



# What it takes to keep the Netherlands moving

A Mission Critical Software perspective of the Dutch transportation system



# Welcome!

## Personal introduction

- ❖ Name, company
- ❖ Experience, undisclosed client, role
- ❖ Goals for this lecture

# ▲ Topics

1. Introduction
2. Governance
3. Mission critical
4. Break (15 min)
5. Development
6. Operations
7. Questions





# Introduction

Question: What software systems are we dependent upon?



# ▲ Introduction

European: *Network and Information Security Directive (NIS2)*



# Introduction

European: *Network and Information Security Directive (NIS2)*

Dutch: “*Cyberbeveiligingswet*”



## ▲ Introduction

*“The NIS2 Directive focusses on **critical organizations and sectors** where service disruptions can cause **societal and economic disruptions.**”*

# Introduction

*“The NIS2 Directive focusses on **critical organizations and sectors** where service disruptions can cause **societal and economic disruptions.**”*





# Introduction

*“The NIS2 Directive focusses on **critical organizations and sectors** where service disruptions can cause **societal and economic disruptions.**”*



# Introduction



Energie



Transport



Bankwezen



Infrastructuur  
financiële markt



Gezond-  
heidszorg



Drinkwater



Digitale  
infrastructuur



Beheerders van  
ICT-diensten



Afvalwater



Overheids-  
diensten

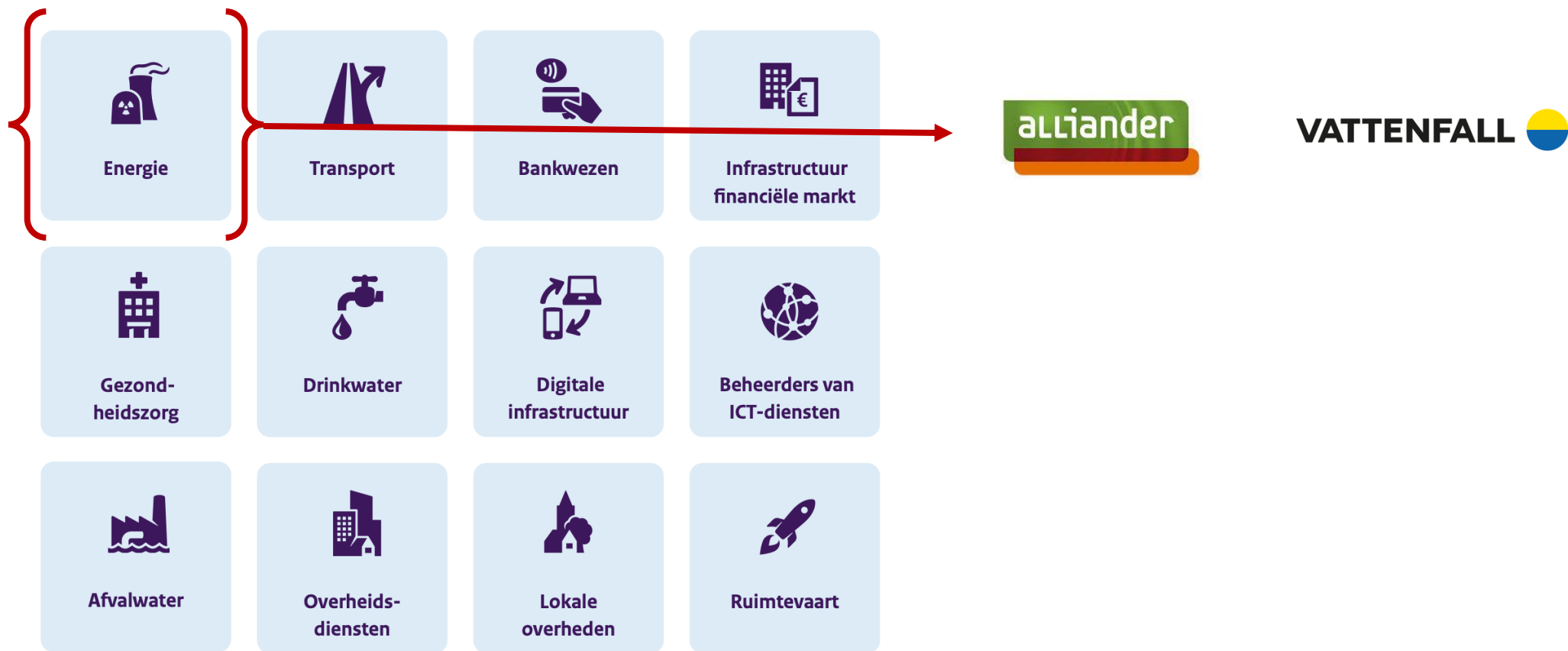


Lokale  
overheden



Ruimtevaart

# Introduction



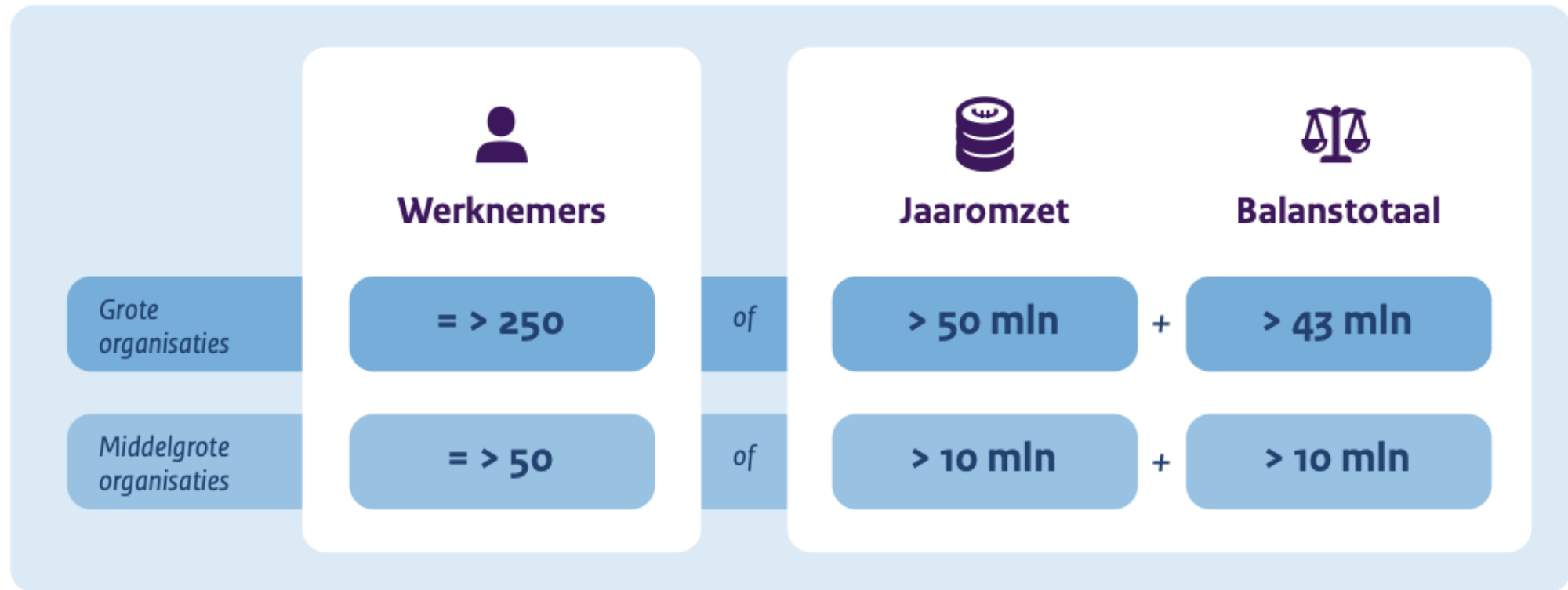
# Introduction



**ProRail**



# Introduction





# ▲ Introduction

- **Measure 1: A risk analysis [...] of information systems;**
- **Measure 3: Measures in the area of business continuity, such as backup management and contingency planning;**
- **Measure 6: Security in processing, developing, and maintaining network and information systems;**
- **Measure 7: Securing the supply chain;**



# Governance

Question: How would we go about implementing this in a large company?



# ▲ Governance

## BIV

- Beschikbaarheid (Availability)
- Integriteit (Integrity)
- Vertrouwelijkheid (Confidentiality)





# ▲ Governance

## BIV

- Beschikbaarheid (Availability)
- Integriteit (Integrity)
- Vertrouwelijkheid (Confidentiality)

National standard

Classification levels 1,2,3

# ▲ Governance

## BIV

- Beschikbaarheid (Availability)
- Integriteit (Integrity)
- Vertrouwelijkheid (Confidentiality)

National standard

Classification levels 1,2,3

	B	I	V
1	Unnecessary	Fragile	Public
2	Required	Trustworthy	Internal
3	Essential	Incorruptible	Confidential

# ▲ Governance



	B	I	V
1	Unnecessary	Fragile	Public
2	Required	Trustworthy	Internal
3	Essential	Incorruptible	Confidential

## ▲ Governance

**Burden of proof!**

	B	I	V
1	Unnecessary	Fragile	Public
2	Required	Trustworthy	Internal
3	Essential	Incorruptible	Confidential

## ▲ Governance



	B	I	V
1	Unnecessary	Fragile	Public
2	Required	Trustworthy	Internal
3	Essential	Incorruptible	Confidential

# ▲ Governance

ISO 27001

– International standard



# ▲ Governance

## ISO 27001

- International standard
- Primarily aimed at information security



# ▲ Governance

## ISO 27001

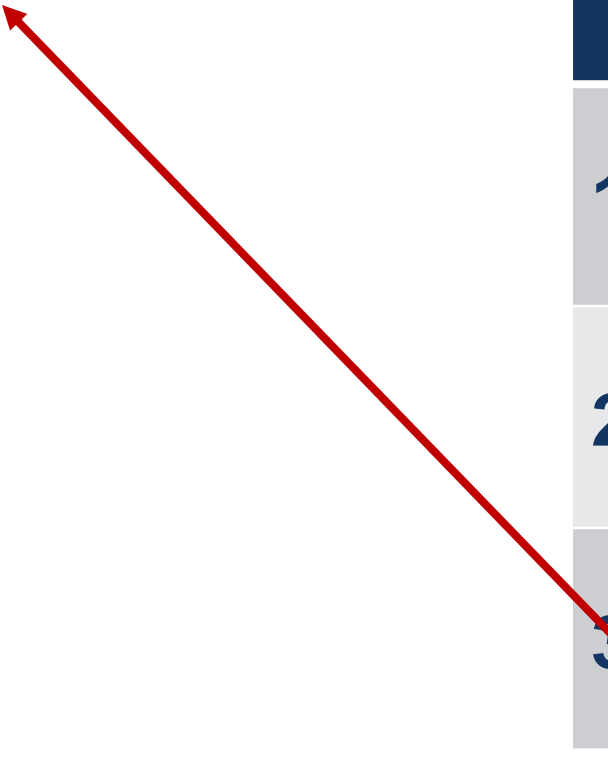
- International standard
- Primarily aimed at information security
- Audit and certification





# ▲ Governance

Service Level Agreement (SLA)



	<b>B</b>	<b>I</b>	<b>V</b>
<b>1</b>	Unnecessary	Fragile	Public
<b>2</b>	Required	Trustworthy	Internal
<b>3</b>	Essential	Incorruptible	Confidential

# ▲ Governance

Service Level Agreement (SLA)  
– Functionality & Performance

	B	I	V
1	Unnecessary	Fragile	Public
2	Required	Trustworthy	Internal
3	Essential	Incorruptible	Confidential

# ▲ Governance

## Service Level Agreement (SLA)

- Functionality & Performance
- Recovery Time Objective (RTO)
  - › 99: 7 hours
  - › 99,9: 44 minutes
  - › 99,95: 22 minutes
  - › 99.99: 4 minutes

	B	I	V
1	Unnecessary	Fragile	Public
2	Required	Trustworthy	Internal
3	Essential	Incorruptible	Confidential

# ▲ Governance

## Service Level Agreement (SLA)
















- Functionality & Performance
- Recovery Time Objective (RTO)
  - › 99: 7 hours
  - › 99,9: 44 minutes
  - › 99,95: 22 minutes
  - › 99.99: 4 minutes
- Recovery Point Objective (RPO)
  - › Hours
  - › Minutes
  - › Seconds
  - › None

	B	I	V
1	Unnecessary	Fragile	Public
2	Required	Trustworthy	Internal
3	Essential	Incorruptible	Confidential

# ▲ Governance

## Service Level Agreement (SLA)

- Functionality & Performance
- Recovery Time Objective (RTO)

- › 99: 7 hours 
- › 99,9: 44 minutes  
- › 99,95: 22 minutes    
- › 99.99: 4 minutes        

- Recovery Point Objective (RPO)

- › Hours 
- › Minutes  
- › Seconds    
- › None       

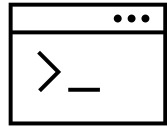
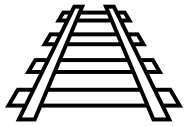
	B	I	V
1	Unnecessary	Fragile	Public
2	Required	Trustworthy	Internal
3	Essential	Incorruptible	Confidential



# Mission critical goal: *Transport people*

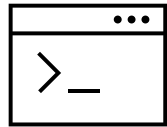
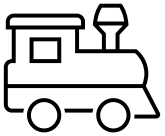
Group exercise: What might the BIV classifications and Service Level Agreements look like in a transportation system?

