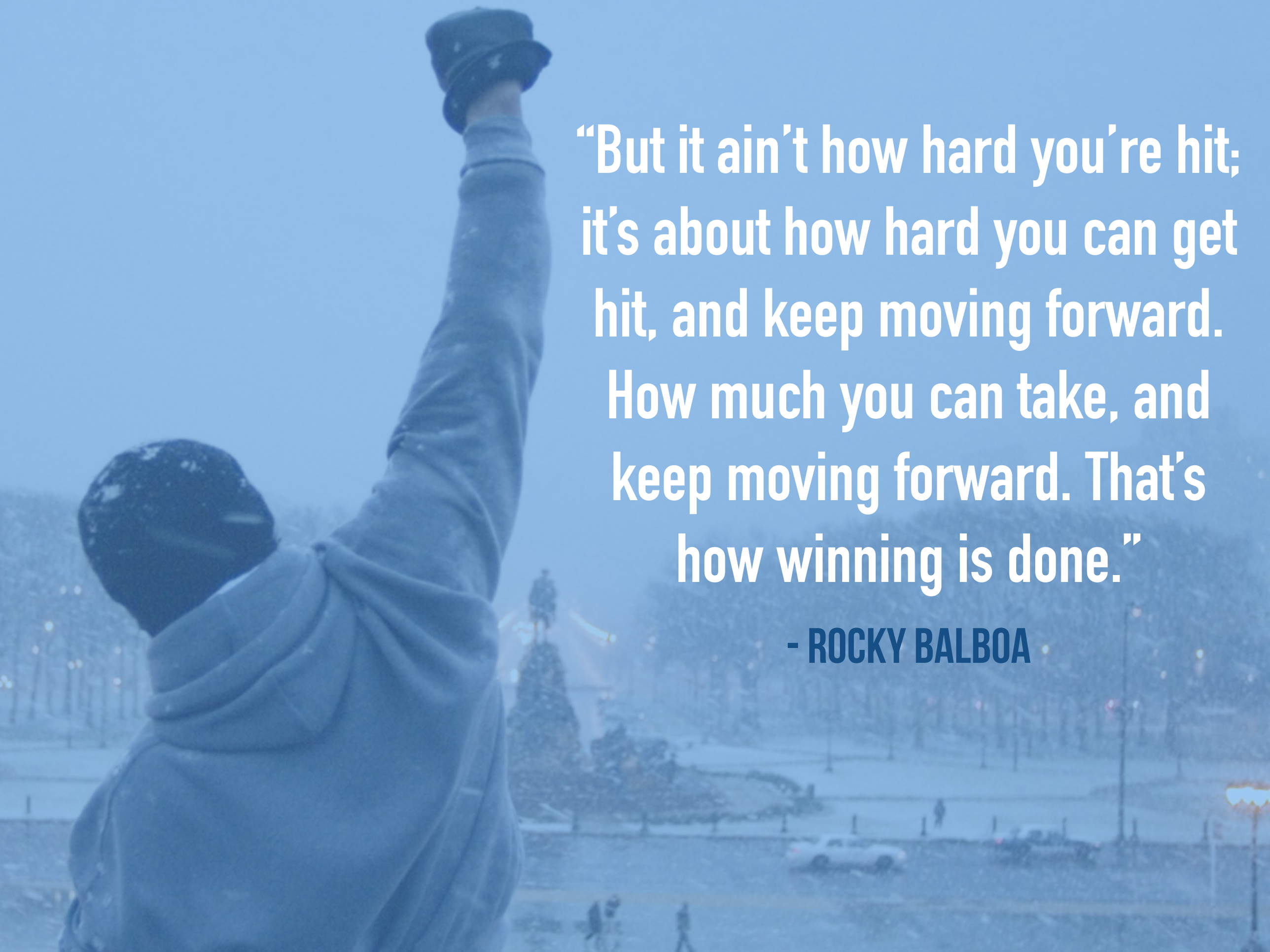
Without Resilience Nothing Else Matters

JONAS BONÉR
CTO TYPESAFE
@JBONER

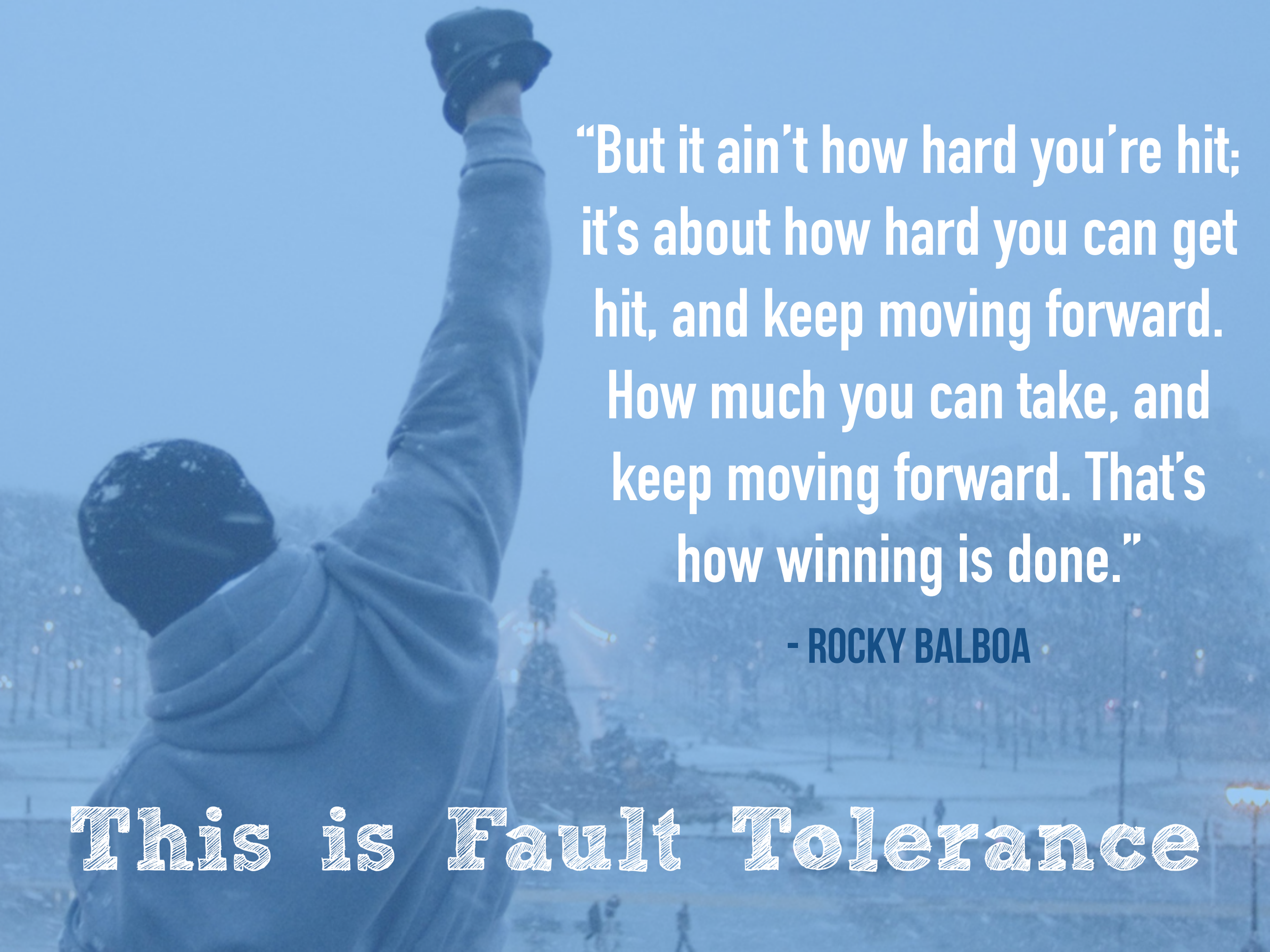
Without Resilience Nothing Else Matters

JONAS BONÉR
CTO TYPESAFE
@JBONER



"But it ain't how hard you're hit; it's about how hard you can get hit, and keep moving forward. How much you can take, and keep moving forward. That's how winning is done."

- ROCKY BALBOA


"But it ain't how hard you're hit; it's about how hard you can get hit, and keep moving forward. How much you can take, and keep moving forward. That's how winning is done."
- ROCKY BALBOA
This is Fault Tolerance

Resilience is Beyond Fault Tolerance

Resilience

"The ability of a substance or object to spring back into shape. The capacity to recover quickly from difficulties."

-MERRIAM WEBSTER

Antifragility

"Antifragility is beyond resilience and robustness. The resilient resists shock and stays the same; the antifragile gets better."

- NASSEM NICHOLAS TALEB

Antifragile: Things That Gain from Disorder - Nassim Nicholas Taleb

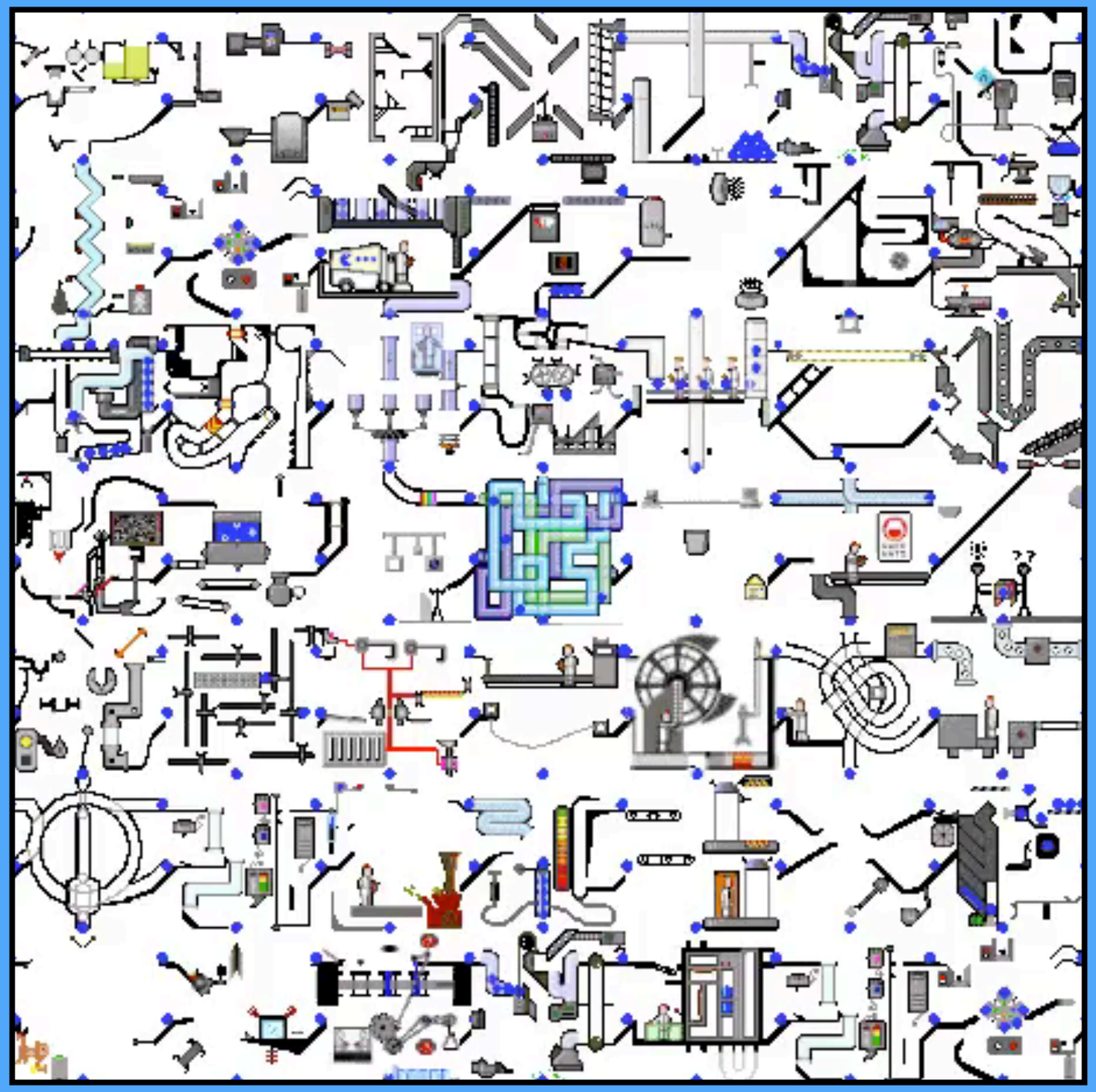
"We can model and understand in isolation.
But, when released into competitive nominally regulated societies, their connections proliferate, their interactions and interdependencies multiply, their complexities mushroom.
And we are caught short."

