

E-Voting Challenges

15.12.2025





Céline Camacho
E-Voting Software Engineer



Nils Aellen
E-Voting Solution Architect



Swiss Post

- **Physical and digital world**
- **Bound to mail secrecy & trusted**
- **Cryptography competence center**

E-Voting

- **Codebase bought in 2020**
- **Productive again since June 2023**

E-Voting Phases

Setup

Configure election

Generate keys

Generate return codes

E-Voting Phases

Voting

1. Authenticate
2. Send vote
3. Confirm vote

E-Voting Phases

The screenshot displays the Swiss Post e-voting interface. At the top left is the Swiss Post logo (a red cross on a yellow square followed by a black 'P'). To the right of the logo are language options: DE, FR, IT, RM, **EN**, and a Help icon with a question mark. Below the logo is a vertical navigation menu with seven steps: 1. Explanations and legal regulations (checked), 2. **Start Voting** (highlighted with a triangle), 3. Select your choices, 4. Verify your vote, 5. Verify codes, 6. Enter your confirmation code, and 7. Verify finalization code.

The main content area is titled '2 Start voting' and contains two sections:

- Enter the Initialization Code**: A sub-header with the instruction 'The code is printed card 2.' Below this is a grey header bar with a triangle icon and the text 'Initialization Code', followed by a link: '? What is the Initialization Code?'. A text input field contains the alphanumeric code 'a w g 5 3 1 k j s d v 9 2 0 9 3 4 8 n d j g v c' with a clear 'X' button on the right.
- Enter your date of birth**: A sub-header with the instruction 'Then press Start.' Below this is a grey header bar with the text 'Date of birth'. A text input field contains the date '0 1 . 0 6 . 1 9 8 0' with a clear 'X' button and a calendar icon on the right.

At the bottom right of the main content area is a dark 'Start →' button.

E-Voting Phases

The screenshot displays the Swiss Post e-voting interface. At the top left is the Swiss Post logo (a red cross on a yellow square followed by a black 'P'). To the right of the logo are language options: DE, FR, IT, RM, **EN**, and a Help icon with a question mark. Below the logo is a vertical progress bar with seven steps: 1. Explanations and legal regulations, 2. Start Voting, 3. Select your choices, 4. **Verify your vote** (current step), 5. Verify codes, 6. Enter your confirmation code, and 7. Verify finalization code. The main content area is titled '4 Verify your vote' and 'Review your choices and seal your ballot'. It features a 'Preferences' section with a 'Hide' button and an upward arrow. The first preference is '1. Do you like sunny weather?' with a text input field containing 'Yes'. Below this is an information box with an 'i' icon, stating: 'After sealing the ballot you will not be able to change your choices. As long as you have not entered the confirmation code in the following step 6, you can cancel the process at any time and instead vote by mail or at the ballot box. You can obtain the voting materials for postal voting or voting at the ballot box from [your municipality](#).' At the bottom, there are three buttons: 'Cancel voting process' (with a broken link icon), 'Change choices' (with a pencil icon), and 'Seal ballot' (with a lock icon).

E-Voting Phases

The screenshot displays the Swiss Post e-voting interface. At the top left is the Swiss Post logo (a red cross on a yellow background with a black 'P'). To the right of the logo are language options: DE, FR, IT, RM, **EN**, and a Help icon with a question mark. Below the logo is a vertical navigation menu with seven steps, each with a checkmark or icon and a description. Step 6 is highlighted with a circle around the number 6. The main content area is titled '6 Enter Confirmation Key' and contains the following elements:

- A heading: **Enter your Confirmation Key below and cast your vote into the electronic ballot box.**
- A section labeled 'Confirmation Key' with a black pentagon icon and a link: [? What is the Confirmation Key?](#)
- A text input field containing the code: 3 5 6 4 9 0 9 8 2, with a close button (X) on the right.
- An information box with an 'i' icon containing the text: "After confirming your vote, your vote is cast and you can no longer vote by mail or at the ballot box. As long as you have not entered the confirmation code, you can cancel the electronic voting process and instead vote by mail or at the polling station. You can obtain the voting material for postal voting or voting at the polling station from [your municipality](#)."
- At the bottom, there are three buttons: [Cancel voting process](#), [Back](#), and a dark button labeled **Confirm the vote** with a downward arrow icon.