## ▲ Mission critical



**Infra. sensors**

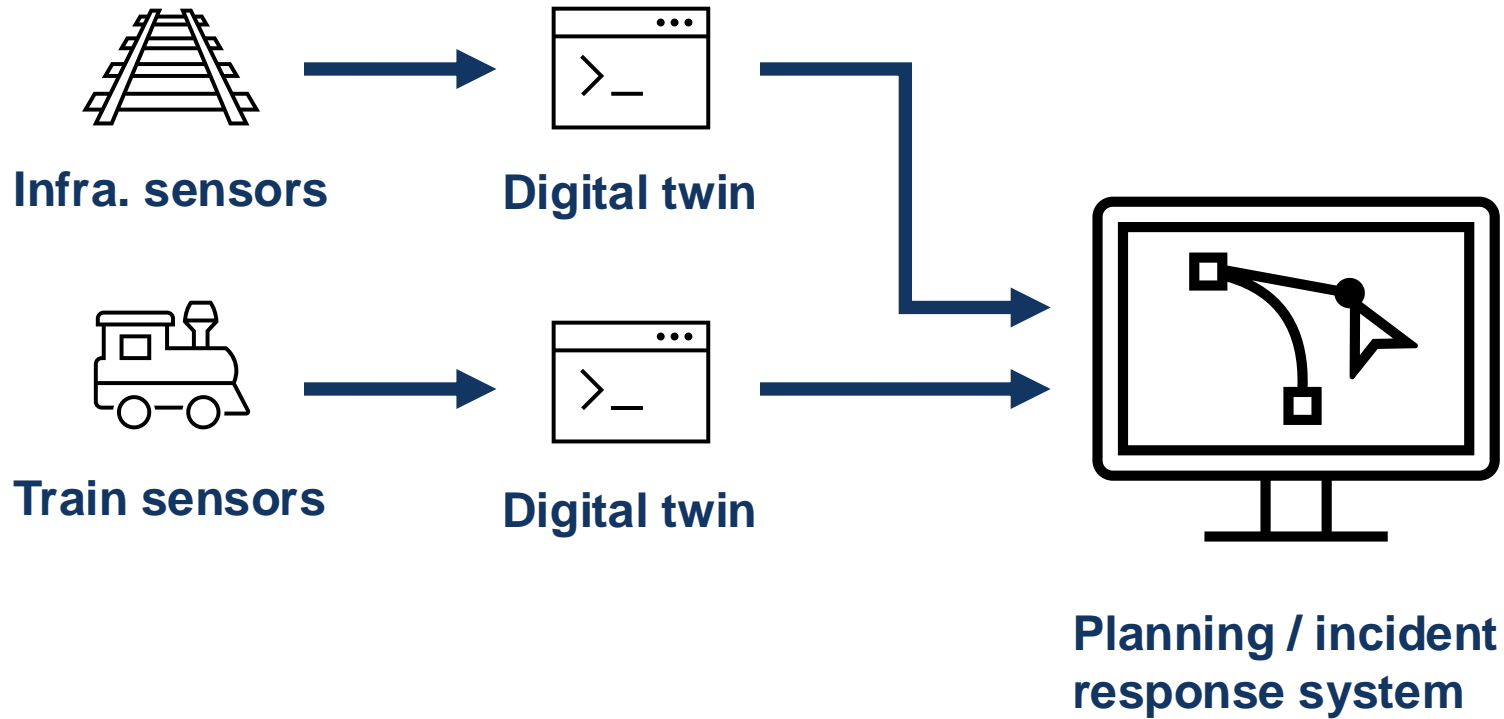
**Digital twin**



**Train sensors**

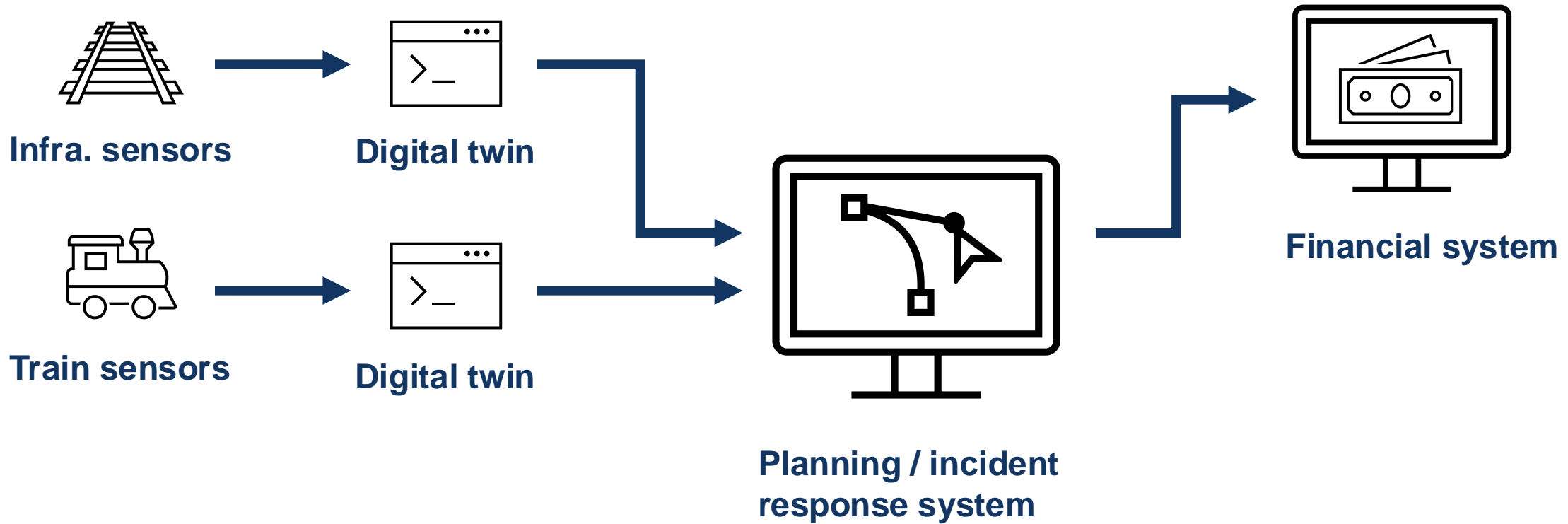
**Digital twin**

## ▲ Mission critical

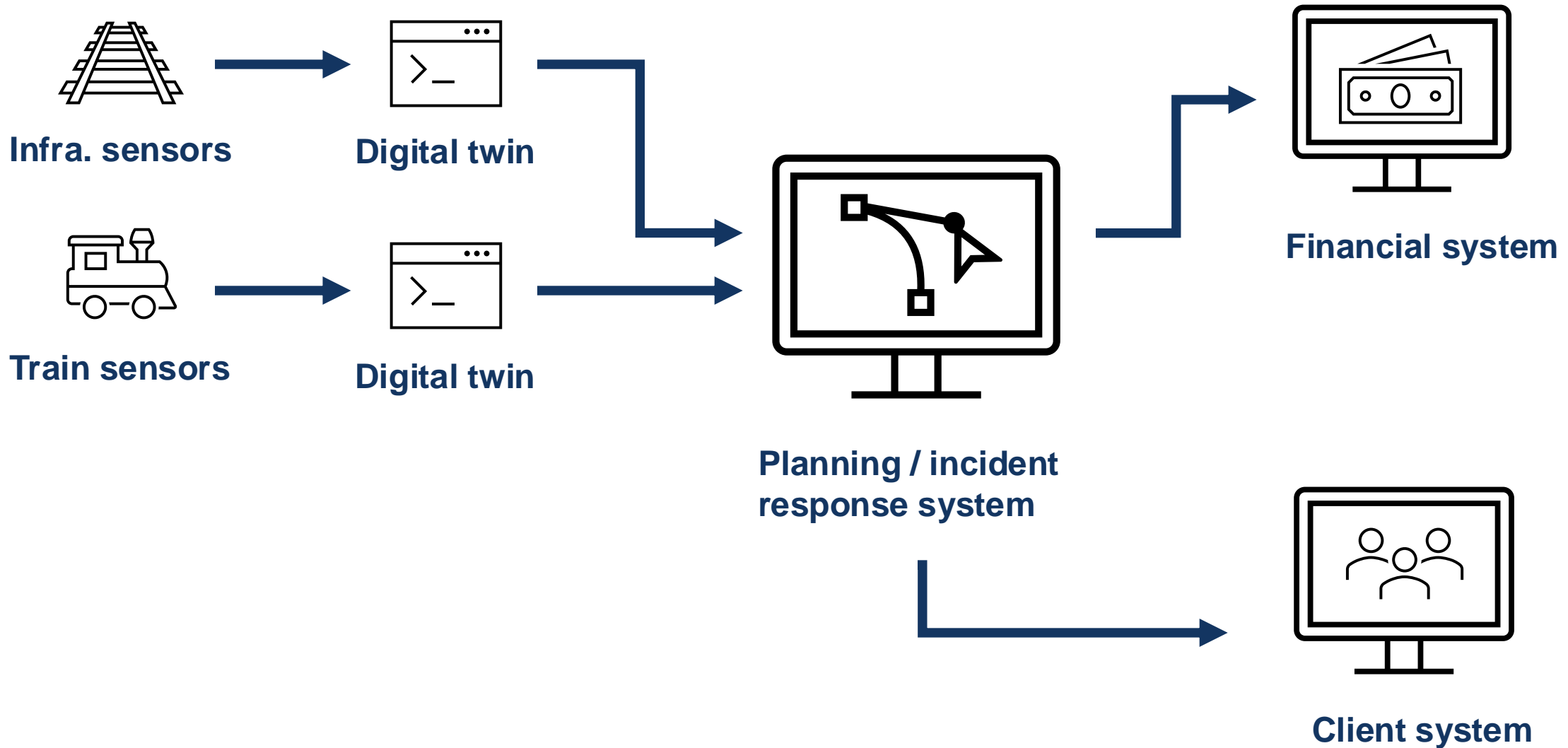




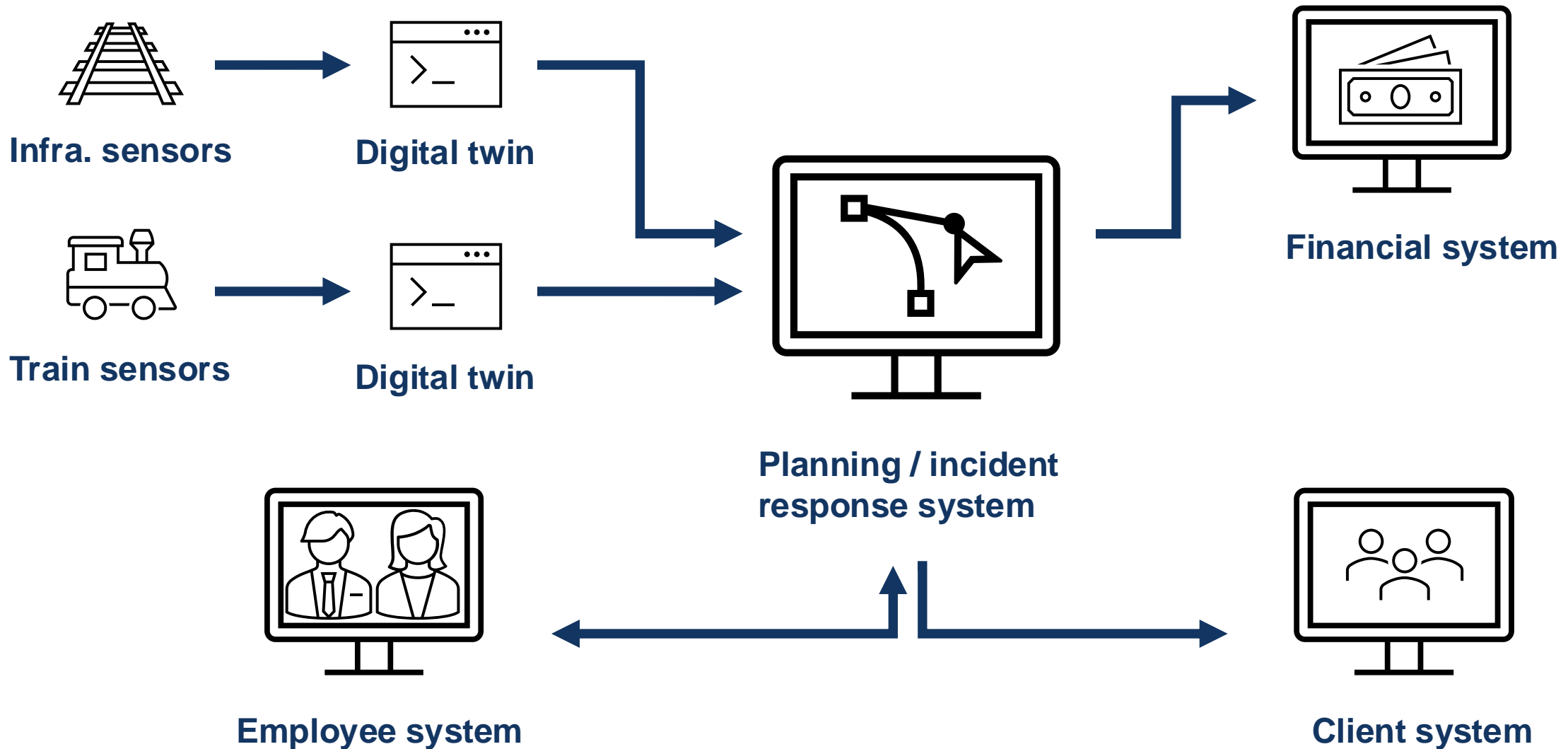
## ▲ Mission critical



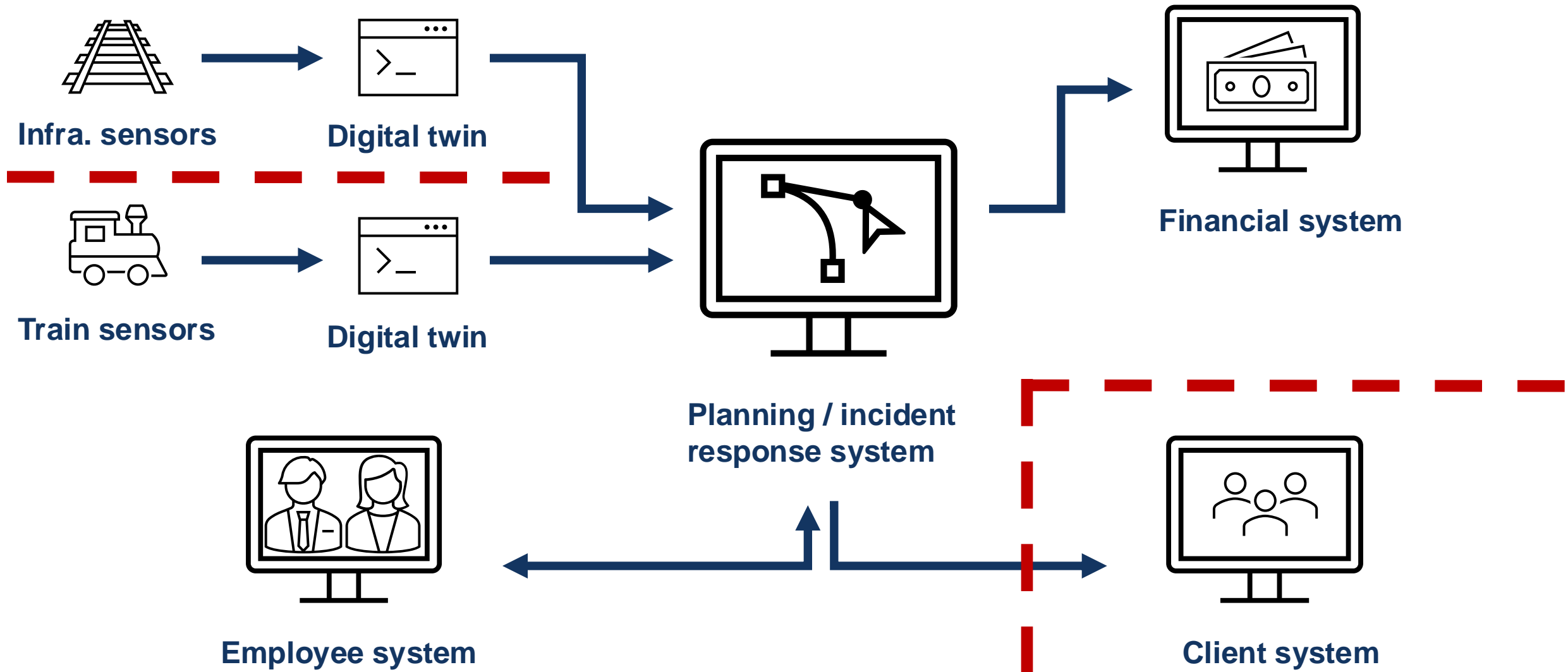
## ▲ Mission critical



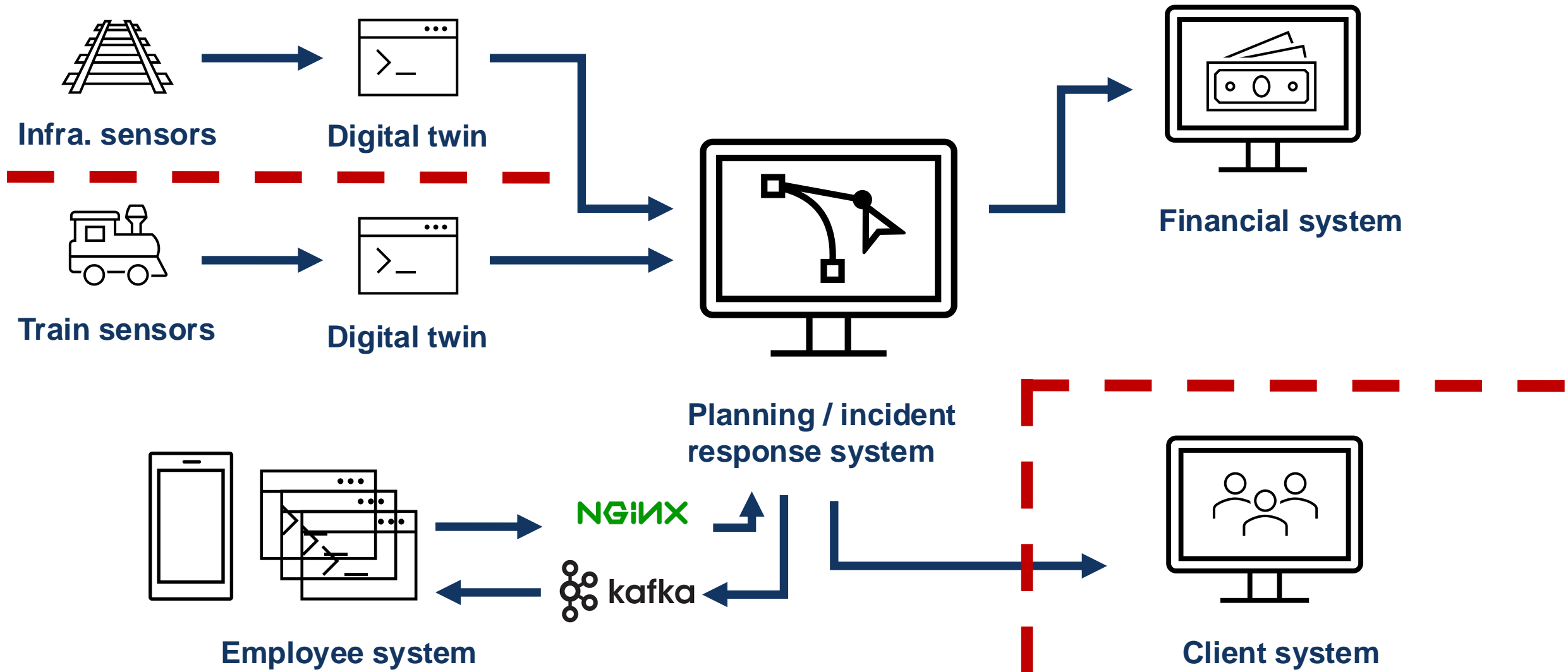