- SIDNEY DEKKER

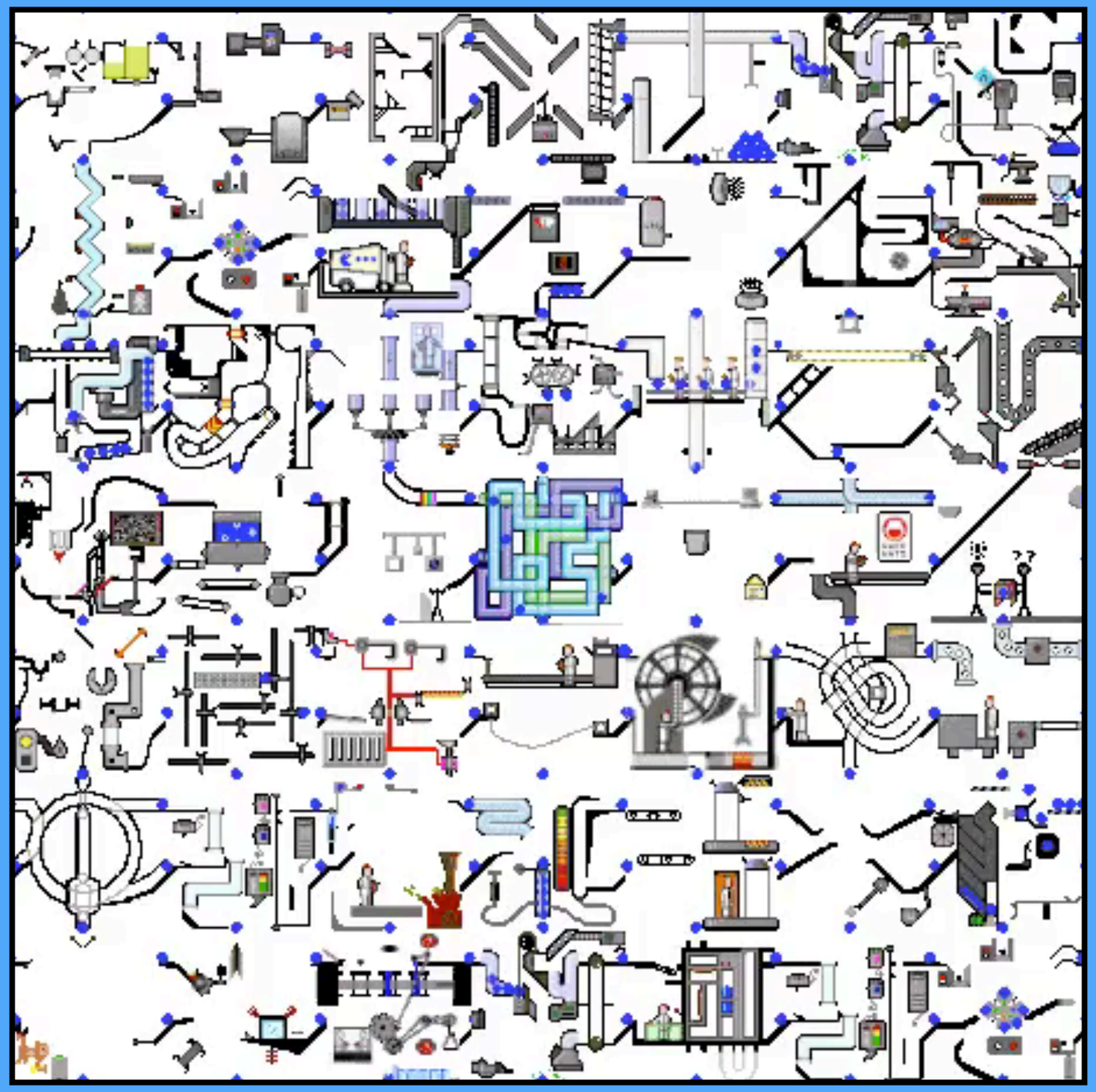
Drift into Failure - Sidney Dekker

We Need to Study Resilience in Complex Systems

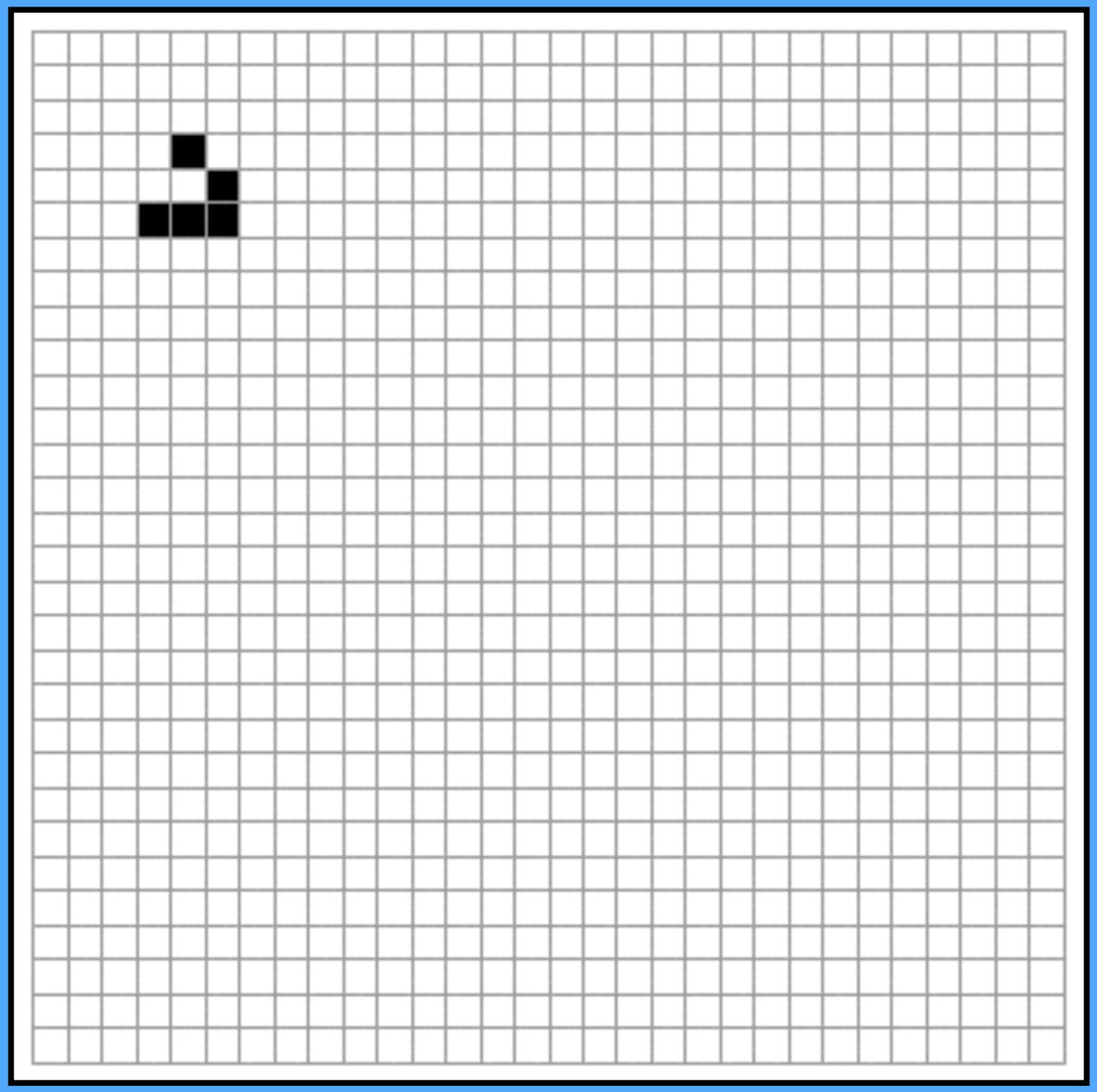
Complicated System



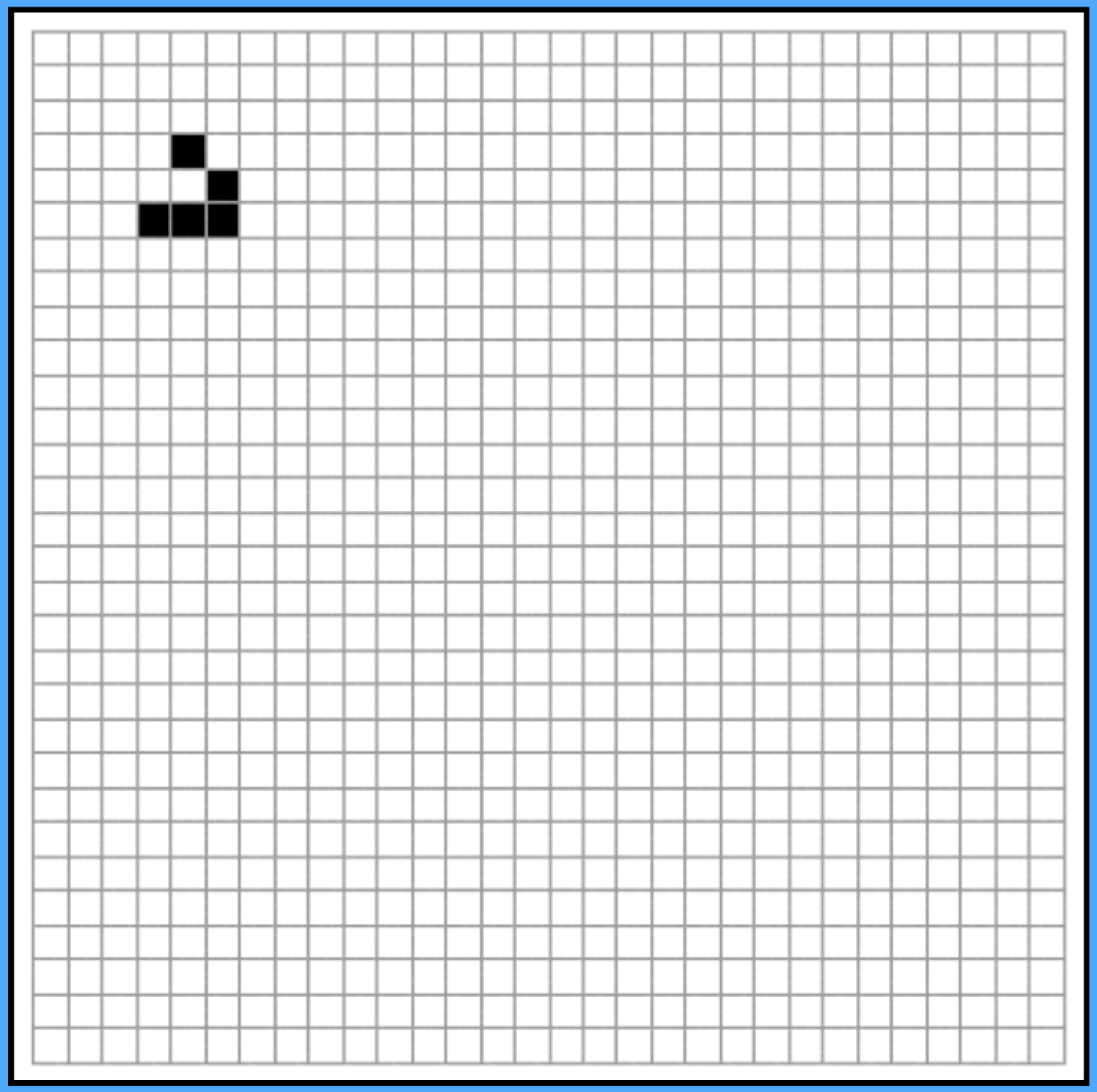
Complicated System



Complex System



Complex System



Complex System

COMPLICATED ≠ COMPLEX

"Counterintuitive. That's [Jay] Forrester's word to describe complex systems. Leverage points are not intuitive. Or if they are, we intuitively use them backward, systematically worsening whatever problems we are trying to solve."

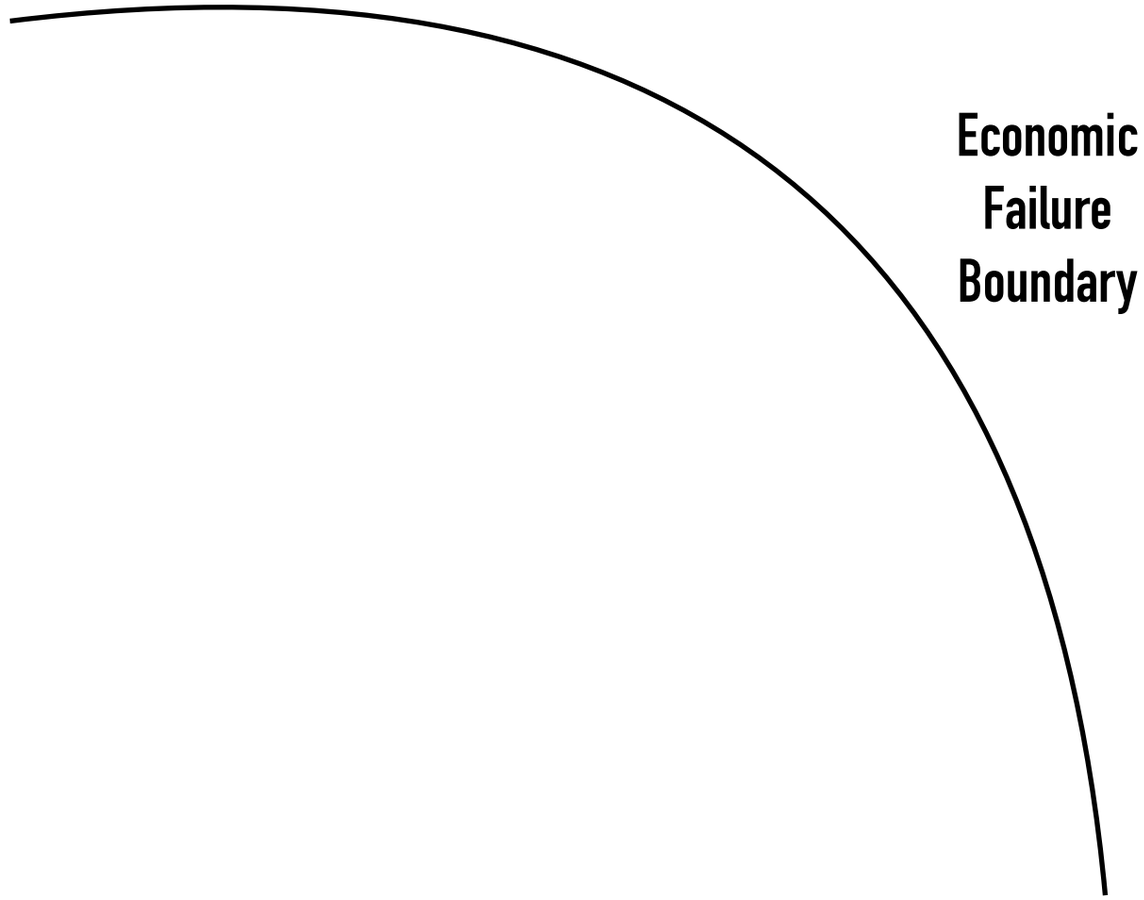
- DONELLA MEADOWS

Leverage Points: Places to Intervene in a System - Donella Meadows

Operating at the Edge of Failure

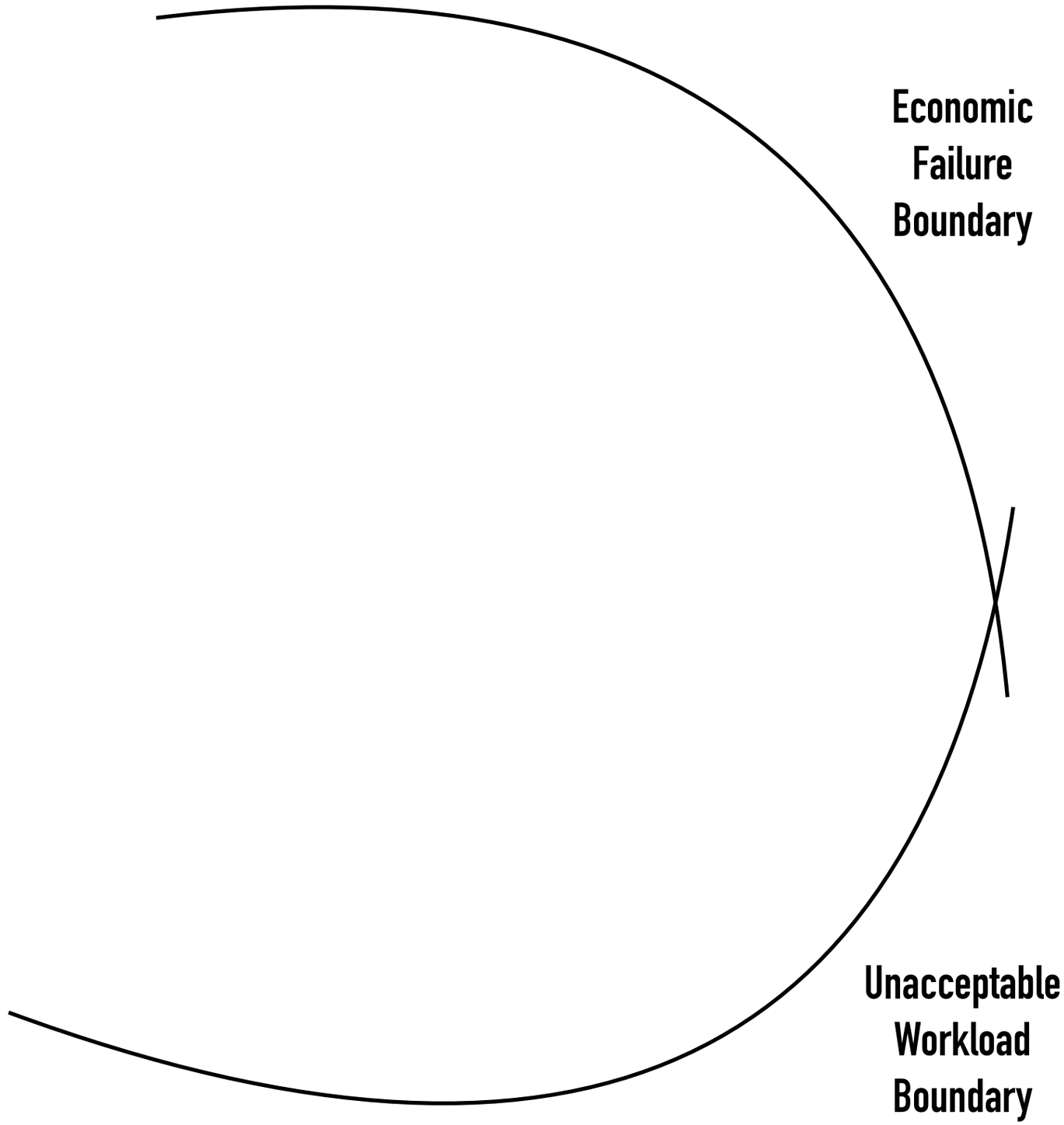
"Going solid": a model of system dynamics and consequences for patient safety - R Cook, J Rasmussen
Resilience in complex adaptive systems: Operating at the Edge of Failure - Richard Cook - Talk at Velocity NY 2013

Operating at the Edge of Failure



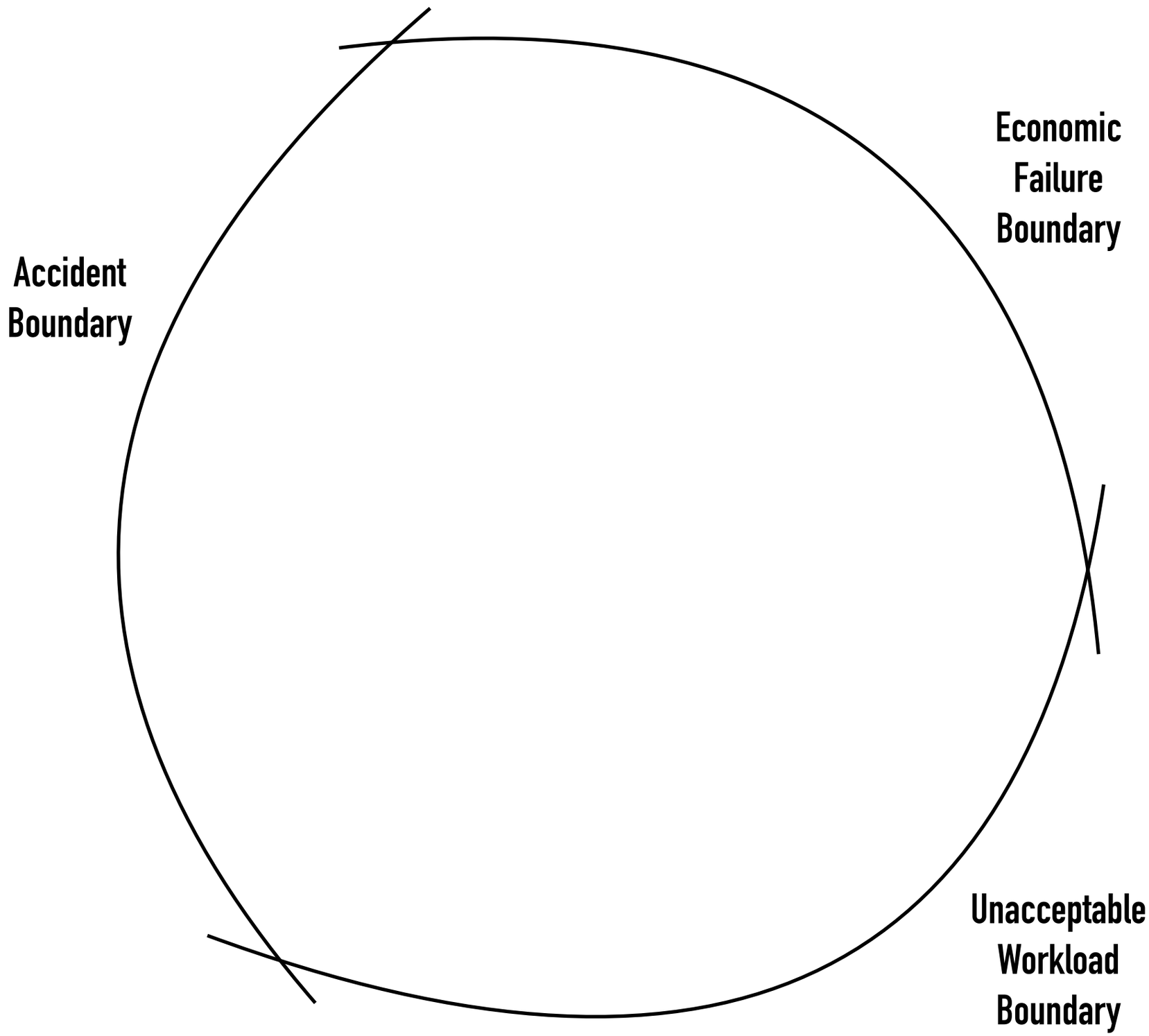
"Going solid": a model of system dynamics and consequences for patient safety - R Cook, J Rasmussen
Resilience in complex adaptive systems: Operating at the Edge of Failure - Richard Cook - Talk at Velocity NY 2013

Operating at the Edge of Failure



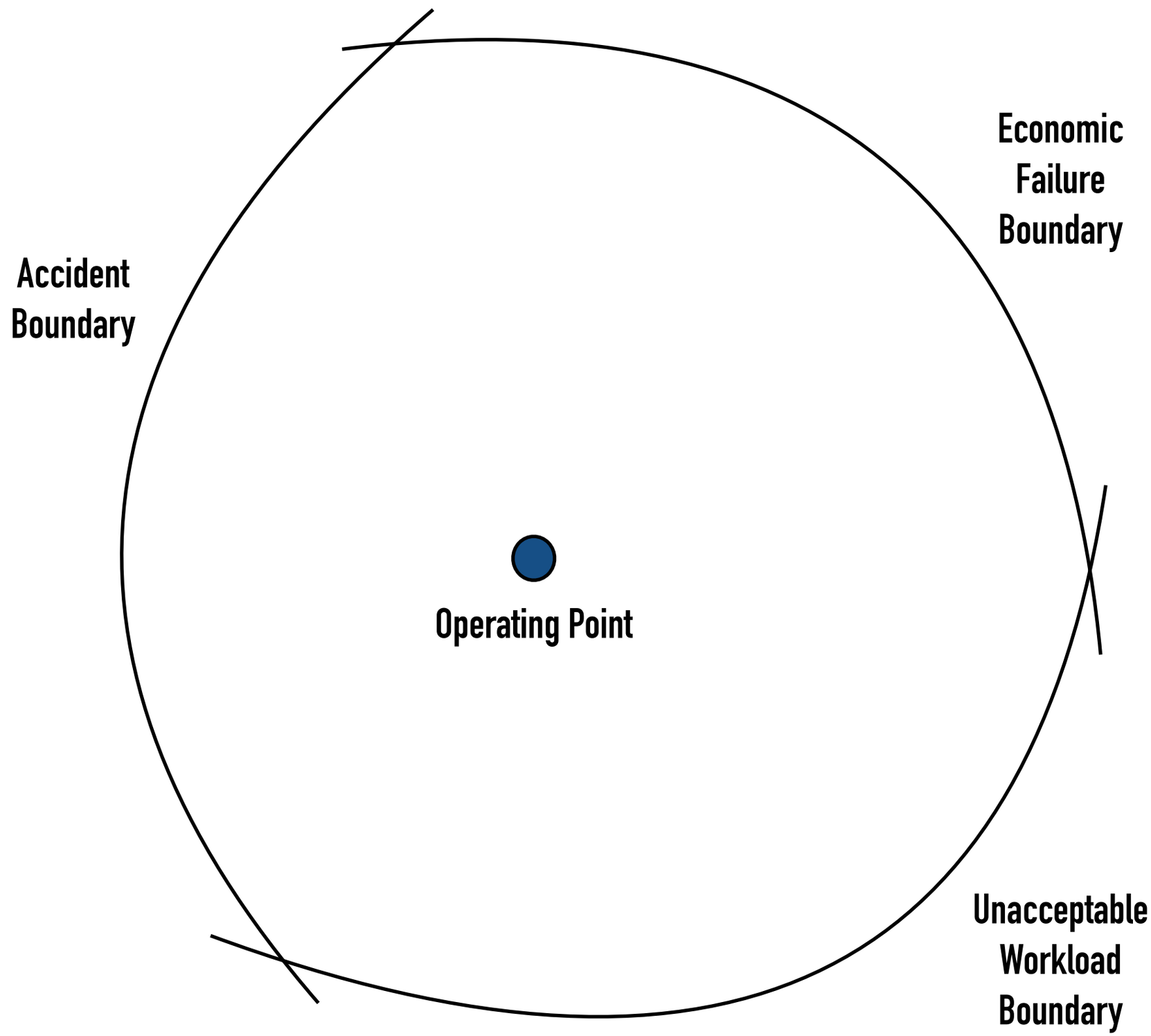
"Going solid": a model of system dynamics and consequences for patient safety - R Cook, J Rasmussen
Resilience in complex adaptive systems: Operating at the Edge of Failure - Richard Cook - Talk at Velocity NY 2013