E-Voting Phases

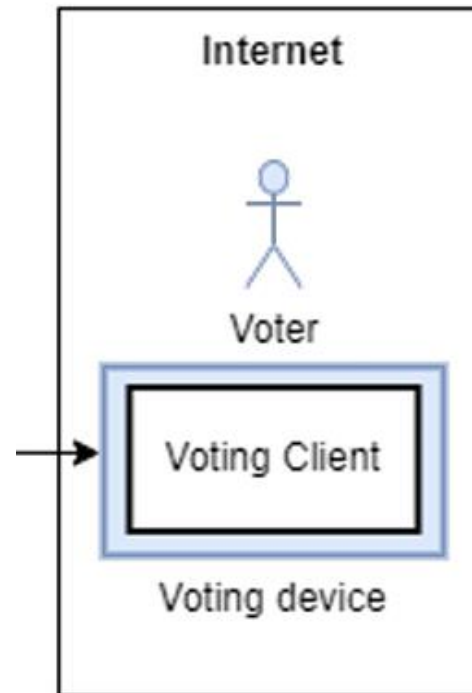
Tally

Mix

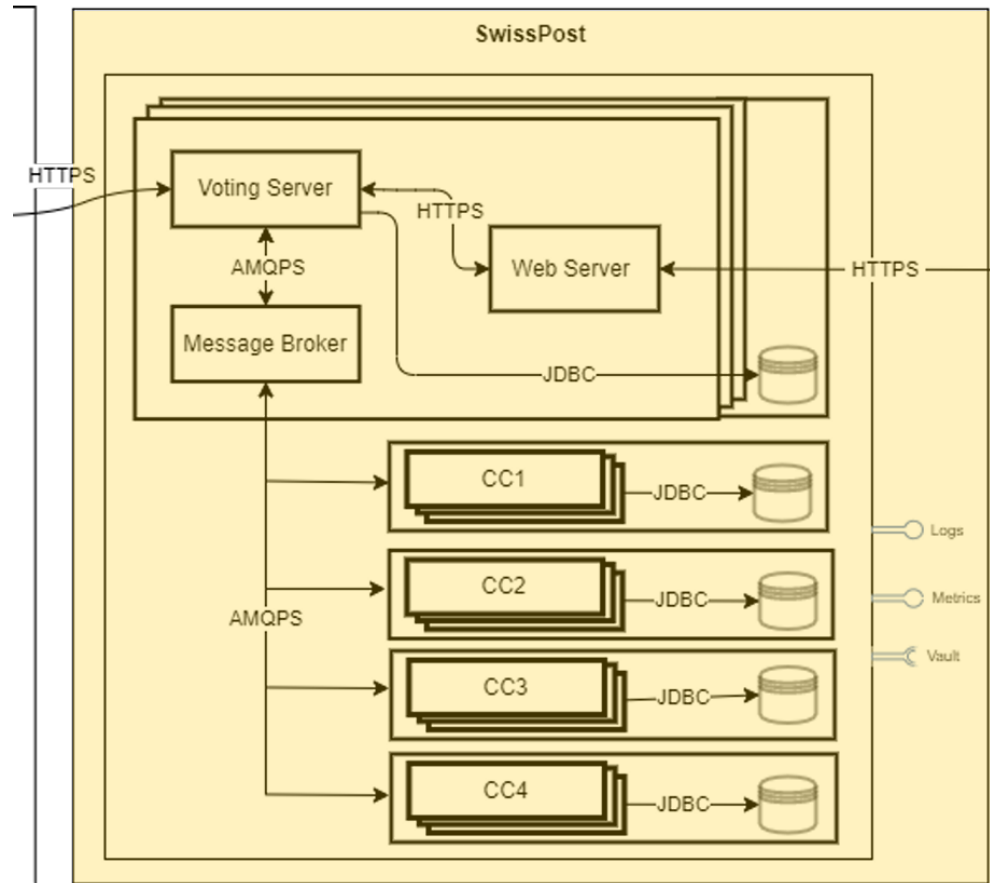
Decrypt

Results of election

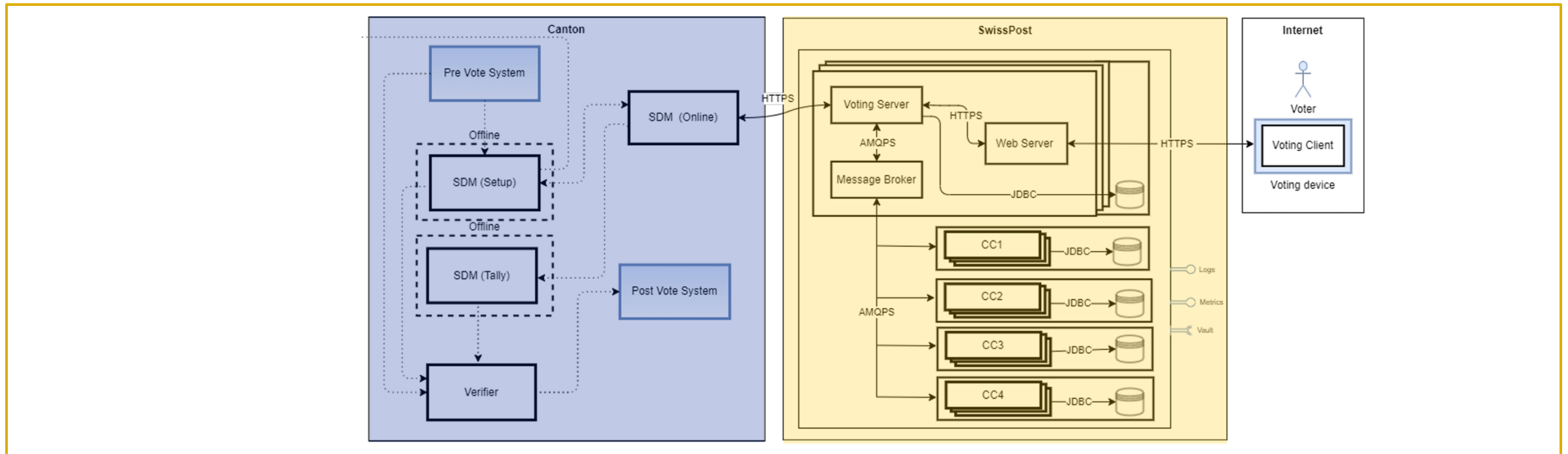
Swiss Post E-Voting



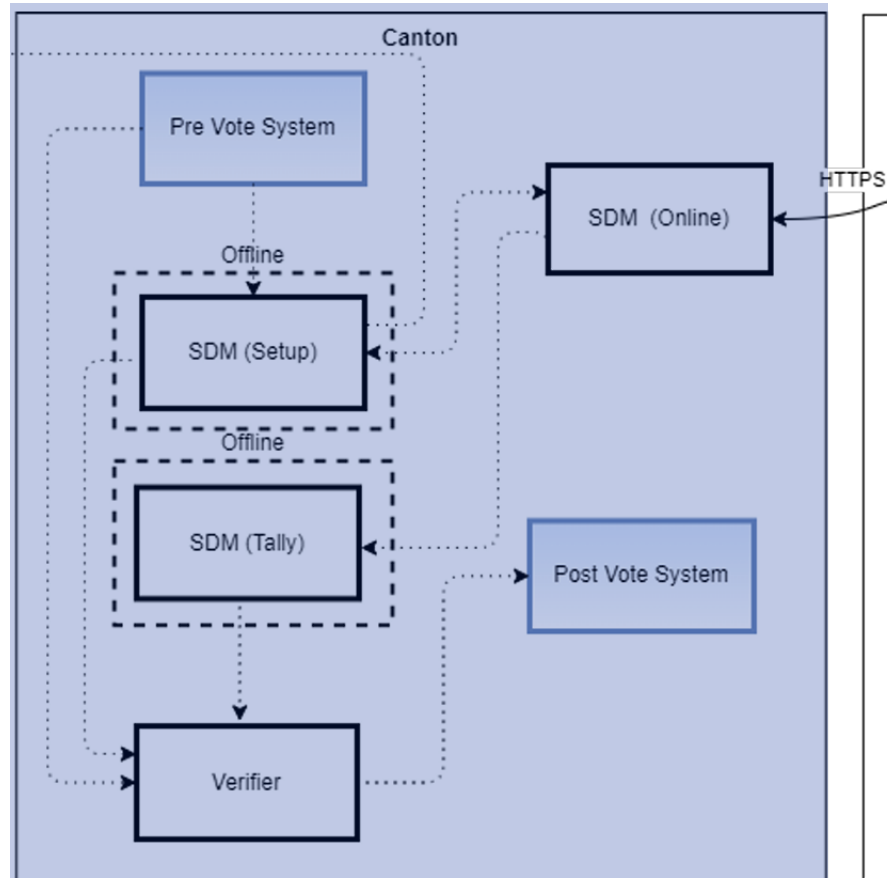
Swiss Post E-Voting



Swiss Post E-Voting



Swiss Post E-Voting

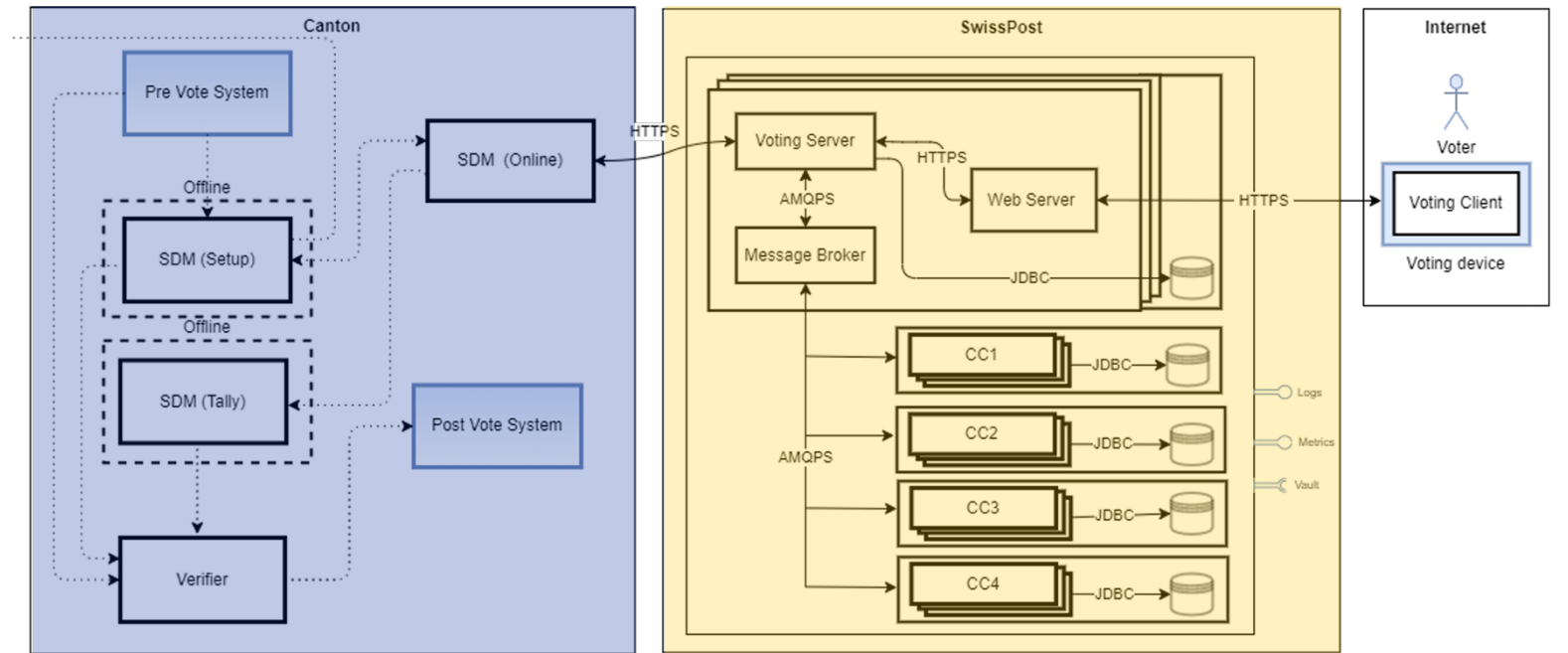


Challenges

1 Scalability

2 Data transfer

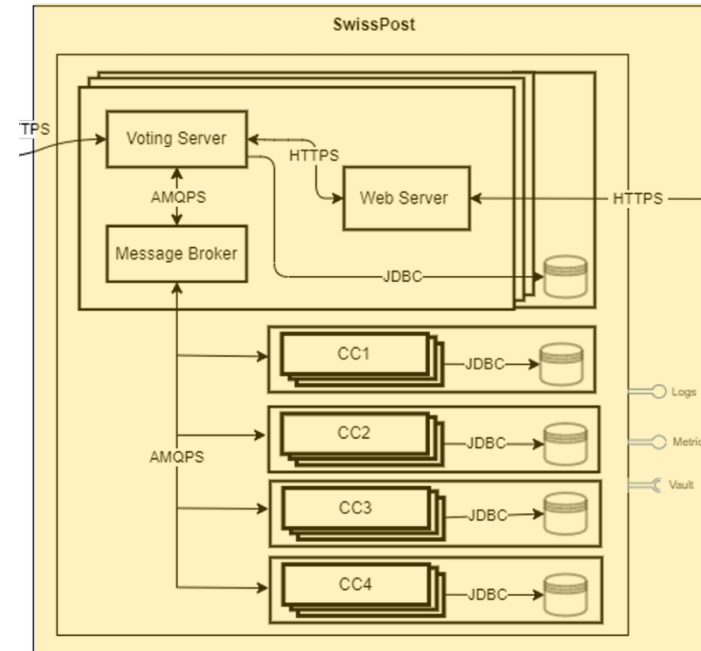
3 Resiliency



1 Challenge – Scalability

From Monolith to Multi-Tenant SaaS

Canton 1

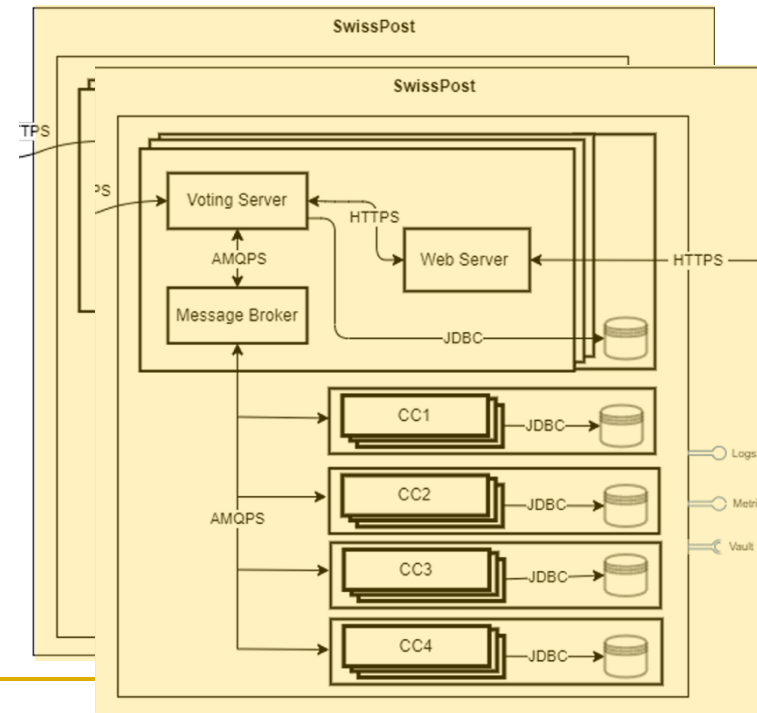


1 Challenge – Scalability

From Monolith to Multi-Tenant SaaS

Canton 1

Canton 2



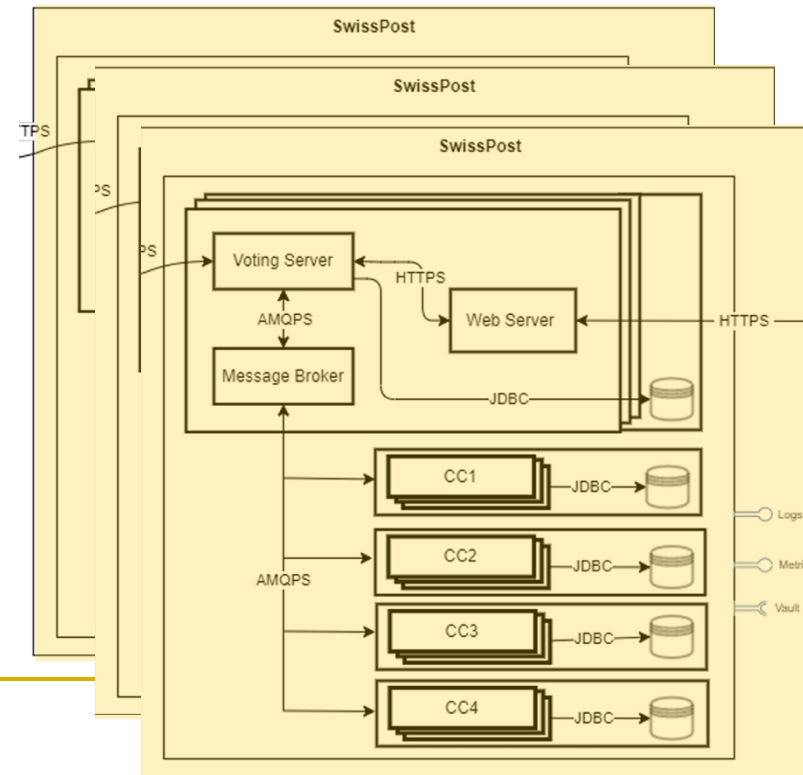
1 Challenge – Scalability

From Monolith to Multi-Tenant SaaS

Canton 1

Canton 2

Canton 3



1 Challenge – Scalability

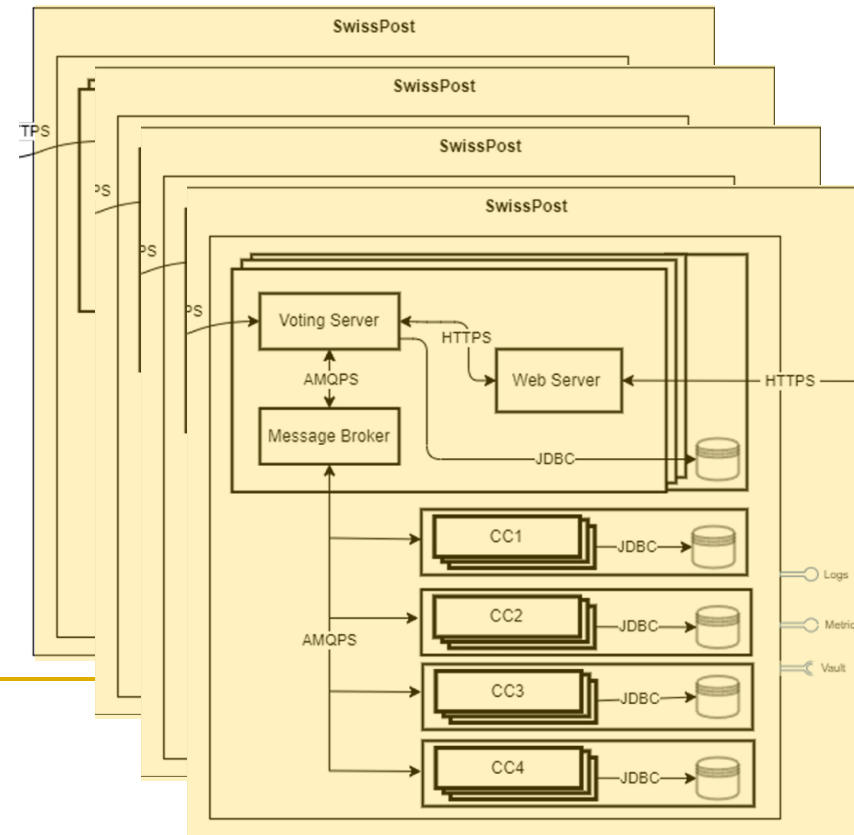
From Monolith to Multi-Tenant SaaS

Canton 1

Canton 2

Canton 3

Canton 4



The 4 Levels of SaaS Maturity

Level 1

- 26 different solutions
- 26 different infrastructures

→ Total duplication



The 4 Levels of SaaS Maturity

Level 2

- 1 configurable solution
- 26 different infrastructures

→ Unified source code

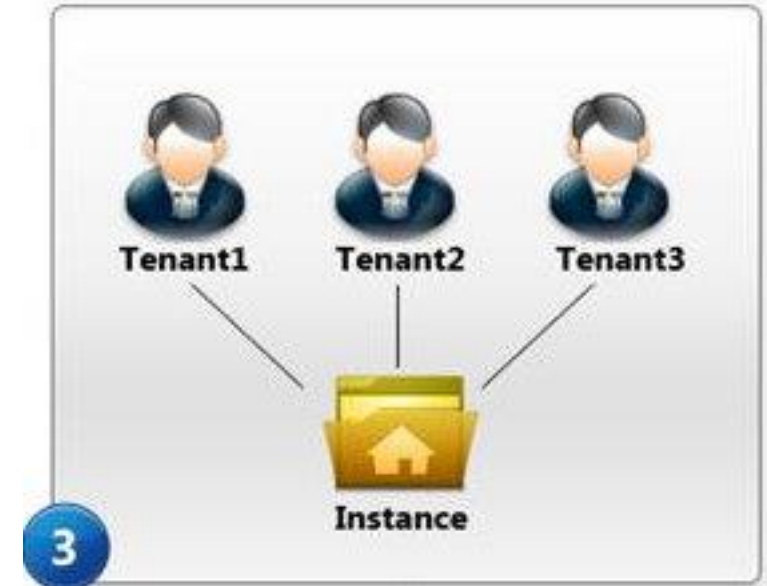


The 4 Levels of SaaS Maturity

Level 3

- 1 configurable solution
- 1 shared infrastructure

→ Multi-tenancy



The 4 Levels of SaaS Maturity

Level 4

- 1 configurable solution
- 1 auto-scalable infrastructure

→ Mature SaaS

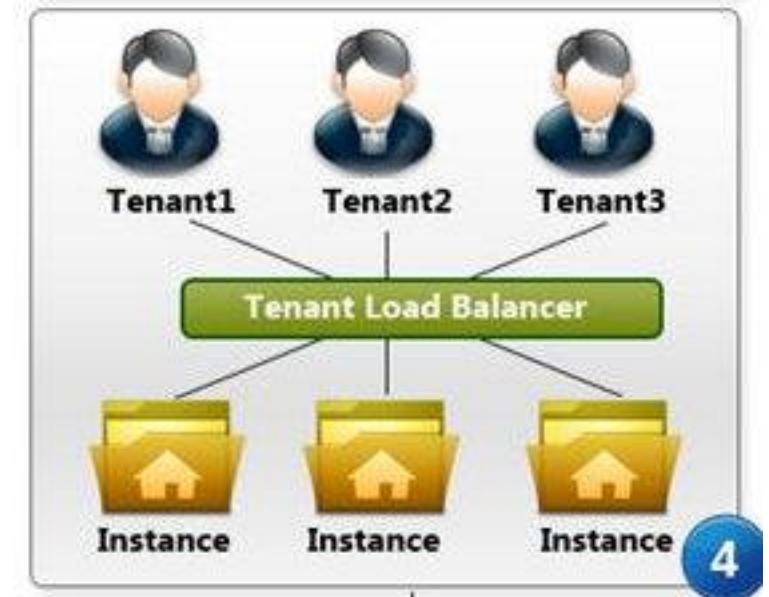


The 4 Levels of SaaS Maturity

Level 4

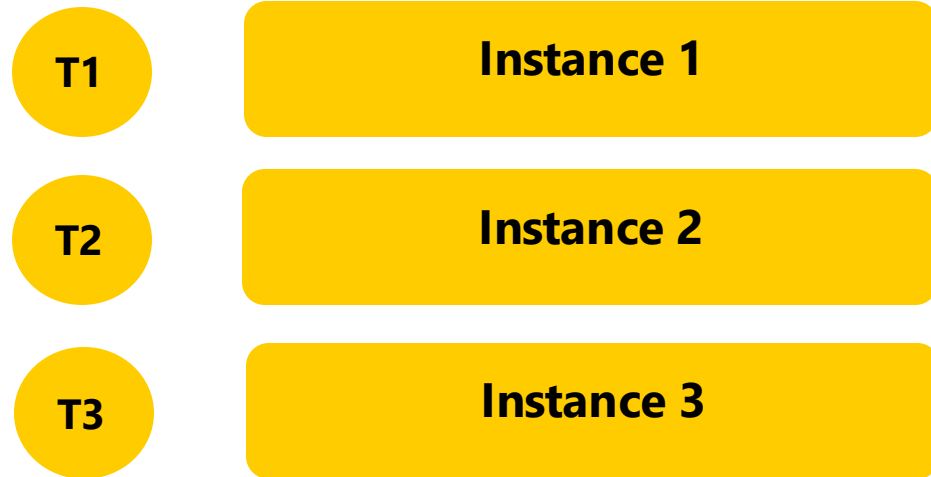
- 1 configurable solution
- 1 auto-scalable infrastructure

→ Mature SaaS



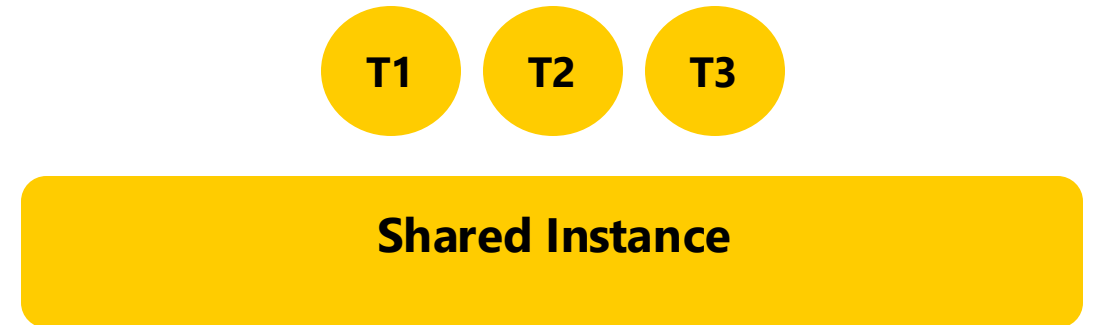
Single-Tenant vs Multi-Tenant

Single-Tenant



- ✓ Complete isolation
- ✗ Major costs
- ✗ Complex maintenance

Multi-Tenant



- ✓ Economies of scale
- ✓ Simplified maintenance
- ✗ Isolation to manage

Key Technical Aspects

Tenant identification

 Claim JWT

 URL Parameter

 HTTP Header

 Sub-domain

Database strategies

Shared tables

tenant_id column present in each table

A database per tenant

Complete data isolation

1 Key Takeaways

Objectives

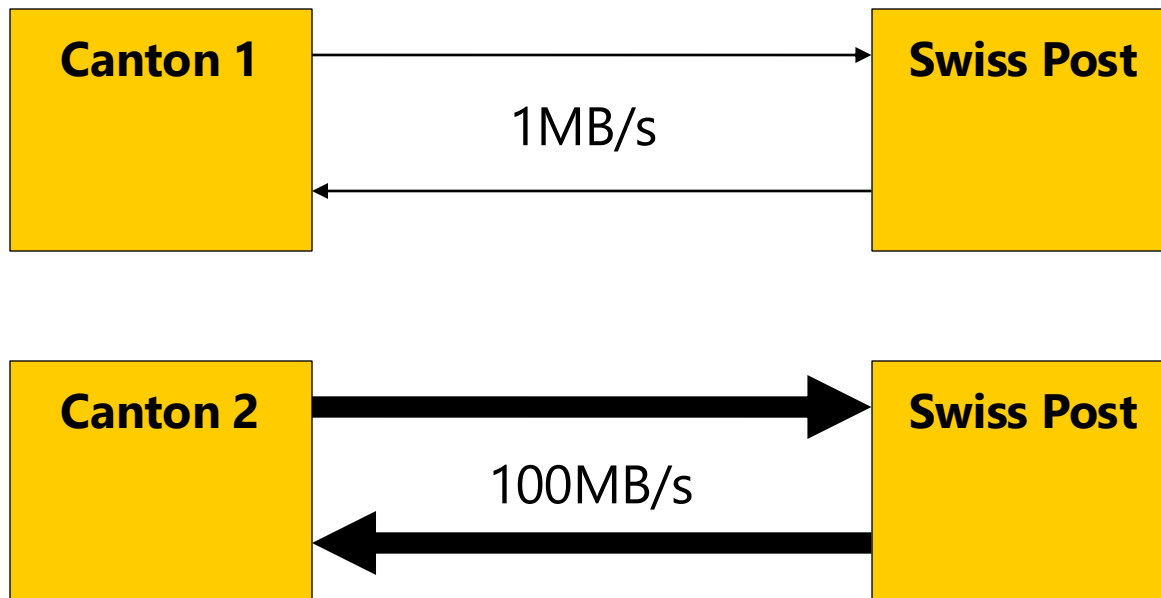
- Costs reduction
- Simplify maintenance
- Enable scaling
- Standardize code

Trade-offs

- Increased complexity
- Security to strengthen
- Data isolation
- Per-tenant configuration

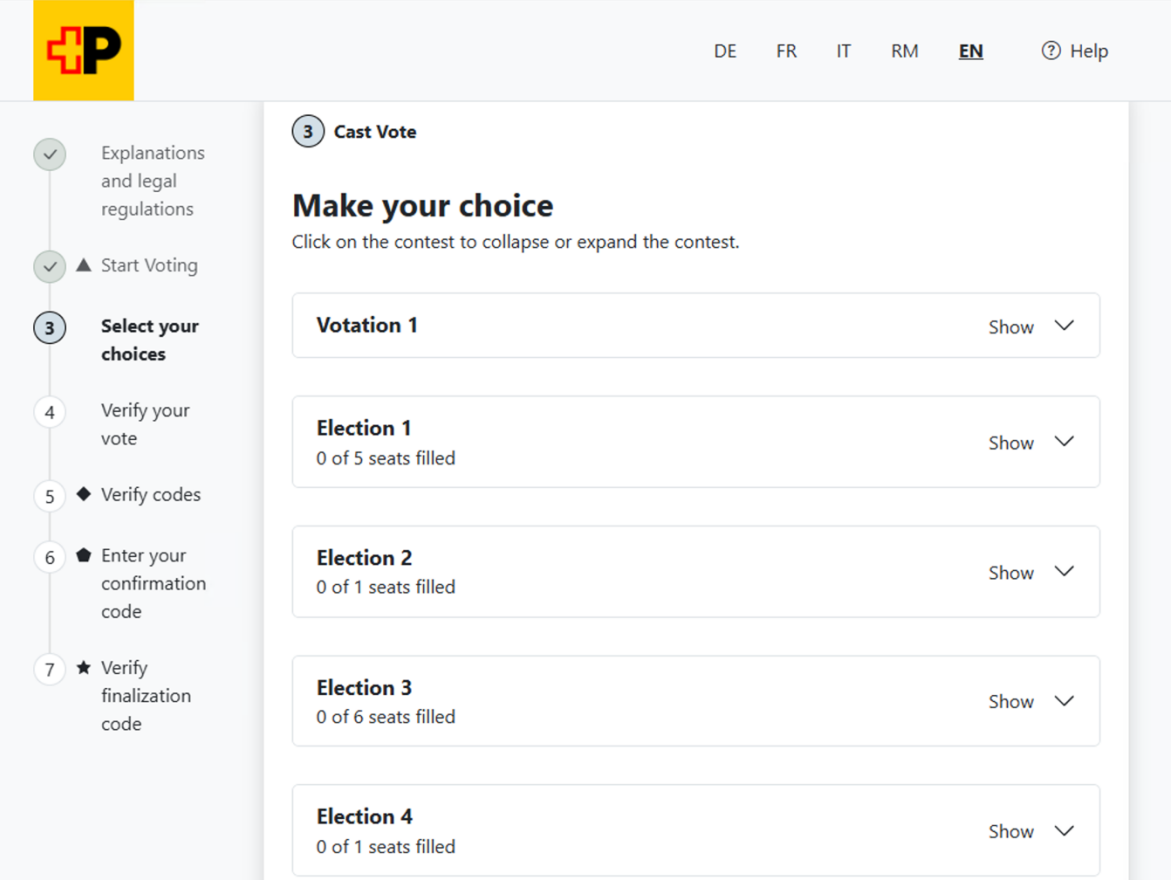
Multi-tenancy is a major architectural choice that must be planned from the design phase

2 Challenge – Data transfer



- Bandwidth depends on the worst infrastructure

2 Challenge – Data transfer



The screenshot displays the Swiss Post e-voting interface. At the top left is the Swiss Post logo (a red cross on a yellow square followed by a black 'P'). To the right of the logo are language options: DE, FR, IT, RM, **EN**, and a Help icon. A vertical progress bar on the left side of the page shows seven steps: 1. Explanations and legal regulations, 2. Start Voting, 3. **Select your choices** (highlighted), 4. Verify your vote, 5. Verify codes, 6. Enter your confirmation code, and 7. Verify finalization code. The main content area is titled '3 Cast Vote' and 'Make your choice'. Below the title, it says 'Click on the contest to collapse or expand the contest.' There are four election cards, each with a 'Show' button and a dropdown arrow. The cards are: 'Votation 1', 'Election 1' (0 of 5 seats filled), 'Election 2' (0 of 1 seats filled), and 'Election 3' (0 of 6 seats filled). A fourth card, 'Election 4' (0 of 1 seats filled), is partially visible at the bottom.