## ▲ Mission critical



## Mission critical

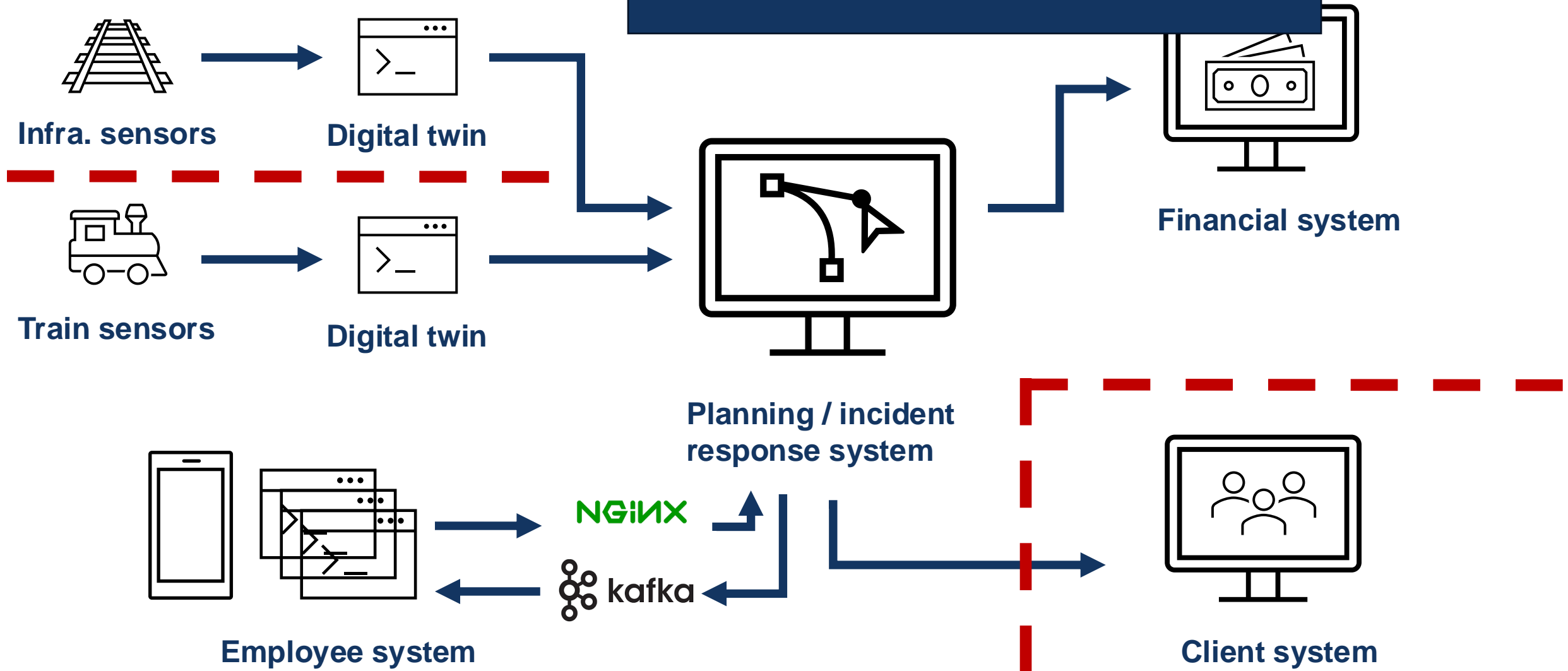


## Mission critical



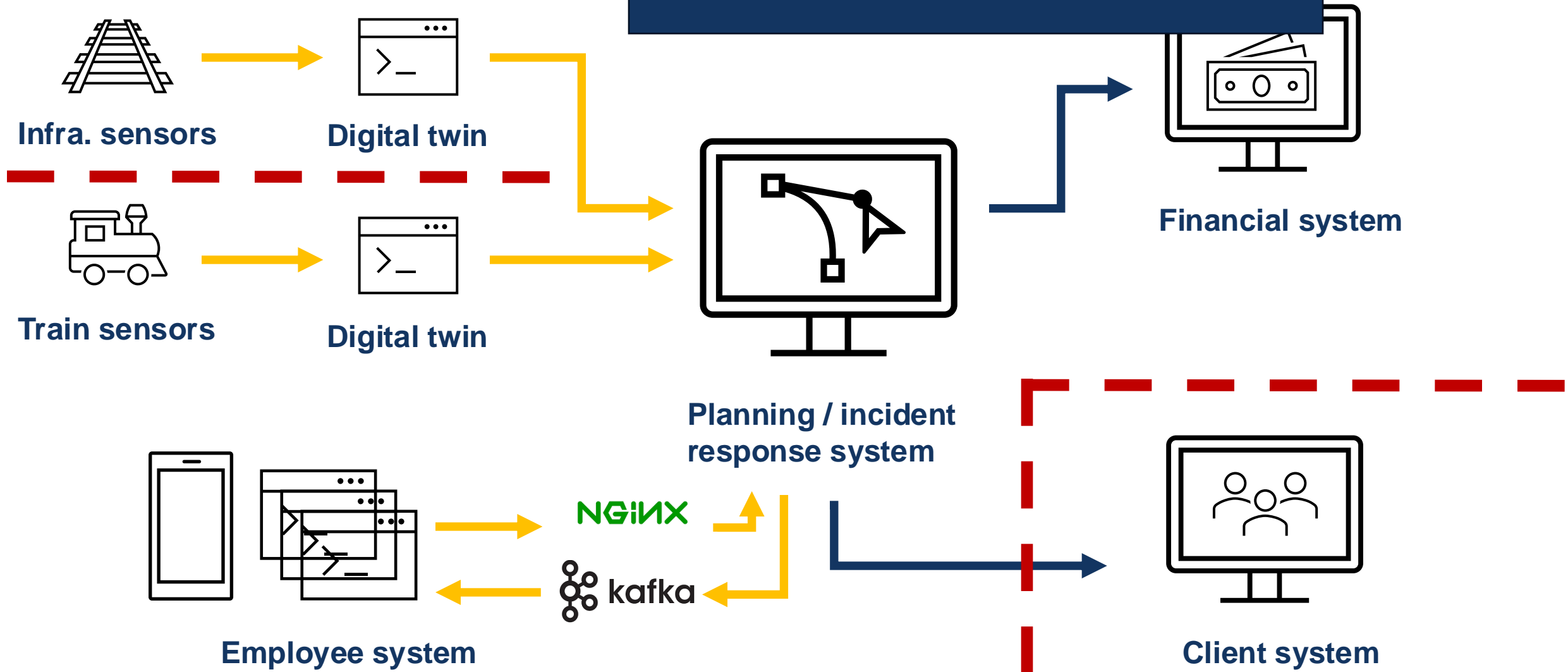
# ▲ Mission critical

Group exercise:  
What might the BIV classifications and  
Service Level Agreements look like in a  
transportation system?



## Mission critical

- Things to think about:
1. Chain of applications supports business goal
  2. Dependencies should have higher SLA