Operating at the Edge of Failure



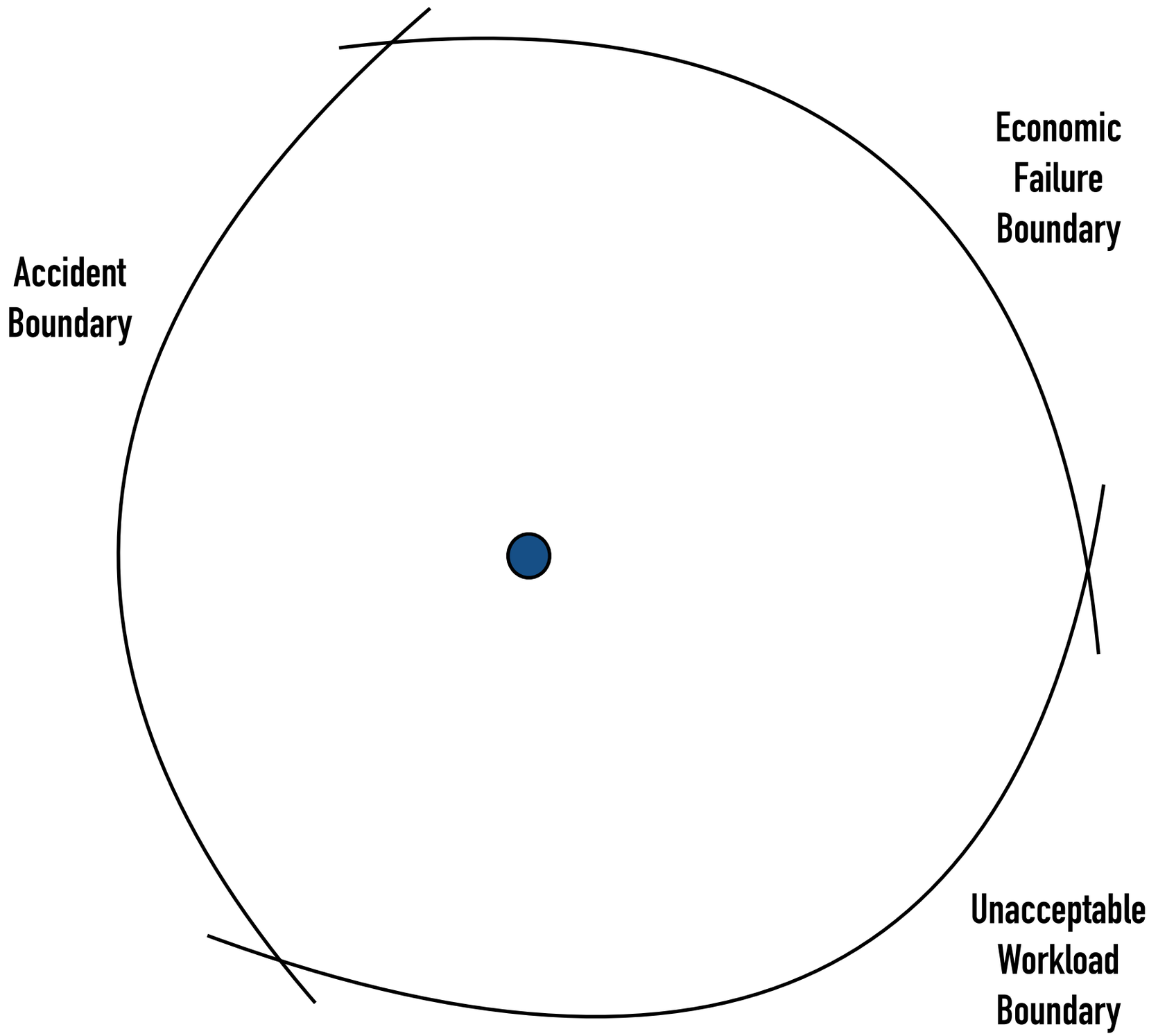
"Going solid": a model of system dynamics and consequences for patient safety - R Cook, J Rasmussen
Resilience in complex adaptive systems: Operating at the Edge of Failure - Richard Cook - Talk at Velocity NY 2013

Operating at the Edge of Failure



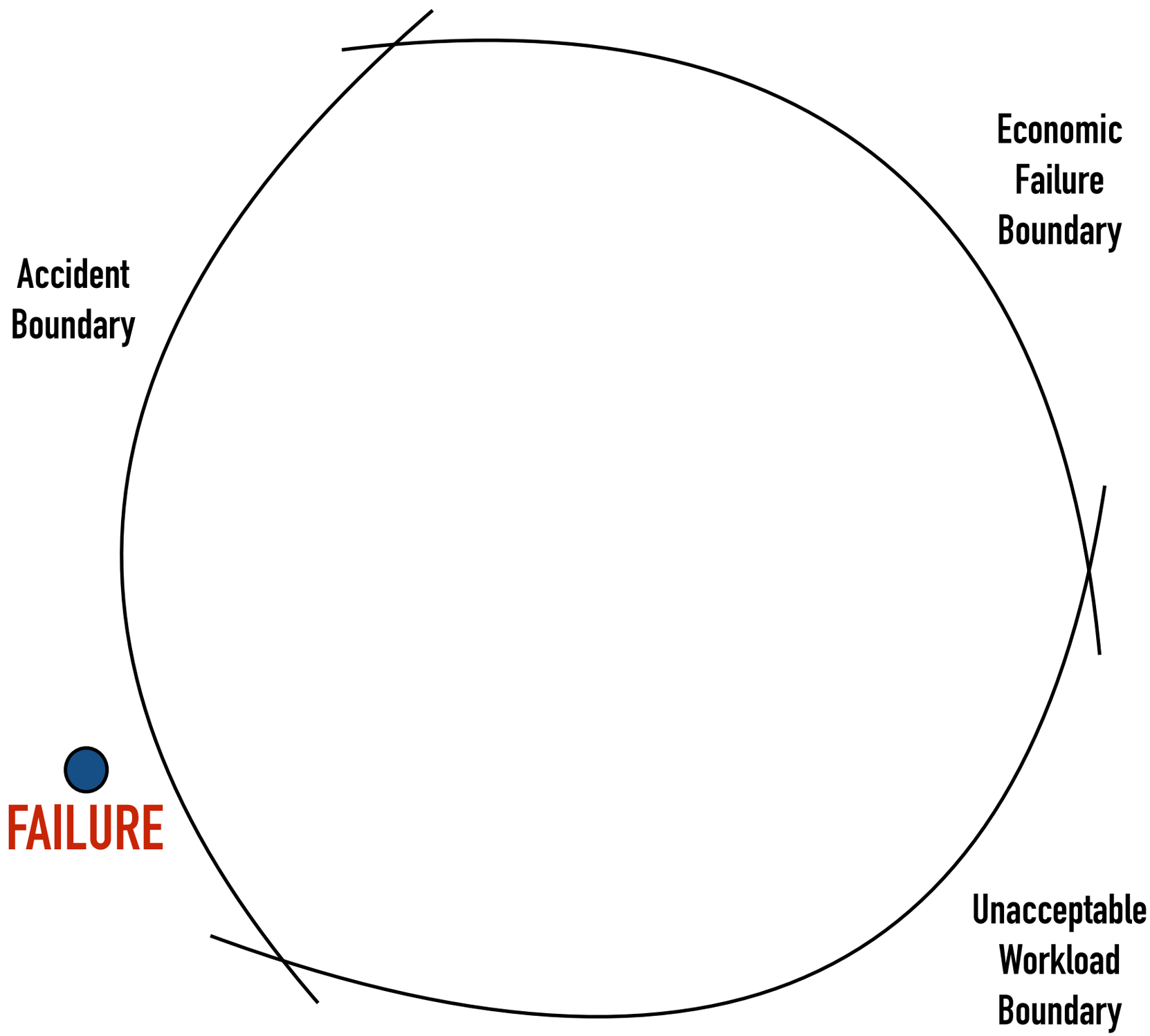
"Going solid": a model of system dynamics and consequences for patient safety - R Cook, J Rasmussen
Resilience in complex adaptive systems: Operating at the Edge of Failure - Richard Cook - Talk at Velocity NY 2013

Operating at the Edge of Failure



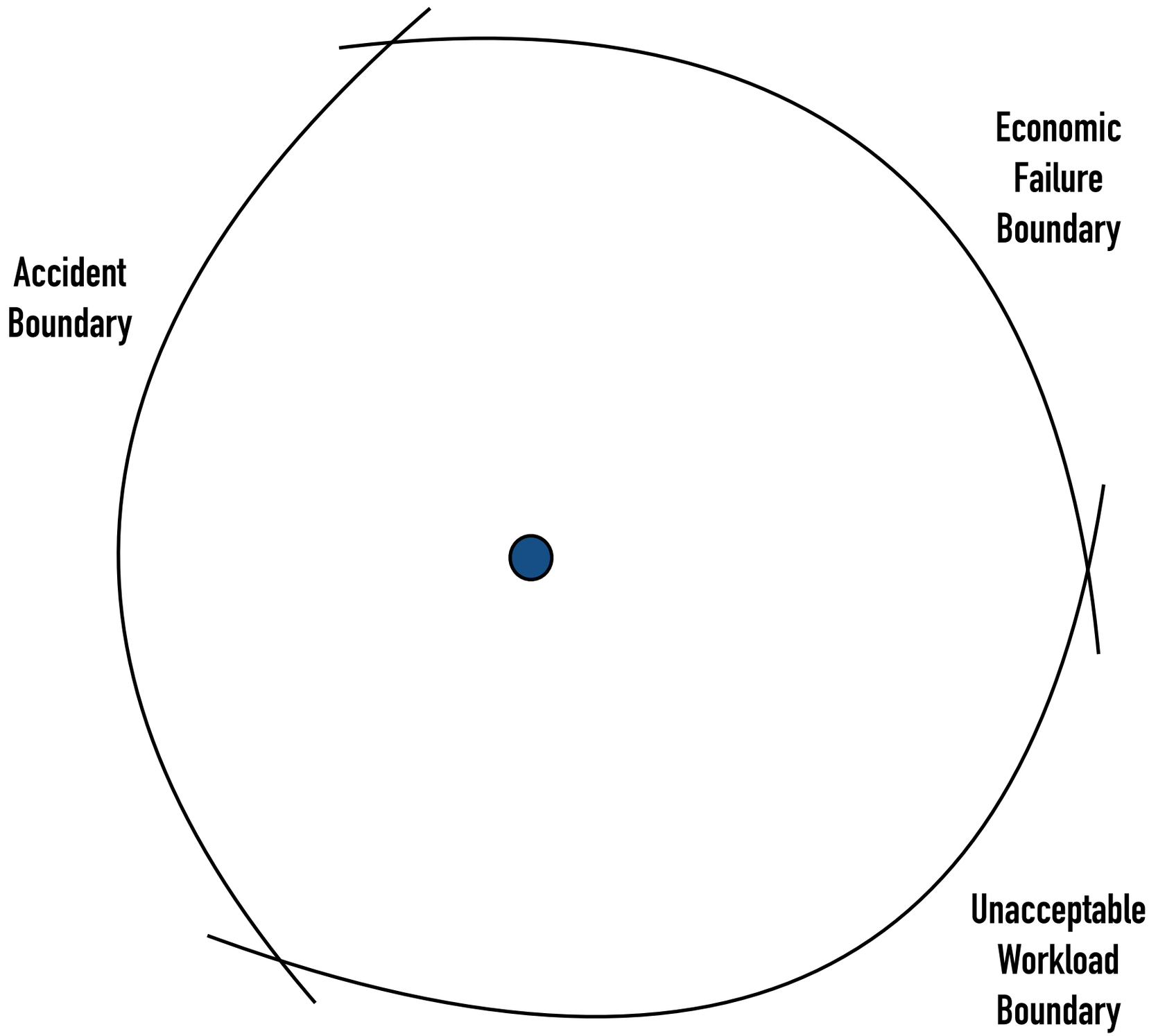
"Going solid": a model of system dynamics and consequences for patient safety - R Cook, J Rasmussen
Resilience in complex adaptive systems: Operating at the Edge of Failure - Richard Cook - Talk at Velocity NY 2013

Operating at the Edge of Failure



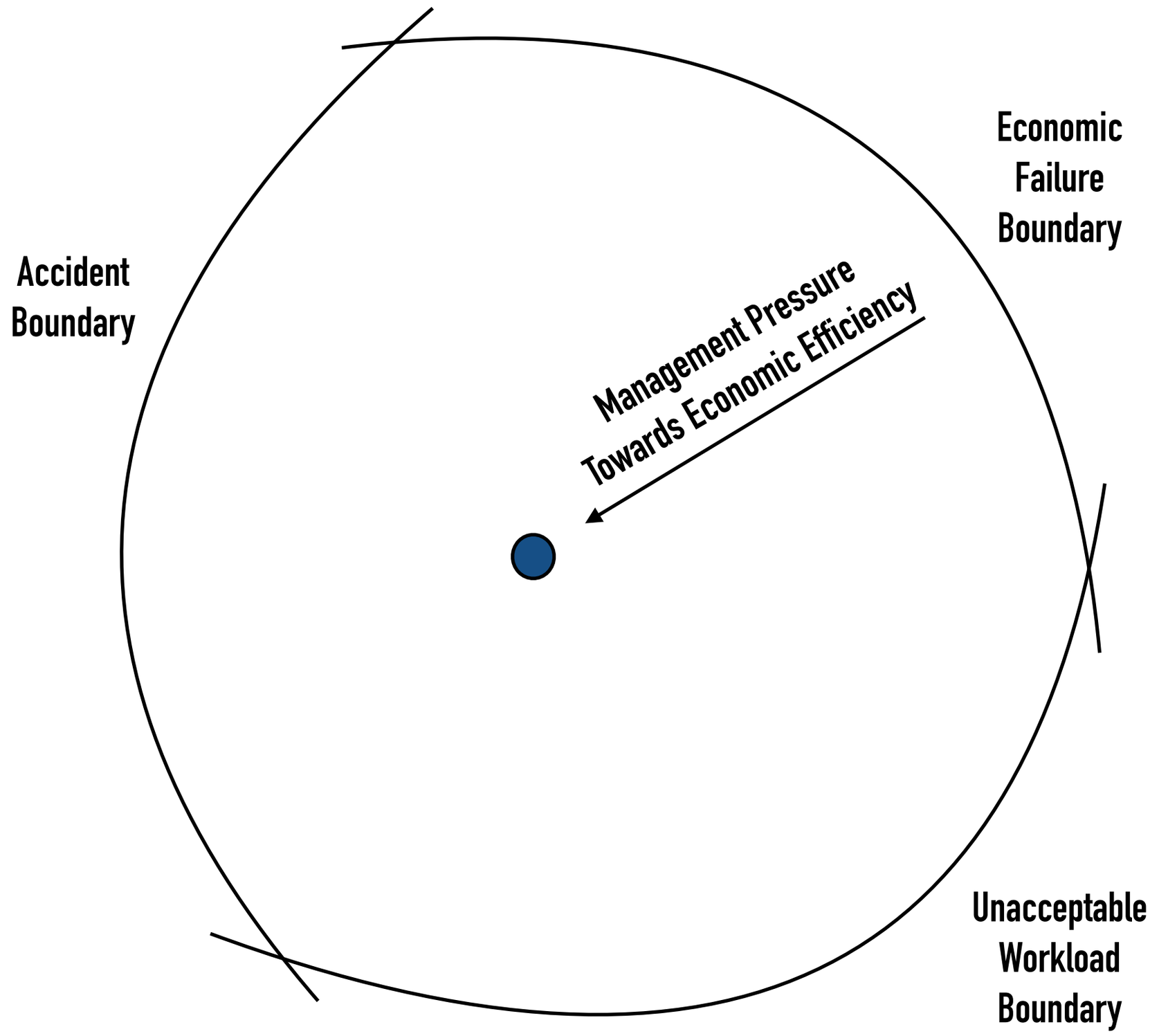
"Going solid": a model of system dynamics and consequences for patient safety - R Cook, J Rasmussen
Resilience in complex adaptive systems: Operating at the Edge of Failure - Richard Cook - Talk at Velocity NY 2013

Operating at the Edge of Failure



"Going solid": a model of system dynamics and consequences for patient safety - R Cook, J Rasmussen
Resilience in complex adaptive systems: Operating at the Edge of Failure - Richard Cook - Talk at Velocity NY 2013

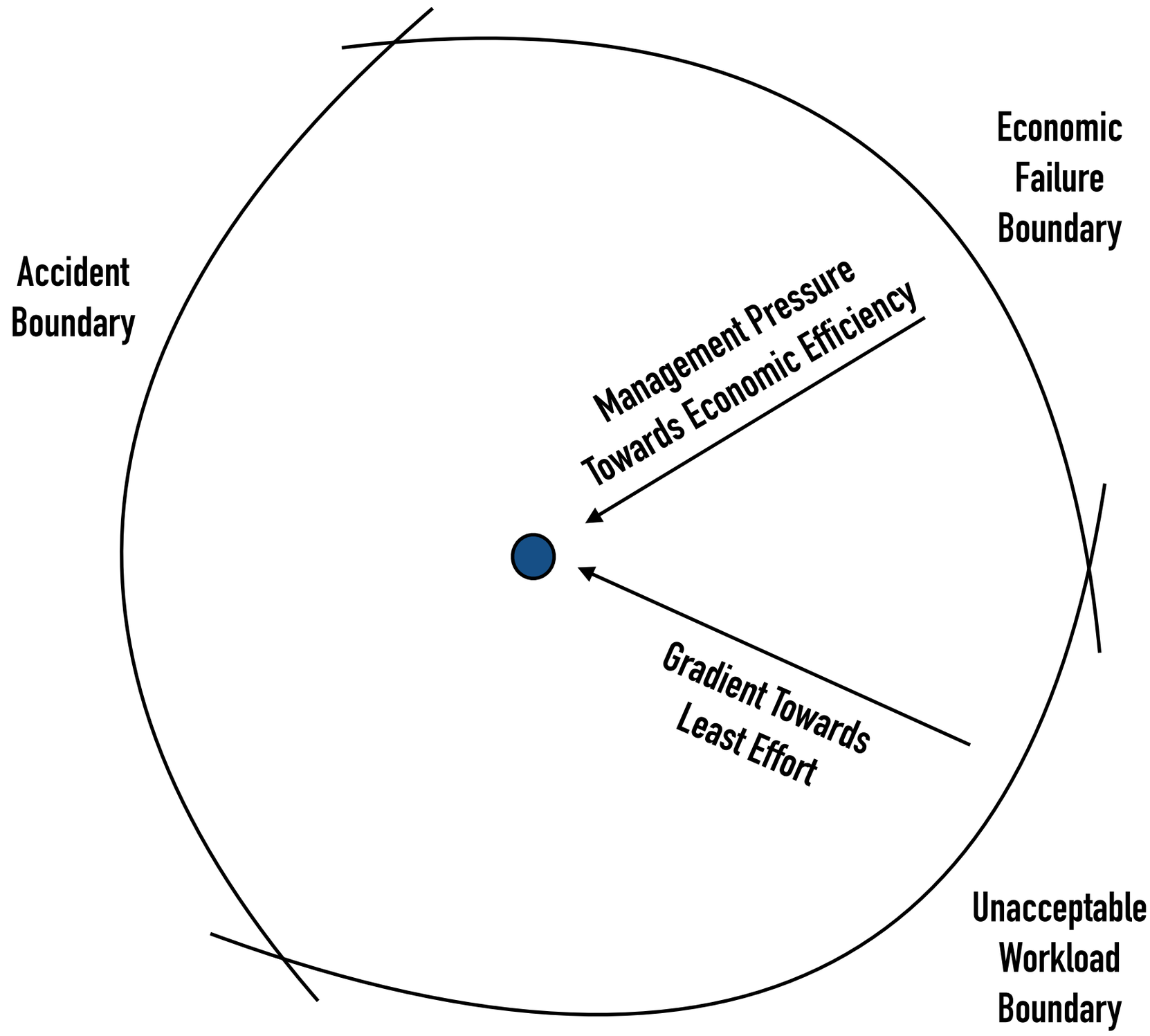
Operating at the Edge of Failure



"Going solid": a model of system dynamics and consequences for patient safety - R Cook, J Rasmussen