- Bandwidth depends on the worst infrastructure
- Data depends on size and complexity of election

2 Challenge – Data transfer

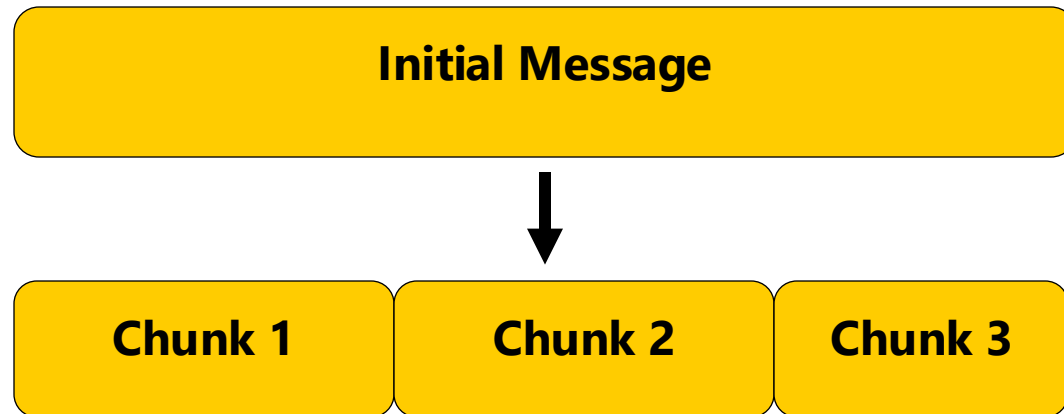
Symmetric Authenticated Encryption

- > Digital Signatures
- > ElGamal Cryptosystem
- > Mix Net
- > Zero-Knowledge Proofs

- Bandwidth depends on the worst infrastructure
- Data depends on size and complexity of election
- Certified and recognized cryptography generates voluminous data

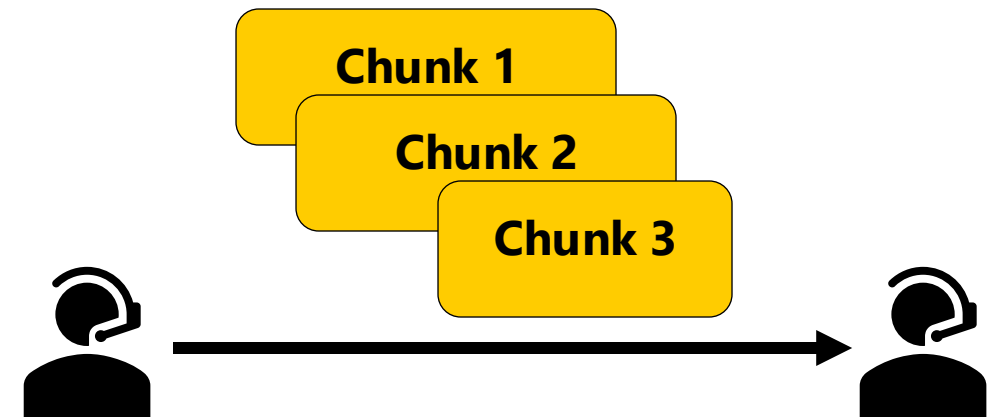
Chunking

Break large messages into smaller parts



- ✓ Avoid timeouts
- ✓ Reduce memory load
- ✓ Enables streaming

Sequential or Parallel

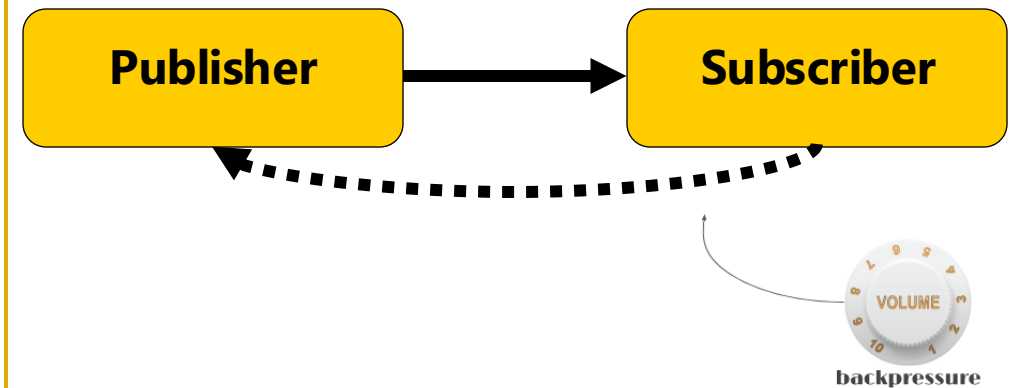


Reactive Streams & Backpressure

- Asynchronous data flow
- Backpressure signals when receiver is overwhelmed
- System adapts dynamically to load

- ✓ Prevents overload
- ✓ Improves resilience
- ✓ Enables real-time responsiveness

Backpressure



Key Technical Aspects

Chunk Parameters

Chunk size

Many small chunks vs. Fewer big chunks

Chunk order

Needed to reconstruct messages

Backpressure Mechanisms

Request

Receiver requests messages

Limit

Receiver limits number of messages

2

Key Takeaways

Objectives

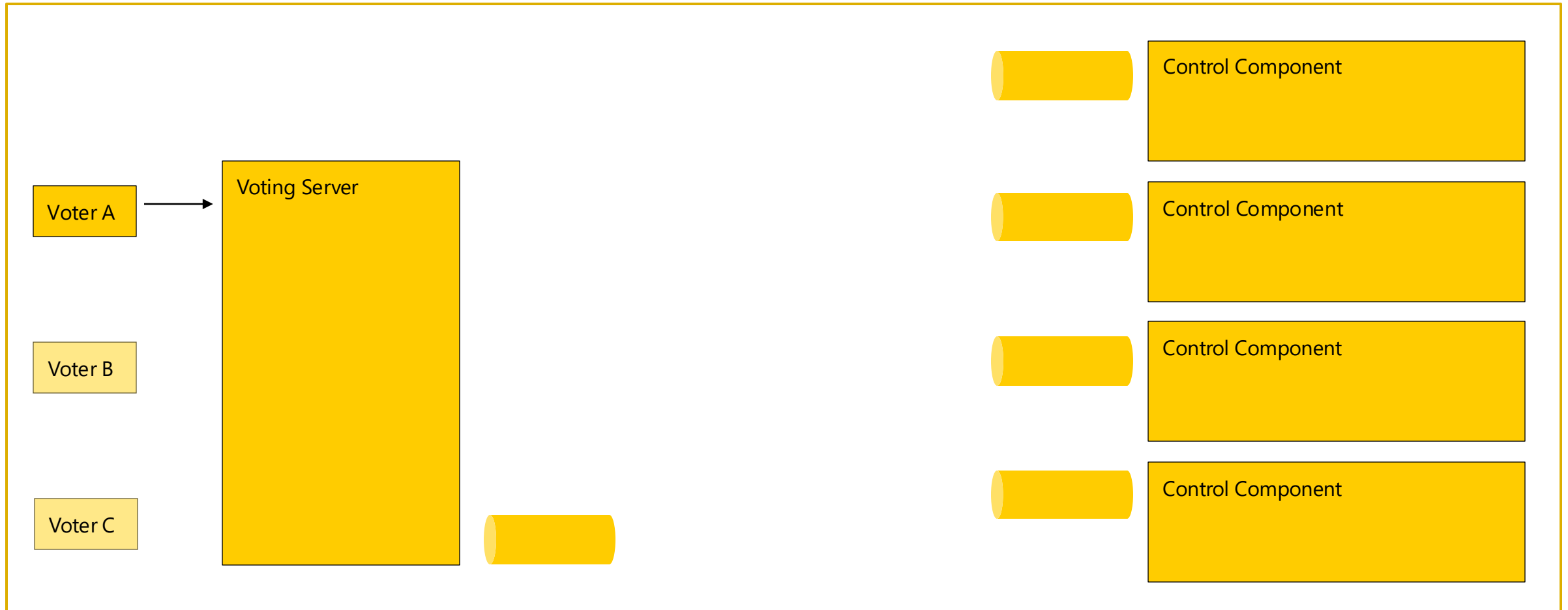
- Stable communication
- Scalability
- Improve performance
- Prevent crashes

Trade-offs

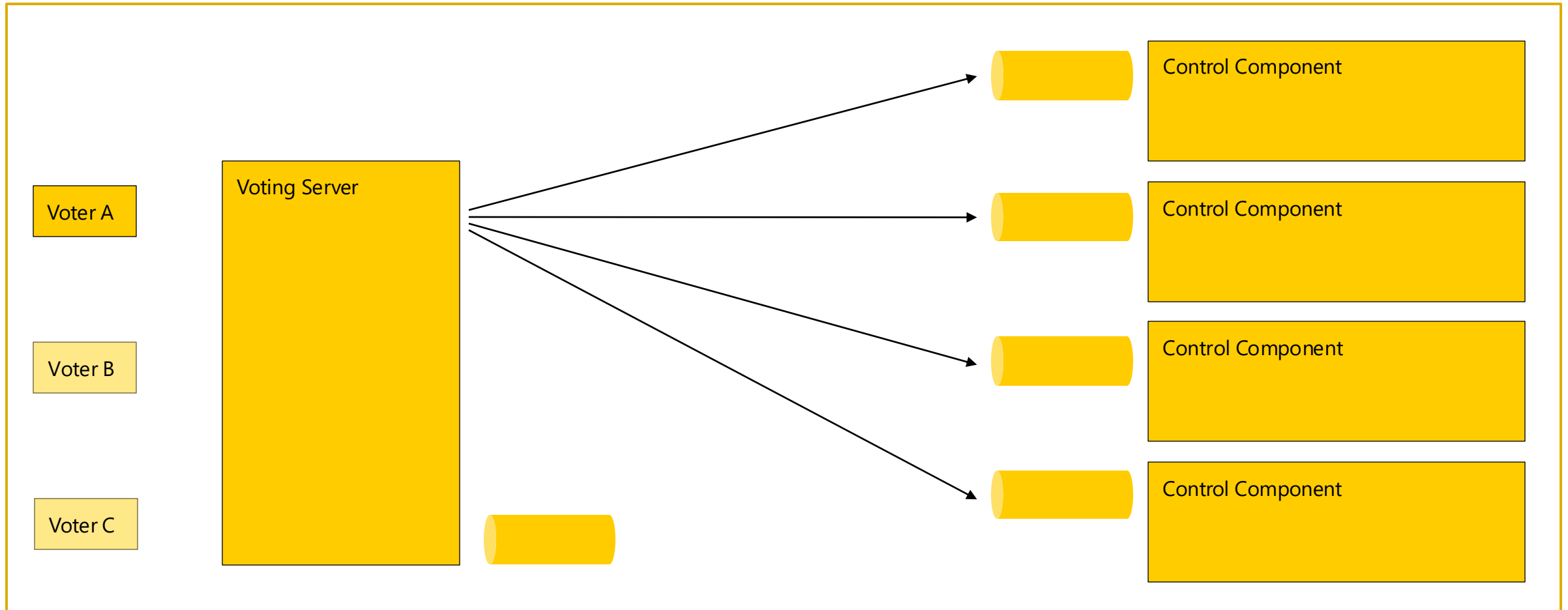
- Increased complexity
- Debuggability
- Error handling

The amount of data transmitted is a design consideration when building a scalable and resilient communication layer