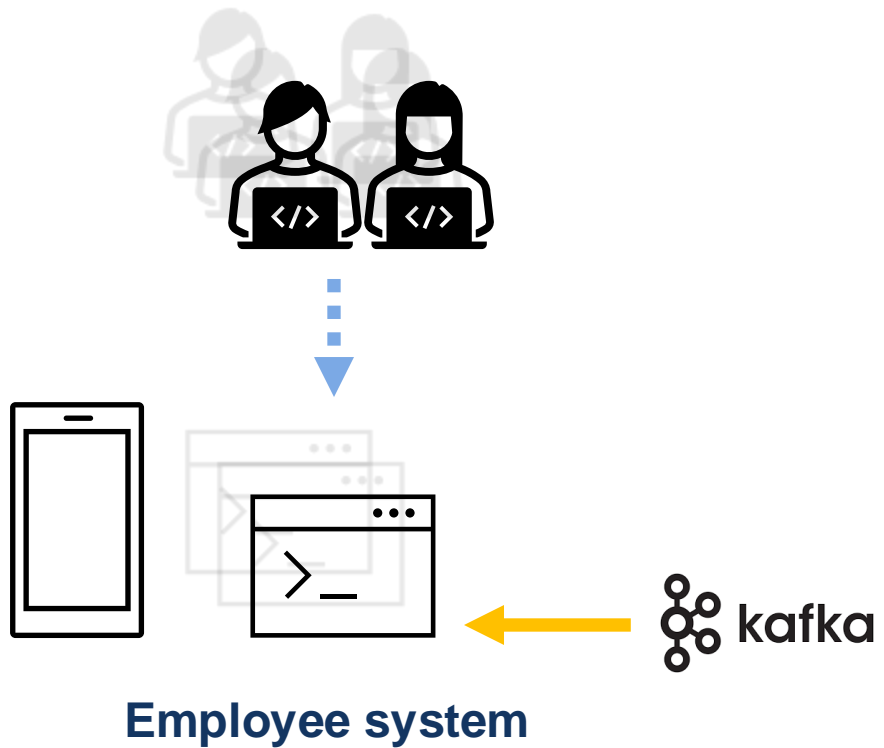


## Mission critical

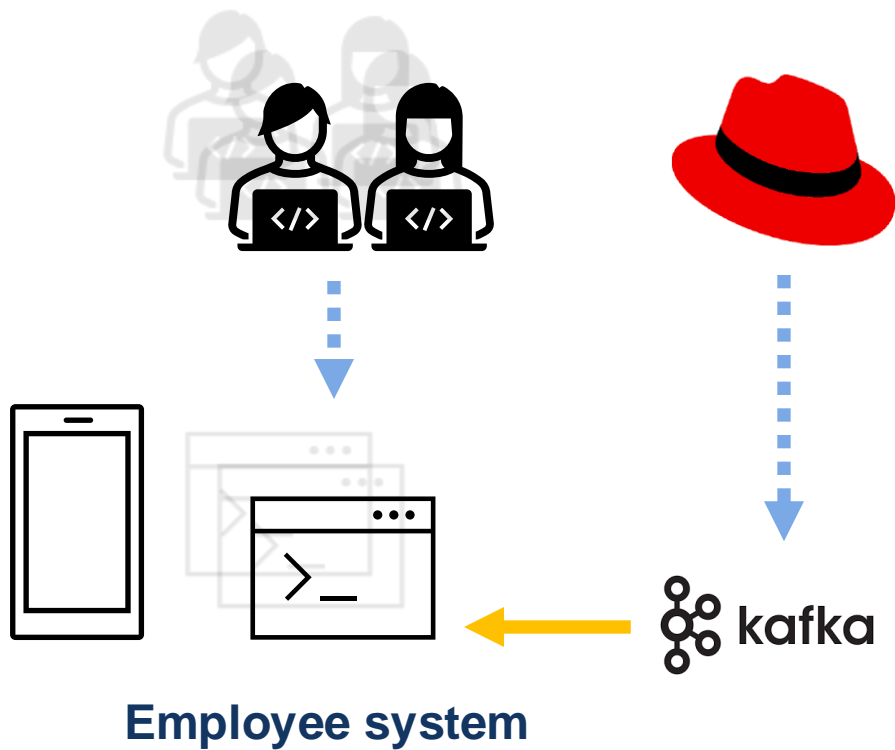




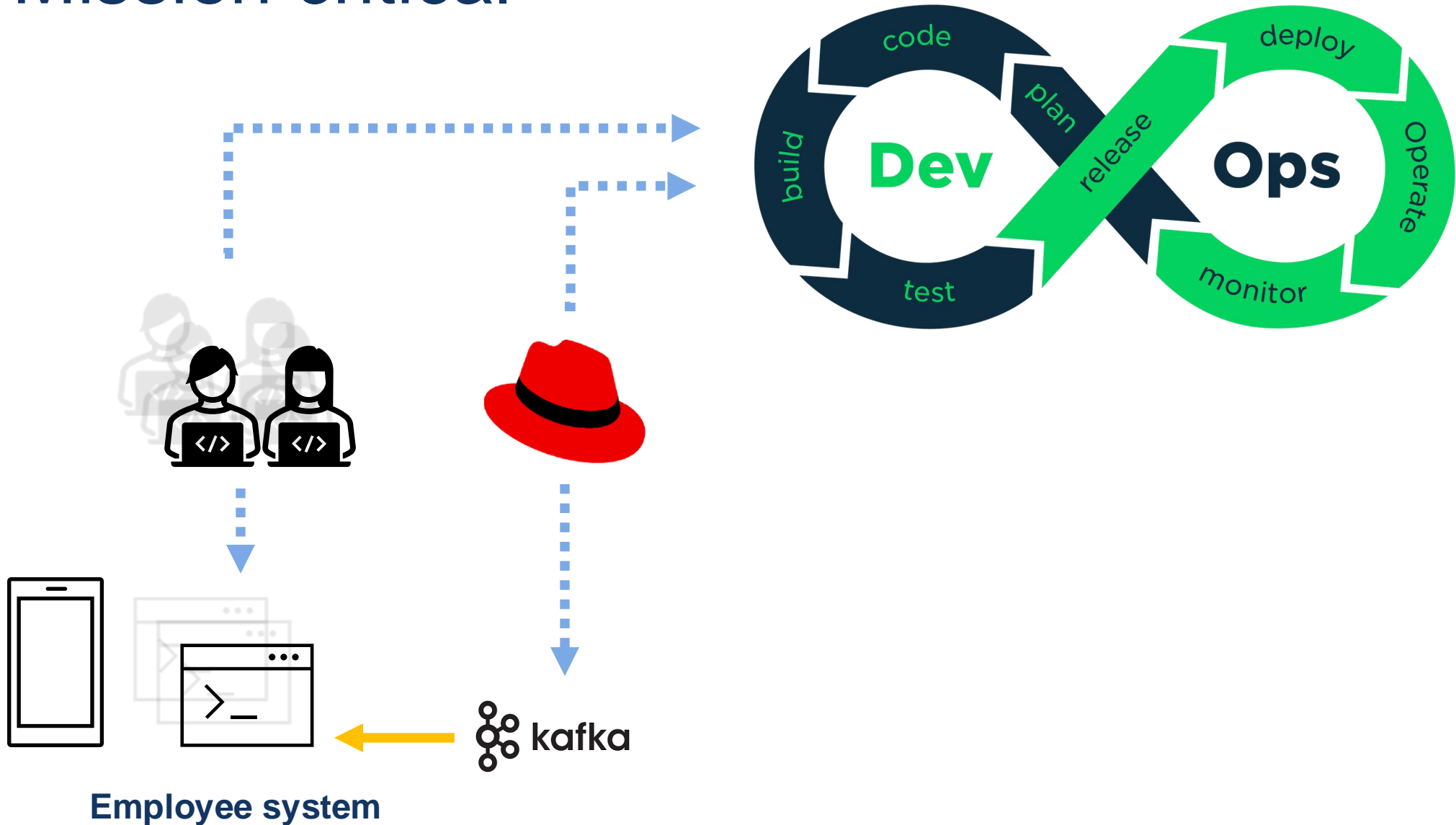
## ▲ Mission critical



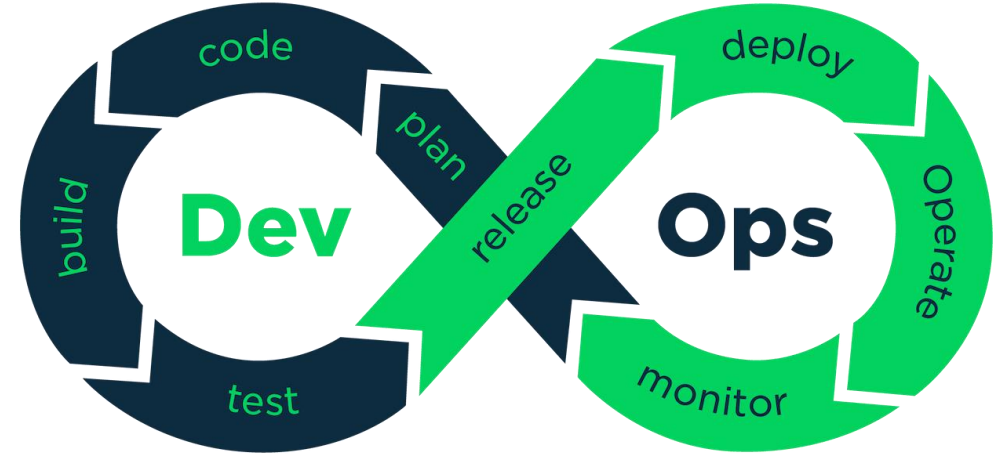
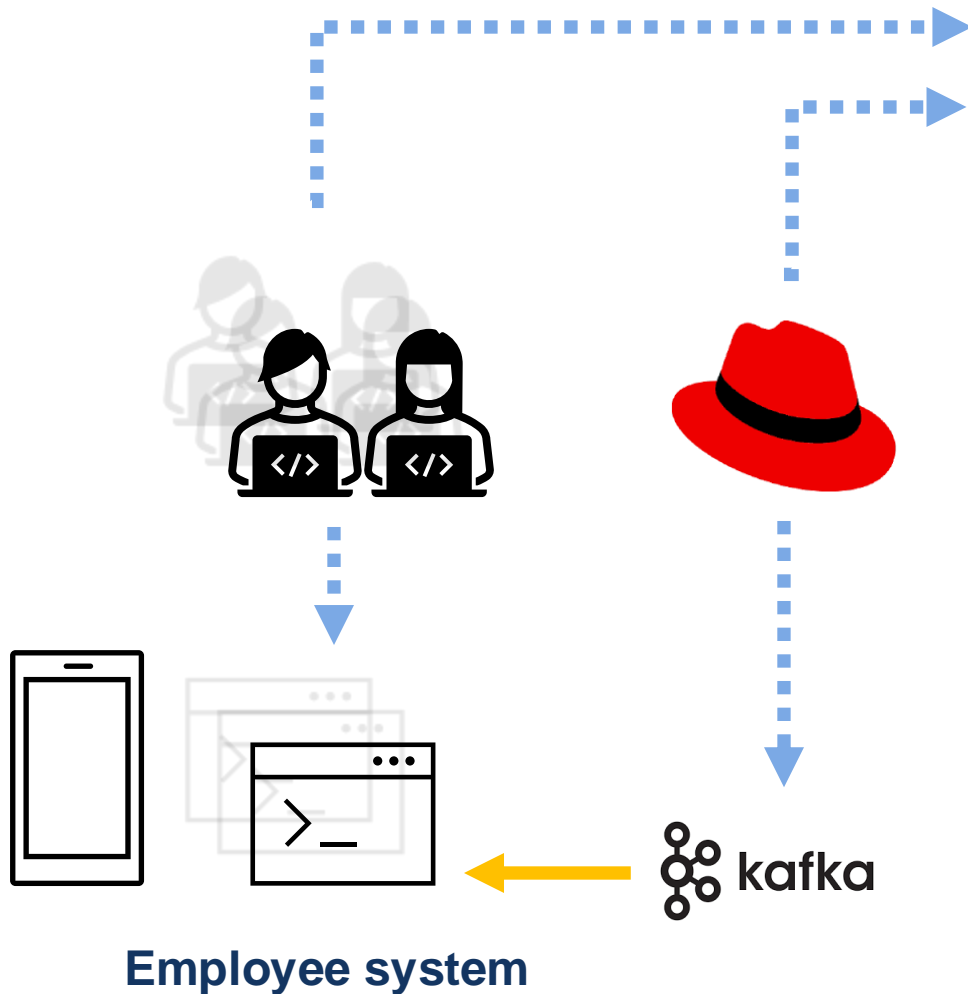
## ▲ Mission critical



## Mission critical

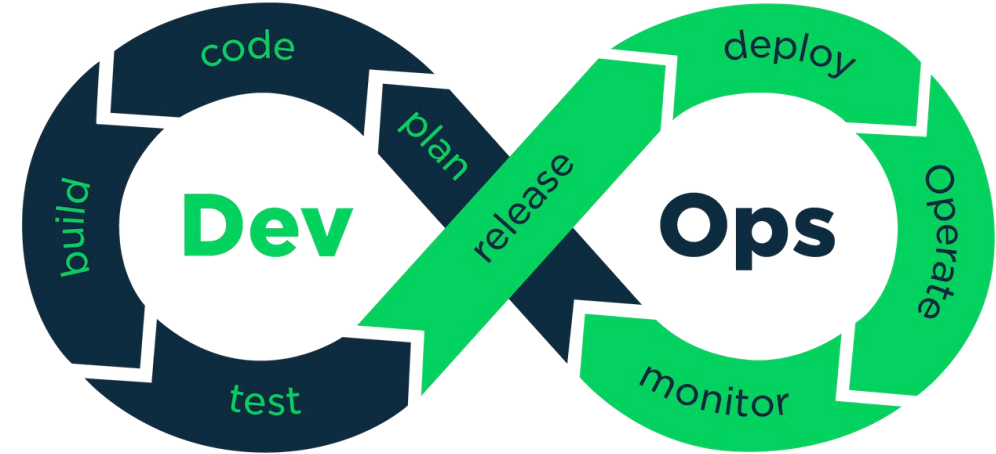
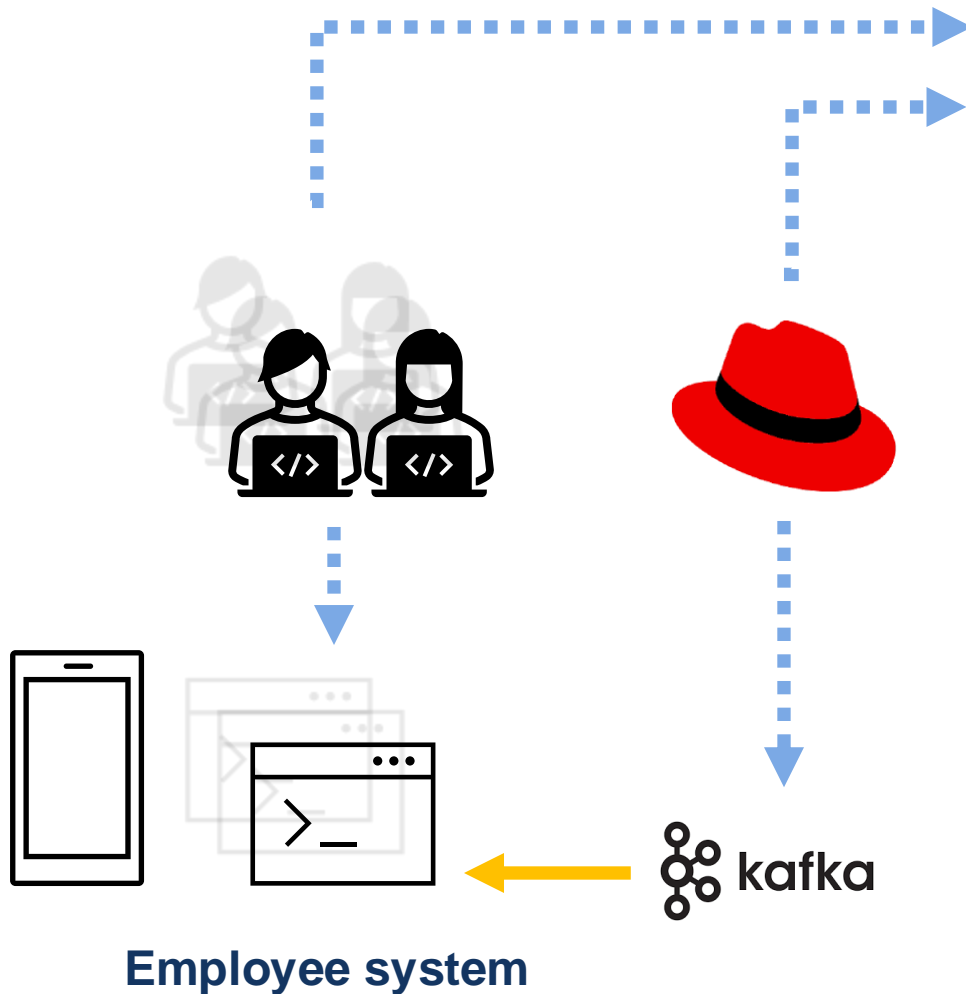


## Mission critical



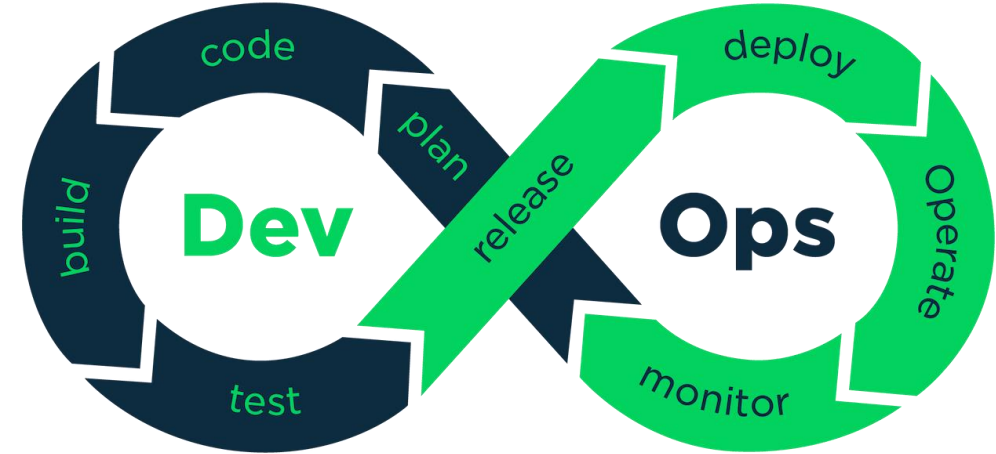
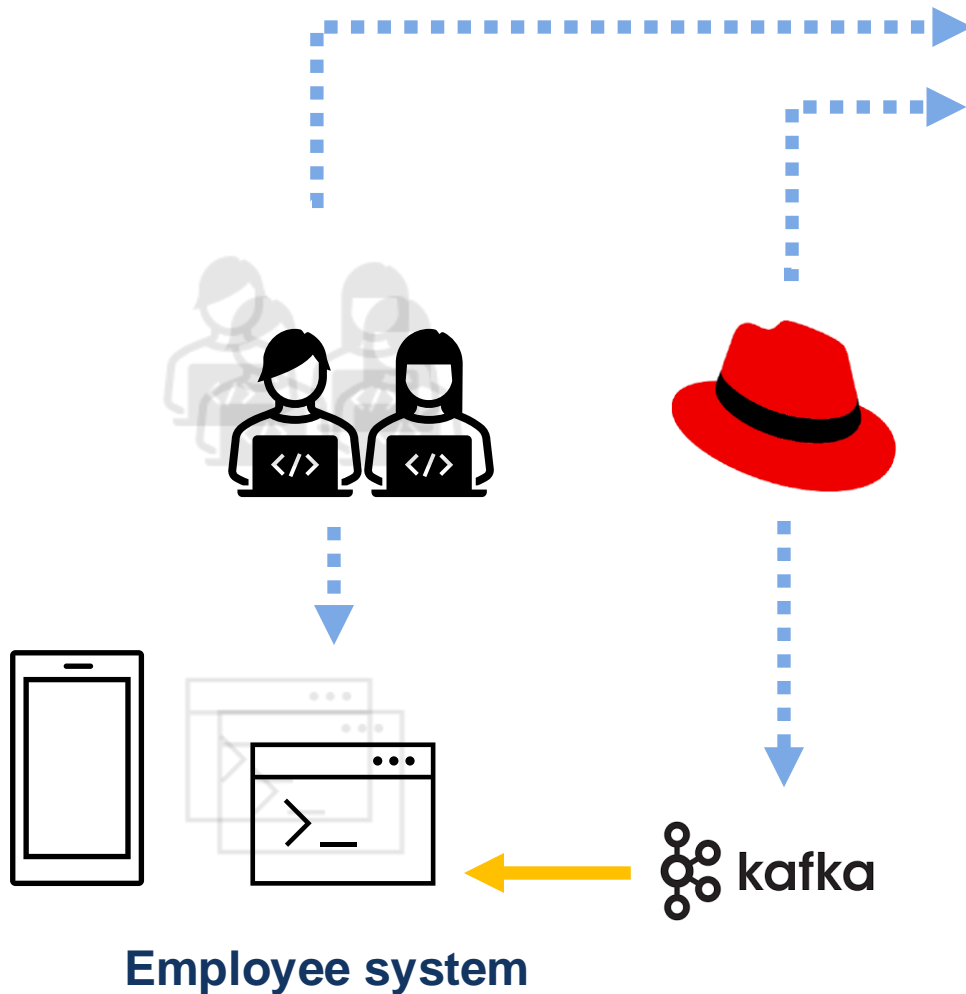
1. We need to make changes to the system

## Mission critical



1. We need to make changes to the system
2. Risk of system failure

## Mission critical



1. We need to make changes to the system
2. Risk of system failure
3. Additional measures for mission critical DevOps



# Break (15 min)



# Development

Requirements: 332 & 99.95 (RTO 20m, RPO 0m)