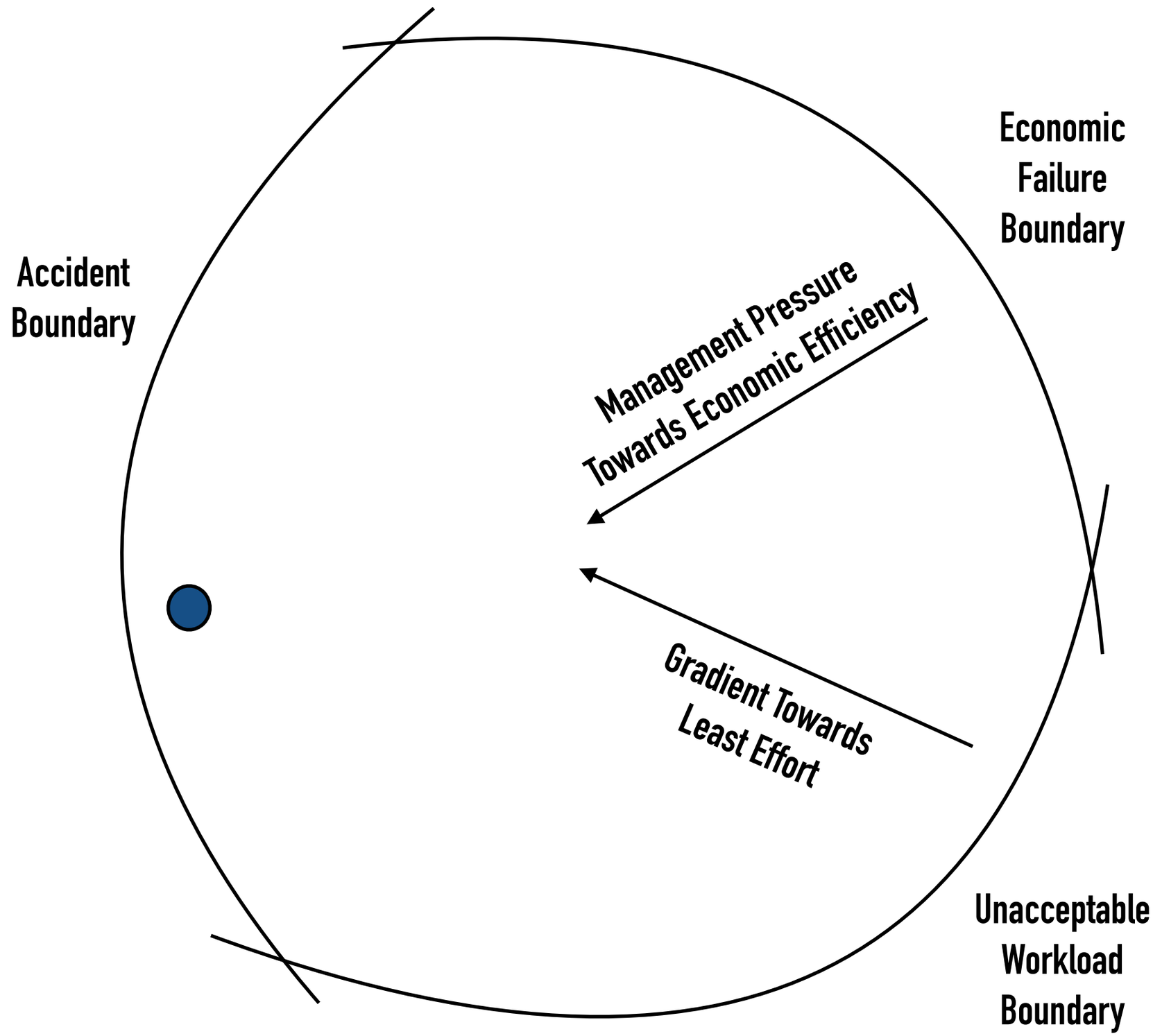
Resilience in complex adaptive systems: Operating at the Edge of Failure - Richard Cook - Talk at Velocity NY 2013

Operating at the Edge of Failure



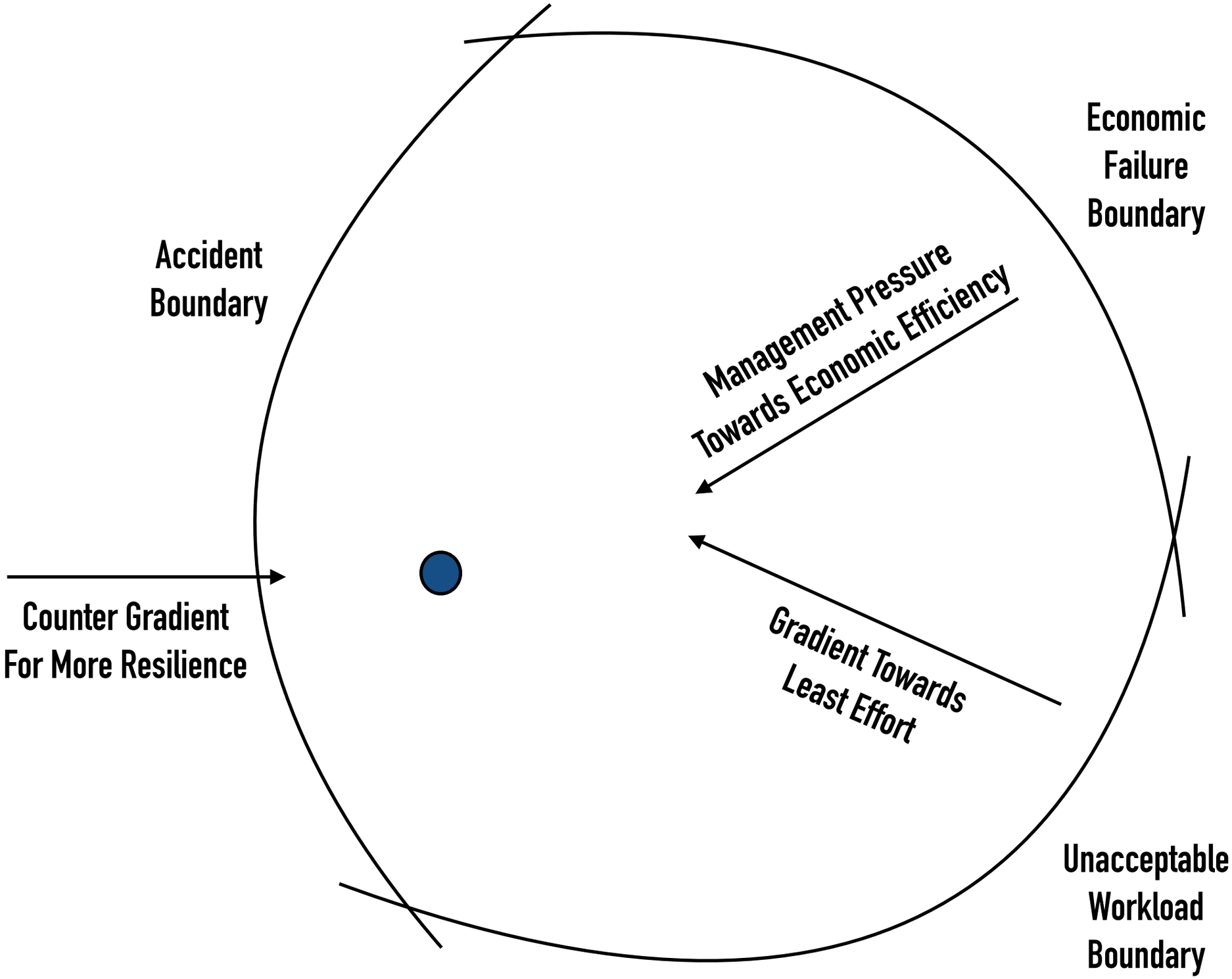
"Going solid": a model of system dynamics and consequences for patient safety - R Cook, J Rasmussen
Resilience in complex adaptive systems: Operating at the Edge of Failure - Richard Cook - Talk at Velocity NY 2013

Operating at the Edge of Failure



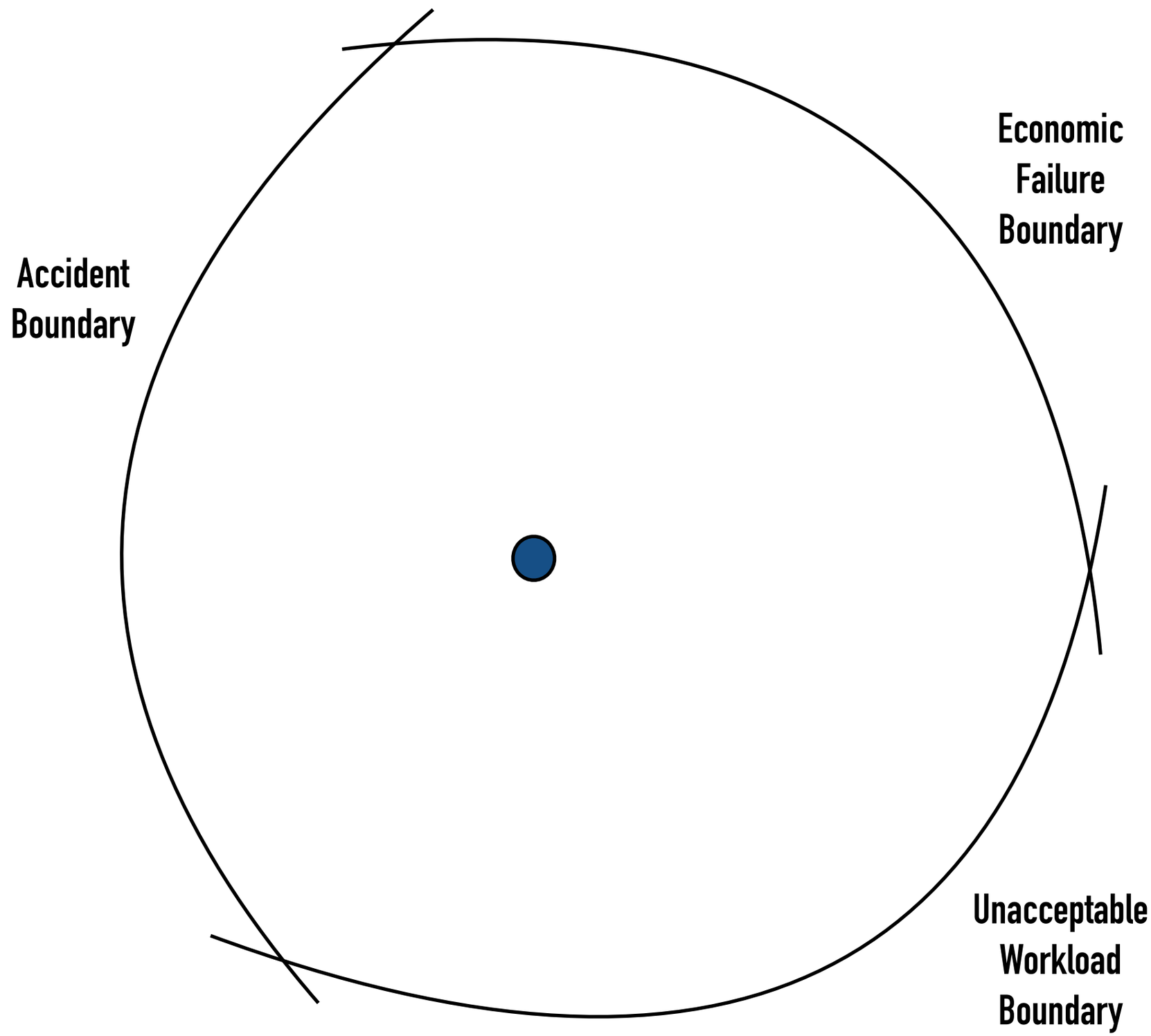
"Going solid": a model of system dynamics and consequences for patient safety - R Cook, J Rasmussen
Resilience in complex adaptive systems: Operating at the Edge of Failure - Richard Cook - Talk at Velocity NY 2013

Operating at the Edge of Failure



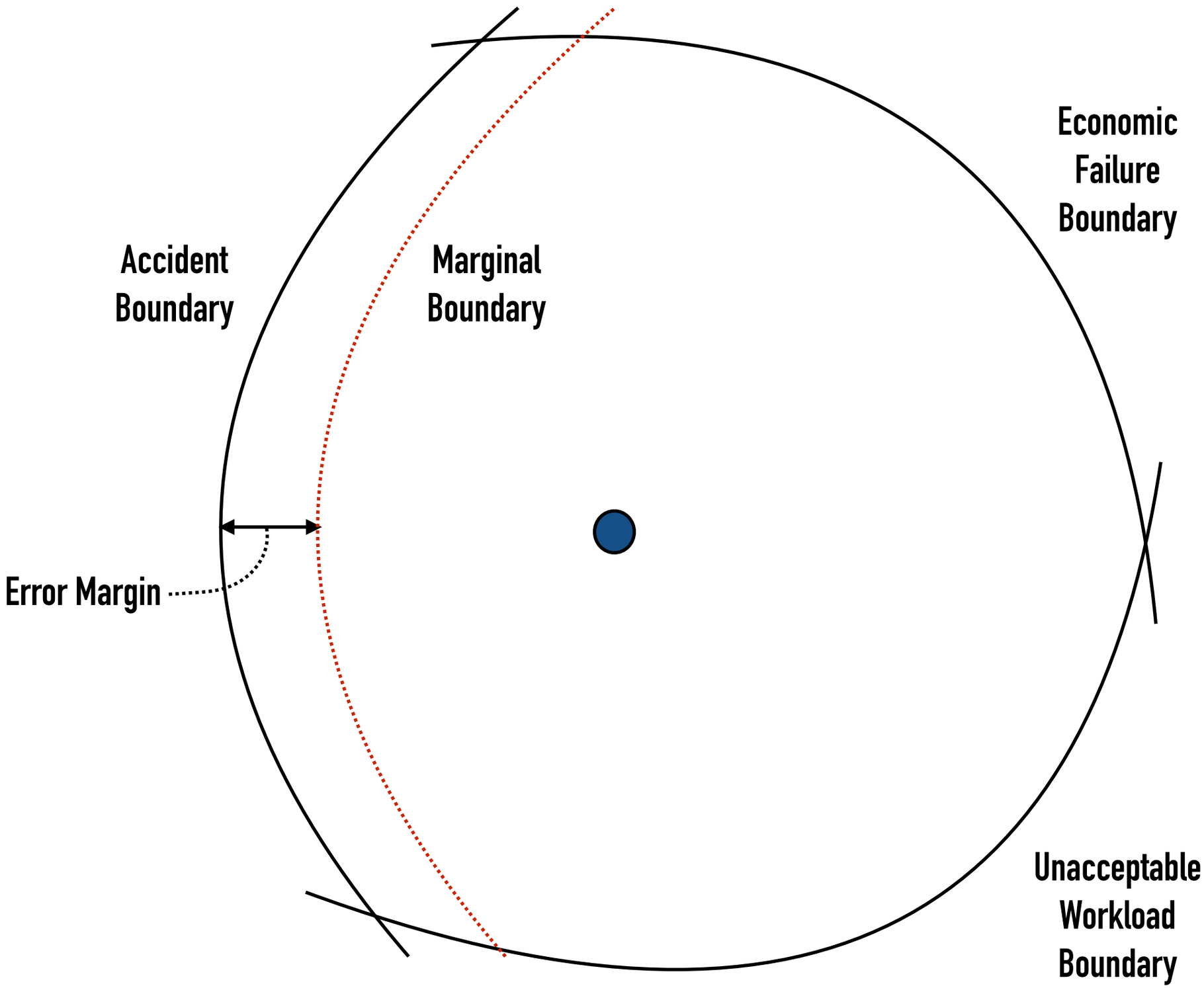
"Going solid": a model of system dynamics and consequences for patient safety - R Cook, J Rasmussen
Resilience in complex adaptive systems: Operating at the Edge of Failure - Richard Cook - Talk at Velocity NY 2013

Operating at the Edge of Failure



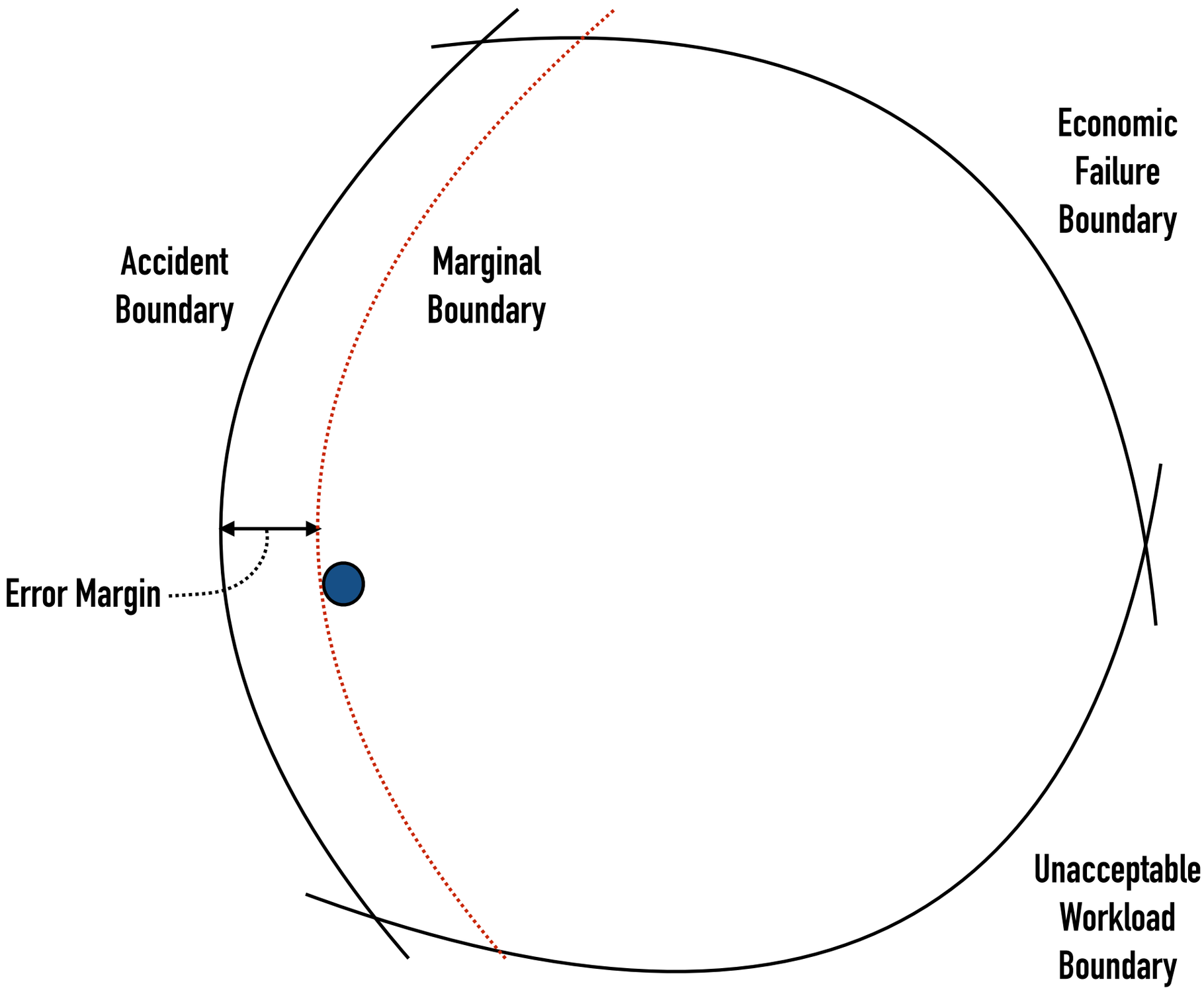
"Going solid": a model of system dynamics and consequences for patient safety - R Cook, J Rasmussen
Resilience in complex adaptive systems: Operating at the Edge of Failure - Richard Cook - Talk at Velocity NY 2013