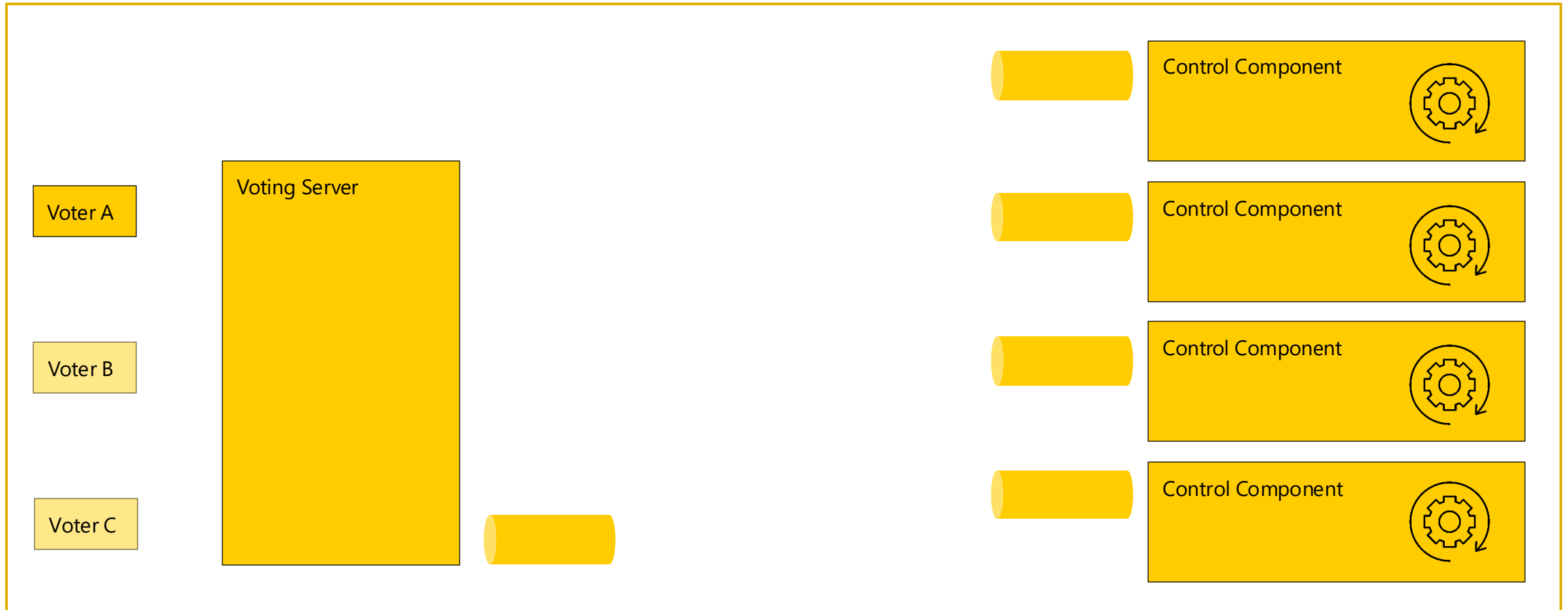
3 Challenge – Resiliency



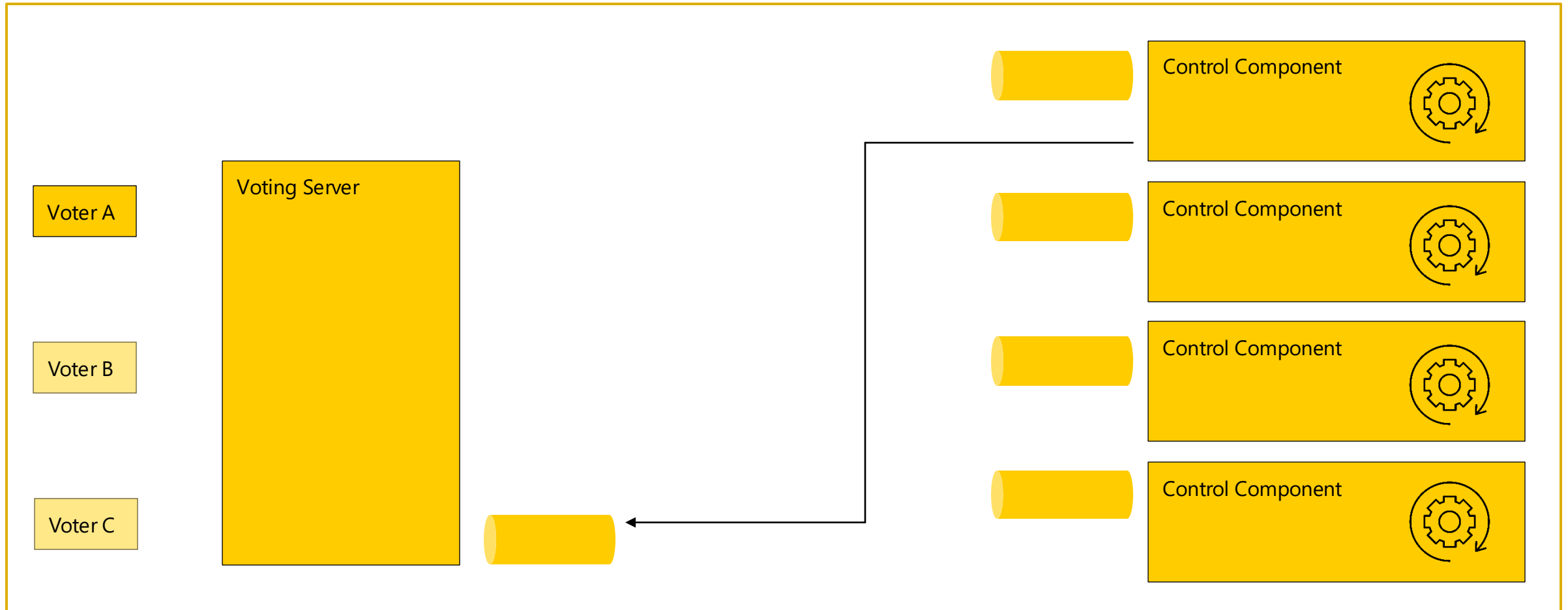
3 Challenge – Resiliency



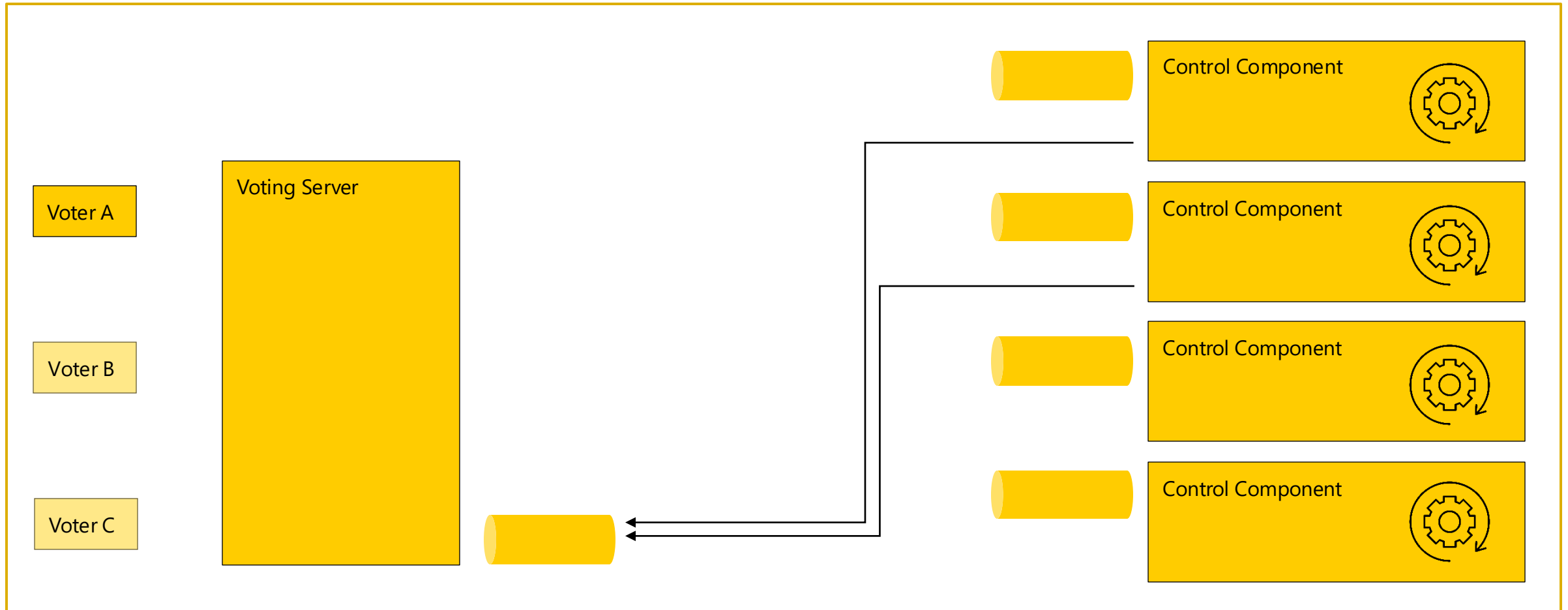
3 Challenge – Resiliency



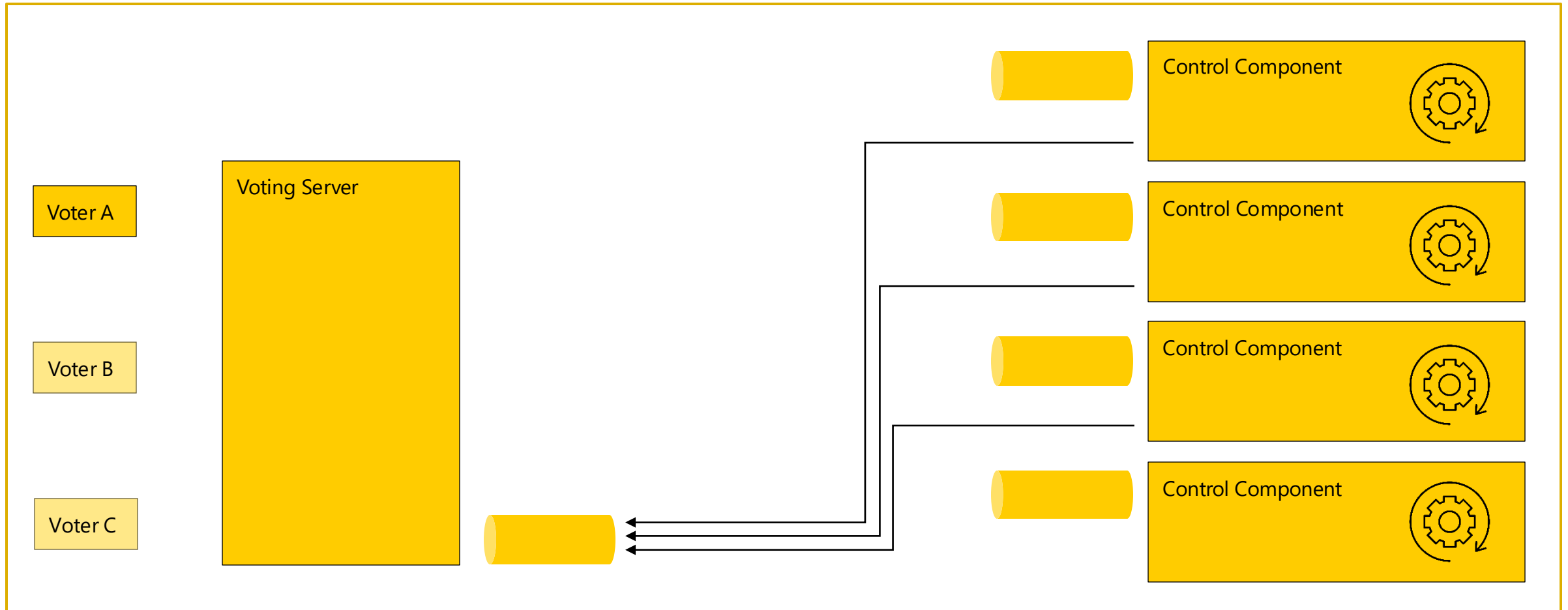
3 Challenge – Resiliency



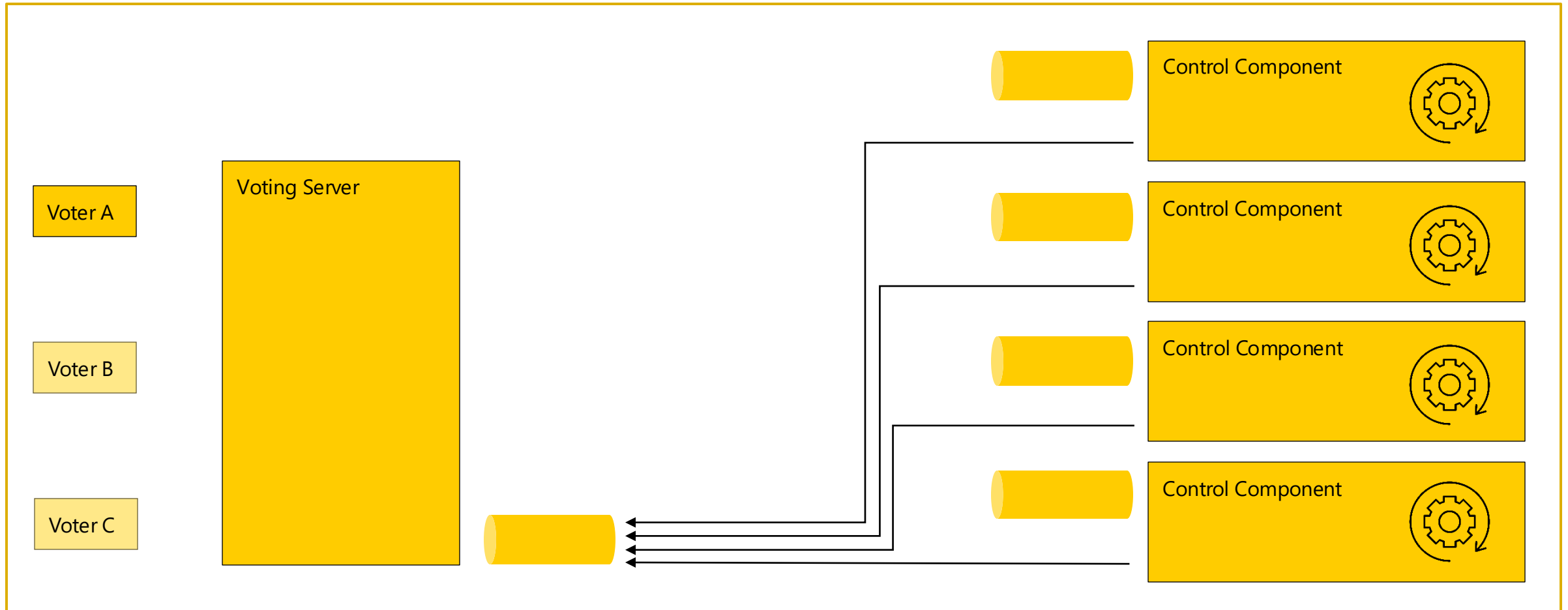
3 Challenge – Resiliency



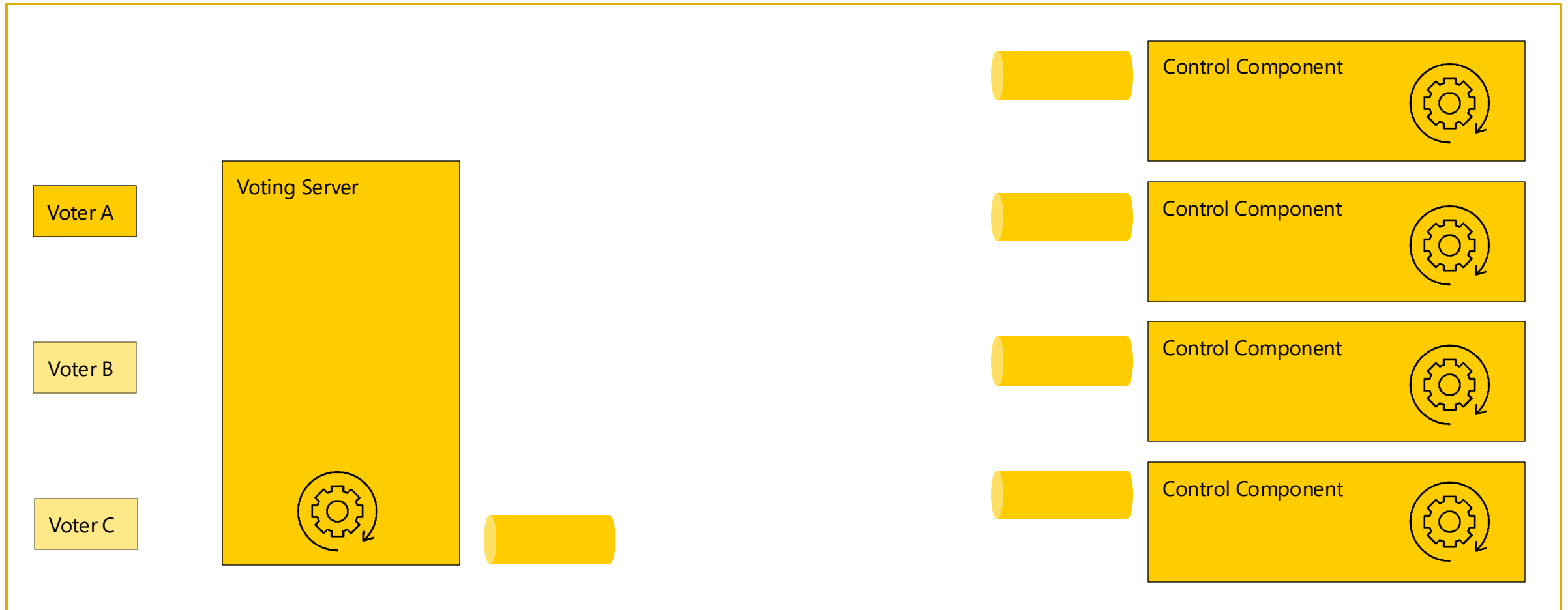
3 Challenge – Resiliency



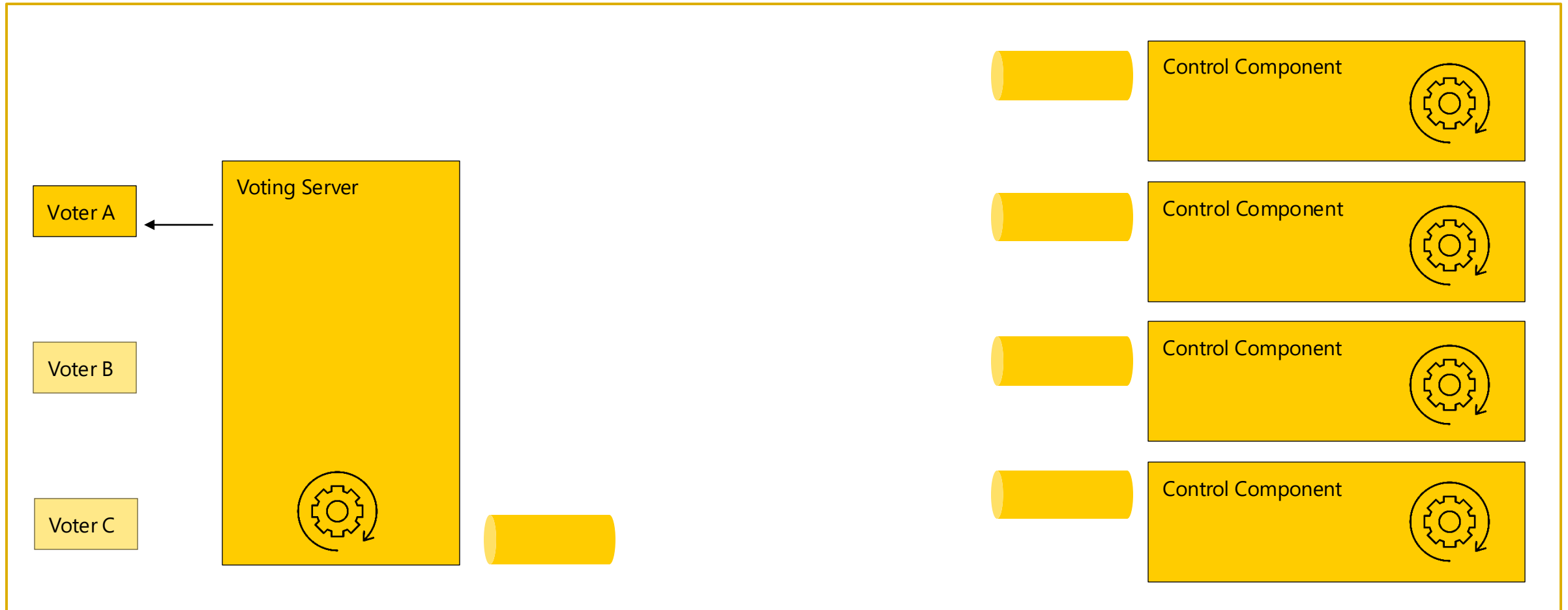
3 Challenge – Resiliency

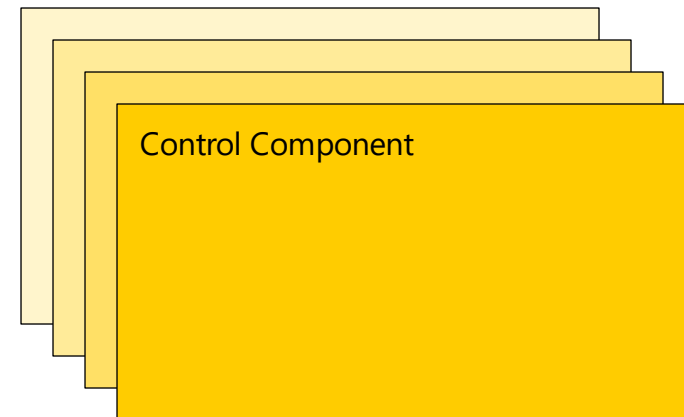
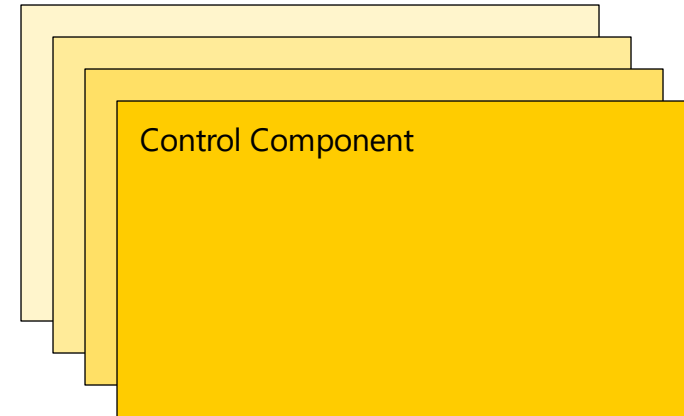
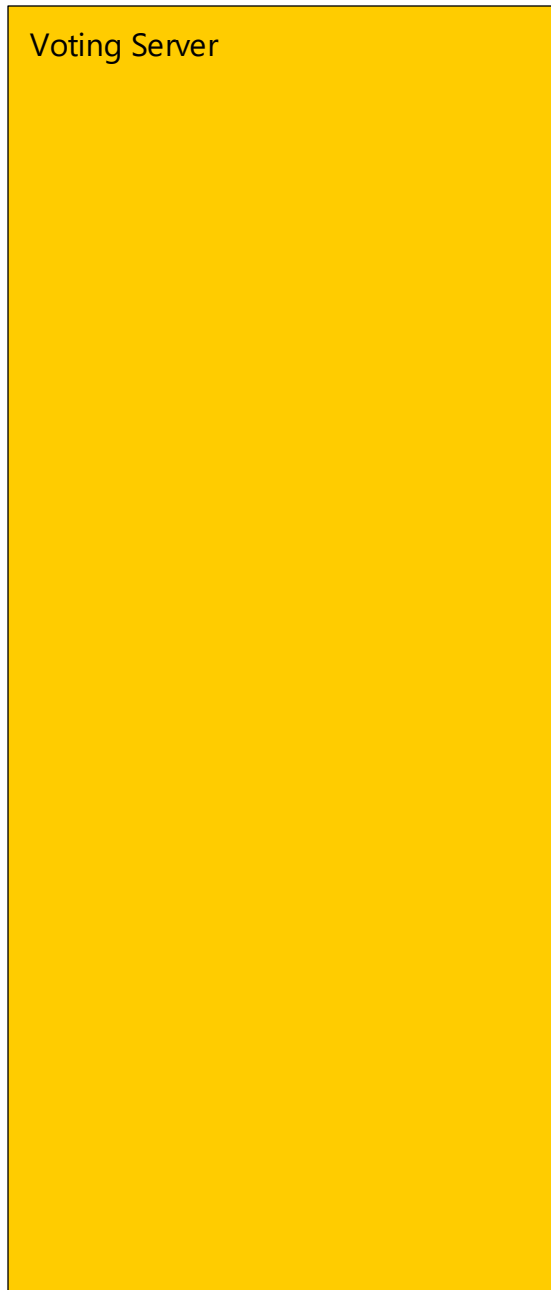


