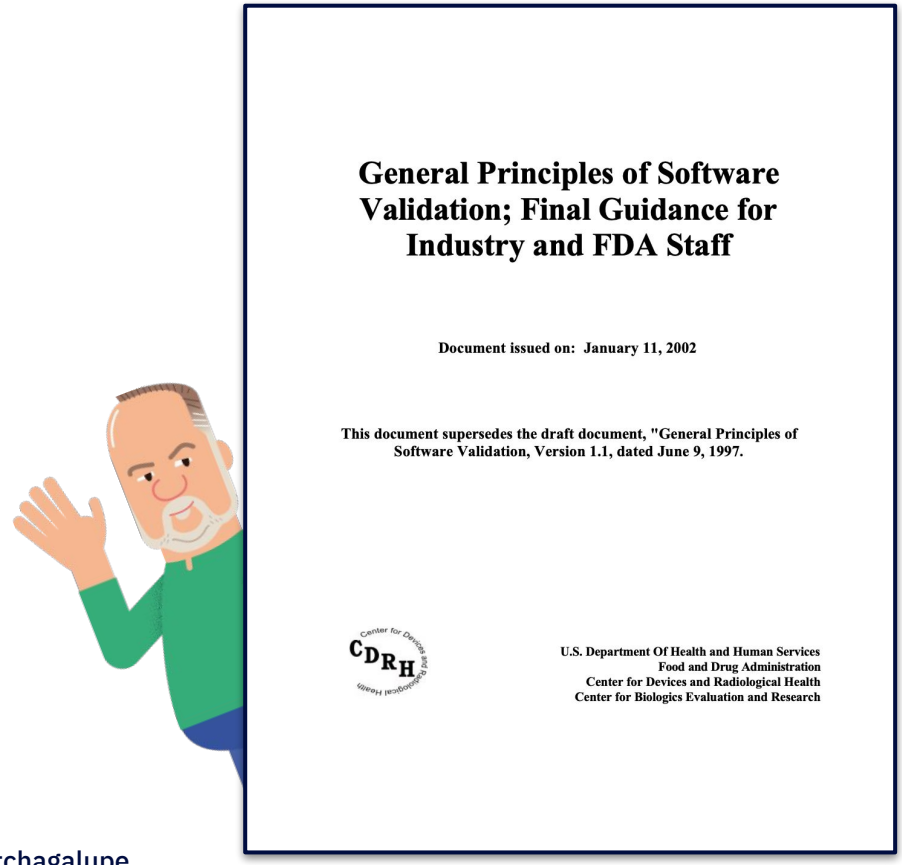
John Willis @botchagalupe

Container Scan Vulnerability Fails



Complex Industry Risk Architectures

FDA 21 CFR Part 11 Pharmaceutical Industry



General Principles of Software Validation; Final Guidance for Industry and FDA Staff

Document issued on: January 11, 2002

This document supersedes the draft document, "General Principles of Software Validation, Version 1.1, dated June 9, 1997.