Operating at the Edge of Failure



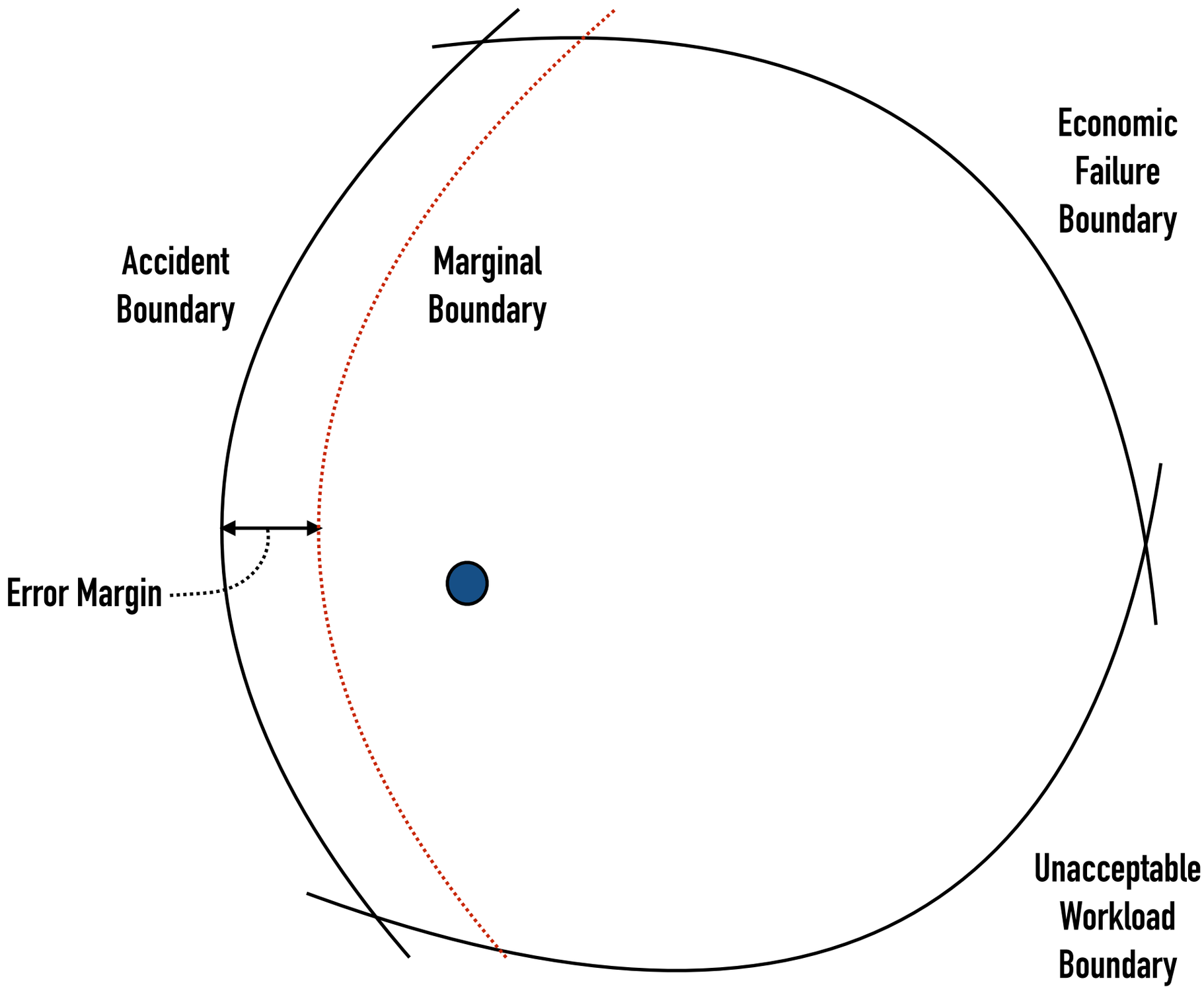
"Going solid": a model of system dynamics and consequences for patient safety - R Cook, J Rasmussen
Resilience in complex adaptive systems: Operating at the Edge of Failure - Richard Cook - Talk at Velocity NY 2013

Operating at the Edge of Failure



"Going solid": a model of system dynamics and consequences for patient safety - R Cook, J Rasmussen
Resilience in complex adaptive systems: Operating at the Edge of Failure - Richard Cook - Talk at Velocity NY 2013

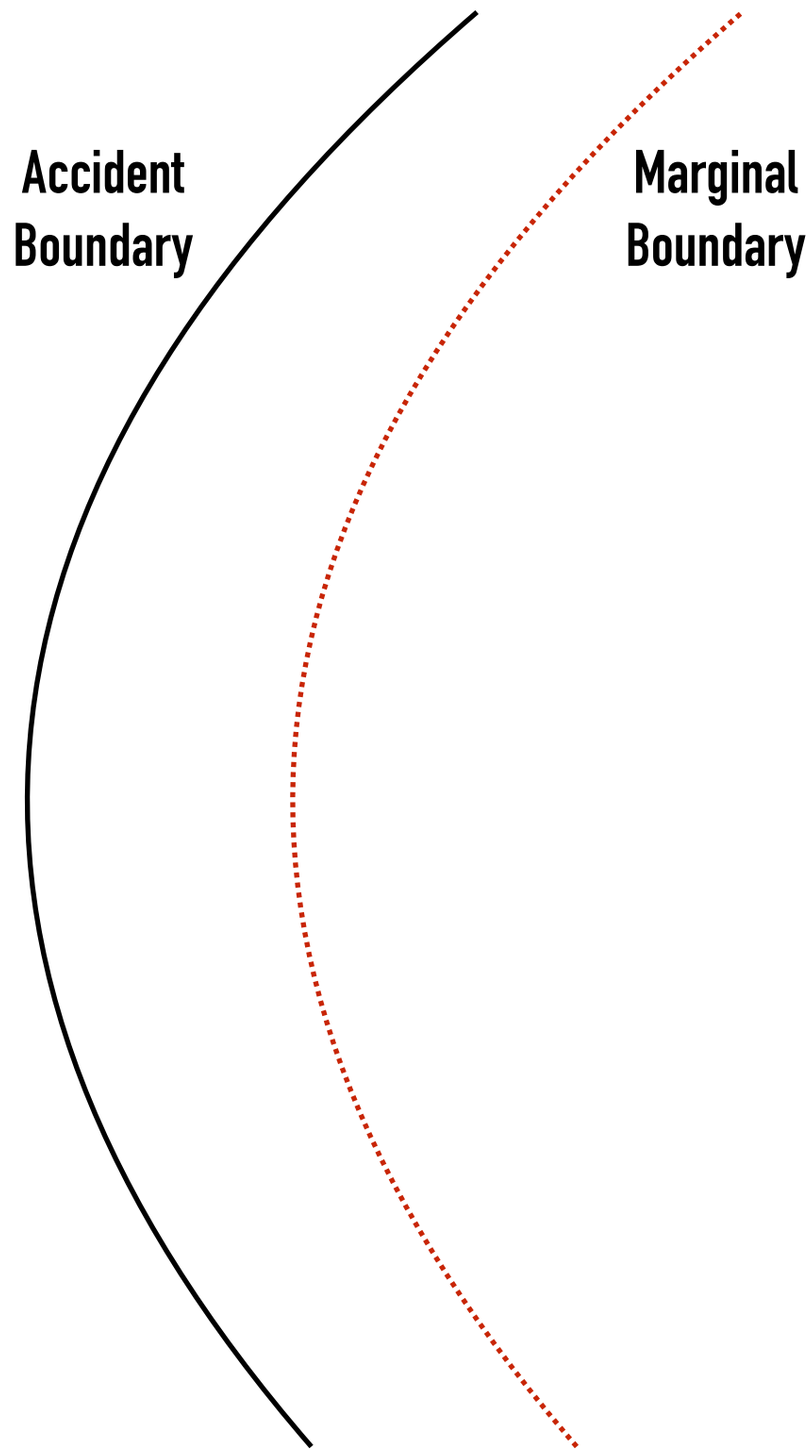
Operating at the Edge of Failure



"Going solid": a model of system dynamics and consequences for patient safety - R Cook, J Rasmussen

Resilience in complex adaptive systems: Operating at the Edge of Failure - Richard Cook - Talk at Velocity NY 2013

Operating at the Edge of Failure

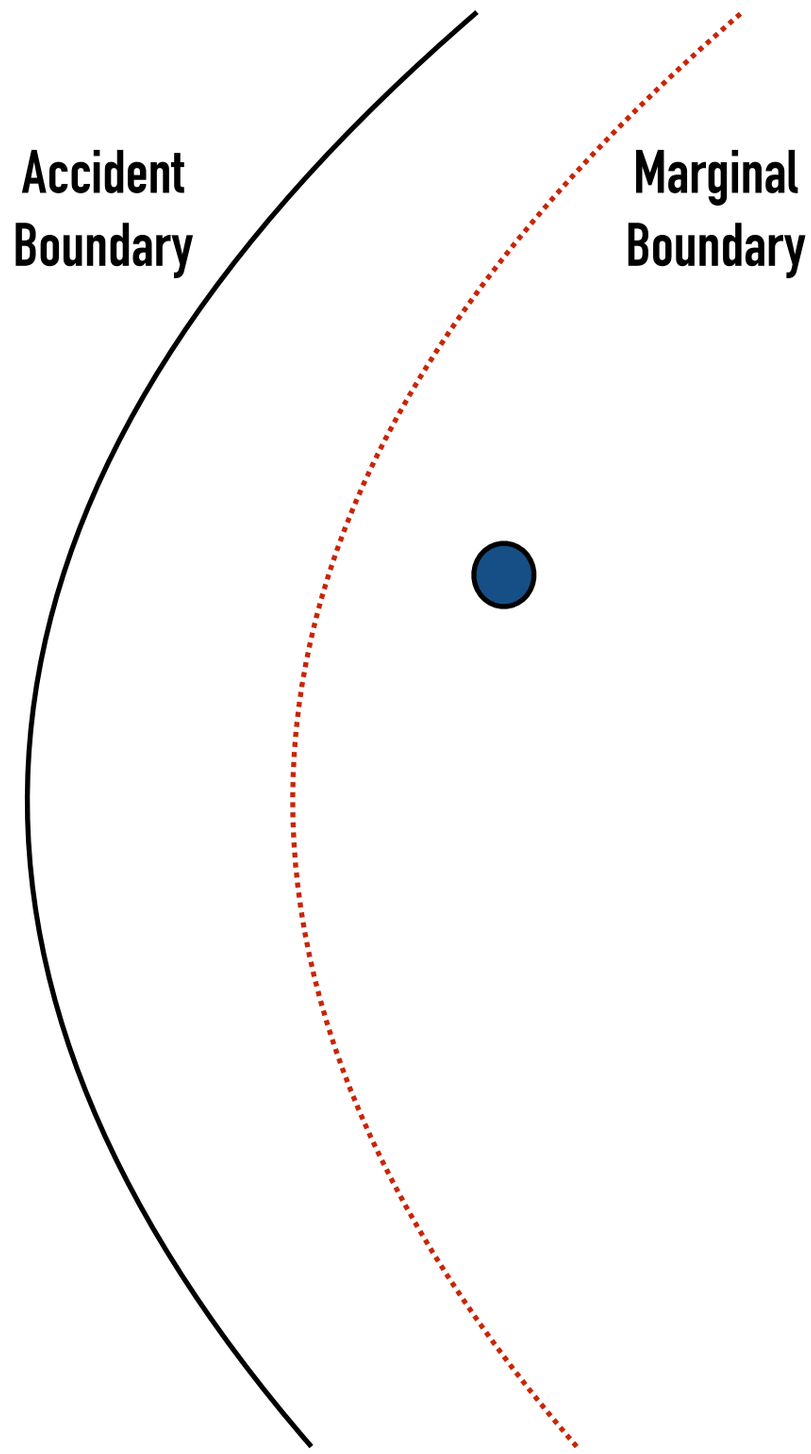


"Going solid": a model of system dynamics and consequences for patient safety - R Cook, J Rasmussen
Resilience in complex adaptive systems: Operating at the Edge of Failure - Richard Cook - Talk at Velocity NY 2013

Operating at the Edge of Failure

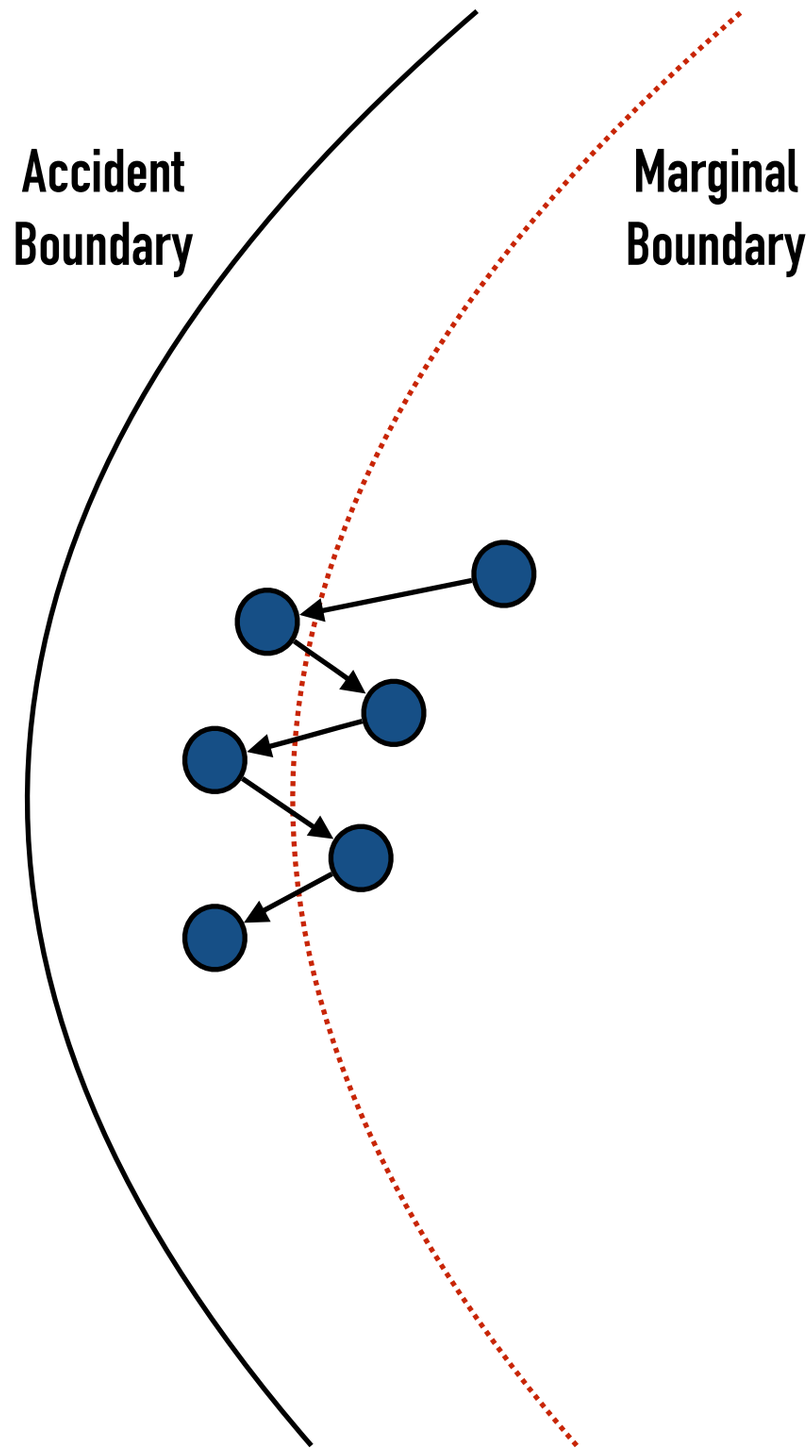
"Going solid": a model of system dynamics and consequences for patient safety - R Cook, J Rasmussen
Resilience in complex adaptive systems: Operating at the Edge of Failure - Richard Cook - Talk at Velocity NY 2013

Operating at the Edge of Failure



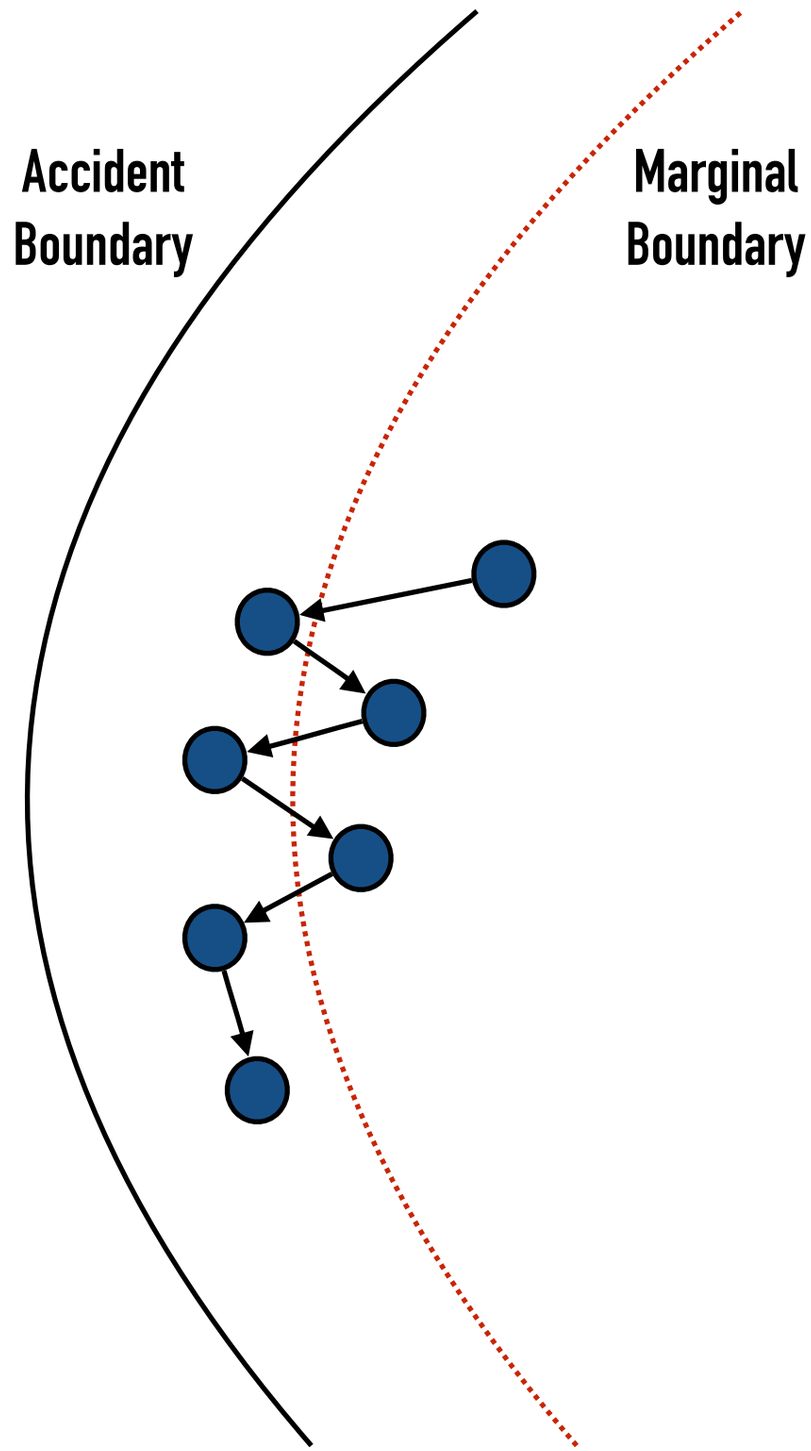
"Going solid": a model of system dynamics and consequences for patient safety - R Cook, J Rasmussen
Resilience in complex adaptive systems: Operating at the Edge of Failure - Richard Cook - Talk at Velocity NY 2013