3 Challenge – Resiliency



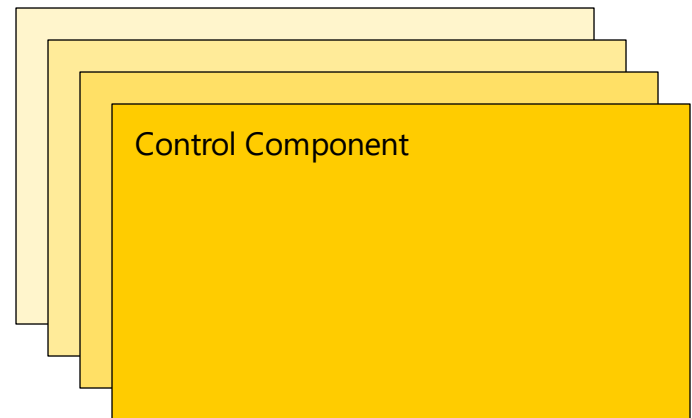
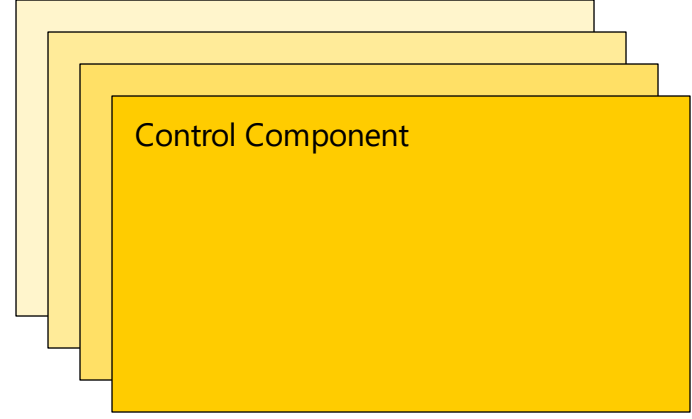
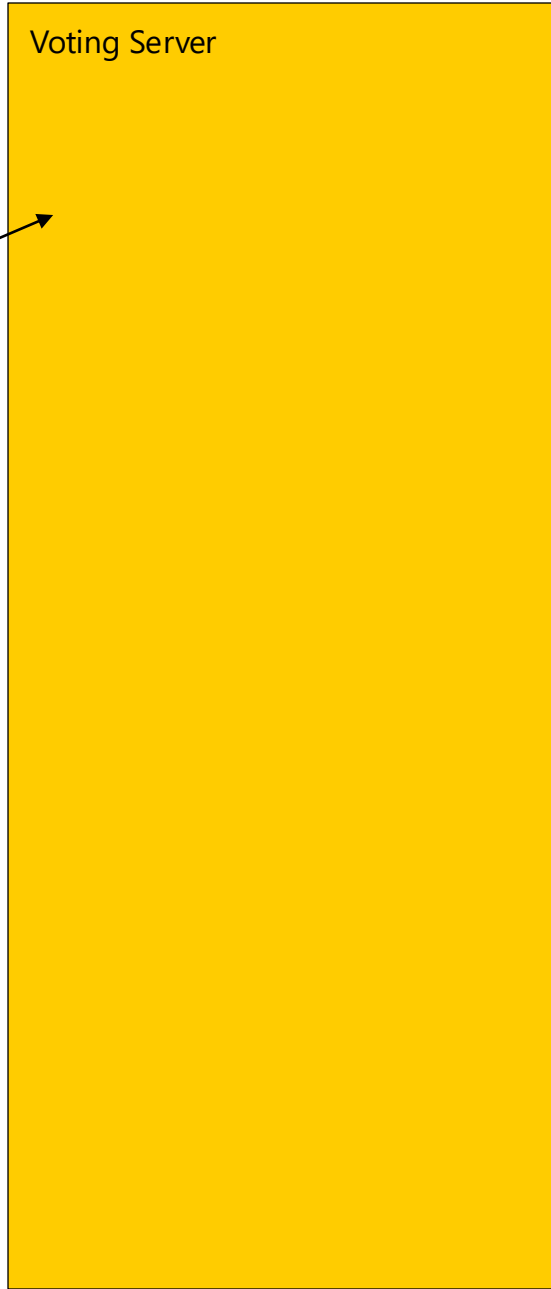
3 Challenge – Resiliency





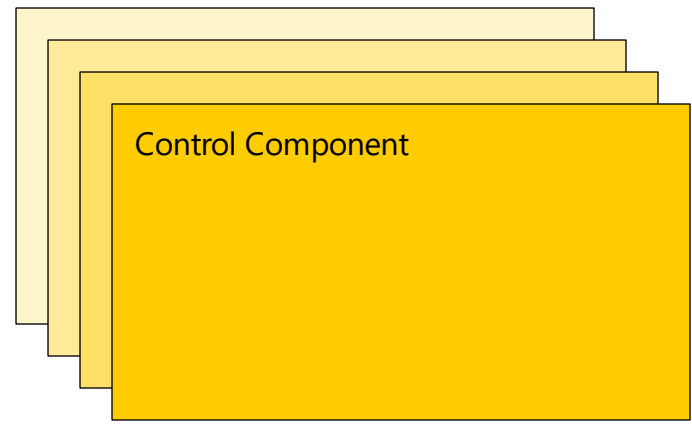
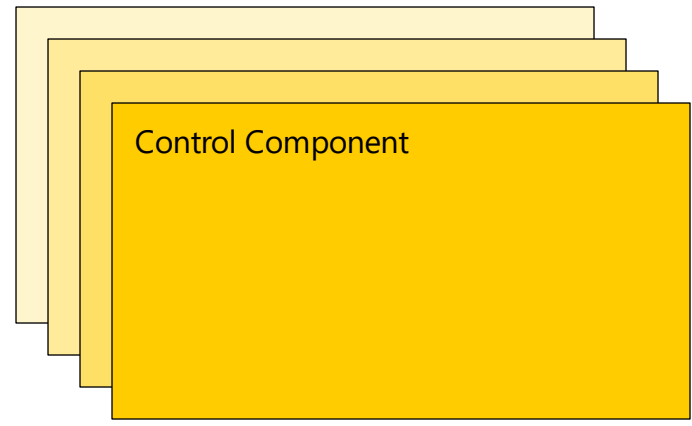
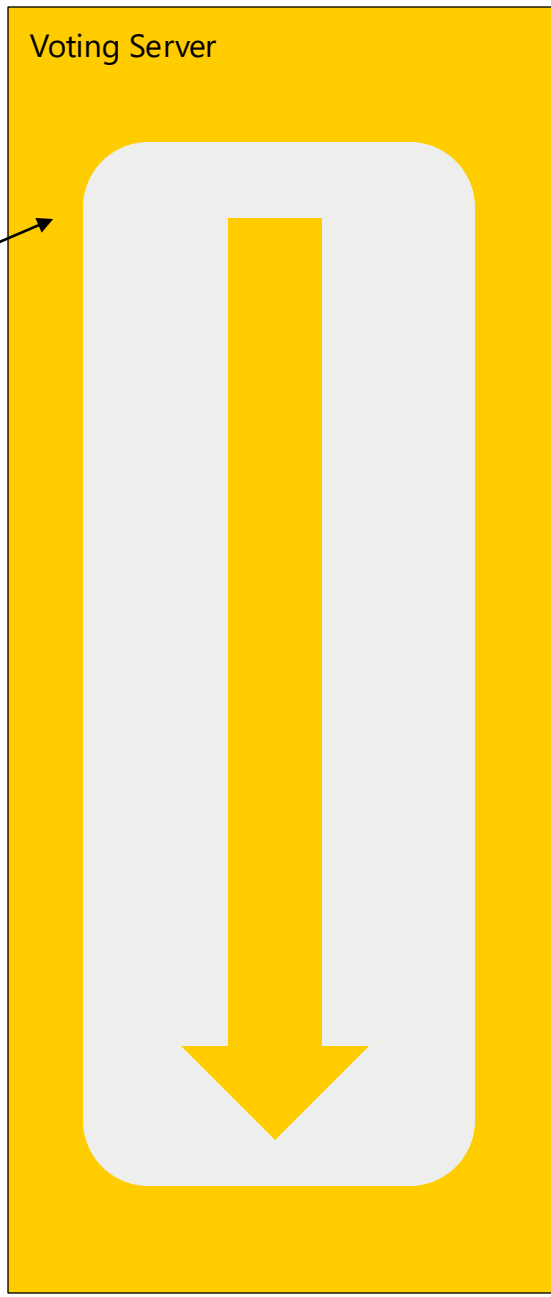


send vote



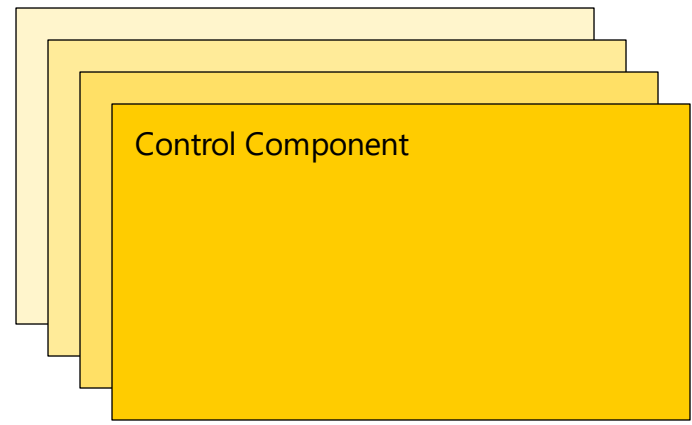
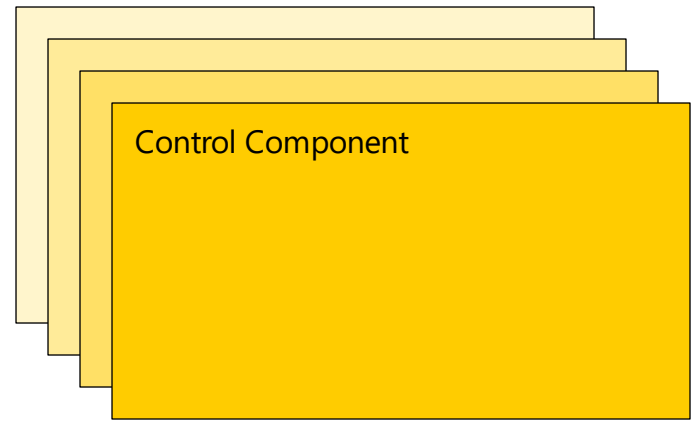
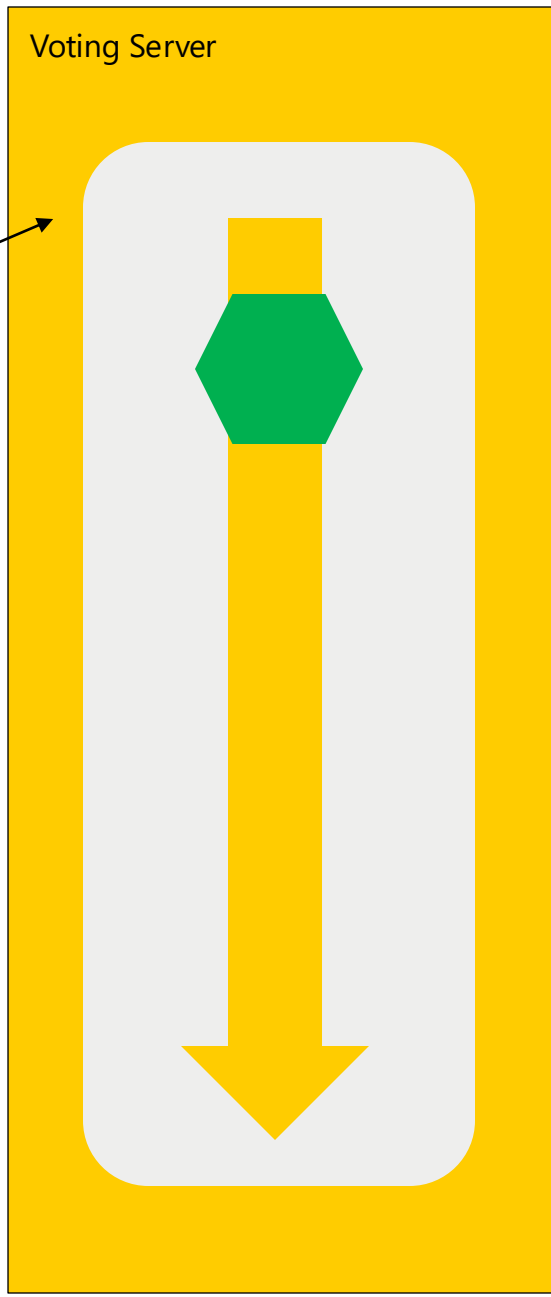


send vote



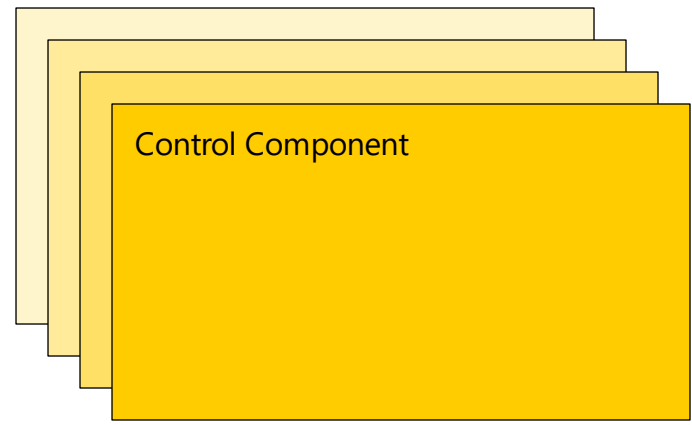
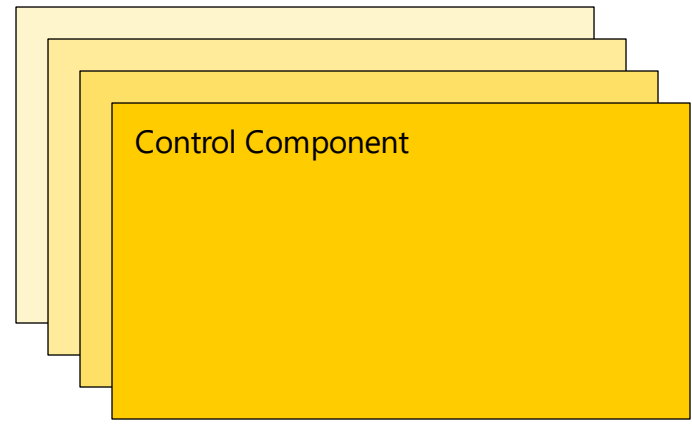
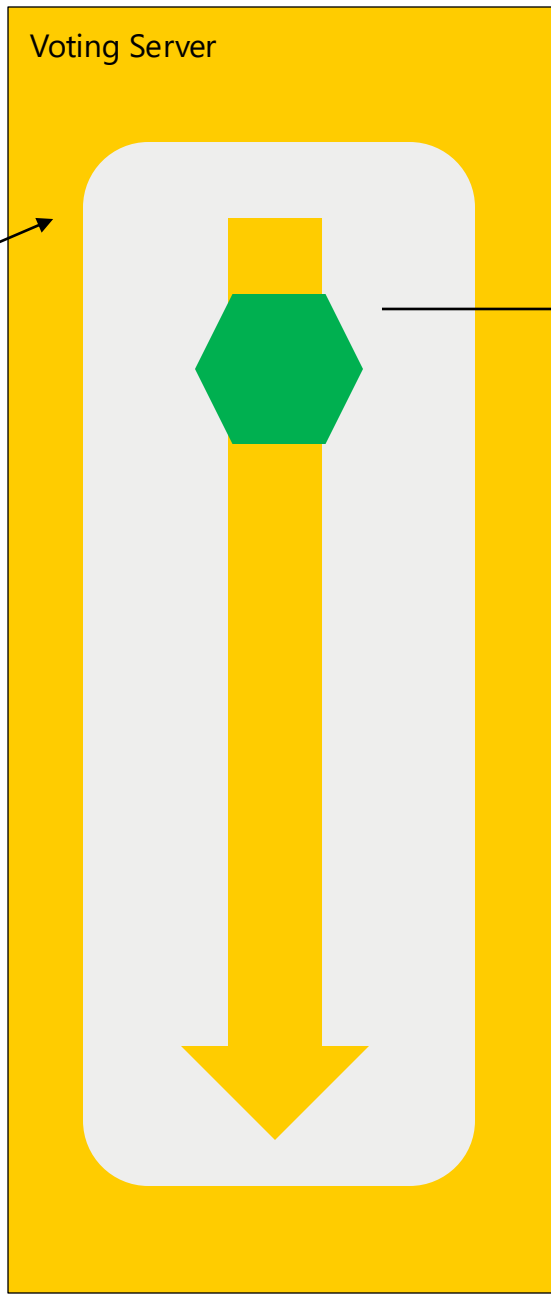


send vote



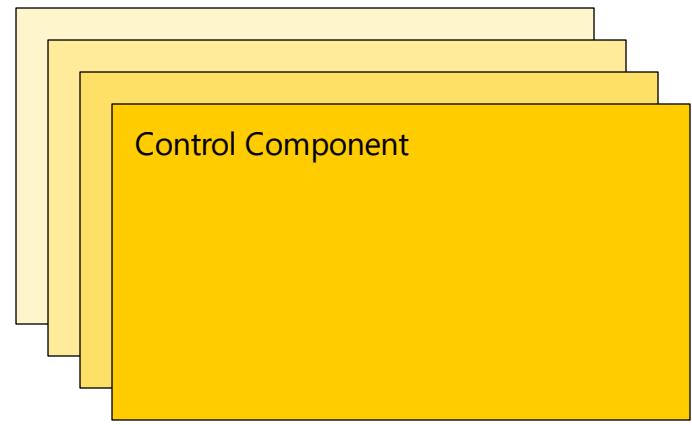
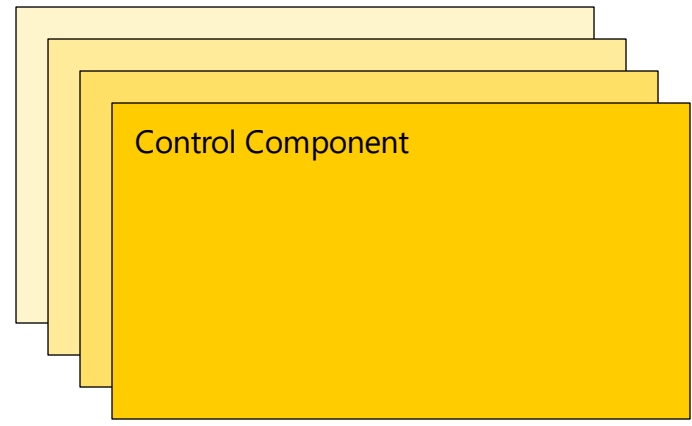
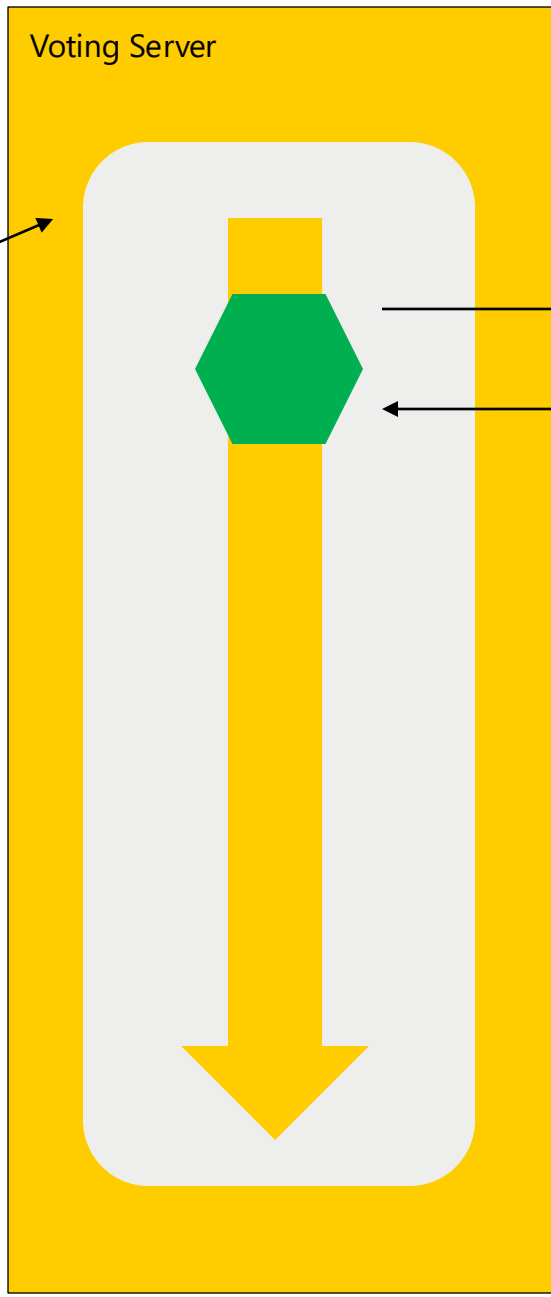