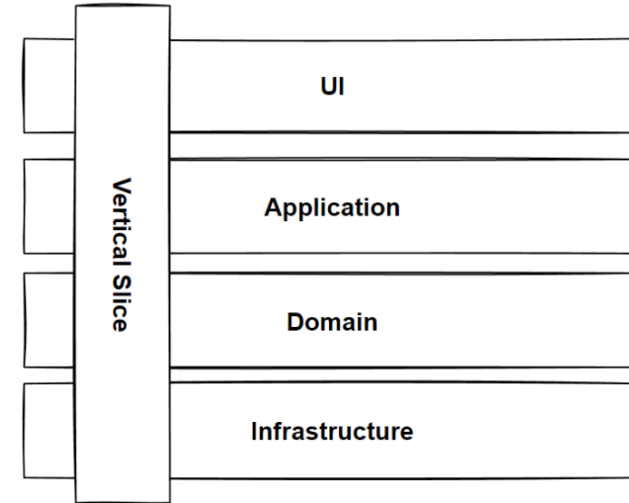
Plan – Code – Build - Test



# ▲ Plan for separation of concerns

## Segmentation of business processes

- Vertical slicing in code
- Microservices



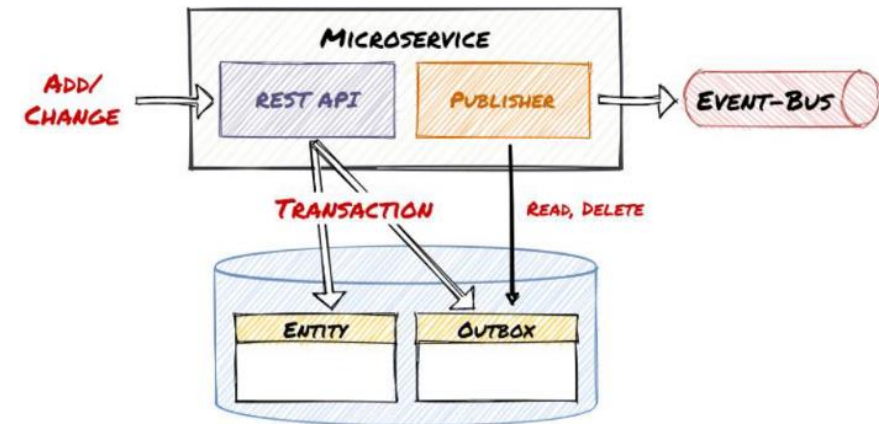
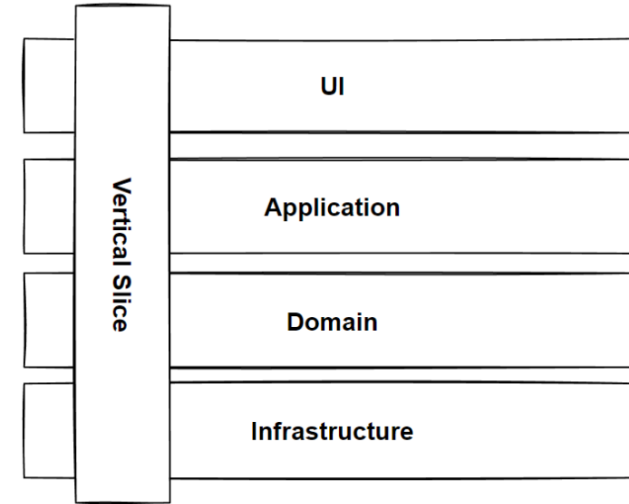
# Plan for separation of concerns

## Segmentation of business processes

- Vertical slicing in code
- Microservices

## Transactional boundaries

- Consider eventual consistency
- Outbox pattern
- Saga pattern



# Plan for separation of concerns

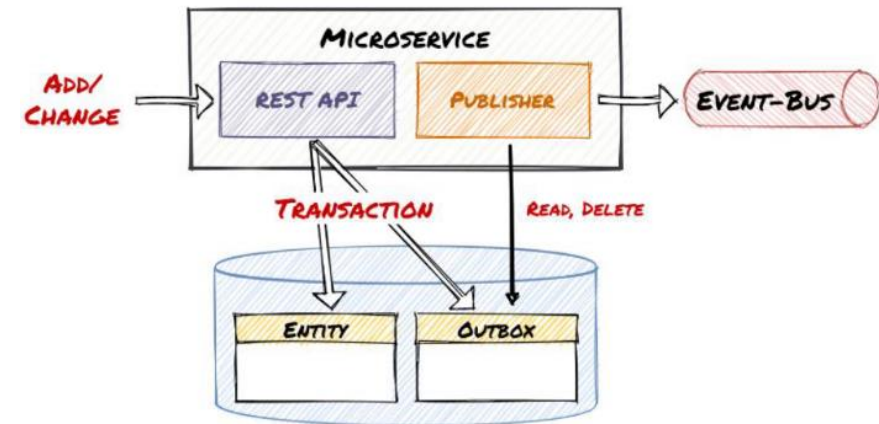
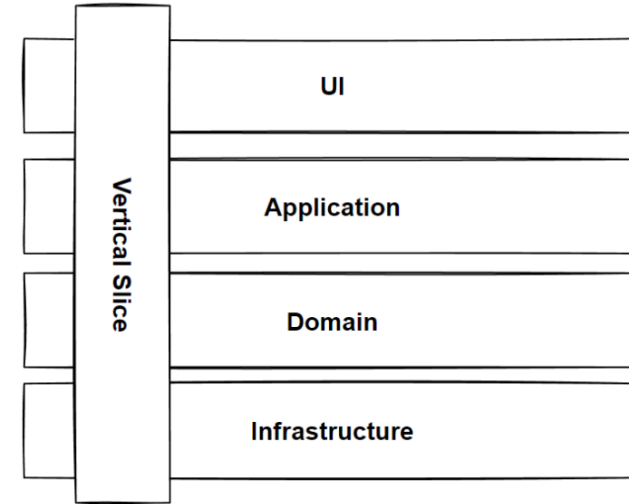
## Segmentation of business processes

- Vertical slicing in code
- Microservices

## Transactional boundaries

- Consider eventual consistency
- Outbox pattern
- Saga pattern

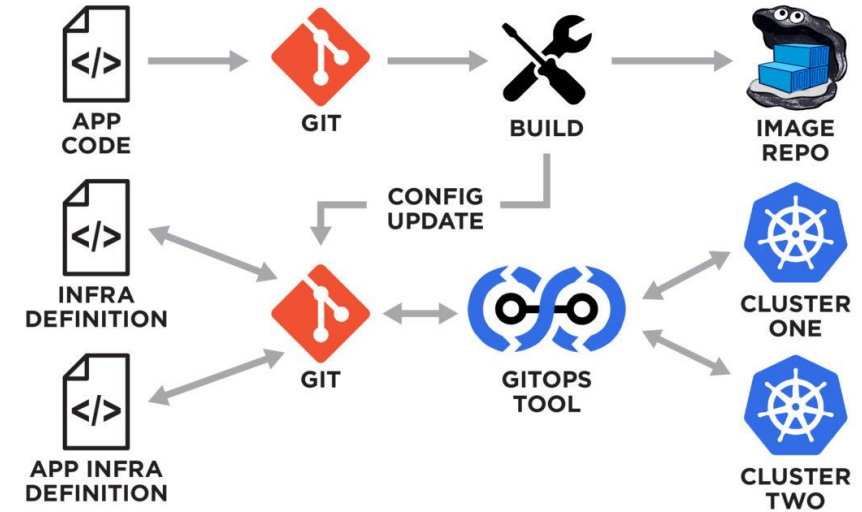
## Least privilege principles



# Plan a disaster recovery

## Application

- Infrastructure as Code
- Cloud
- GitOps



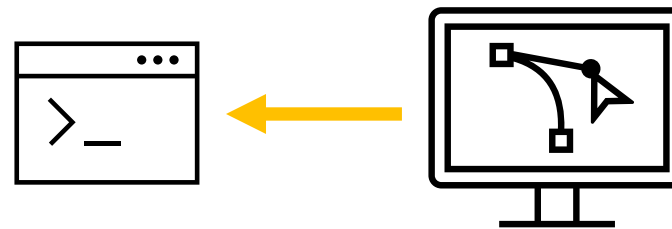
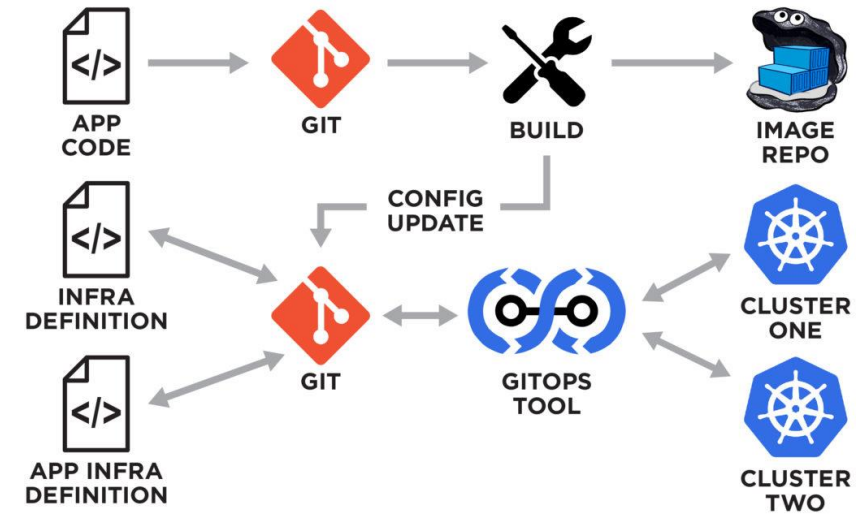
# Plan a disaster recovery

## Application

- Infrastructure as Code
- Cloud
- GitOps

## Data

- Restore backups
- Recreate database state



# Plan a disaster recovery

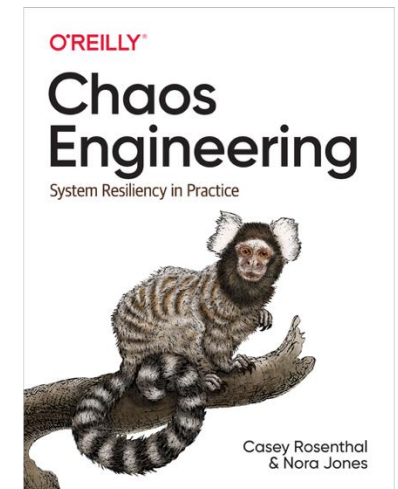
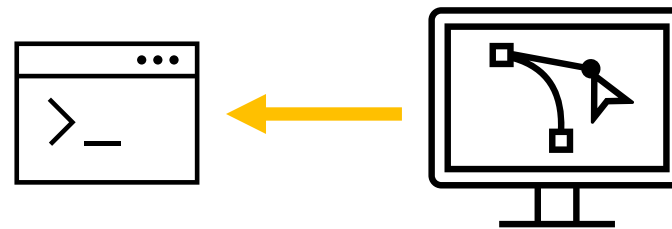
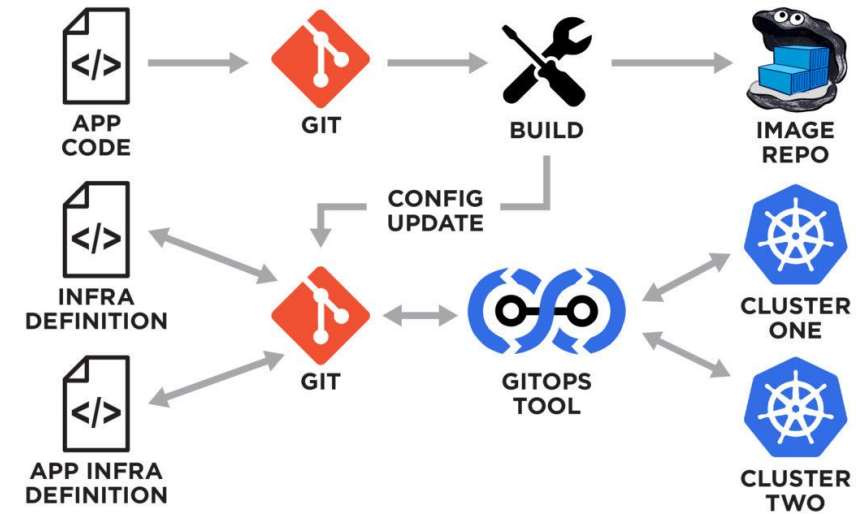
## Application

- Infrastructure as Code
- Cloud
- GitOps

## Data

- Restore backups
- Recreate database state

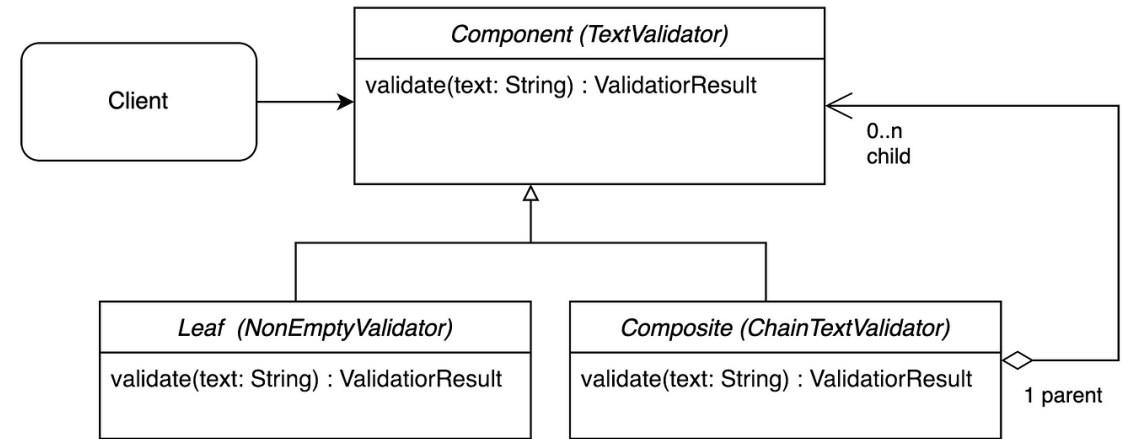
## Practice (game days)



# Code for unexpected behavior

## Defensive programming

- Understand all input data
- Validators (whitelisting)
- Shared contracts



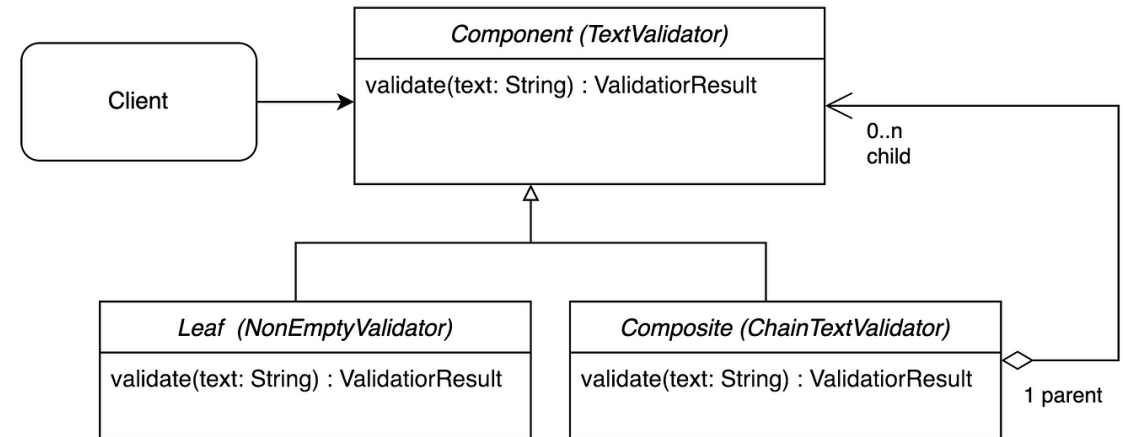
# Code for unexpected behavior

## Defensive programming

- Understand all input data
- Validators (whitelisting)
- Shared contracts

## Explicit programming

- Expect exceptions (Polly)
- Clear log levels
- Explicit code branches



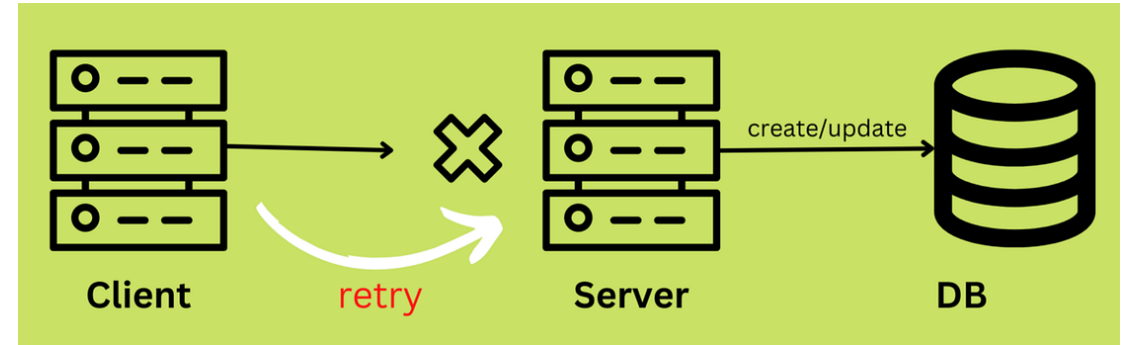
```
// =====
// PLEASE DO NOT ATTEMPT TO SIMPLIFY THIS CODE.
// KEEP THE SPACE SHUTTLE FLYING.
// =====
//
// This controller is intentionally written in a very verbose style. You will
// notice:
//
// 1. Every 'if' statement has a matching 'else' (exception: simple error
//    checks for a client API call)
// 2. Things that may seem obvious are commented explicitly
```