Operating at the Edge of Failure



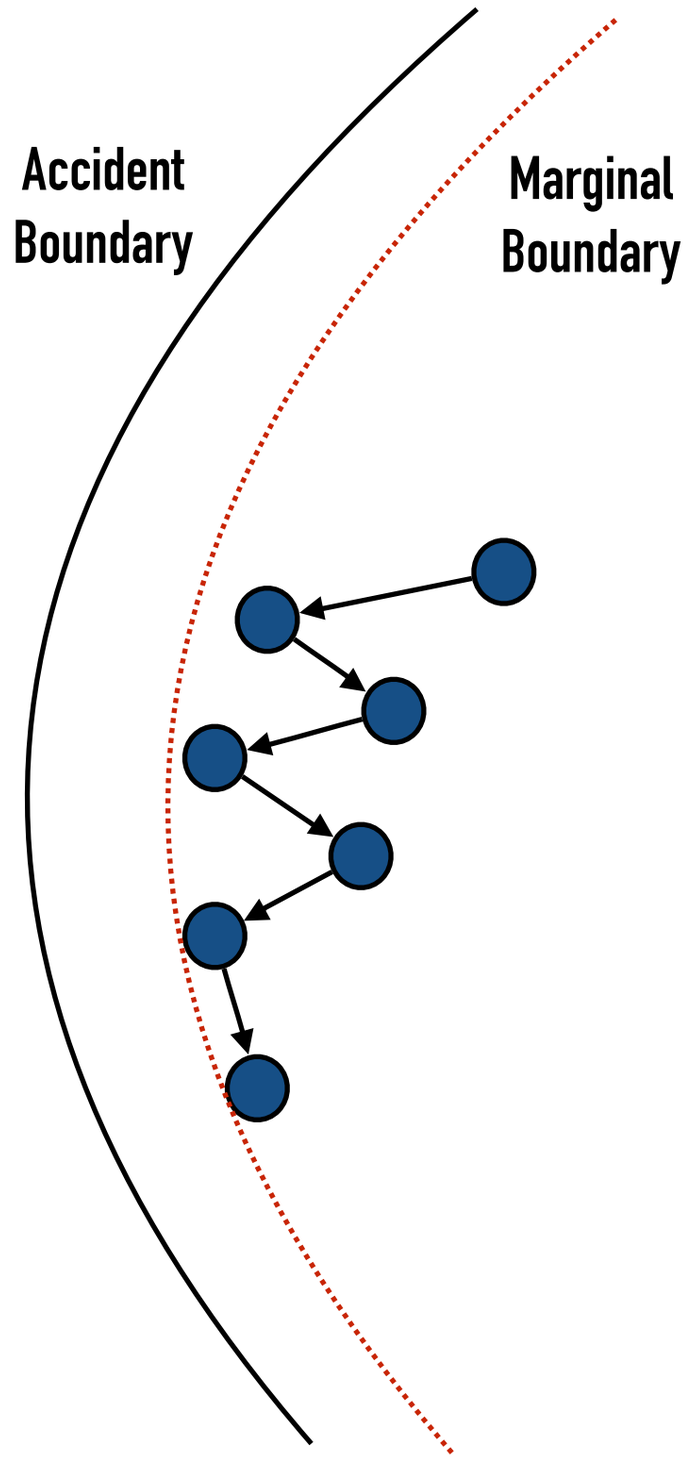
"Going solid": a model of system dynamics and consequences for patient safety - R Cook, J Rasmussen
Resilience in complex adaptive systems: Operating at the Edge of Failure - Richard Cook - Talk at Velocity NY 2013

Operating at the Edge of Failure



"Going solid": a model of system dynamics and consequences for patient safety - R Cook, J Rasmussen
Resilience in complex adaptive systems: Operating at the Edge of Failure - Richard Cook - Talk at Velocity NY 2013

Operating at the Edge of Failure



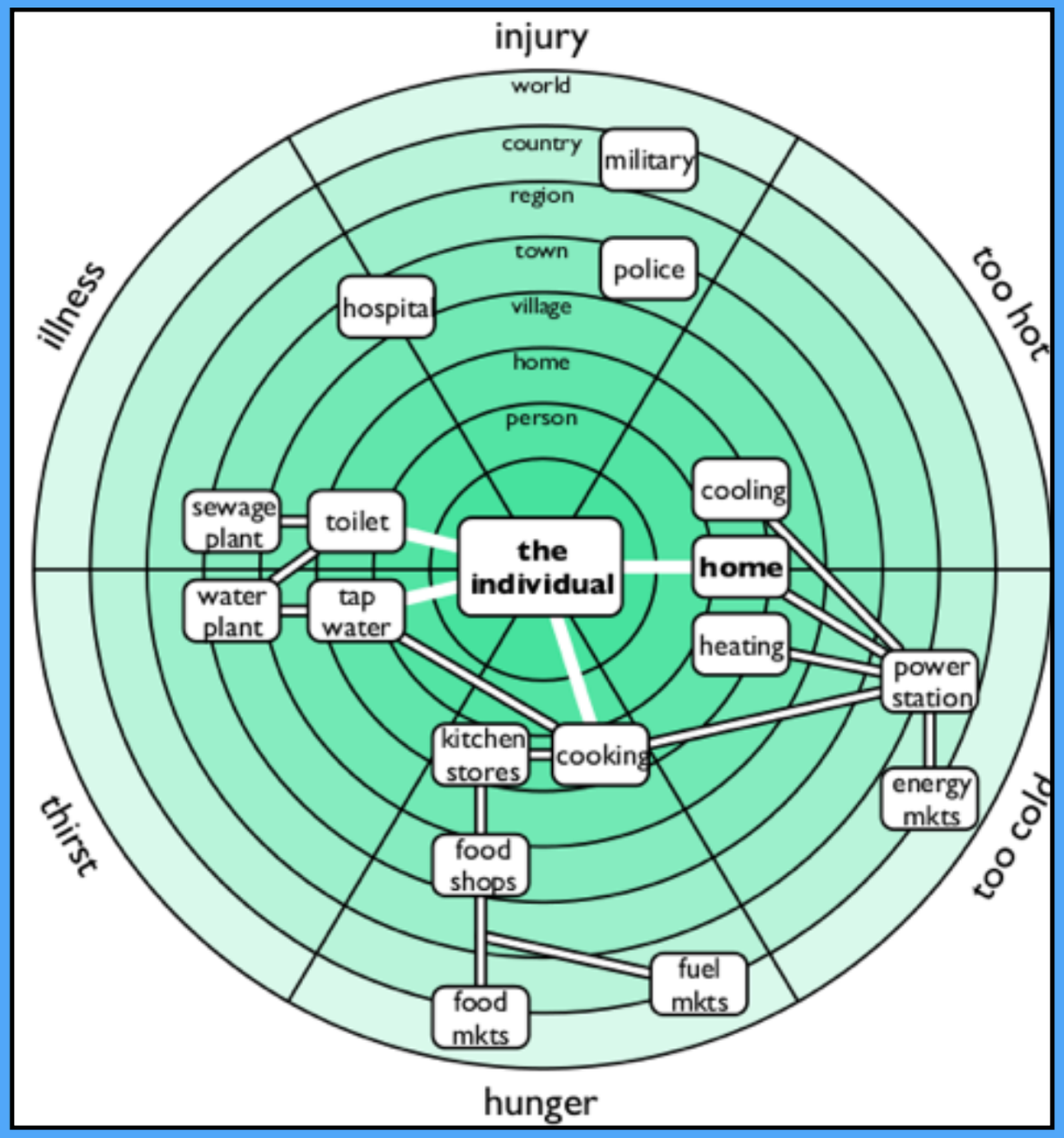
"Going solid": a model of system dynamics and consequences for patient safety - R Cook, J Rasmussen
Resilience in complex adaptive systems: Operating at the Edge of Failure - Richard Cook - Talk at Velocity NY 2013

Embrace Failure

Resilience in Social Systems

Dealing in Security

UNDERSTANDING VITAL SERVICES, AND HOW THEY KEEP YOU SAFE



1 INDIVIDUAL

6 WAYS TO DIE

3 SETS OF ESSENTIAL SERVICES

7 LAYERS OF PROTECTION

7 Principles for Building Resilience in Social Systems

1. MAINTAIN DIVERSITY & REDUNDANCY
2. MANAGE CONNECTIVITY
3. MANAGE SLOW VARIABLES & FEEDBACK
4. FOSTER COMPLEX ADAPTIVE SYSTEMS THINKING
5. ENCOURAGE LEARNING
6. BROADEN PARTICIPATION
7. PROMOTE POLYCENTRIC GOVERNANCE

Applying resilience thinking: Seven principles for building resilience in social-ecological systems - Reinette Biggs et. al.

Resilience in Biological Systems

Meerkats

Puppies! Now that I've got your attention, complexity theory - Nicolas Perony, TED talk

What We Can Learn From Biological Systems

1. FEATURE DIVERSITY AND REDUNDANCY
2. INTER-CONNECTED NETWORK STRUCTURE
3. WIDE DISTRIBUTION ACROSS ALL SCALES
4. CAPACITY TO SELF-ADAPT & SELF-ORGANIZE

"Animals show extraordinary social complexity, and this allows them to adapt and respond to changes in their environment. In three words, in the animal kingdom, simplicity leads to complexity which leads to resilience."

- NICOLAS PERONY

Puppies! Now that I've got your attention, complexity theory - Nicolas Perony, TED talk

Resilience in Computer Systems


Our Disaster Recovery Plan
Goes Something Like This...
HELP!
HELP!
DILBERT
By Scott Adams

“Complex systems run in degraded mode.”

“Complex systems run as broken systems.”

- RICHARD COOK

How Complex Systems Fail - Richard Cook

Resilience is by Design

Photo courtesy of FEMA/Joselyne Augustino

We Need to Manage Failure

“Post-accident attribution to a ‘root cause’ is fundamentally wrong: Because overt failure requires multiple faults, there is no isolated ‘cause’ of an accident.”

- RICHARD COOK

How Complex Systems Fail - Richard Cook

There is No Root Cause

Crash Only Software

STOP = CRASH SAFELY

START = RECOVER FAST

Crash-Only Software - George Candea, Armando Fox

Recursive Restartability

TURNING THE CRASH-ONLY SLEDGEHAMMER INTO A SCALPEL

Recursive Restartability: Turning the Reboot Sledgehammer into a Scalpel - George Candea, Armando Fox

Services need to accept NO for an answer

Classification of State

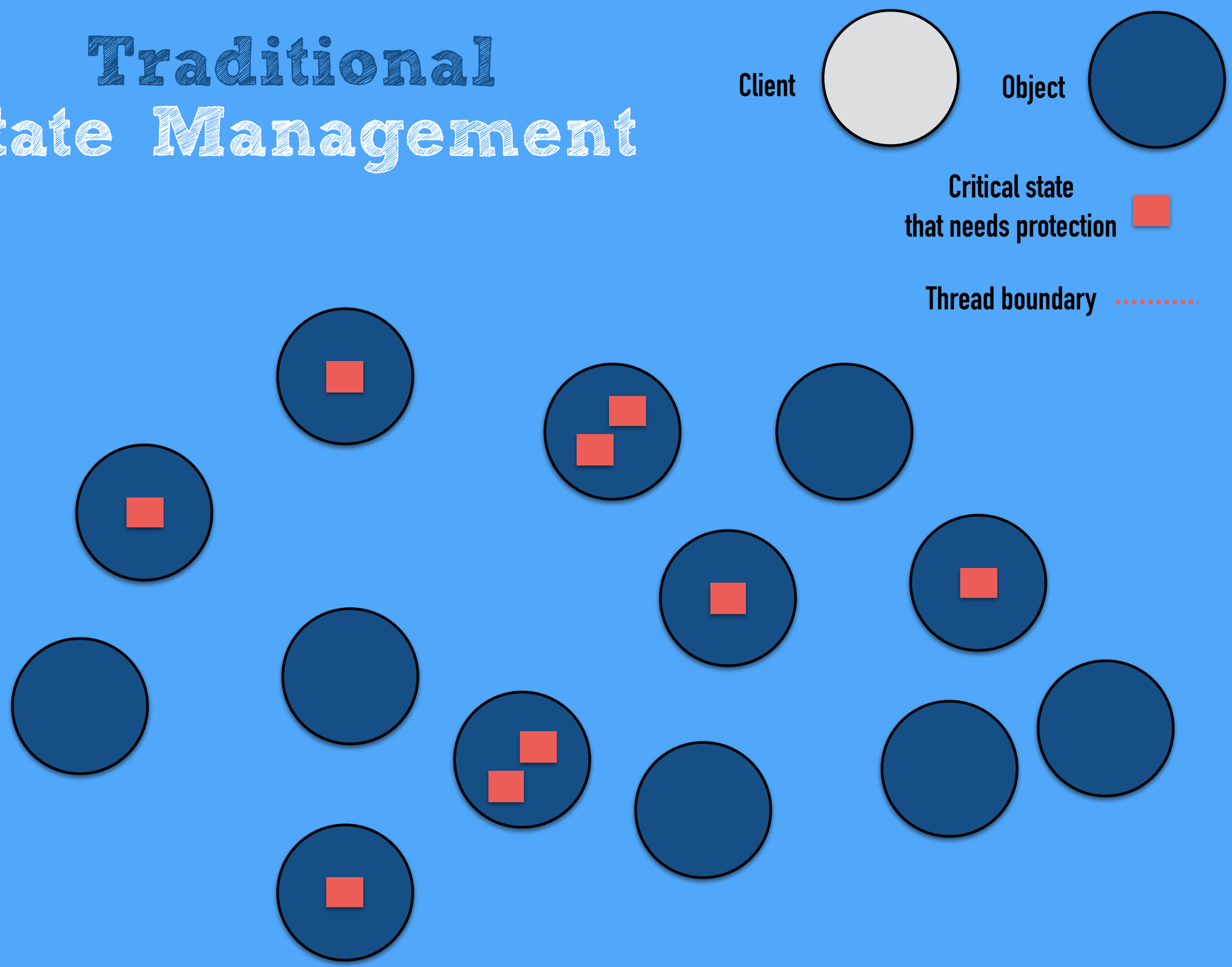
- STATIC DATA
- SCRATCH DATA
- DYNAMIC DATA
  - RECOMPUTABLE
  - NOT RECOMPUTABLE

Classification of State

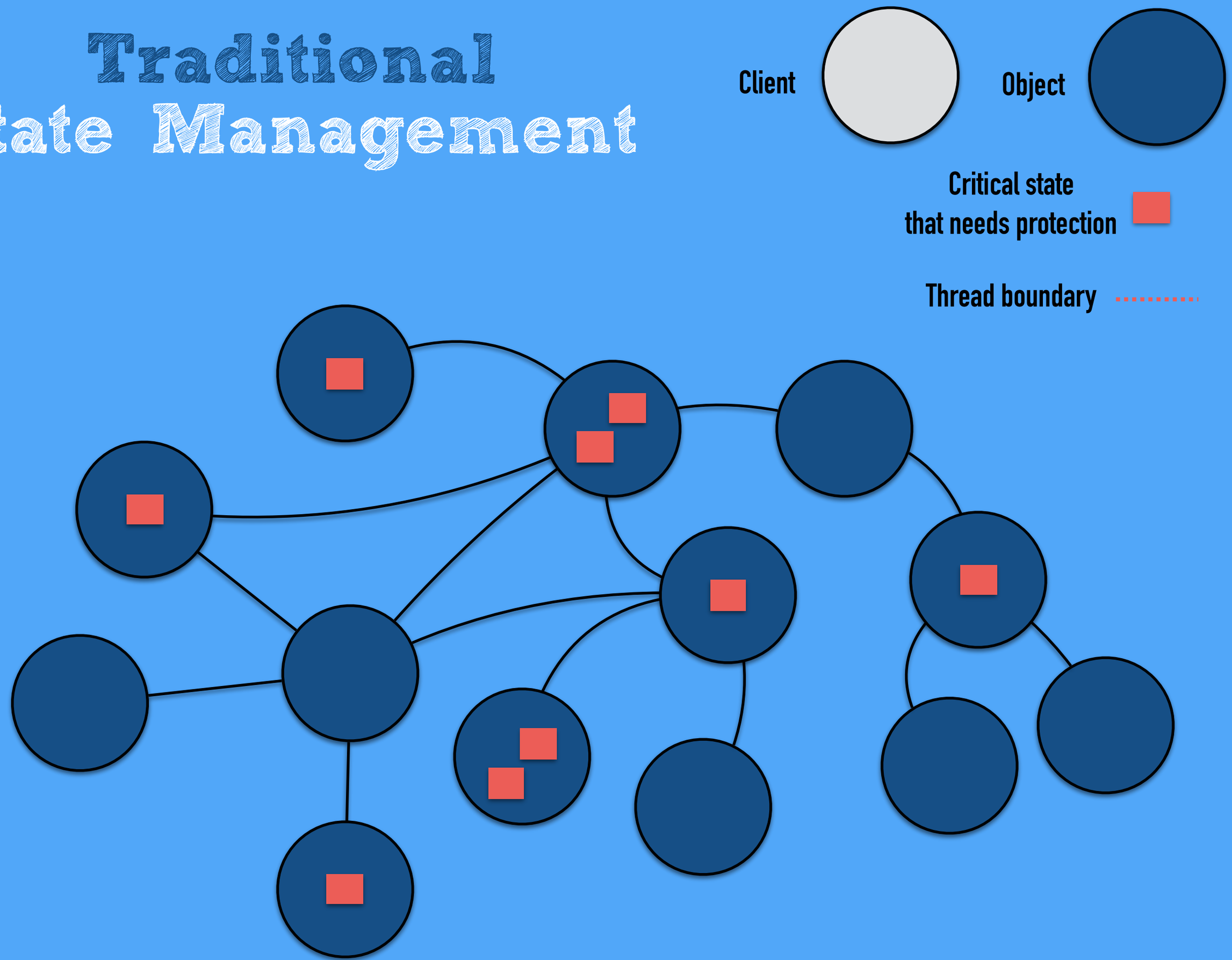
- STATIC DATA
- SCRATCH DATA
- DYNAMIC DATA
  - RECOMPUTABLE
  - NOT RECOMPUTABLE