send vote



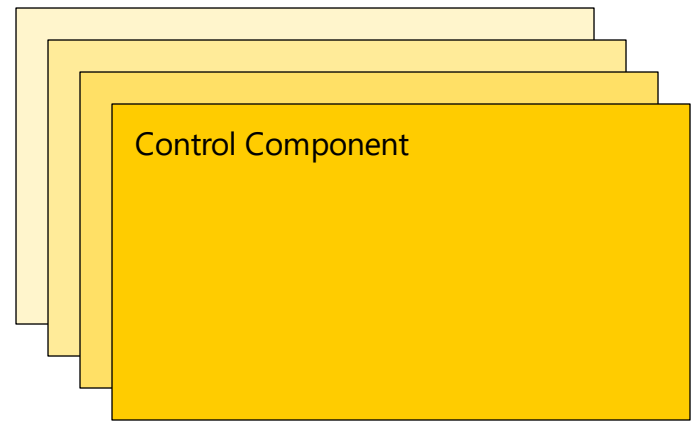
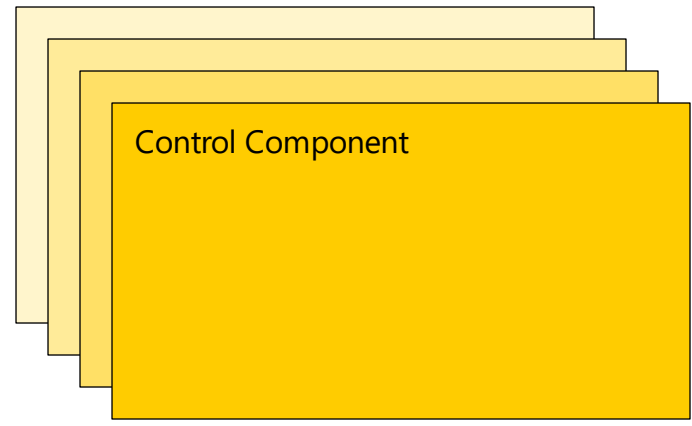
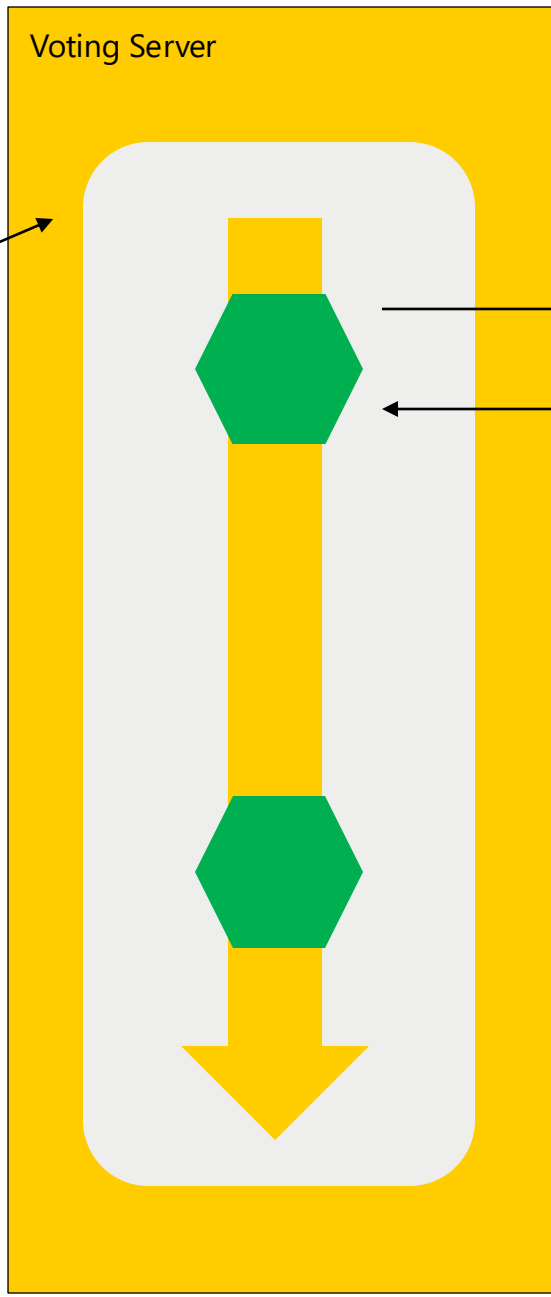


send vote



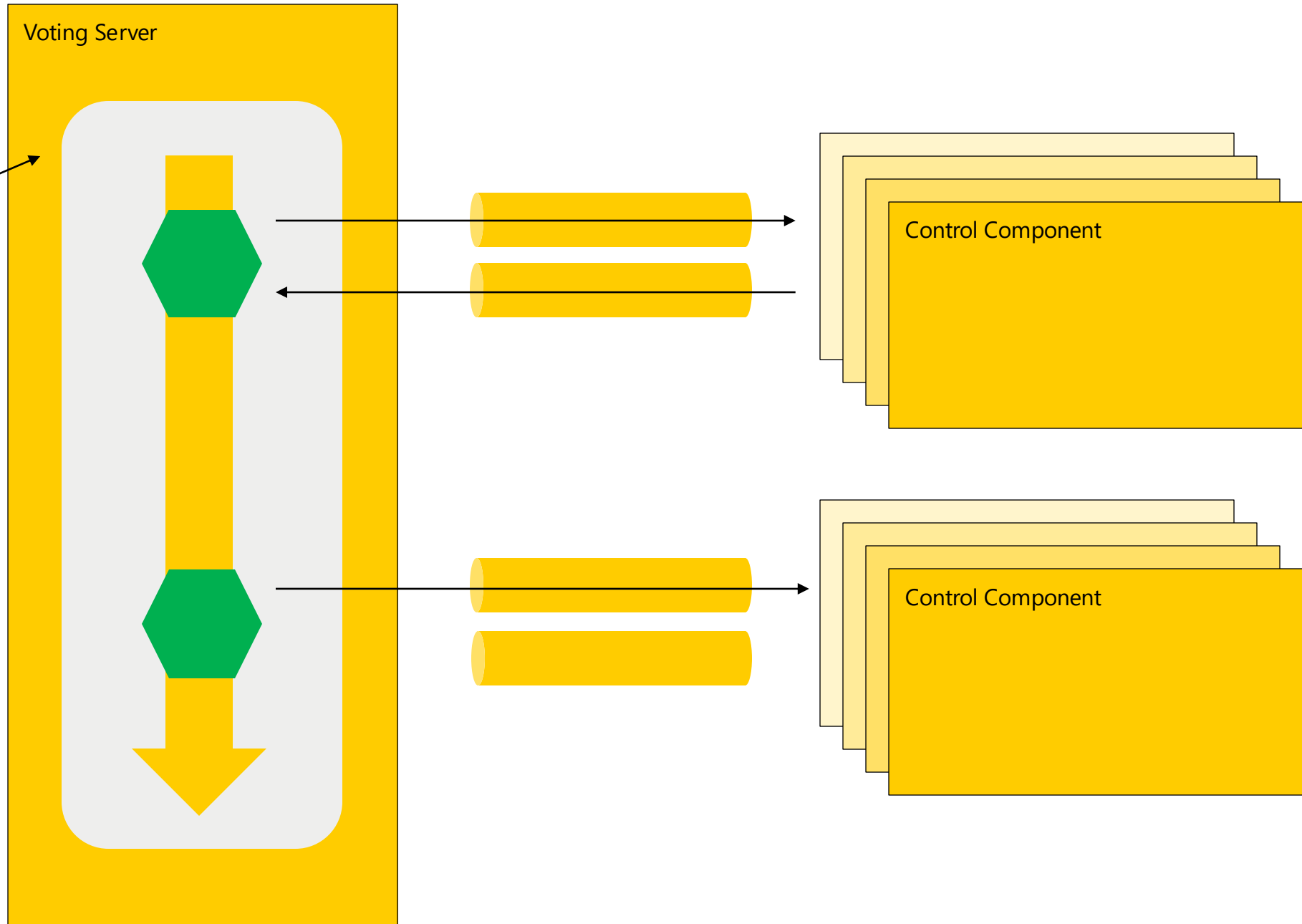


send vote



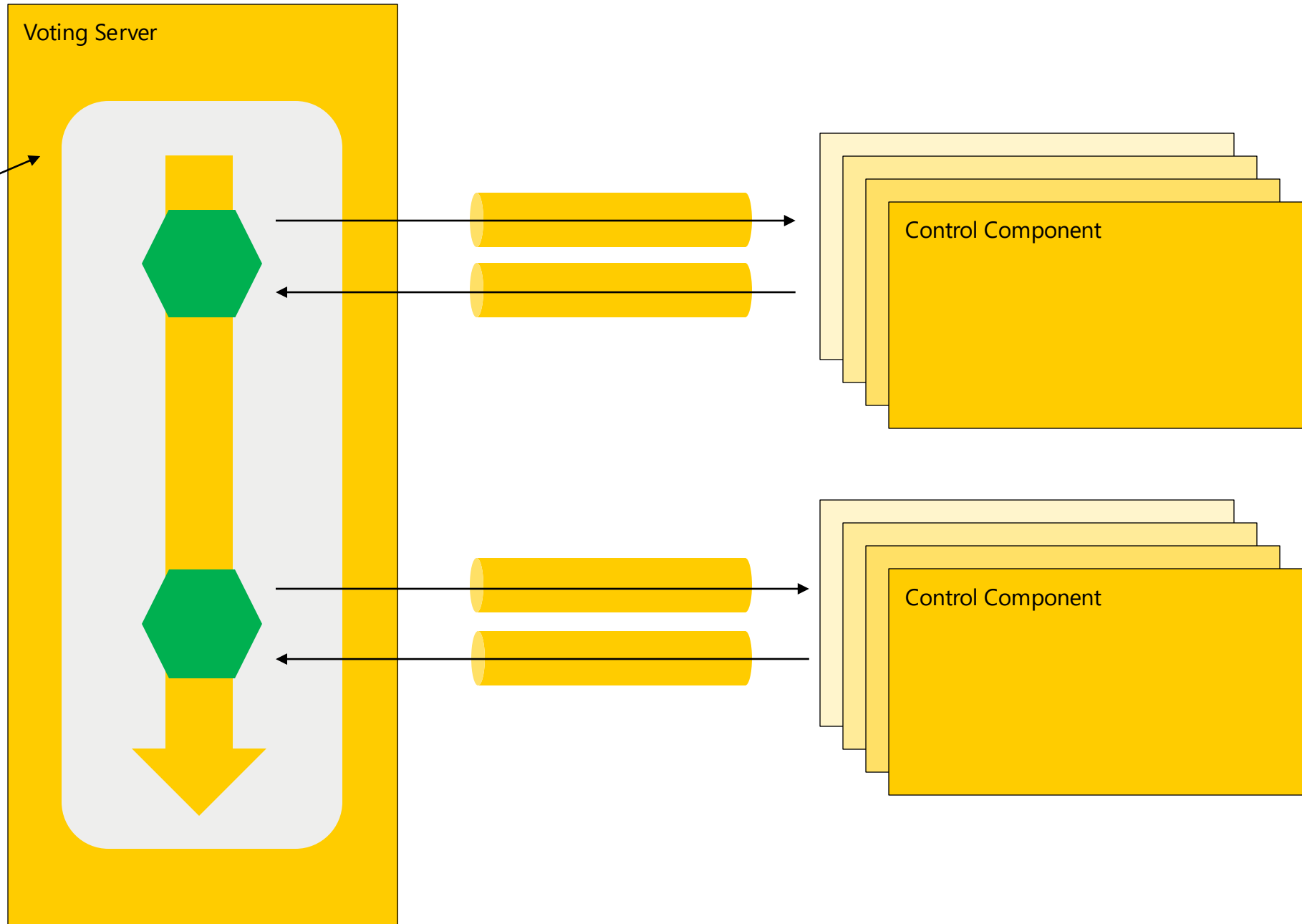


send vote





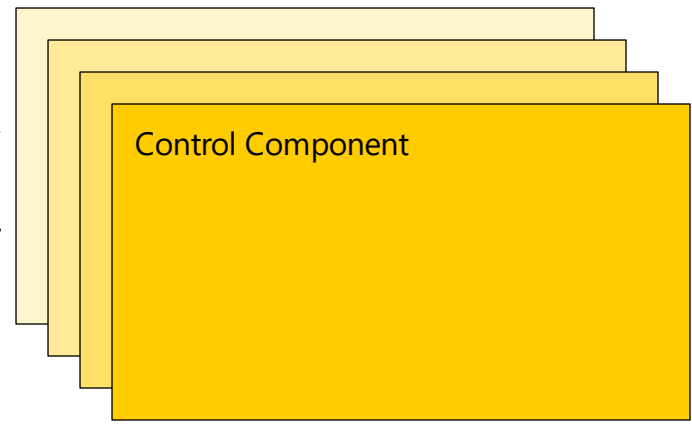
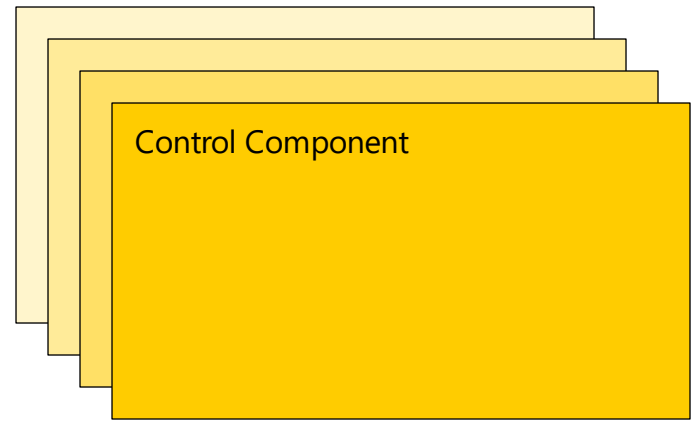
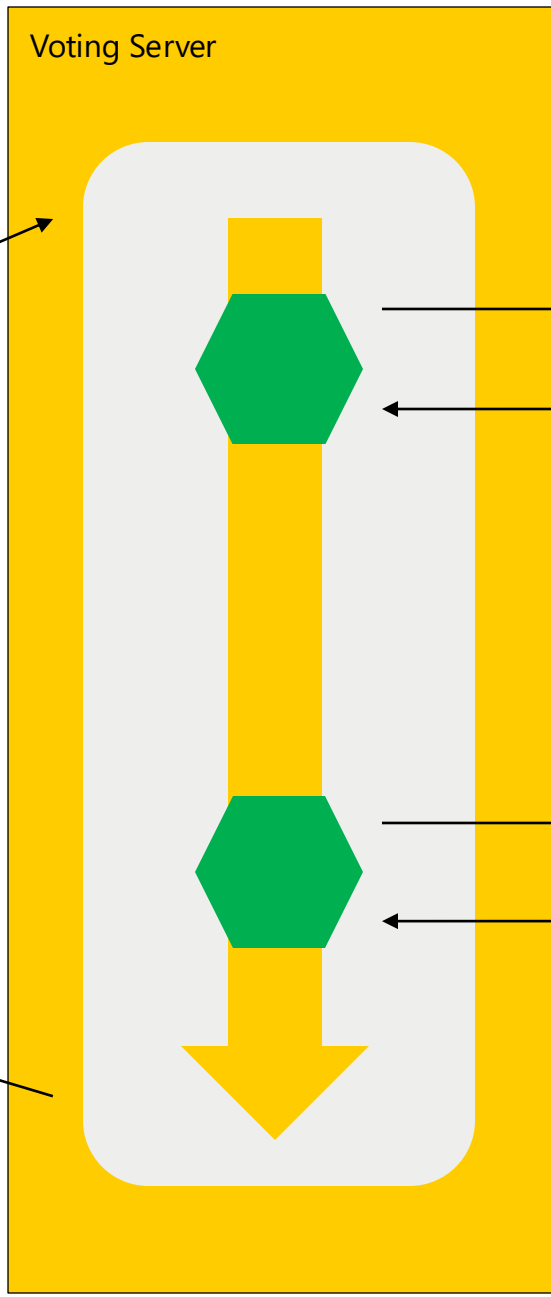
send vote

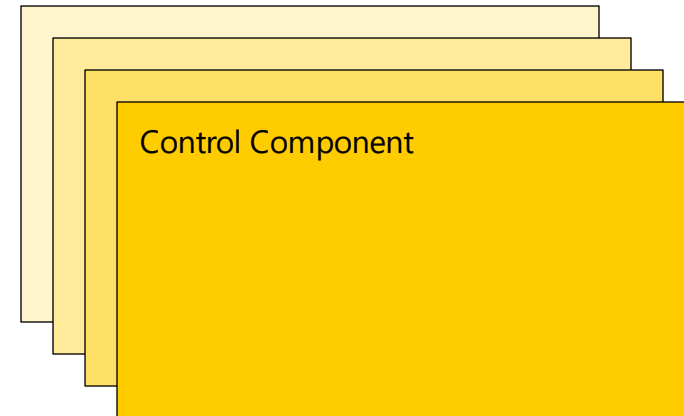
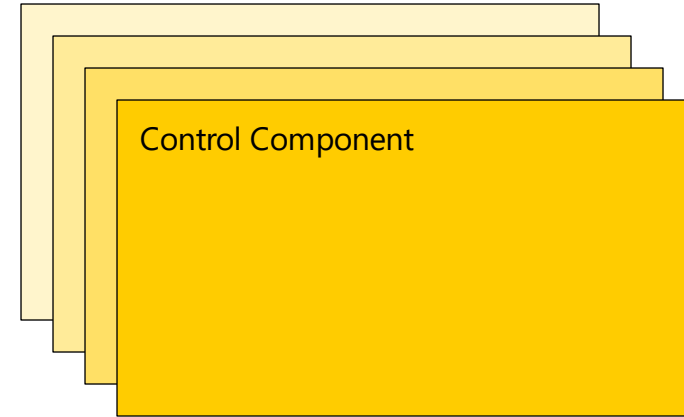
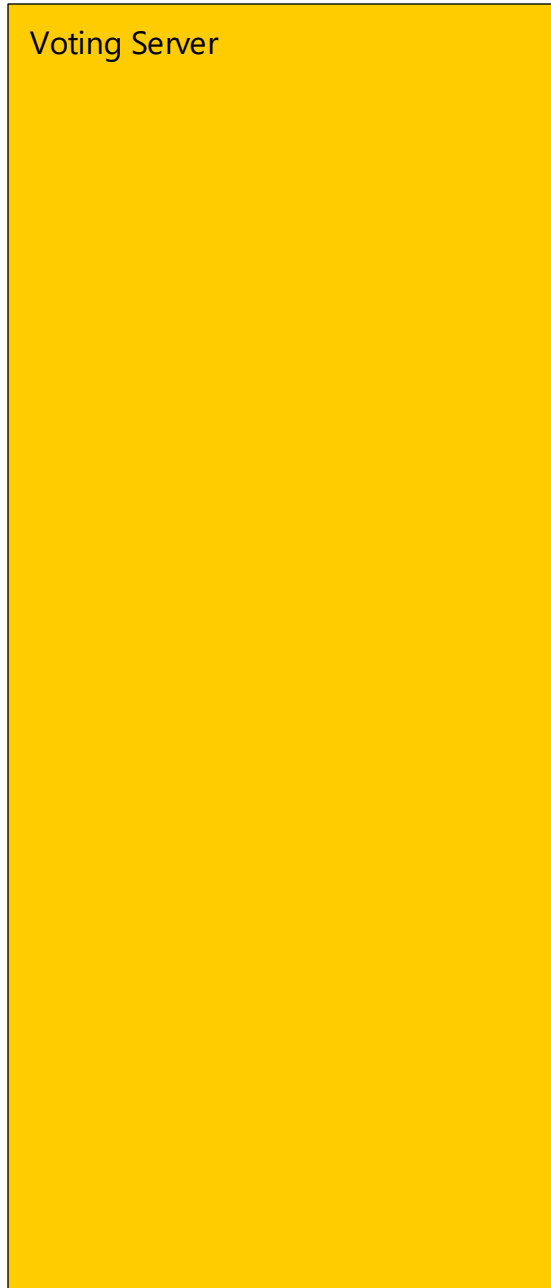