## Code for consistency

Idempotence

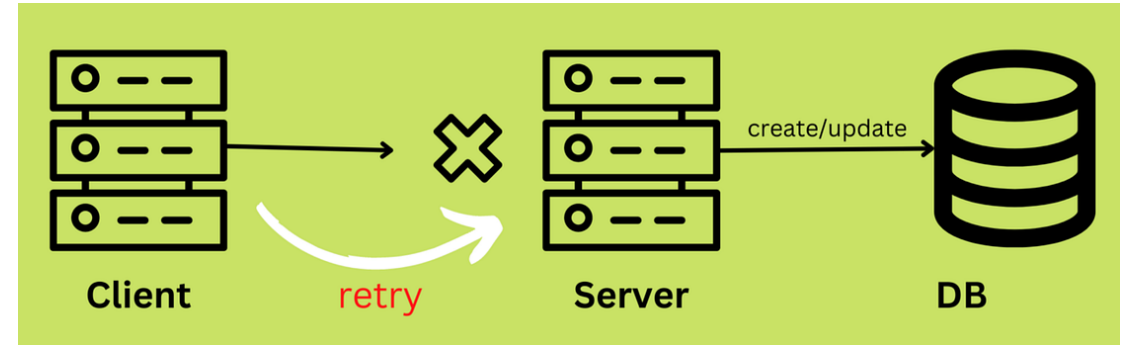
- Identifier with requests



## Code for consistency

### Idempotence

- Identifier with requests
- State machines
- Order of events w/timestamps

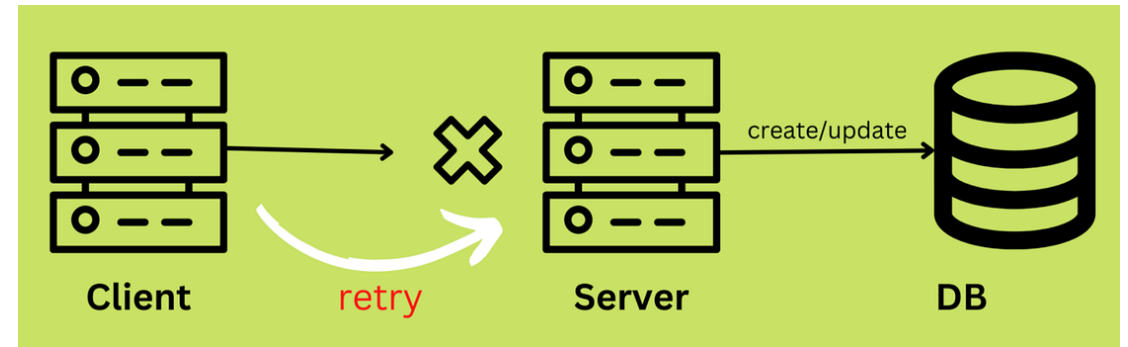


```
var latestUpdate:DateTime = FindLatestUpdate(message.id);  
  
if (latestUpdate >= message.timestamp) return;  
  
Process(message);
```

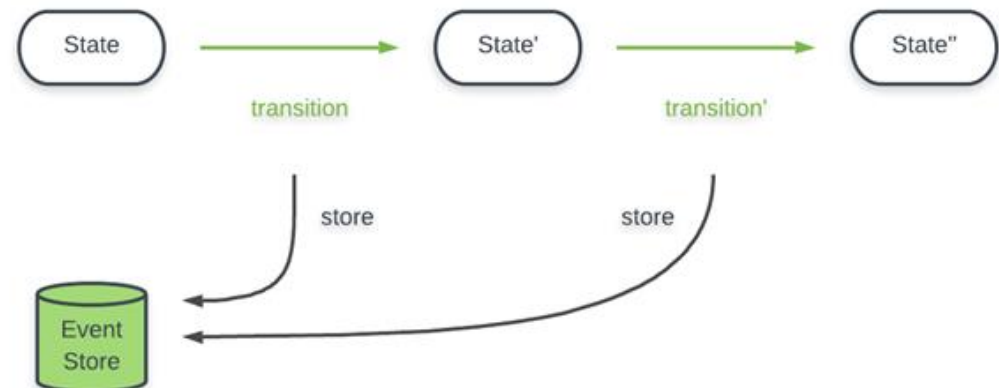
# Code for consistency

## Idempotence

- Identifier with requests
- State machines
- Order of events w/timestamps
- Event sourcing



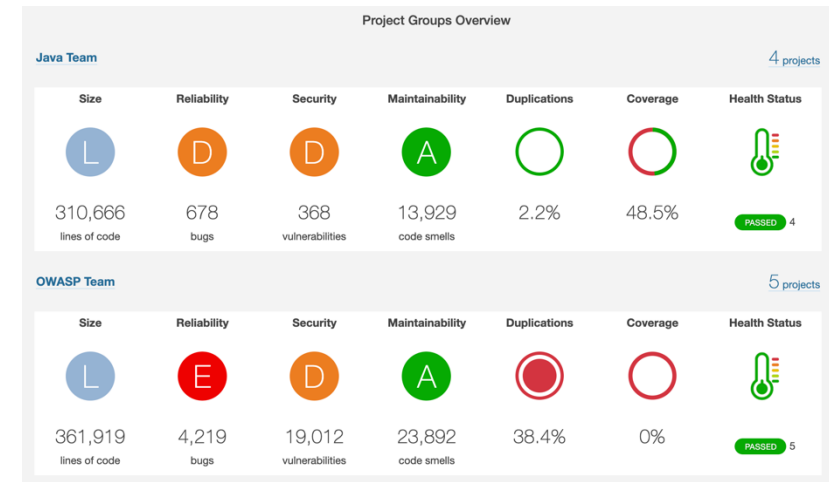
```
var latestUpdate:DateTime = FindLatestUpdate(message.id);  
  
if (latestUpdate >= message.timestamp) return;  
  
Process(message);
```



# Building reliable software

## Static code analysis

- All checks pass before merge



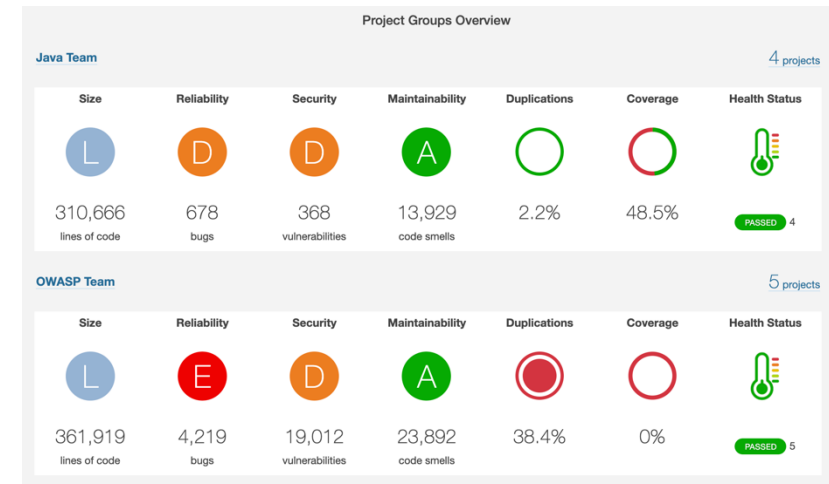
# Building reliable software

## Static code analysis

- All checks pass before merge

## Vulnerability scanning

- Vulnerabilities
- Misconfigurations
- Secrets



Total: 1 (UNKNOWN: 0, LOW: 0, MEDIUM: 0, HIGH: 1, CRITICAL: 0)

LIBRARY	VULNERABILITY ID	SEVERITY	INSTALLED VERSION	FIXED VERSION	TITLE
musl	CVE-2019-14697	HIGH	1.1.22-r2	1.1.22-r3	musl libc through 1.1.23 has an x87 floating-point stack adjustment imbalance, related...

# Building reliable software

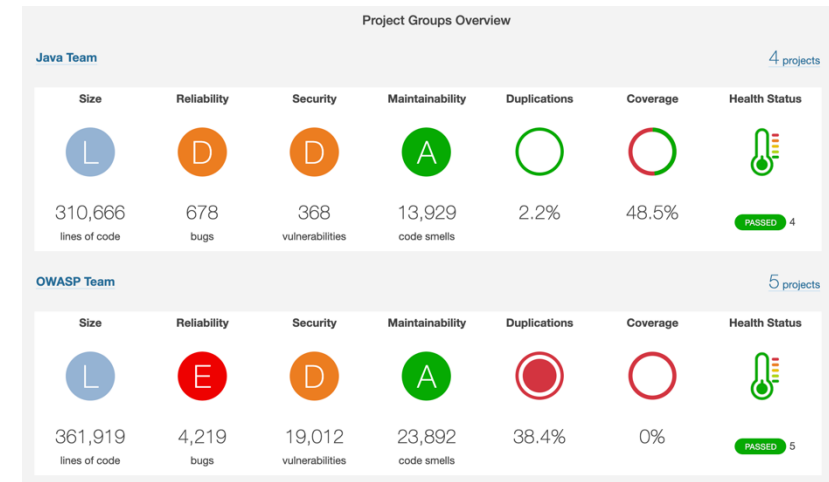
## Static code analysis

- All checks pass before merge

## Vulnerability scanning

- Vulnerabilities
- Misconfigurations
- Secrets

## Semantic versioning of containers



Total: 1 (UNKNOWN: 0, LOW: 0, MEDIUM: 0, HIGH: 1, CRITICAL: 0)

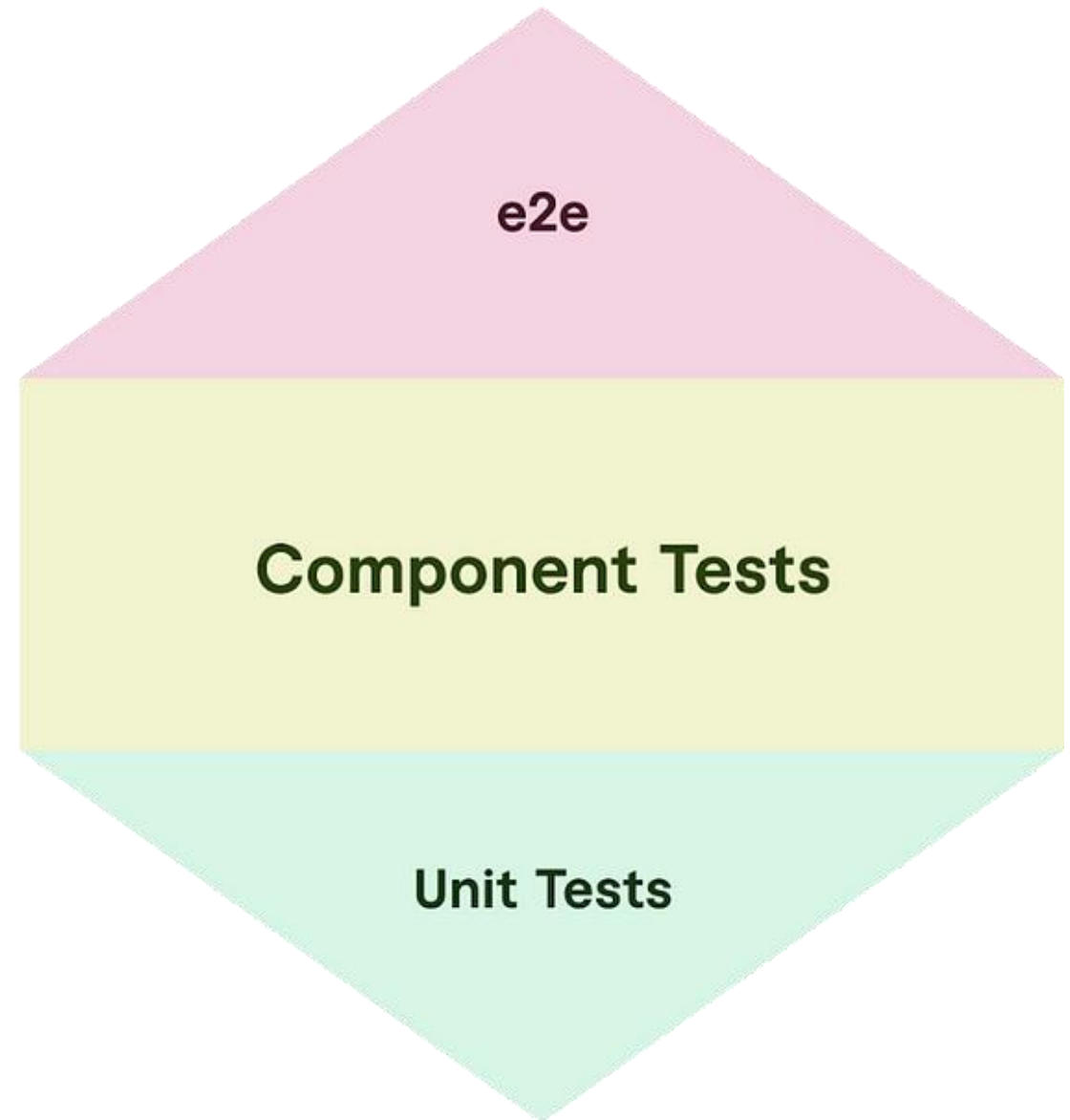
LIBRARY	VULNERABILITY ID	SEVERITY	INSTALLED VERSION	FIXED VERSION	TITLE
musl	CVE-2019-14697	HIGH	1.1.22-r2	1.1.22-r3	musl libc through 1.1.23 has an x87 floating-point stack adjustment imbalance, related...