U.S. Department Of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

Operationalization and FDA

- Specification
- Verification
- Validation

Operationalization and FDA

- Specification --> Criteria
- Verification --> Test
- Validation --> Decision

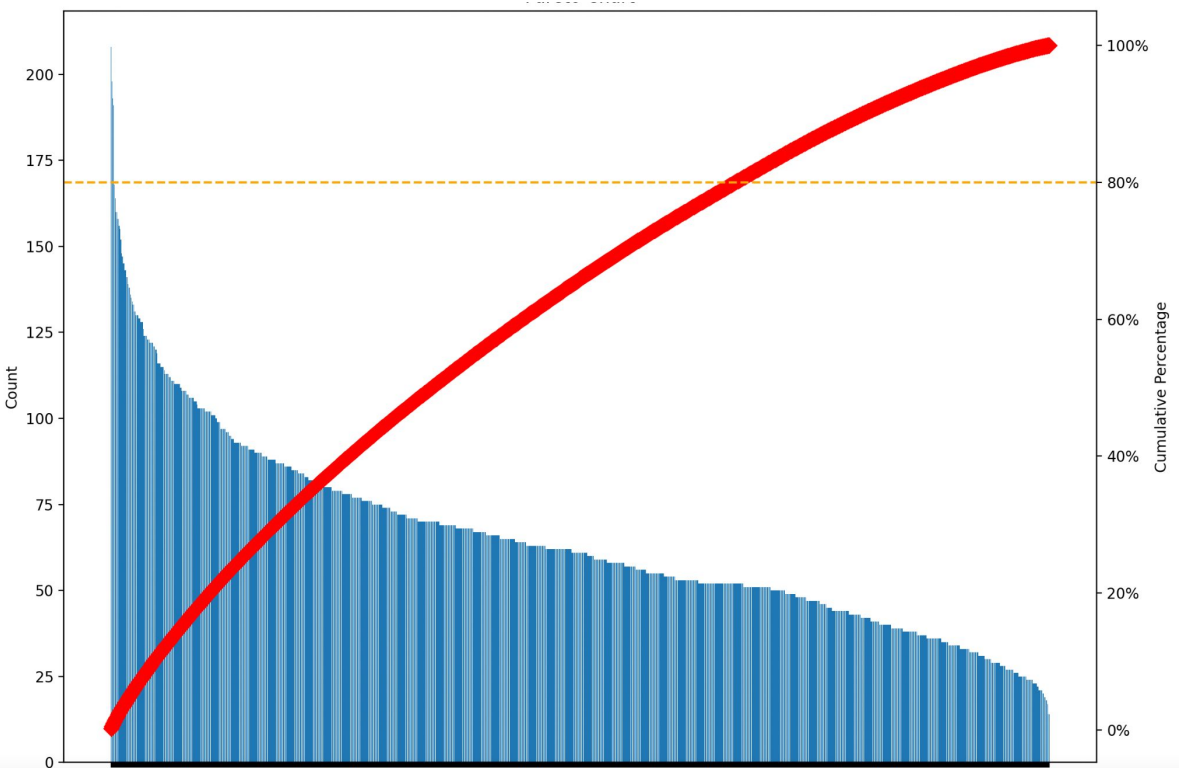
Operationalization and FDA

- Specification --> Criteria --> Plan
- Verification --> Test --> Do
- Validation --> Decision --> Study/Act

Secure Controls Framework

Pareto - Secure Controls Framework (SCF)

1169 Risk Controls
285 Control Frameworks



Secure Controls Framework (SCF)

Sorted Risk Controls by Framework

Control	Count	Percentage	SCF Domain	Control Weight	Grouping
CPL-01	208	72.98%	Compliance	10	Identify
SEA-01	198	69.47%	Secure Engineering & Architecture	10	Protect
DCH-01	193	67.72%	Data Classification & Handling	10	Protect
CPL-02	191	67.02%	Compliance	10	Detect
IAC-01	168	58.95%	Identification & Authentication	10	Protect
RSK-01	164	57.54%	Risk Management	10	Identify
GOV-01	158	55.44%	Cybersecurity & Privacy Governance	10	Identify
TPM-01	156	54.74%	Third-Party Management	10	Identify
CPL-03	155	54.39%	Compliance	10	Detect
RSK-04	148	51.93%	Risk Management	10	Identify
IRO-02	147	51.58%	Incident Response	10	Respond
NET-01	143	50.18%	Network Security	10	Protect
TDA-01	143	50.18%	Technology Development & Acquisition	10	Protect
VPM-05	141	49.47%	Vulnerability & Patch Management	10	Protect
HRS-01	139	48.77%	Human Resources Security	10	Protect
-PES 3	138	48.42%	Physical & Environmental Security	10	Protect
MON-01	136	47.72%	Continuous Monitoring	10	Detect
TPM-05	135	47.37%	Third-Party Management	10	Identify
CFG-02	134	47.02%	Configuration Management	10	Protect
BCD-01	133	46.67%	Business Continuity & Disaster Recovery	10	Recover

Secure Controls Framework

GUIDELINE
[provides additional, recommended guidance]

PROCEDURE
[establishes proper steps to take]

STANDARD
[assigns quantifiable requirements]

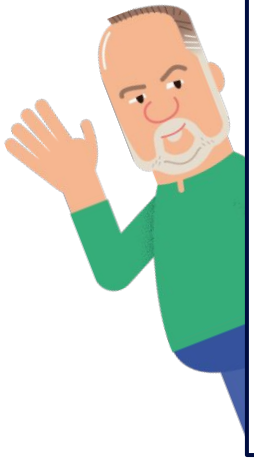
CONTROL OBJECTIVE
[identifies desired conditions to be met]

POLICY
[sets high-level expectations]

SCF as Code

- Standards/Guidelines —> Criteria
- Procedures —> Test
- Control Objectives/Policy —> Decision