send vote

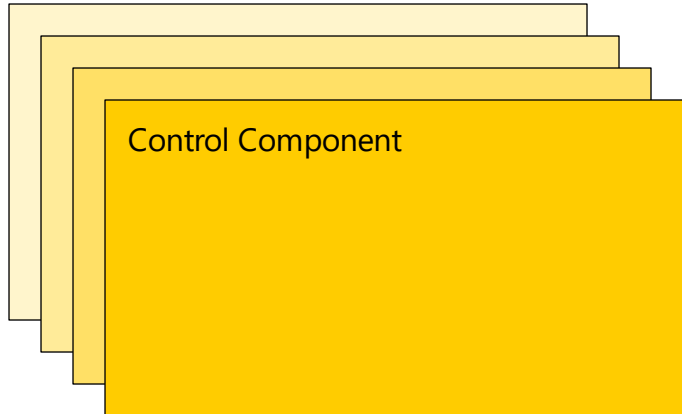
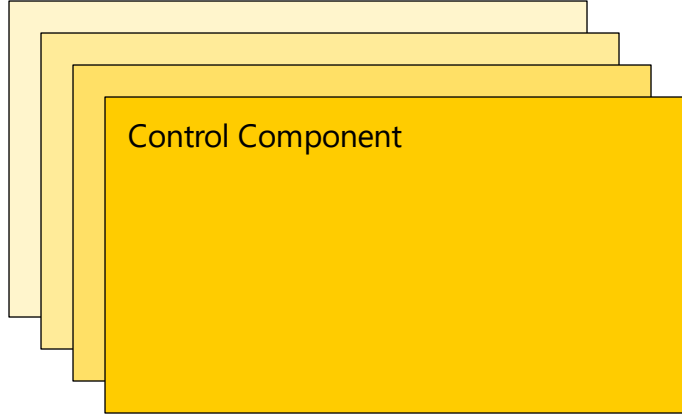
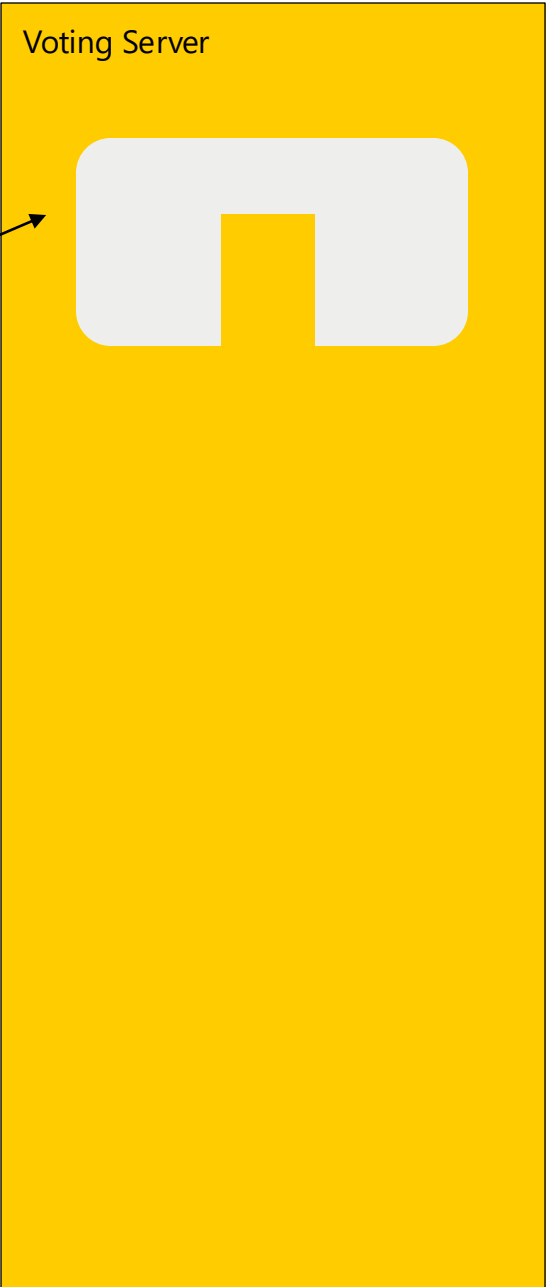
return codes





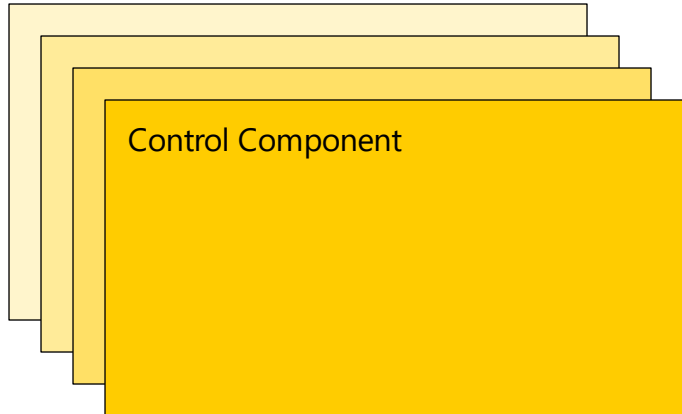
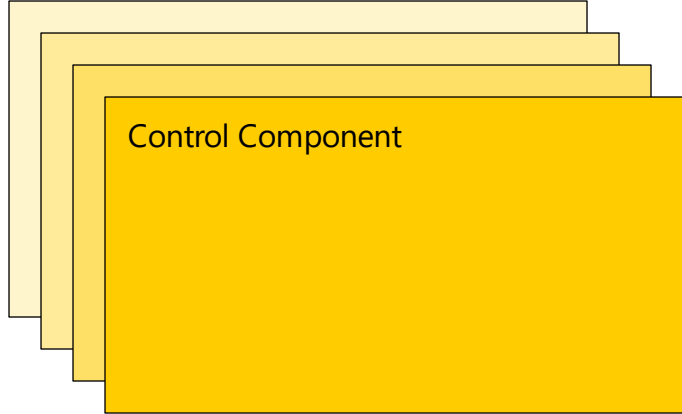
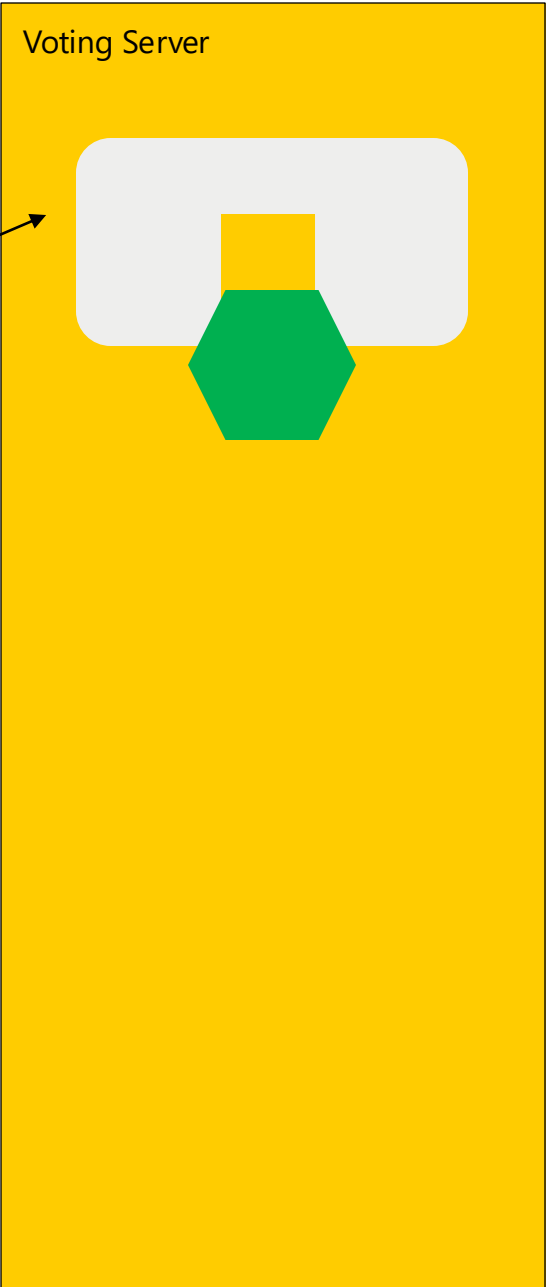


send vote



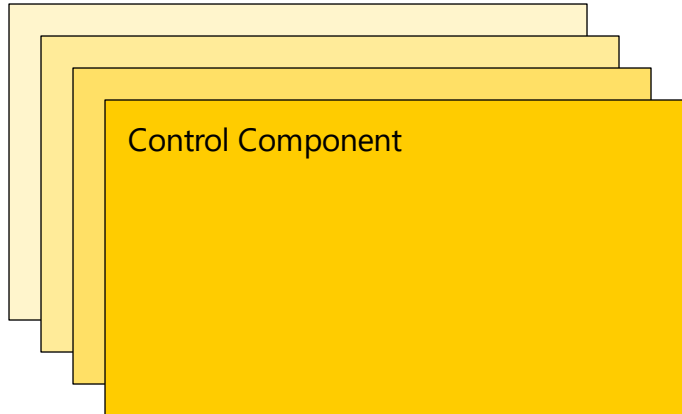
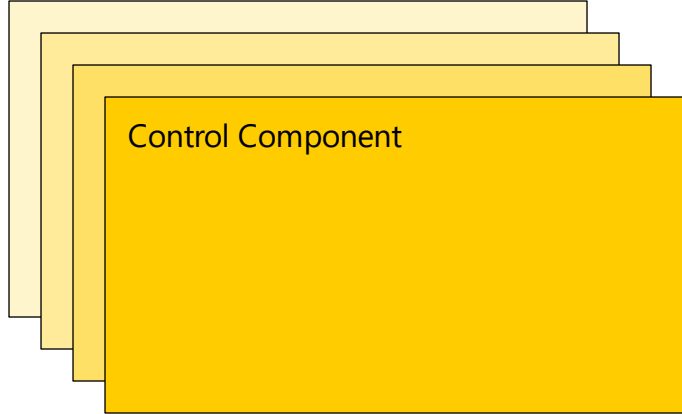
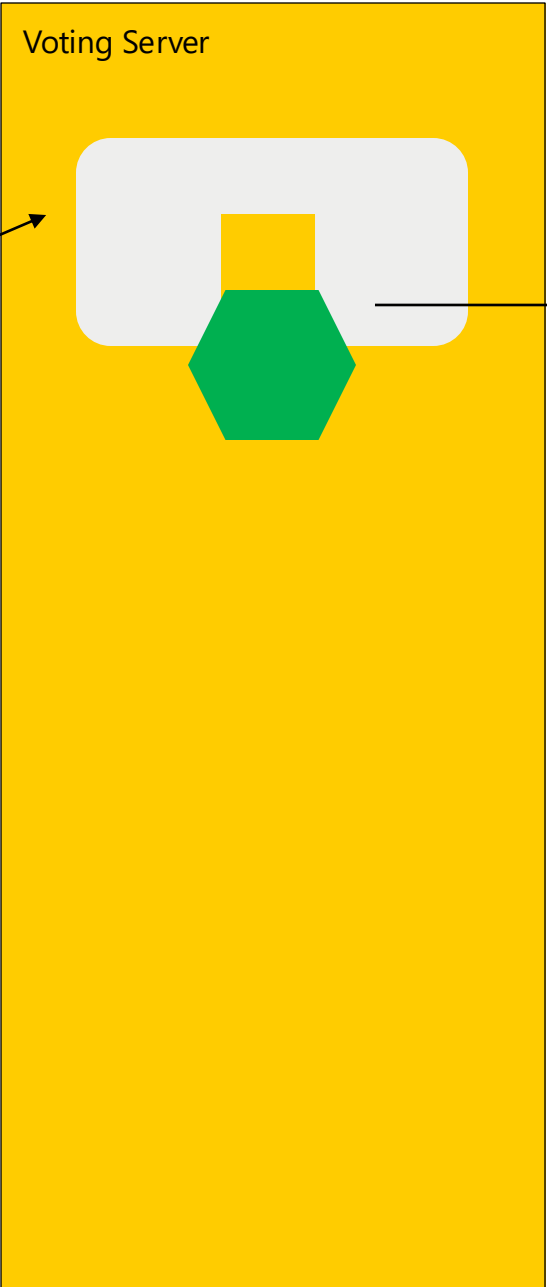


send vote



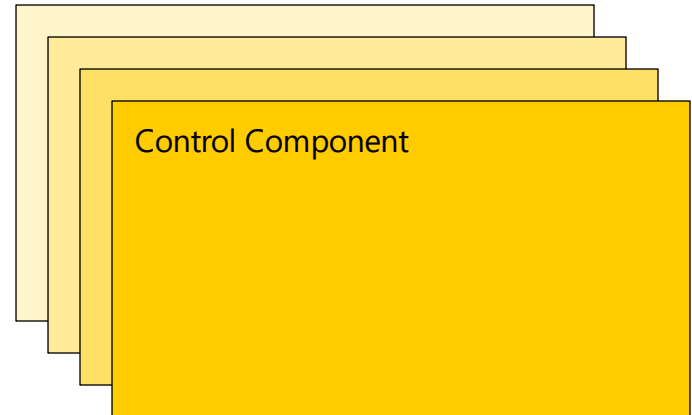
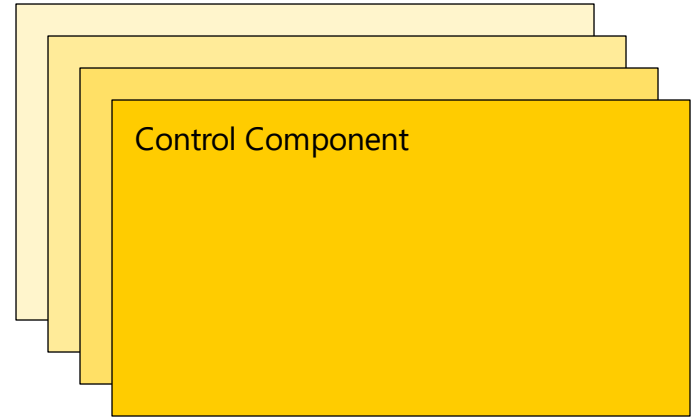
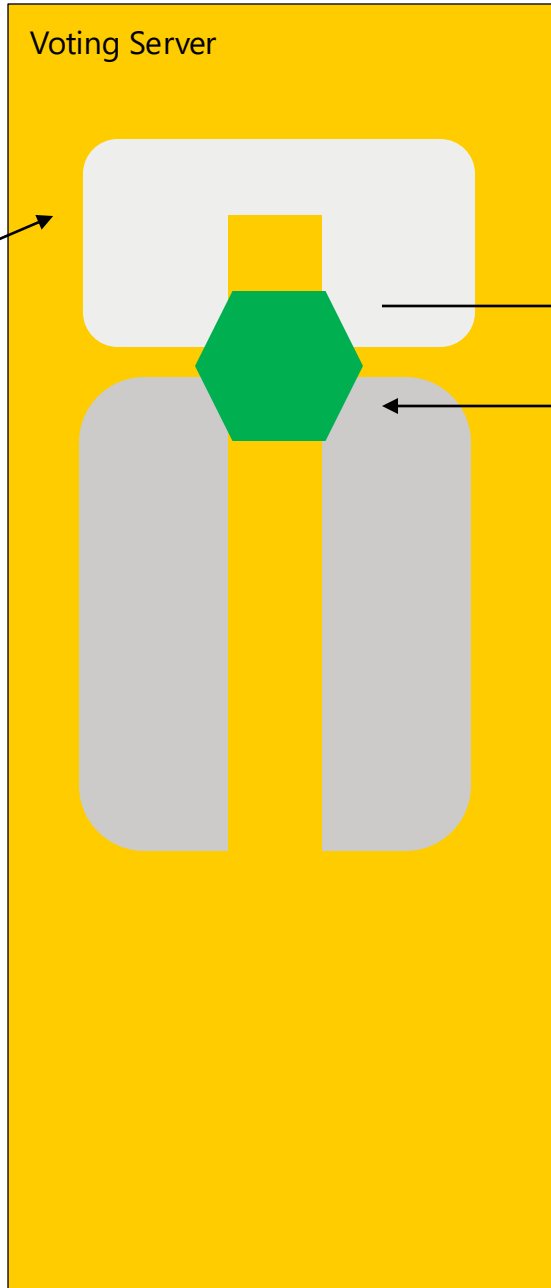