4.2.1  
MAJOR Minor patch

# Testing for regression

Unit tests

- Complex methods



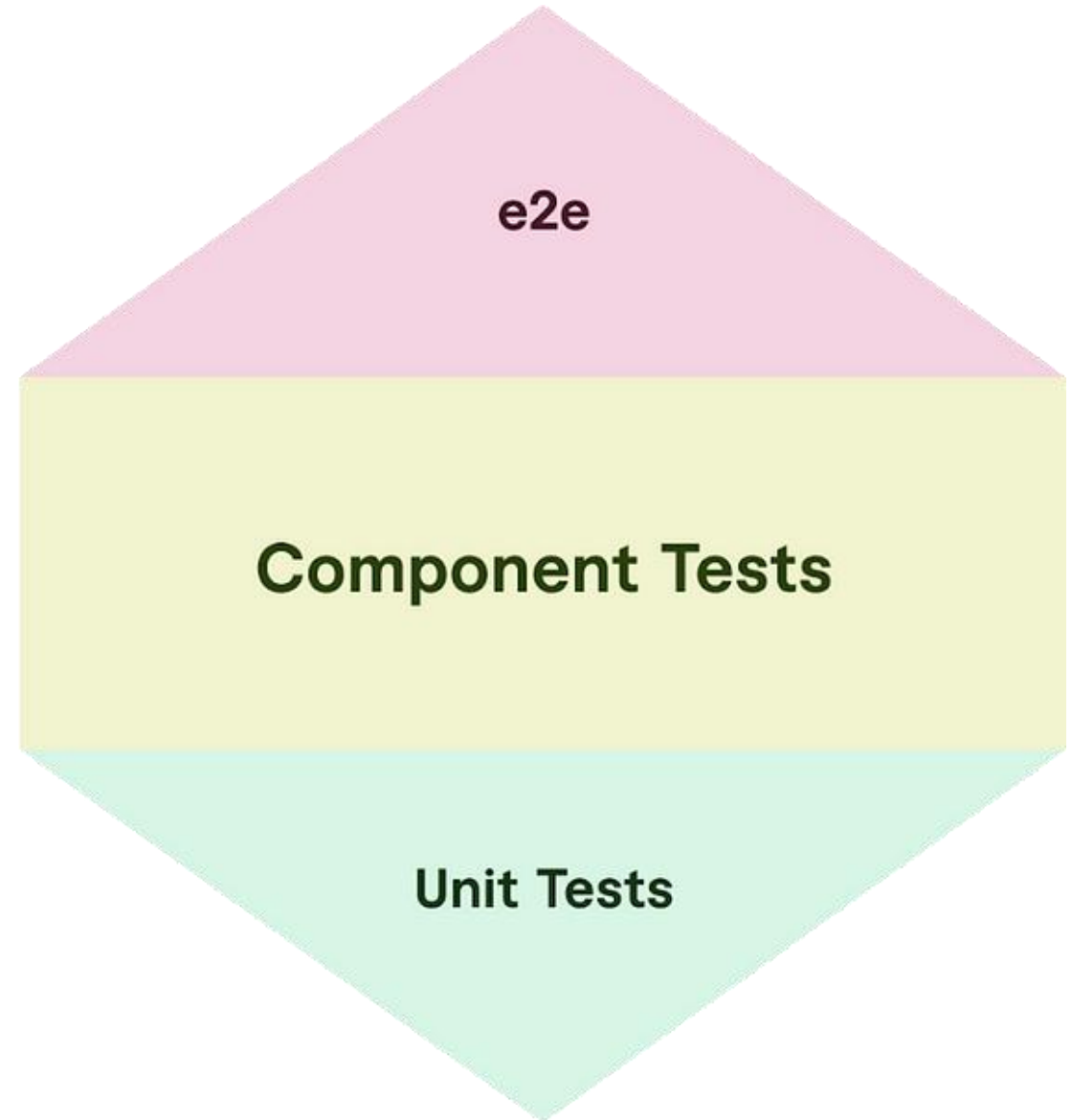
# Testing for regression

Unit tests

- Complex methods

Component tests

- User flows
- Contracts





# Testing for regression

## Unit tests

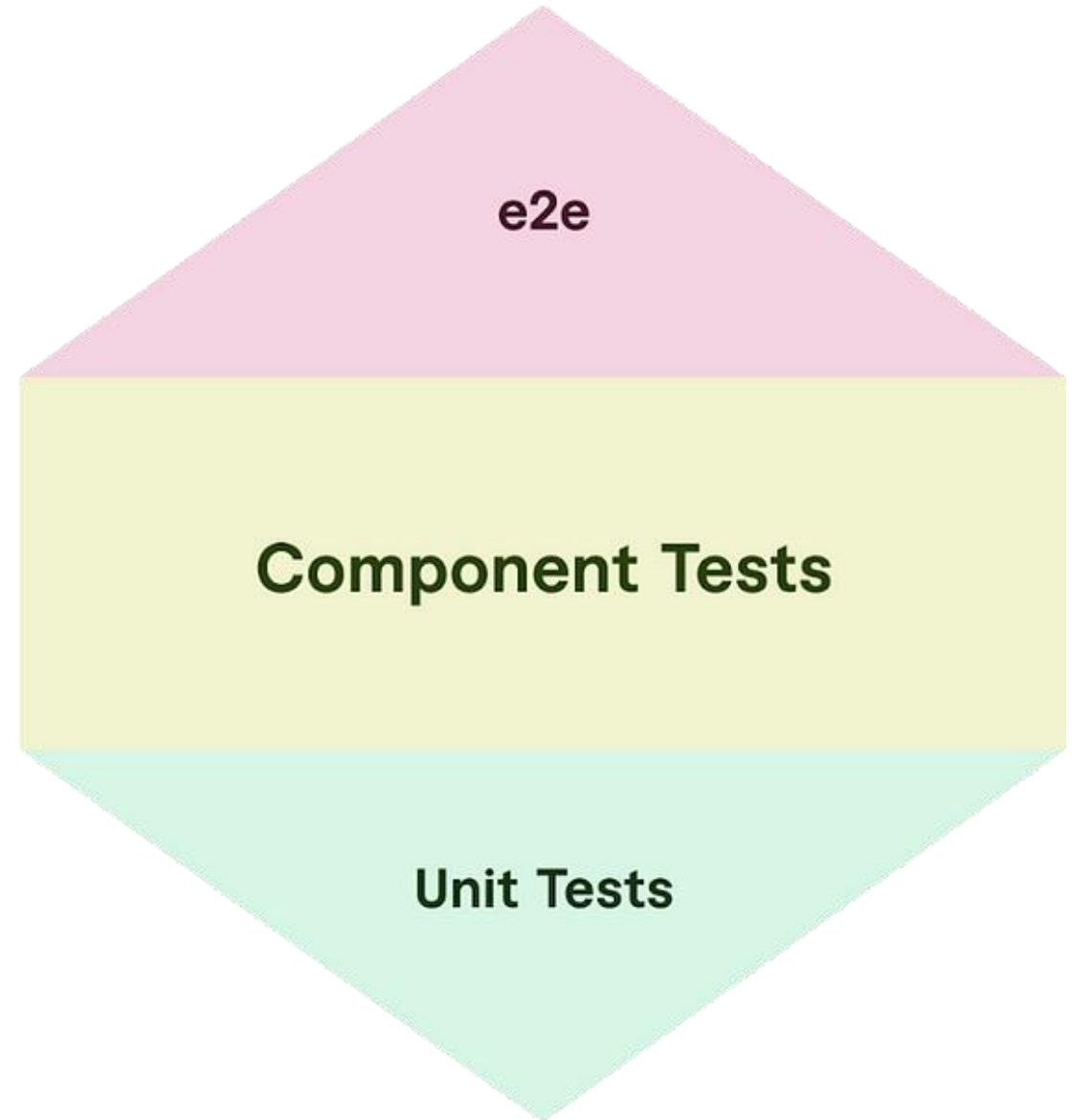
- Complex methods

## Component tests

- User flows
- Contracts

## End-2-End tests on staging

- Mission critical flow
- Performance





# Operations

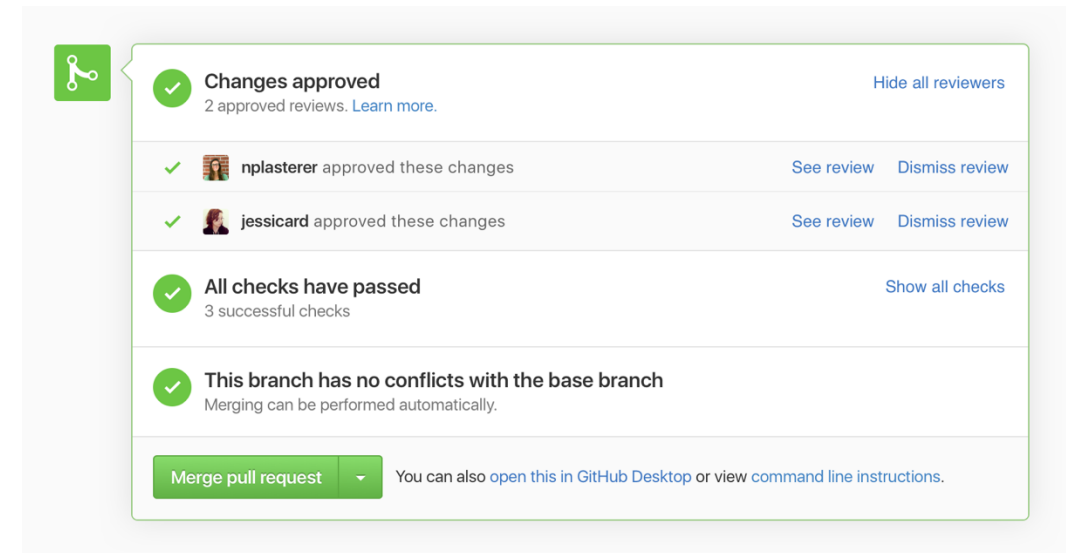
Requirements: 332 & 99.95 (RTO 20m, RPO 0m)

Release – Deploy – Operate - Monitor

# Release with confidence

## Four eyes principle

- Have enough knowledge in the team
- Changes are always traceable



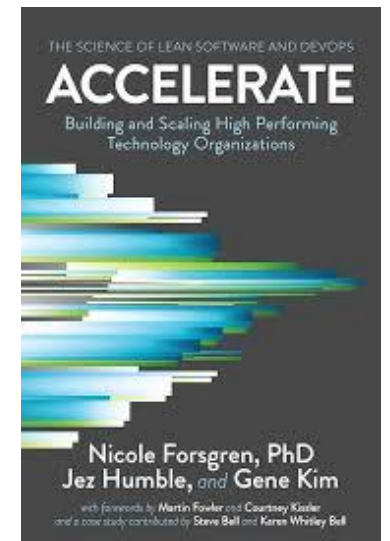
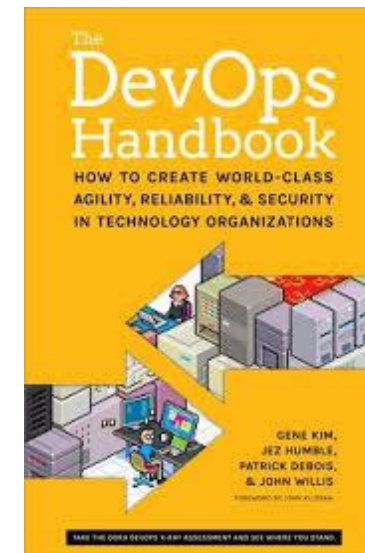
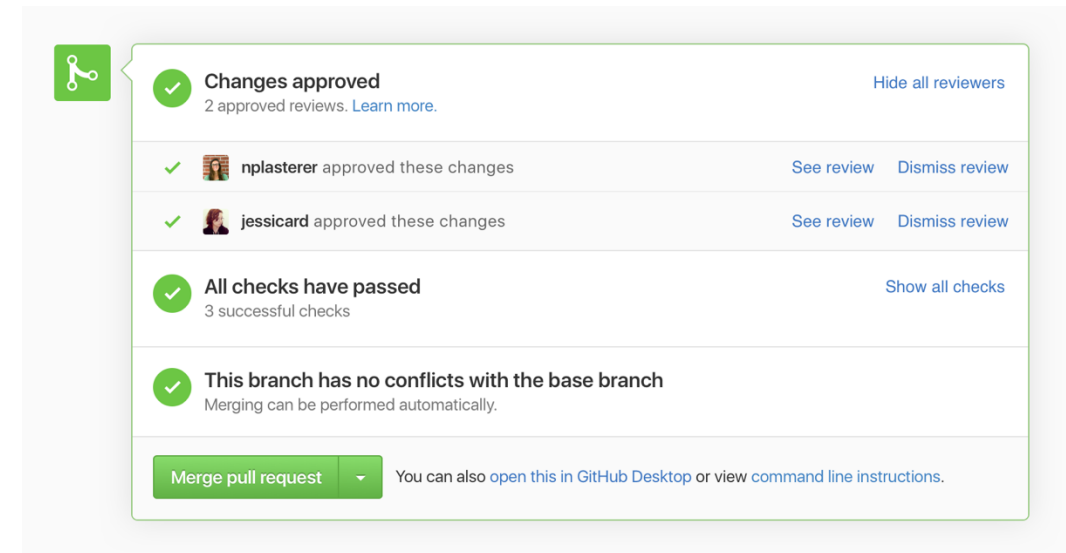
# Release with confidence

## Four eyes principle

- Have enough knowledge in the team
- Changes are always traceable

## Continuous integration & deployment

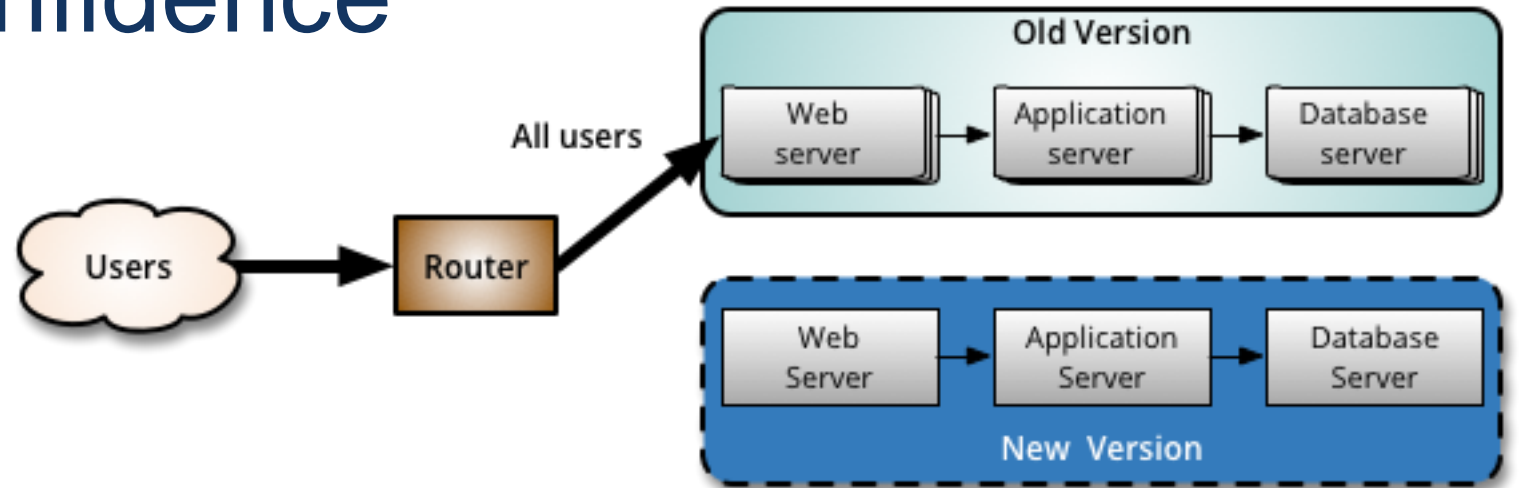
- Trunk based development
- Reduce batch size



# Deploy with confidence

## Canary releases

- Readiness checking
- Canary (back-end)
- Blue/green (front-end)