NIST Documentation as Zero Day



NIST Special Publication 800-204C

Implementation of DevSecOps for a Microservices-based Application with Service Mesh

Ramaswamy Chandramouli

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-204C

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Check for updates

NIST Special Publication
NIST SP 800-207A ipd

A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments

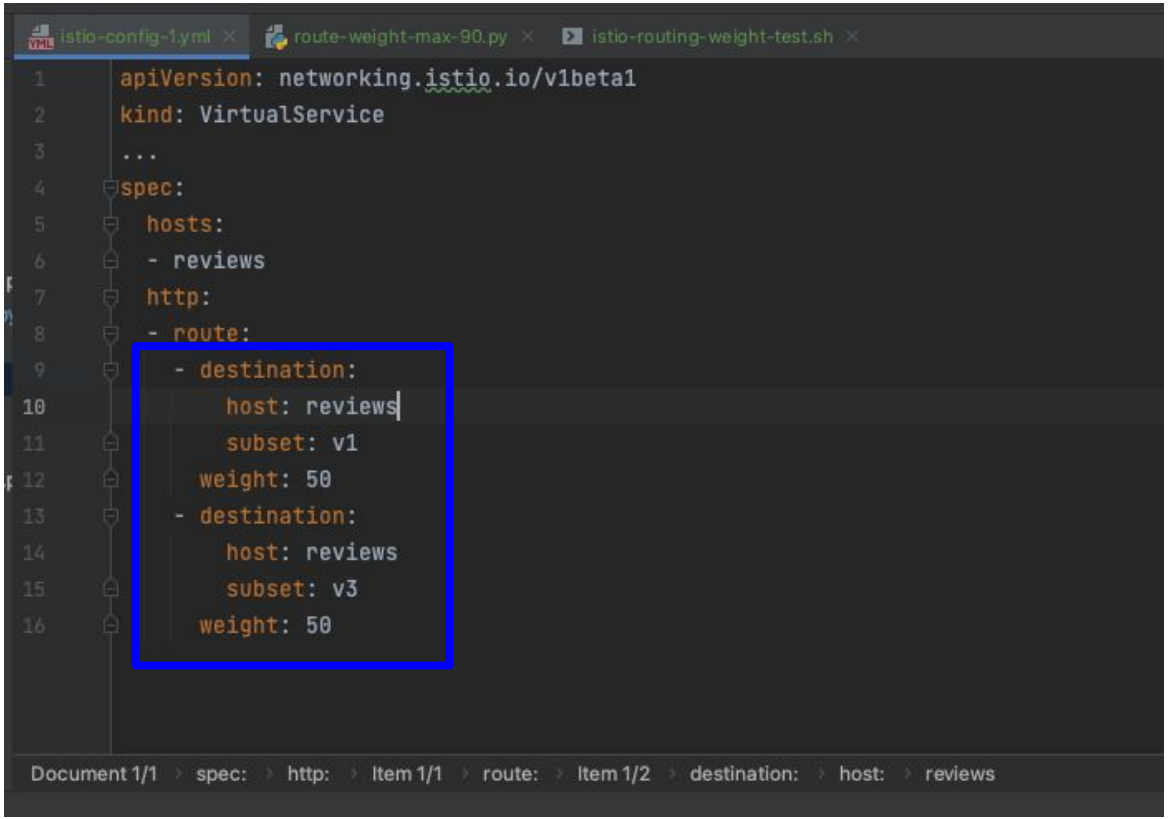
Initial Public Draft

Ramaswamy Chandramouli
Zack Butcher

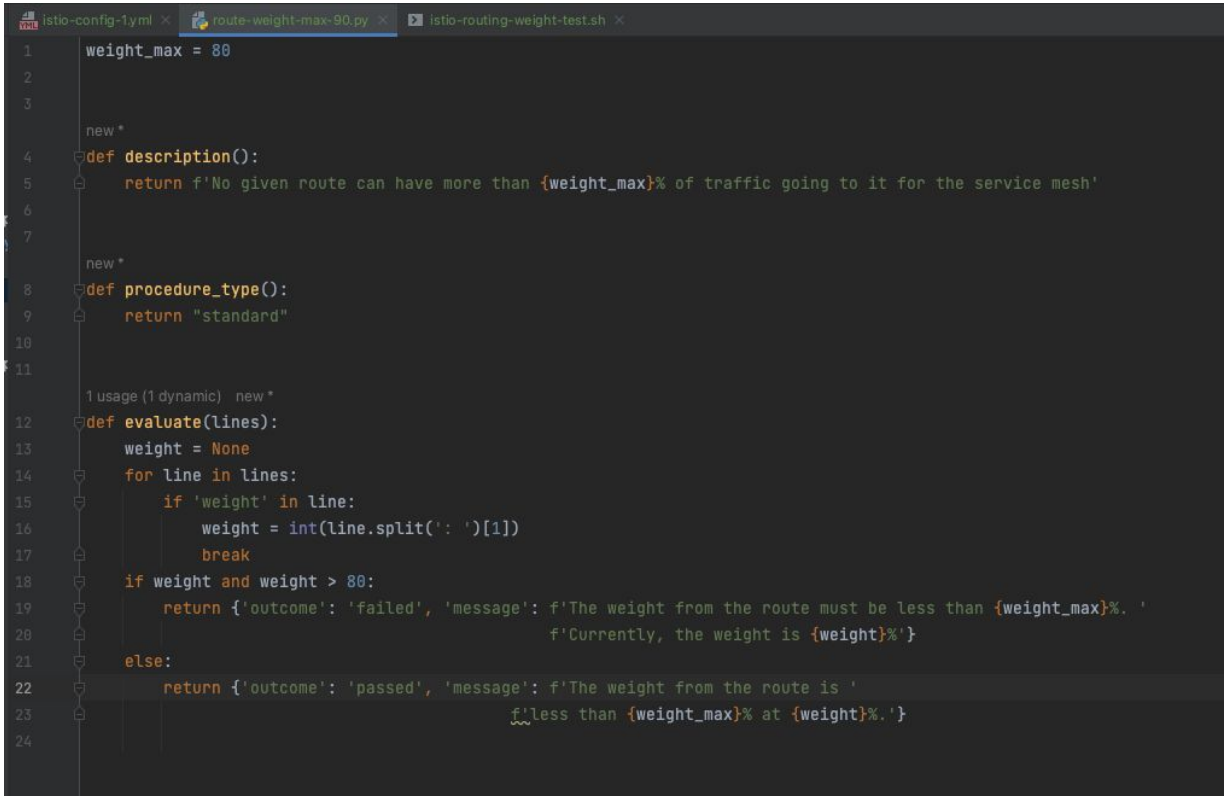
This publication is available free of charge from:
https://doi.org/10.6028/NIST.800-207A.ipd

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