send vote



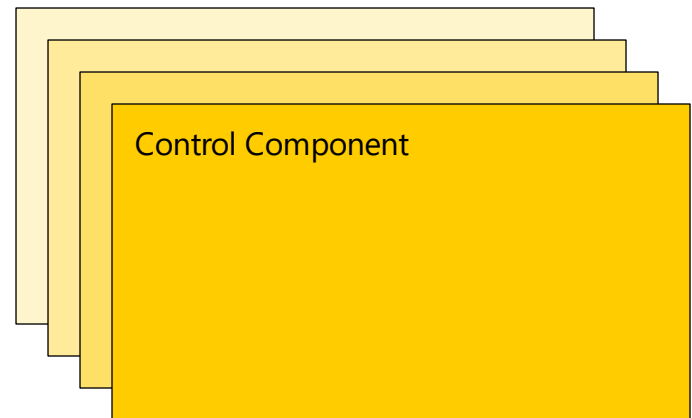
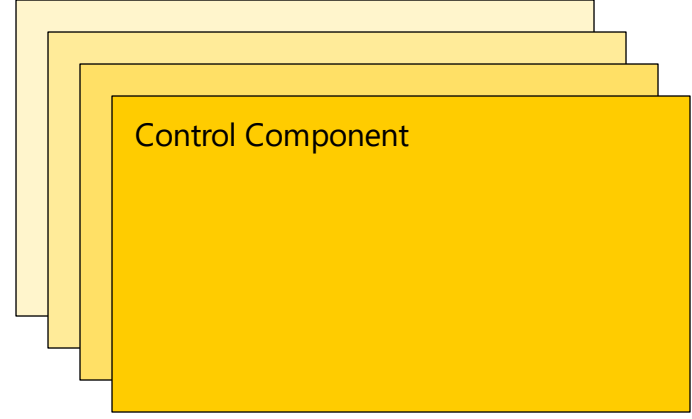
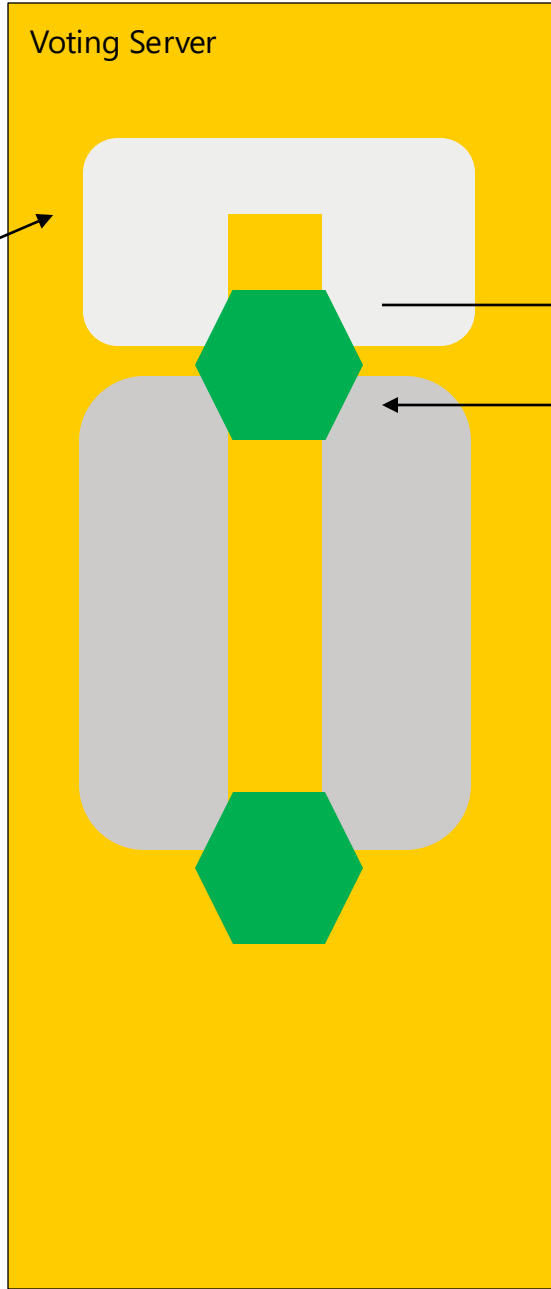


send vote



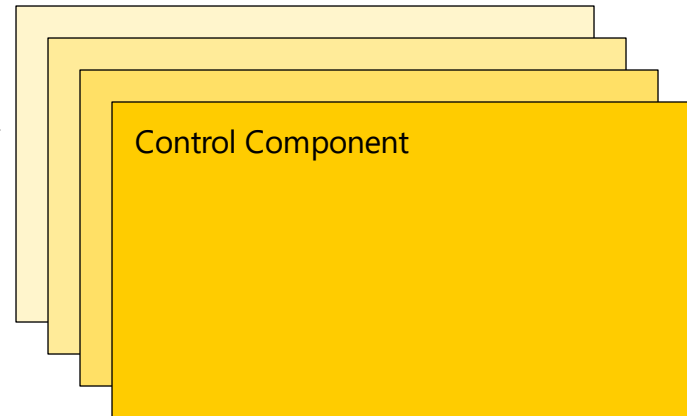
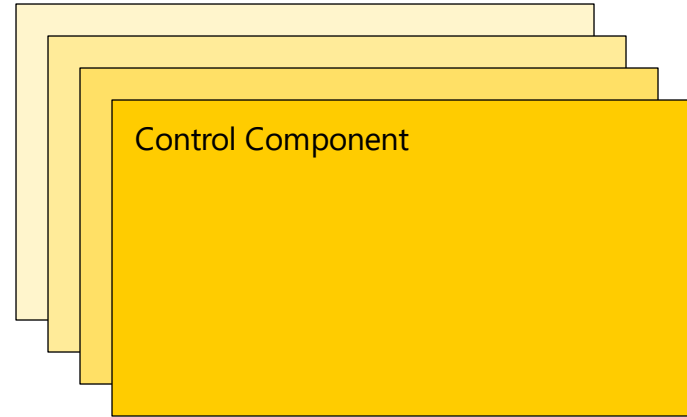
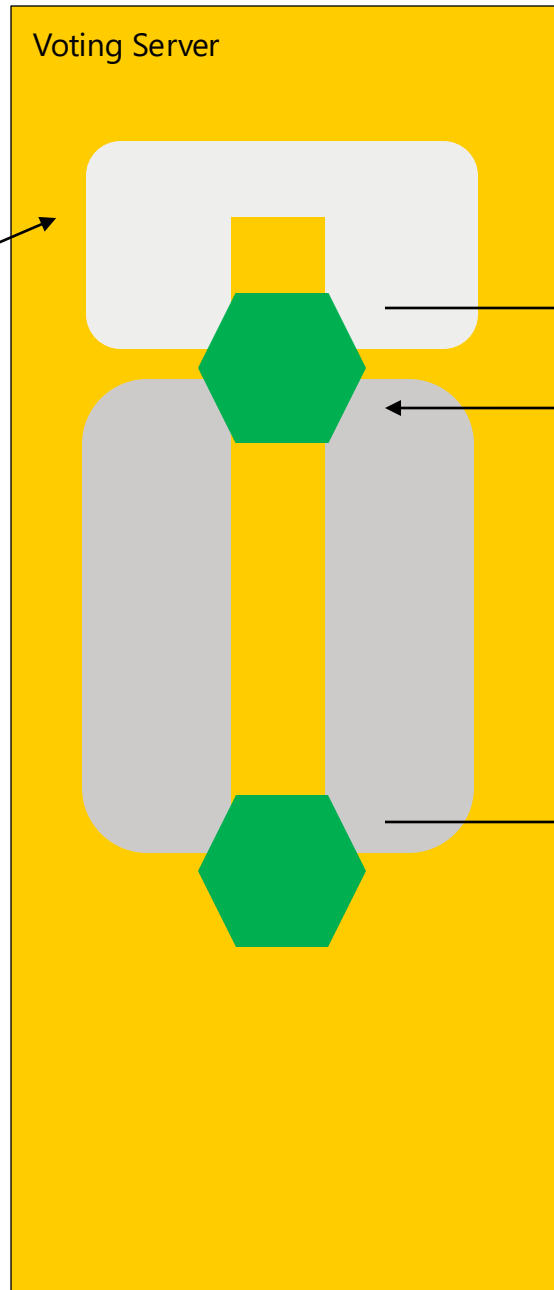


send vote



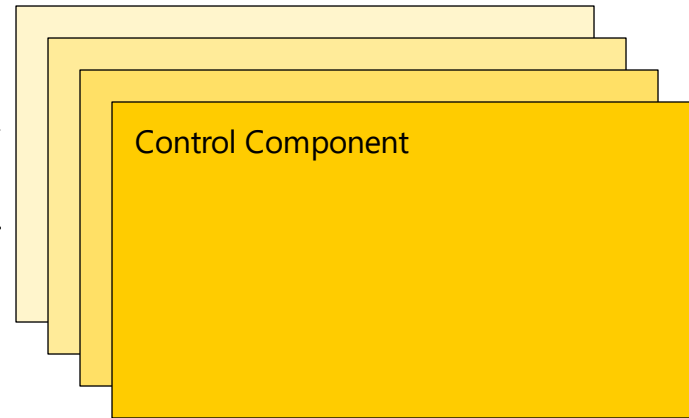
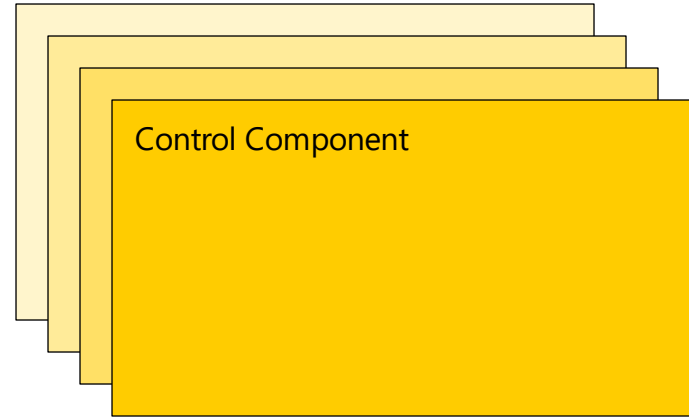
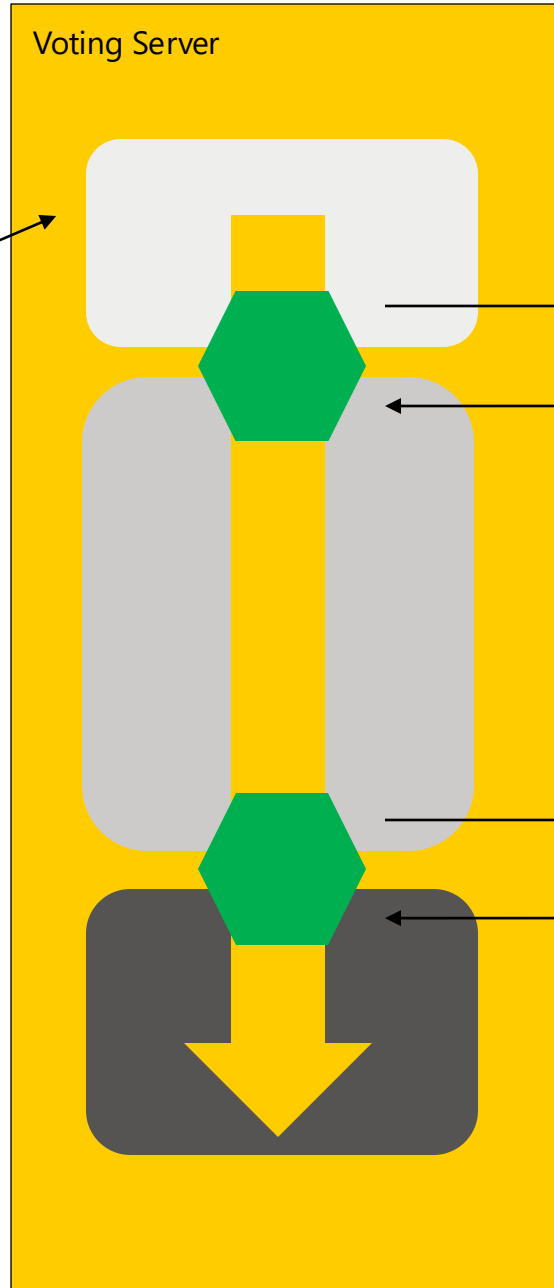


send vote





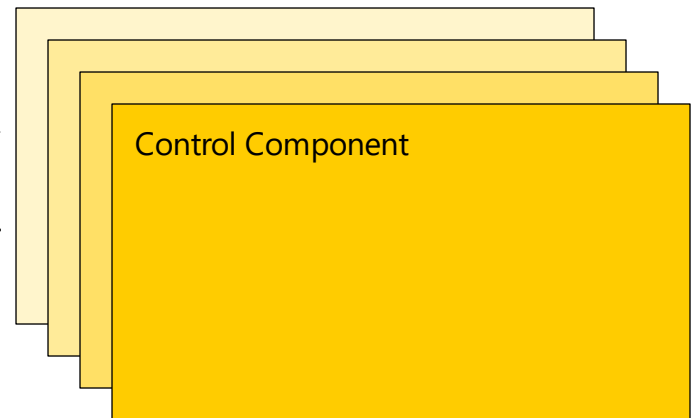
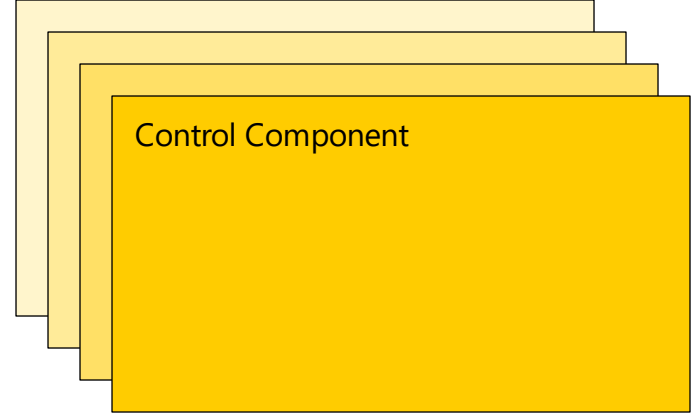
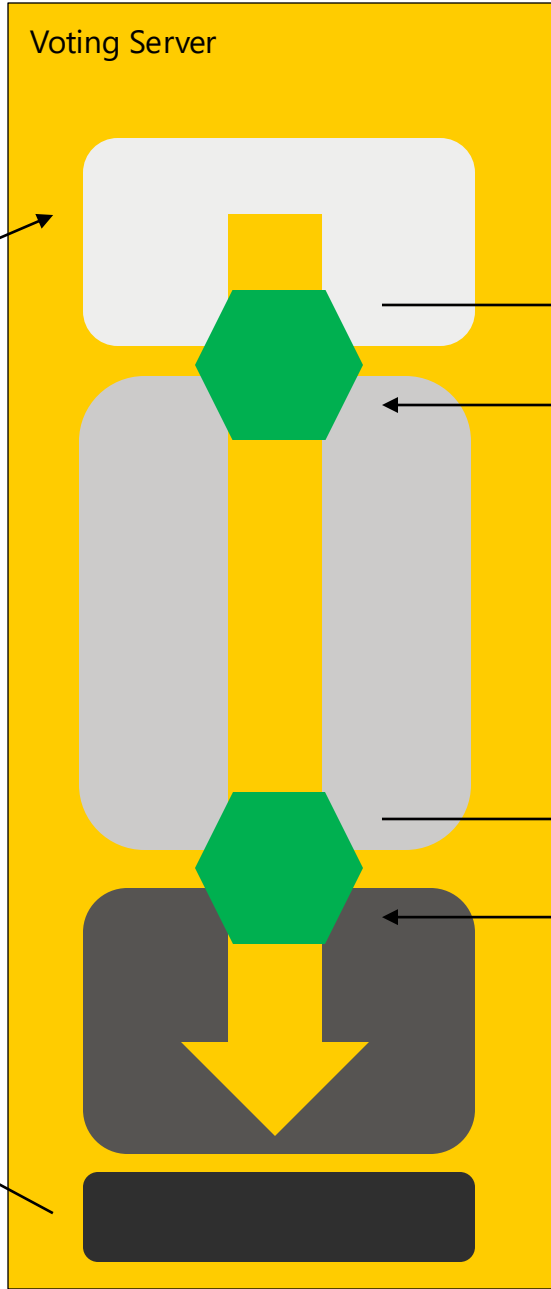
send vote





send vote

return codes



Key Technical Aspects

How to?

Libraries

RabbitMQ, ActiveMQ, etc.

Threads

Async Publish/Subscribe Pattern

Queuing

Pros

Broadcast, Listener, Load Balancing

Cons

Possible duplicate messages

3

Key Takeaways

Objectives

- Scalability
- Availability
- Prevent timeouts
- Transactional (stable states)

Trade-offs

- Increased complexity
- Throughput vs. delay
- Consistency vs. availability
- Operational overhead

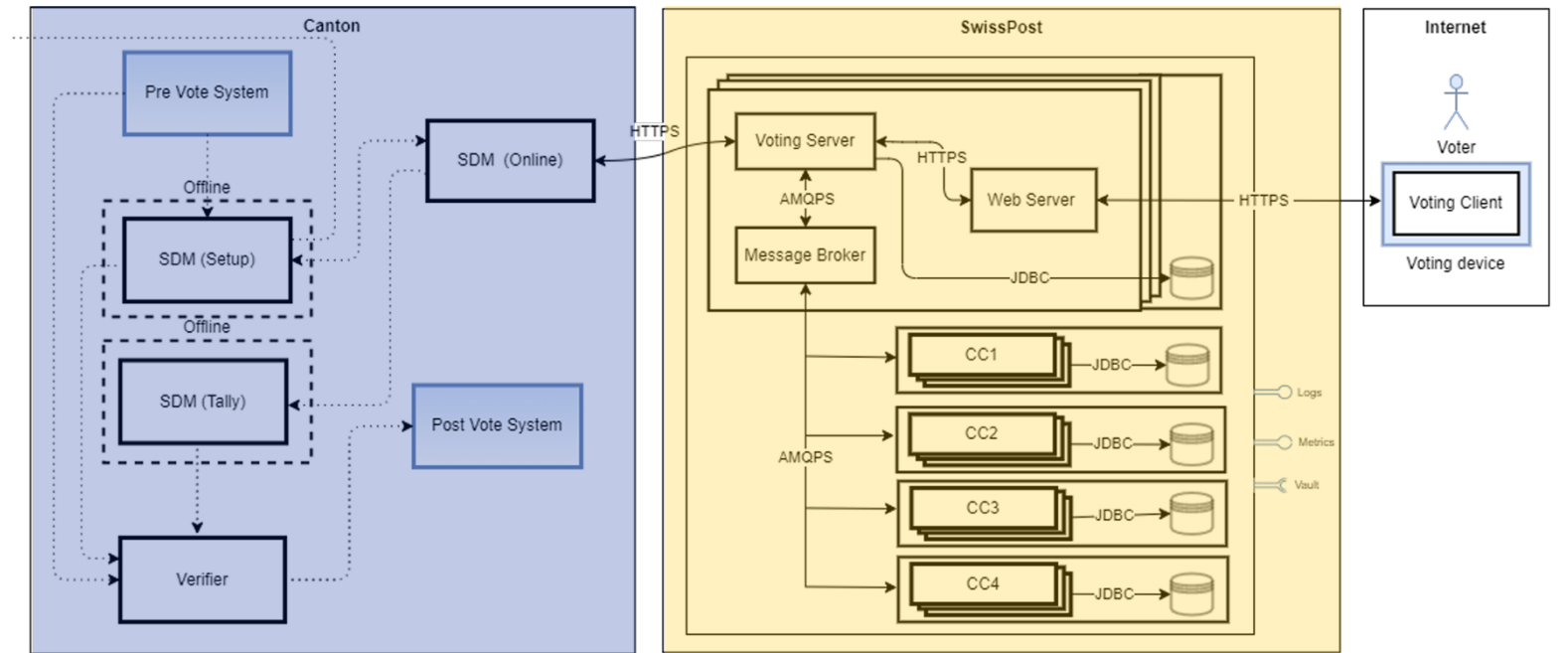
**Interactions between systems must be considered
as soon as possible**

Challenges

1 Scalability

2 Data transfer

3 Resiliency



Want to know more?

Check out our **published code** on
GitLab and test the system



Submit a report to our **bug bounty
programme** in YesWeHack
💰 up to € 230,000



Experience E-Voting with the **demo**



Check the Swiss Post **opportunities**
during and after studies



Thanks!



Céline Camacho

E-Voting Software Engineer

celine.camacho@post.ch

IN'21



Nils Aellen

E-Voting Solution Architect

nils.aellen@post.ch

IN'02



Patrick Andrade

E-Voting People DevOps Lead

patrick.oliveiraandrade@post.ch

IN'17