Critical

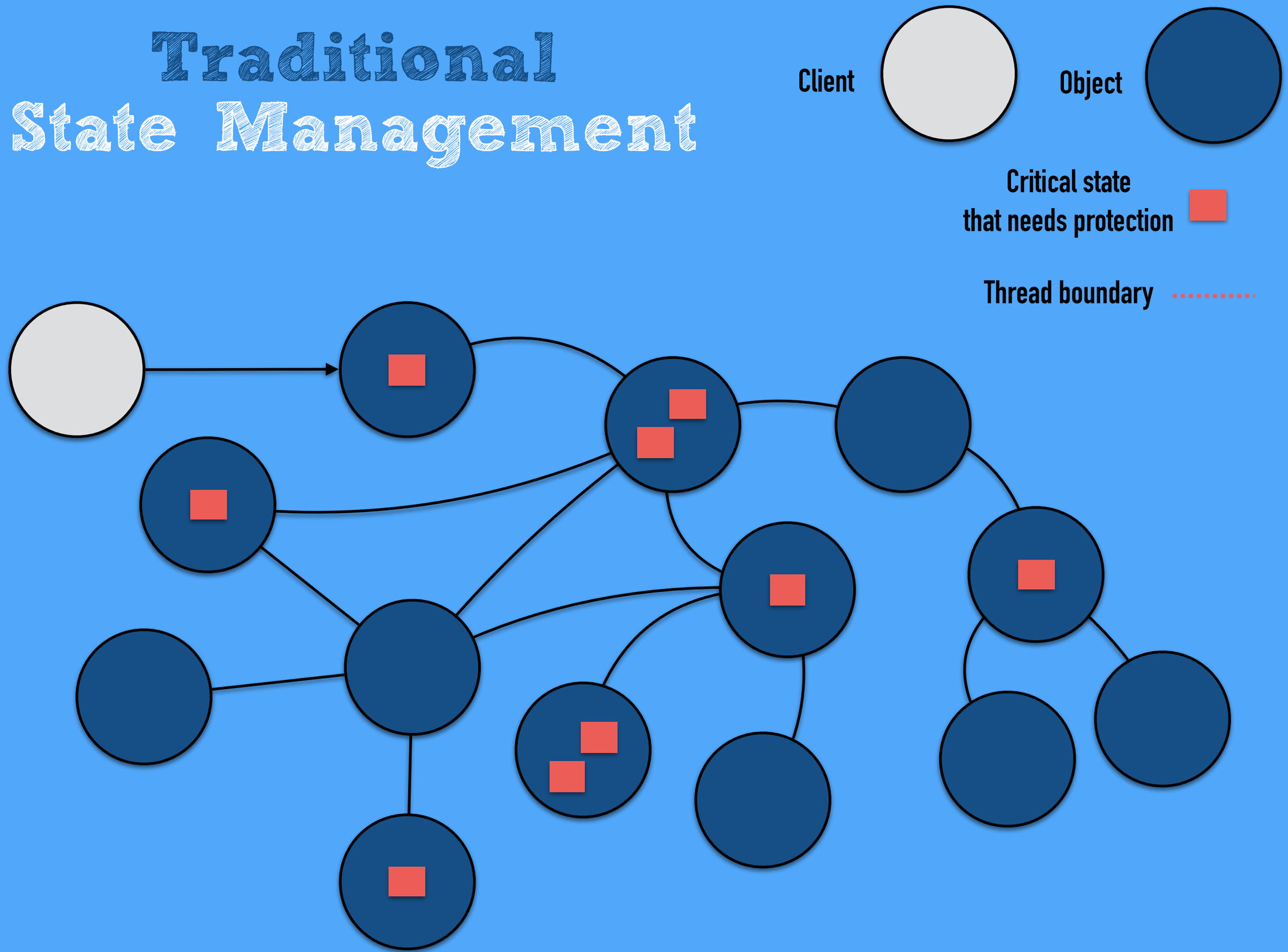
Traditional State Management



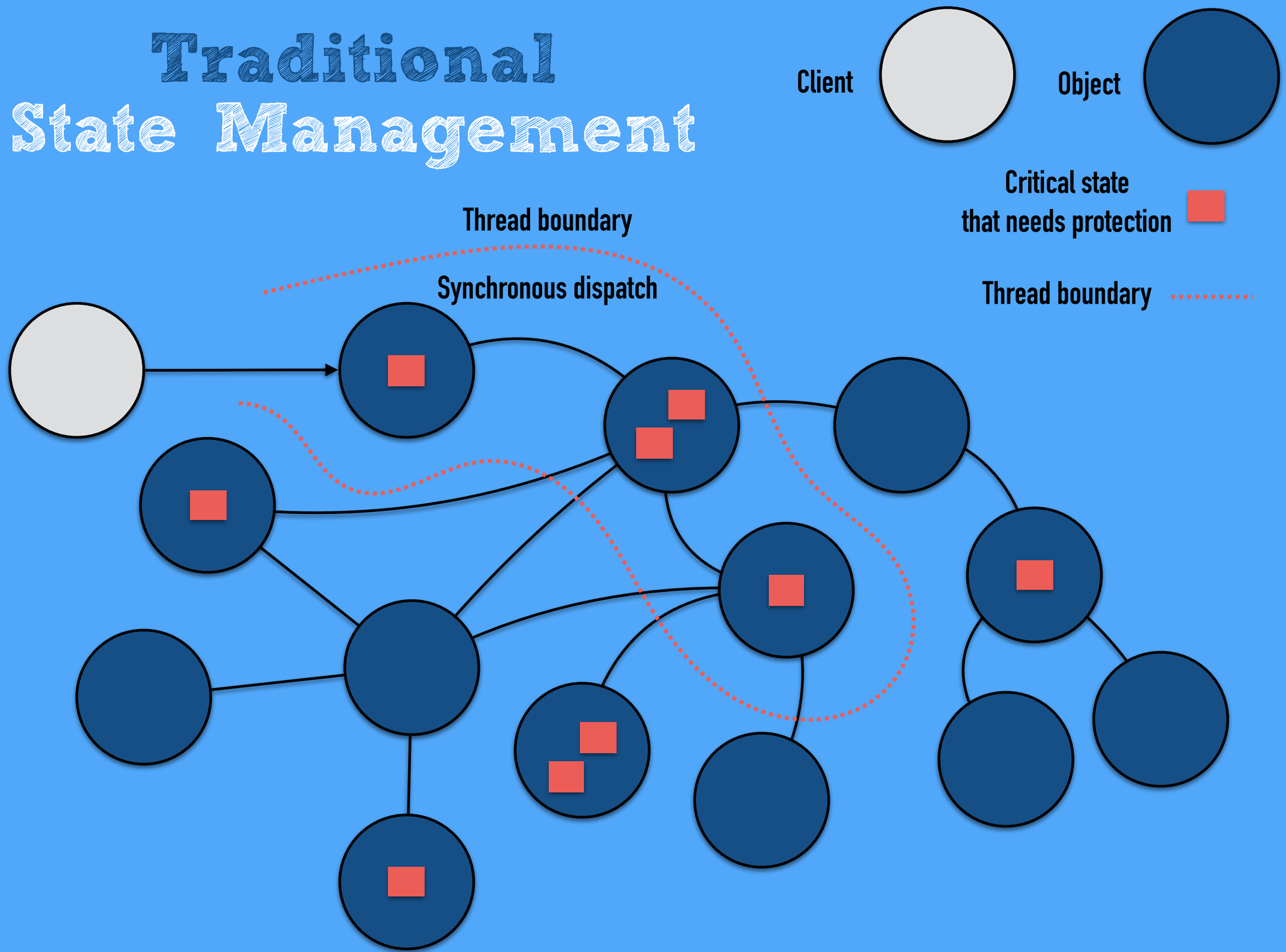
Traditional State Management



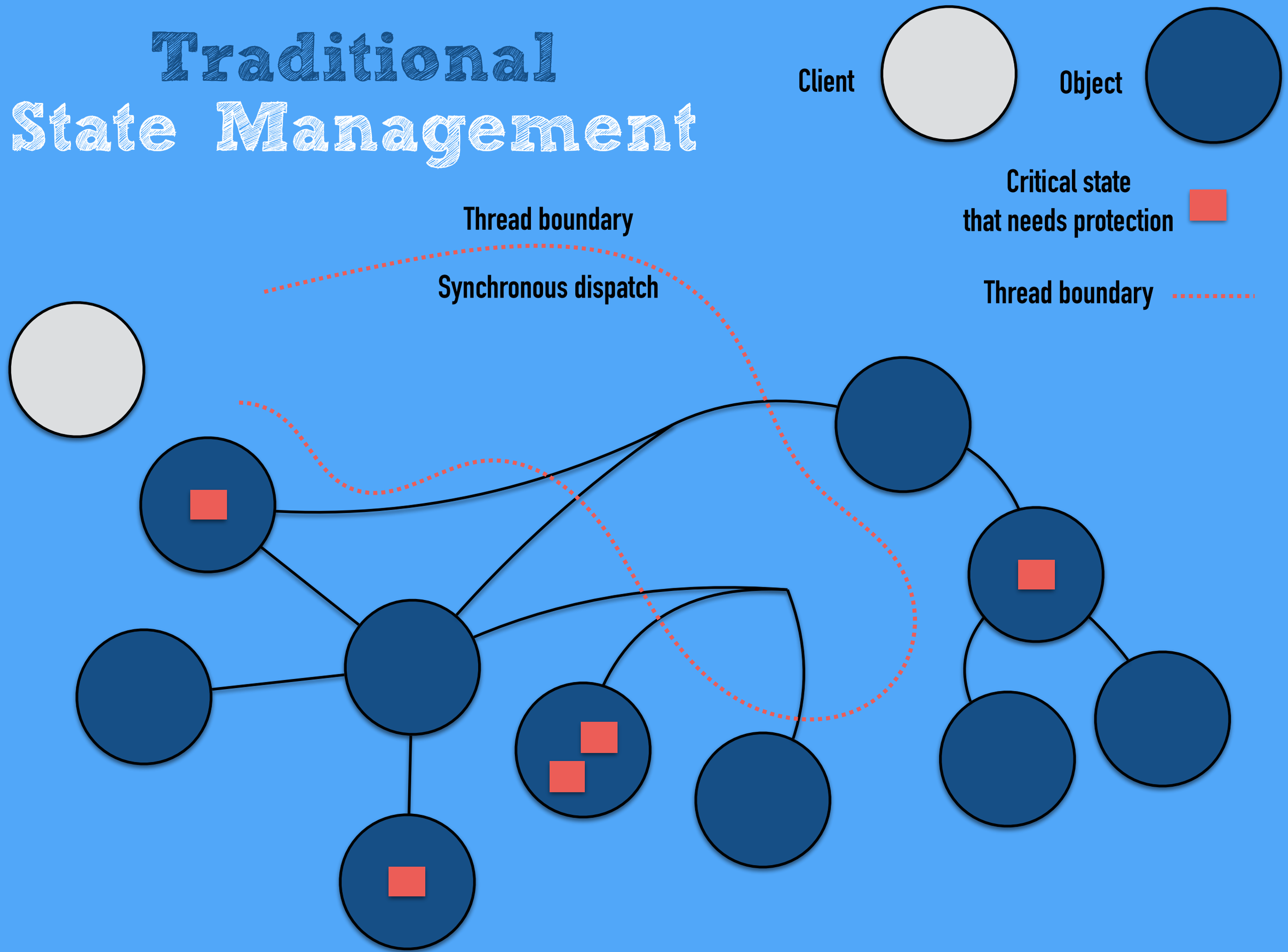
Traditional State Management



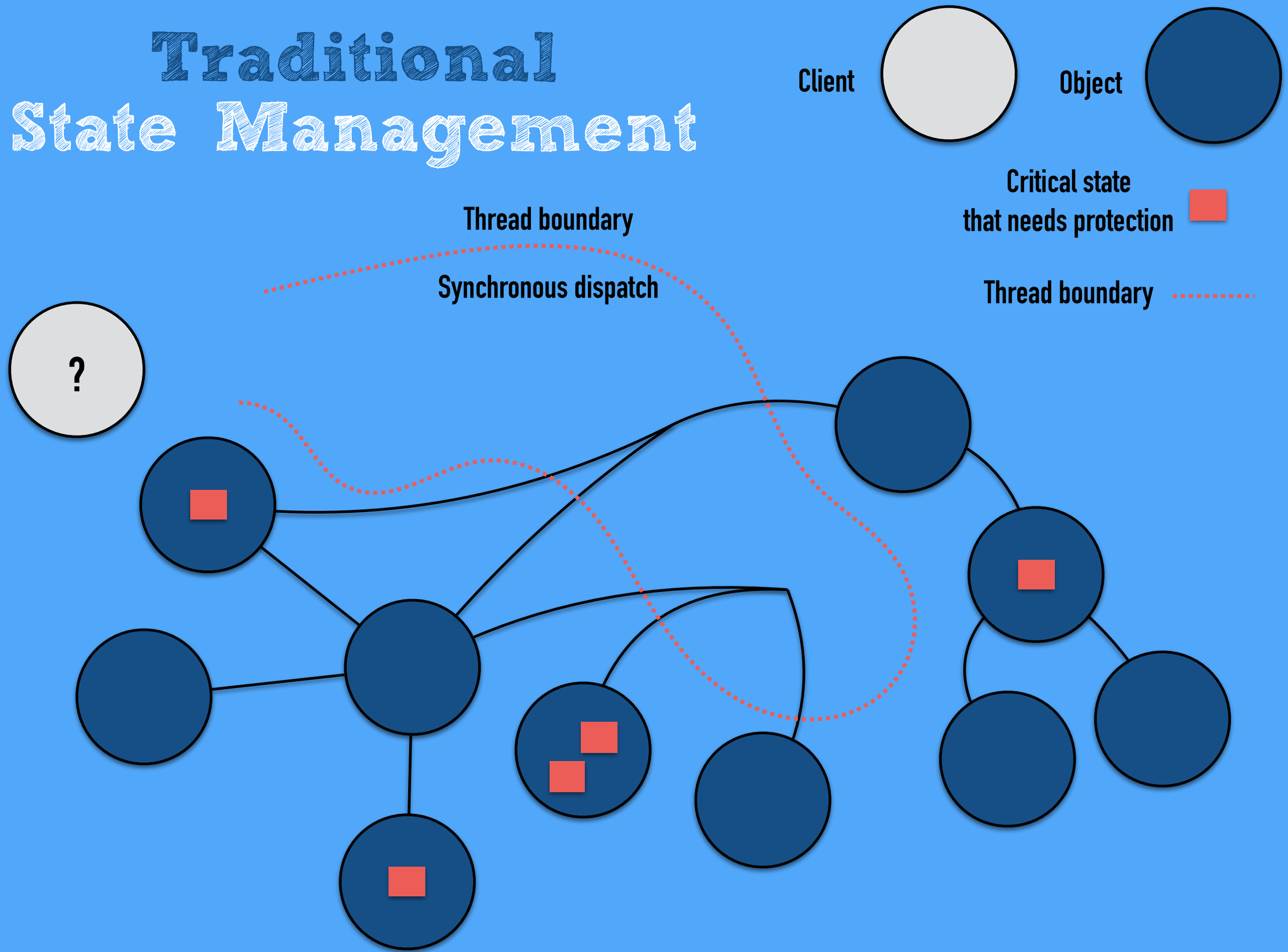
Traditional State Management



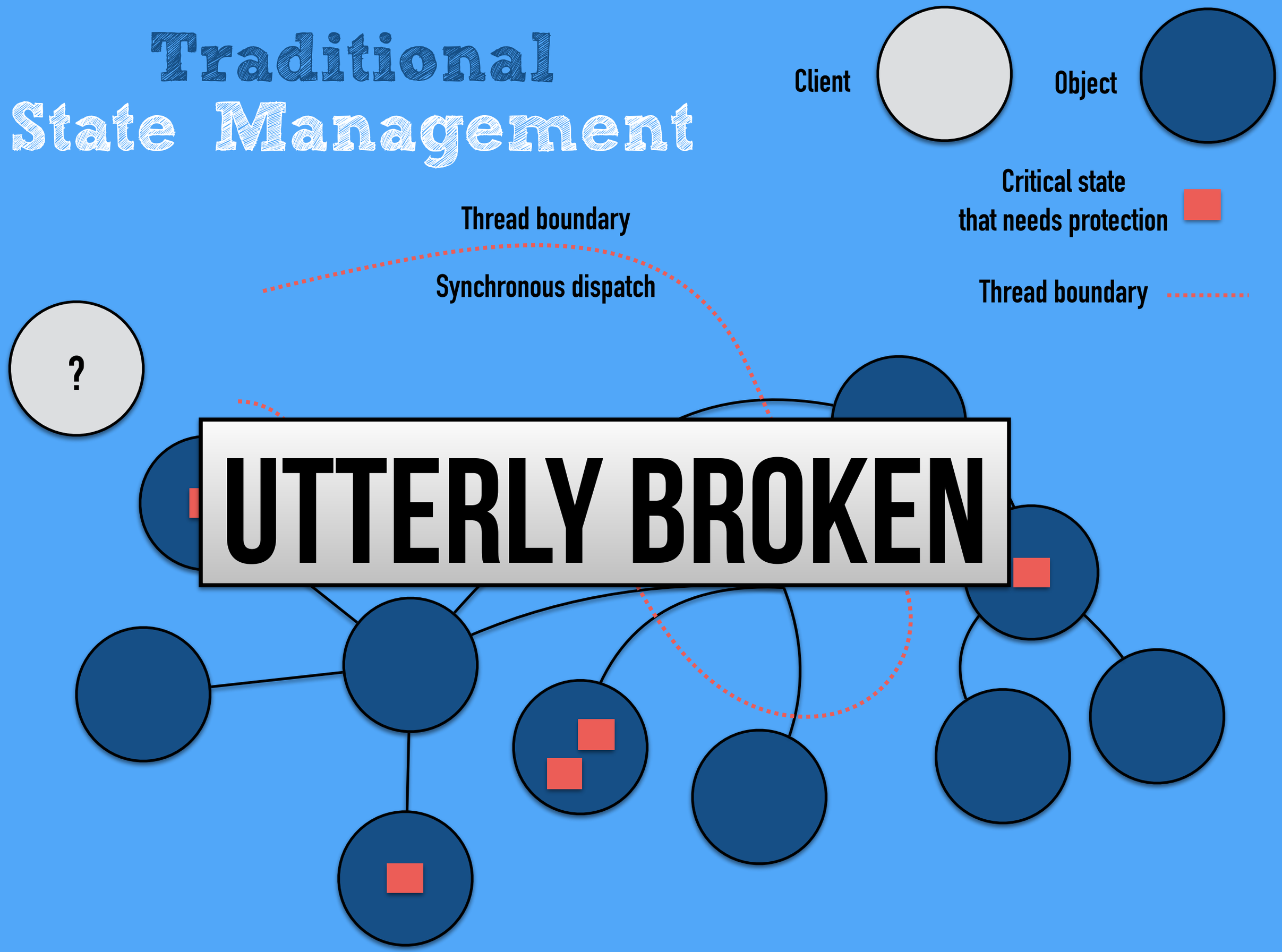
Traditional State Management



Traditional State Management



Traditional State Management



“Accidents come from relationships not broken parts.”