ISTIO Traffic Shaping (Standard/Criteria)



ISTIO Traffic Management (Control/Test)



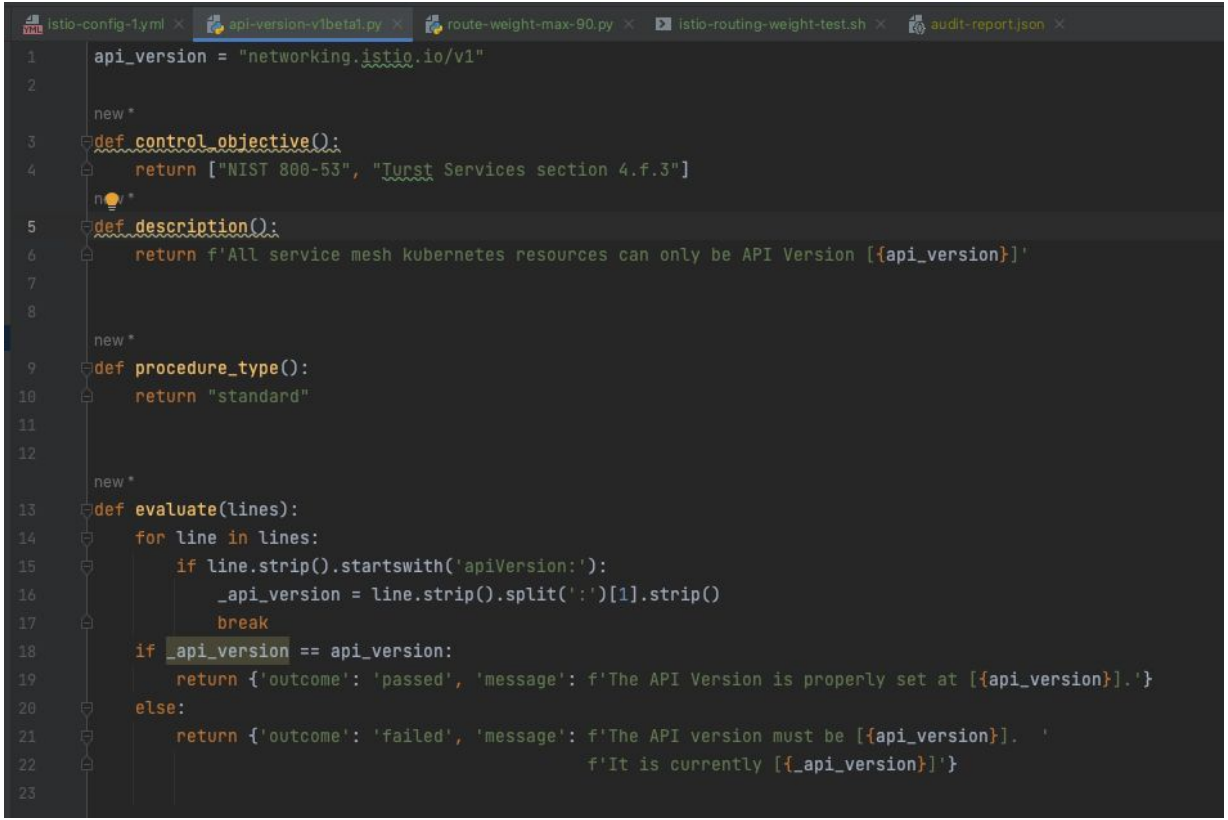
ISTIO Traffic Management (Policy/Decision)

```
--------------------
Target File: istio-config-1.yml
--------------------
Total:  1
Exec:   1
Pass:   1
Fail:   0
--------------------


Standards                                                Outcome    Message
--------------------
No given route can have more than 80% of traffic going to it for the service mesh  pass  The weight from the route is less than 80% at 50%.


Guidelines                                               Outcome    Message
--------------------
```