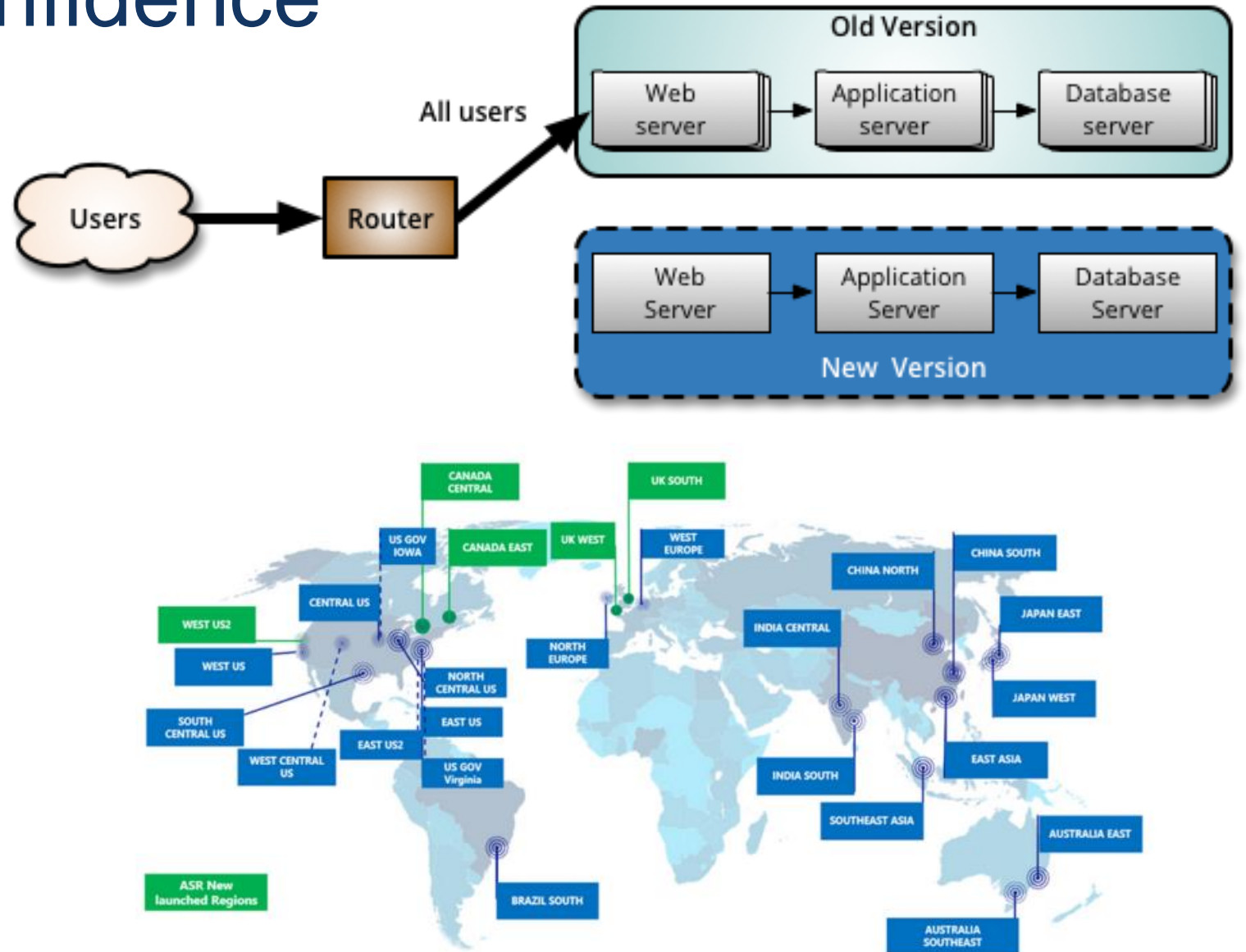
# Deploy with confidence

## Canary releases

- Readiness checking
- Canary (back-end)
- Blue/green (front-end)

## Highly available cluster

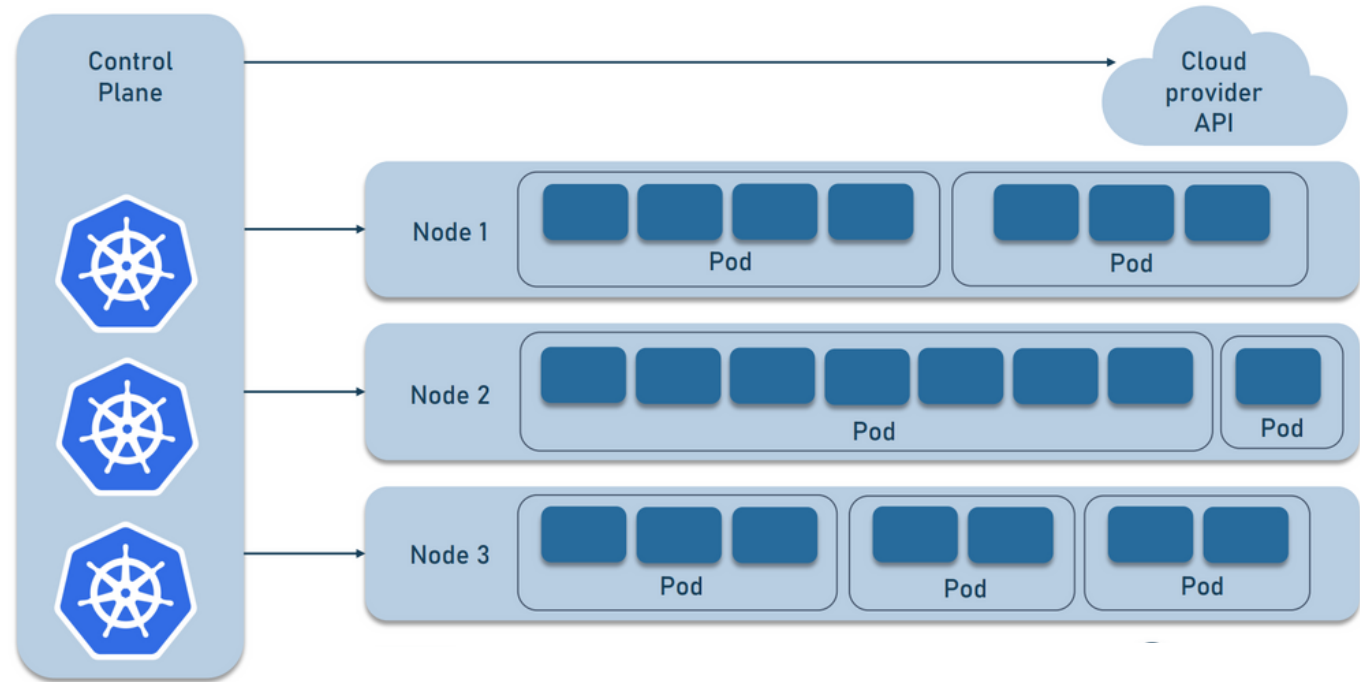
- Active-Active
- Failover zone & region



# ▲ Operate autonomously

## Kubernetes

- Auto scaling
- Self-healing
- Multi-tenancy



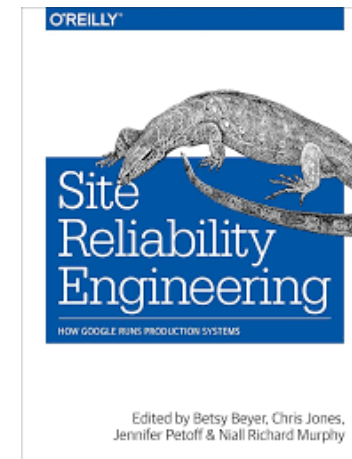
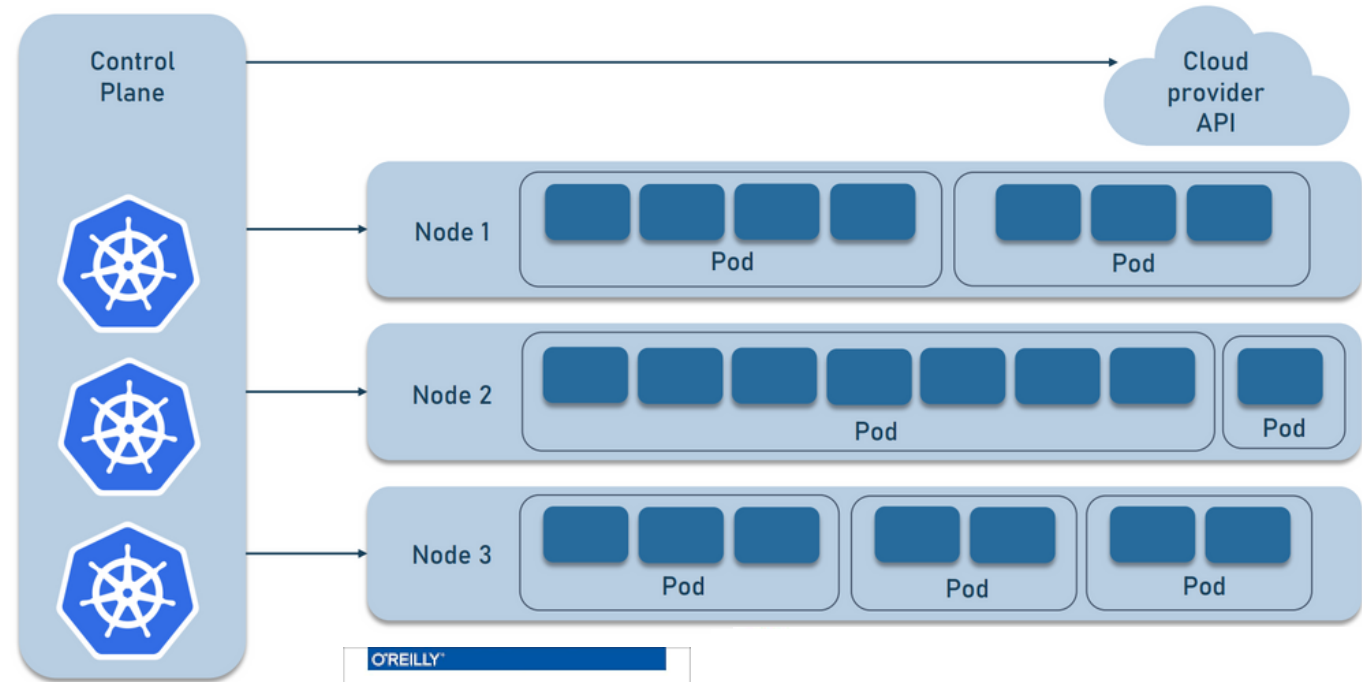
# Operate autonomously

## Kubernetes

- Auto scaling
- Self-healing
- Multi-tenancy

## Stand-by/on-call

- Daytime
- Evenings/Nighttime/Weekends
- Postmortems (with resolution)



A template for a post-mortem report. It includes a title 'Post-mortem', a 'Summary' section with a list, an 'Impact' section with a list, a 'Root Cause Analysis' section with a list, a 'Resolution and Recovery' section with a list, and a 'Corrective and Preventative Measures' section with a table. The table has three columns: 'Measure', 'Responsible Party', and 'Work Ticket'.

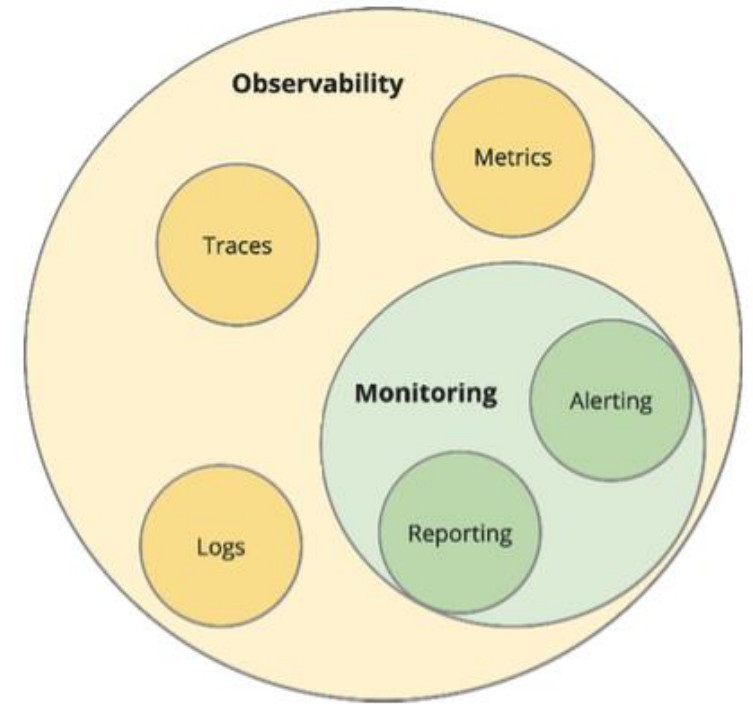
Measure	Responsible Party	Work Ticket



# Monitor for full understanding

## Observability & Monitoring

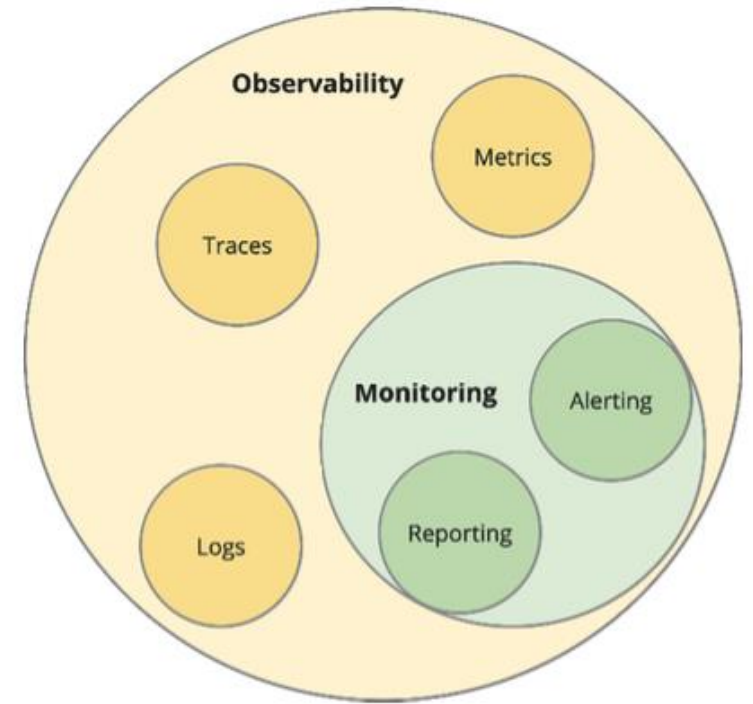
- Metrics, Traces, Logs
- Alerts, Reports



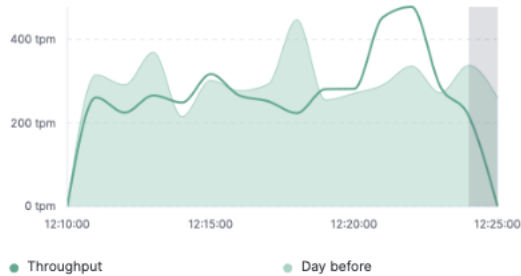
# Monitor for full understanding

## Observability & Monitoring

- Metrics, Traces, Logs
- Alerts, Reports



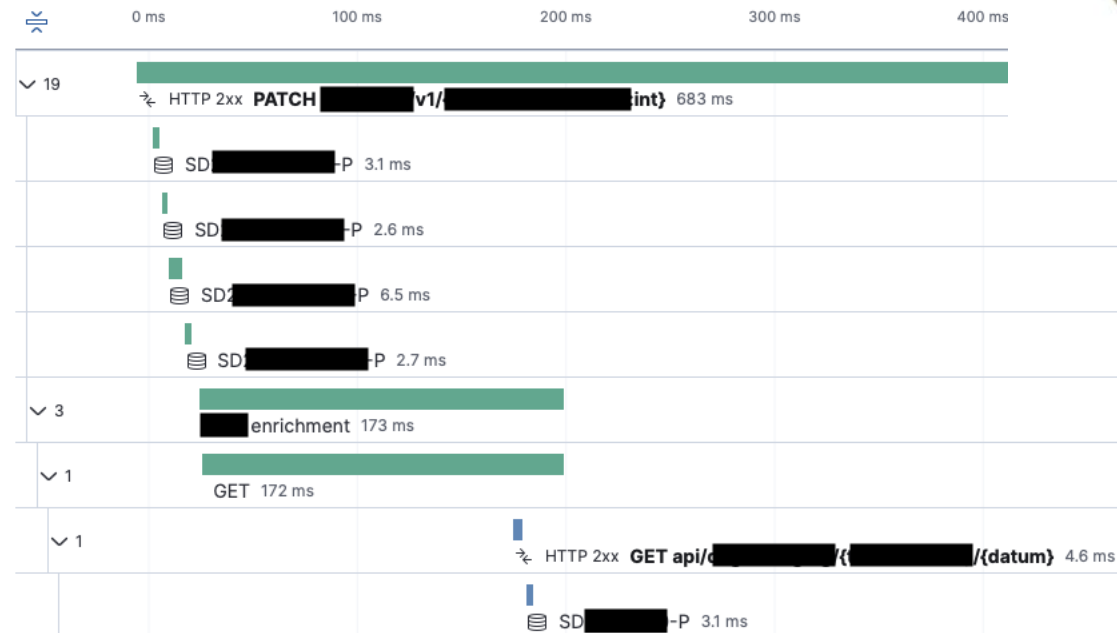
Throughput ②



Failed transaction rate ②



Services ● Service ● System



# Questions



- ❖ Thesis, career?
- ❖ Get in touch!
- ❖ <https://infosupport.com>



- ❖ LinkedIn?
- ❖ Let's link up!
- ❖ [Dimitri.Hoofman@infosupport.com](mailto:Dimitri.Hoofman@infosupport.com)