ISTIO Traffic Management (API Version)



ISTIO Traffic Management (Policy/Decision)

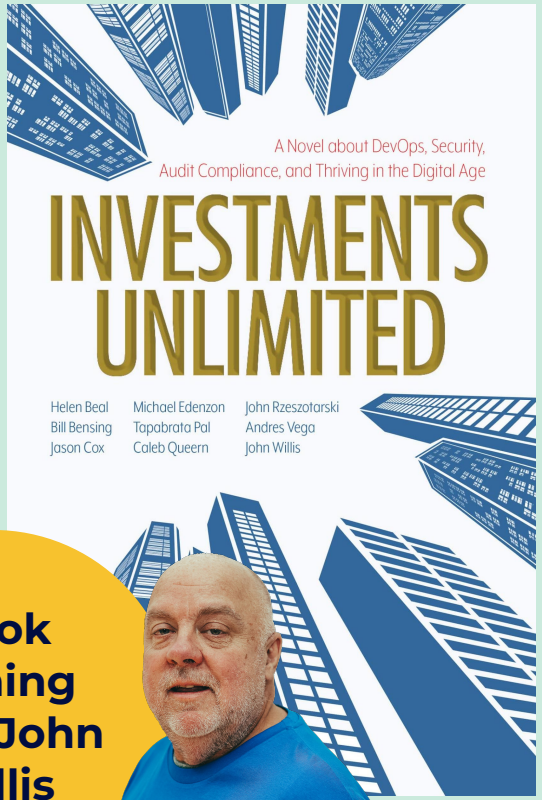
```
--------------------
Target File: istio-config-1.yml
--------------------
Total:  2
Exec:   2
Pass:   1
Fail:   1
--------------------


Standards                                          Outcome    Message
--------------------
All service mesh kubernetes resources can only be API Version [networking.istio.io/v1]  fail  The API version must be [networking.istio.io/v1].  It is currently [networking.istio.io/v1beta1]
No given route can have more than 80% of traffic going to it for the service mesh  pass  The weight from the route is less than 80% at 50%.


Guidelines                                         Outcome    Message
--------------------
```

Grab a FREE copy of Investments Unlimited at the Kosli stand

(Book signing after the Lightning Talks 5:45pm)



Book signing with John Willis

John Willis @botchagalupe

Download a FREE White paper

SLSA 4 - 18 Controls
DAG - 51 Controls

John Willis @botchagalupe

kosli | kosli.com

Find out more at...

- profound-deming.com
- linkedin.com/in/johnwillisatlanta/
- @botchagalupe
- john.willis@kosli.com
- DevOps and Operationalism
  - **https://bit.ly/3ymHVmp**
- Enumerated and Analytical Statistics
  - **https://bit.ly/3ZRH4WI**