- SIDNEY DEKKER

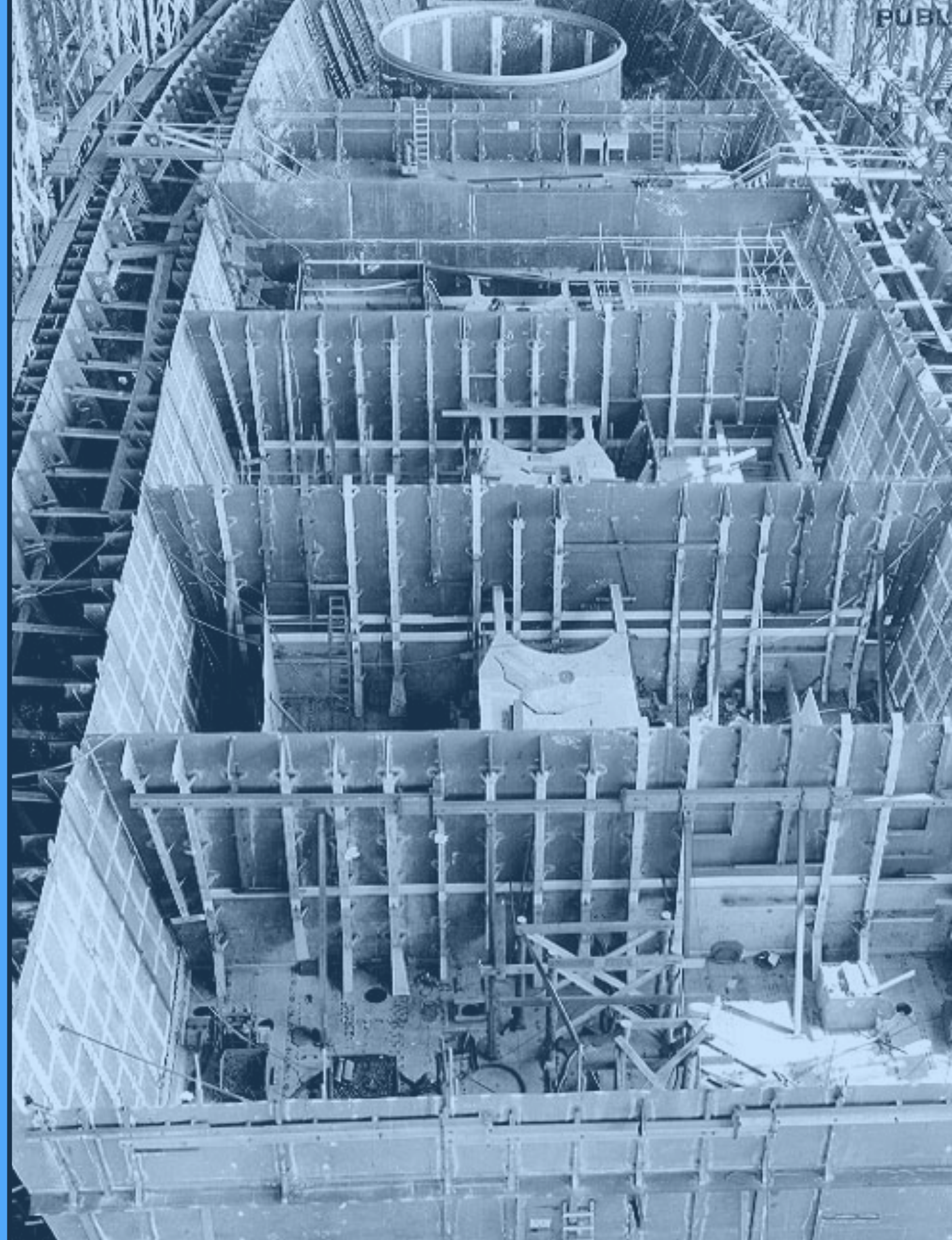
Drift into Failure - Sidney Dekker

Requirements for a Sane Failure Mode

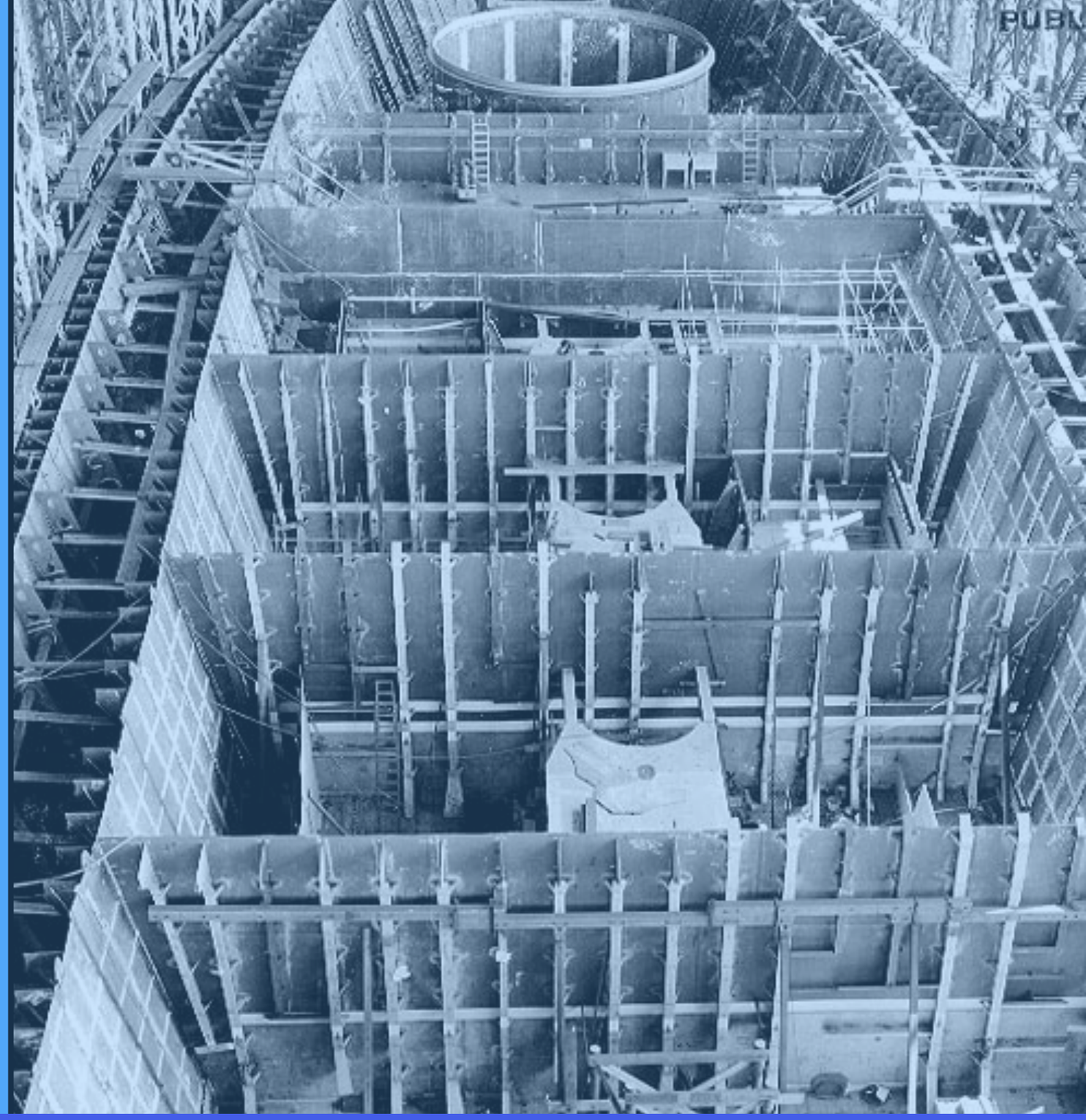
FAILURES NEED TO BE

1. CONTAINED
2. REIFIED—AS MESSAGES
3. SIGNALLED—ASYNCHRONOUSLY
4. OBSERVED—BY 1-N
5. MANAGED

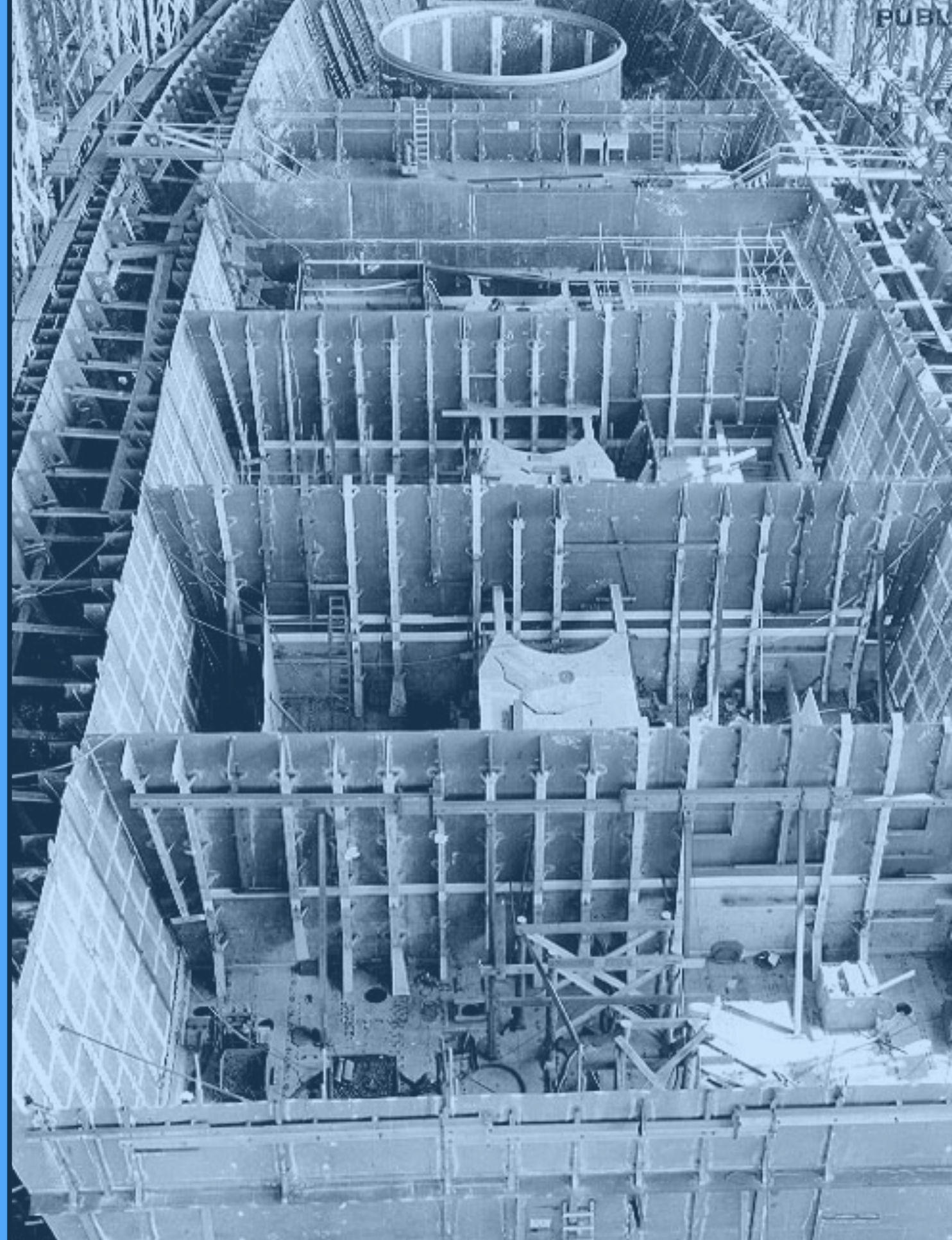
Bulkhead Pattern



Bulkhead Pattern

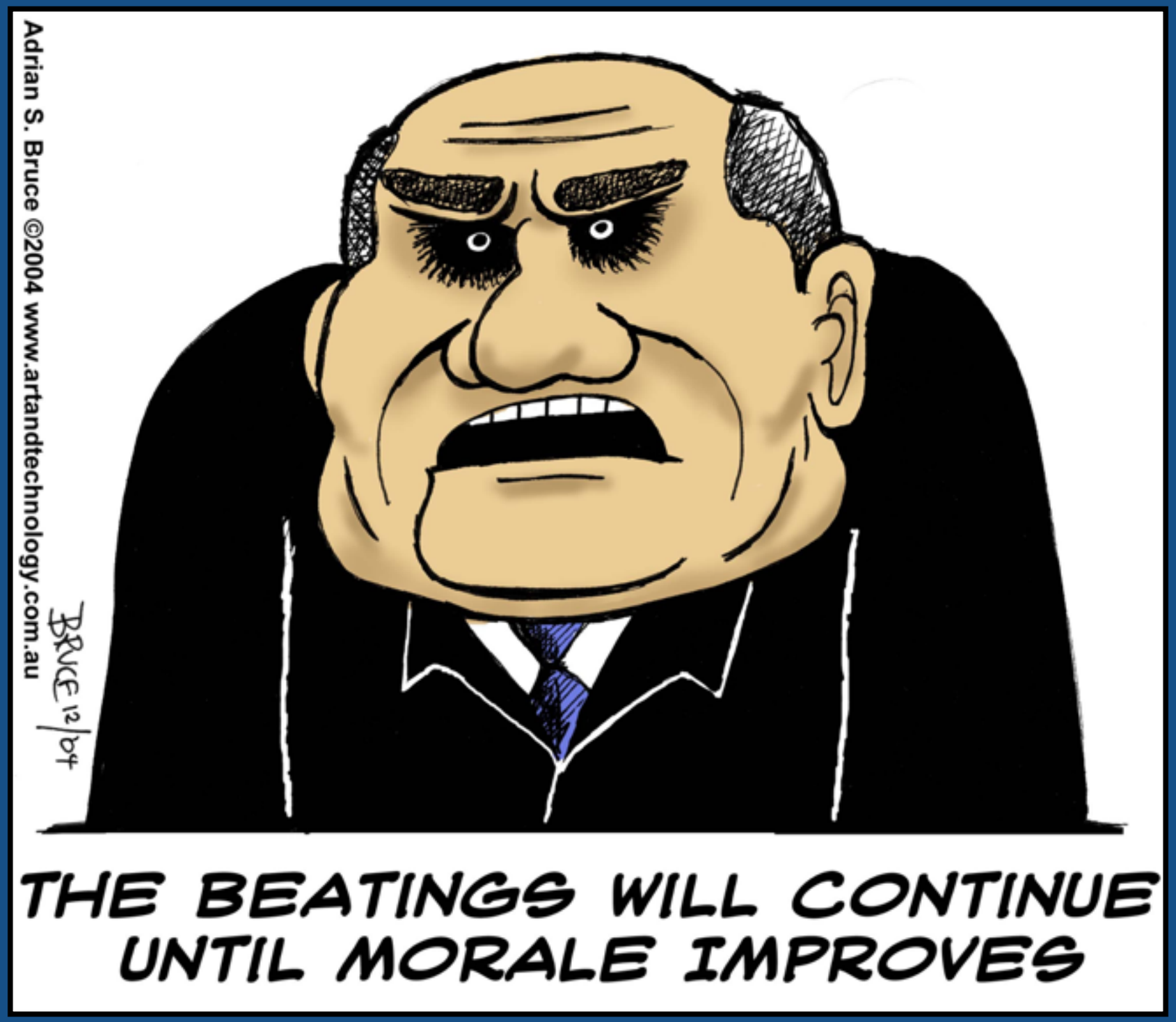


Bulkhead Pattern



Enter Supervision

Enter Supervision



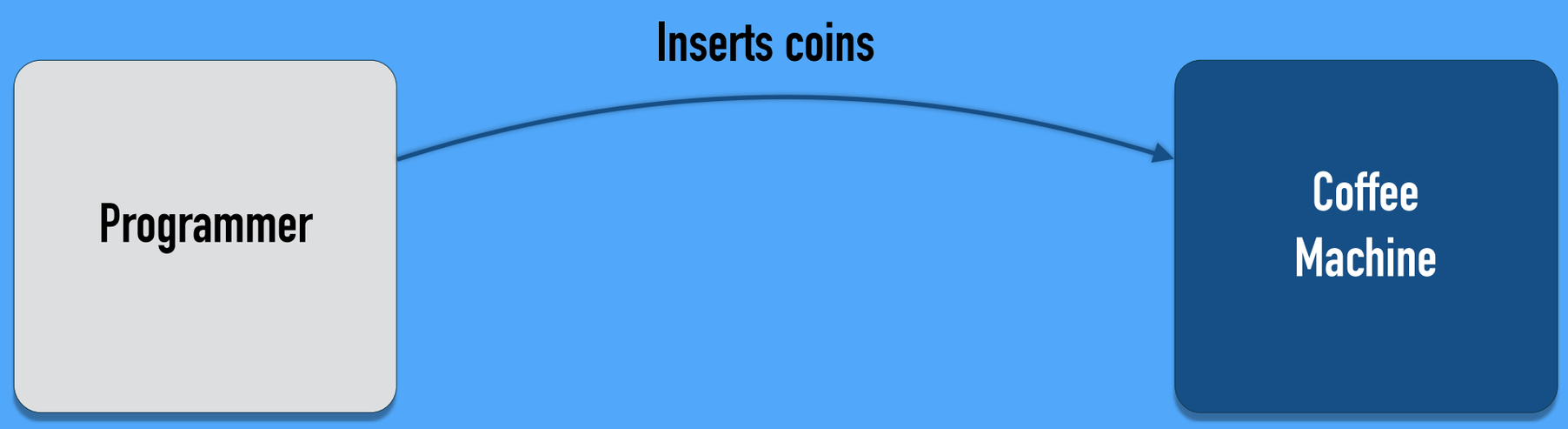
The Vending Machine Pattern

Think Vending Machine

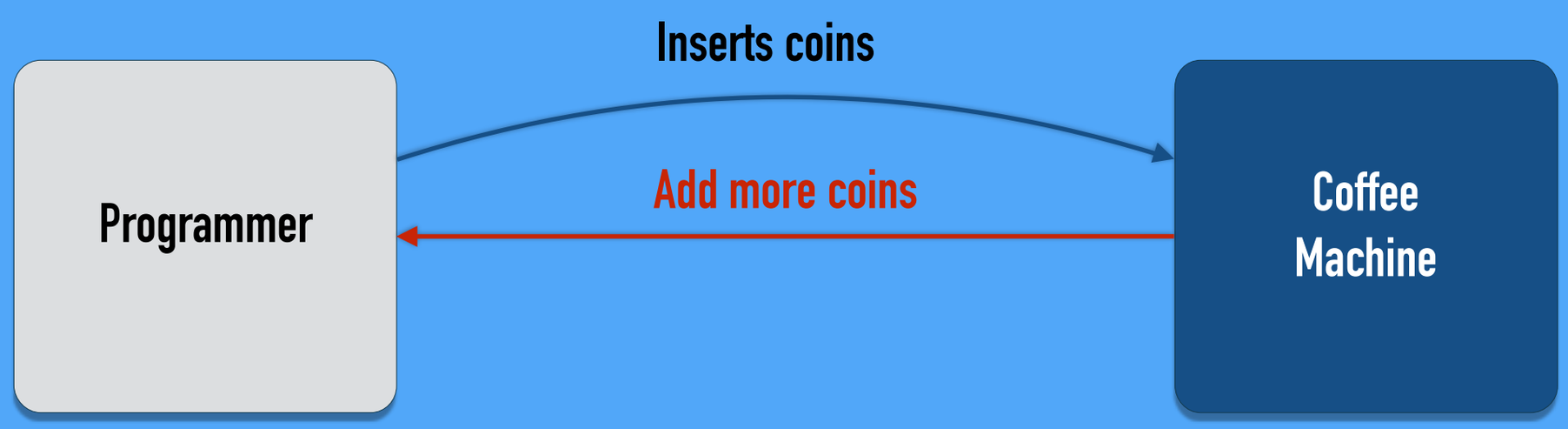
Programmer

Coffee
Machine

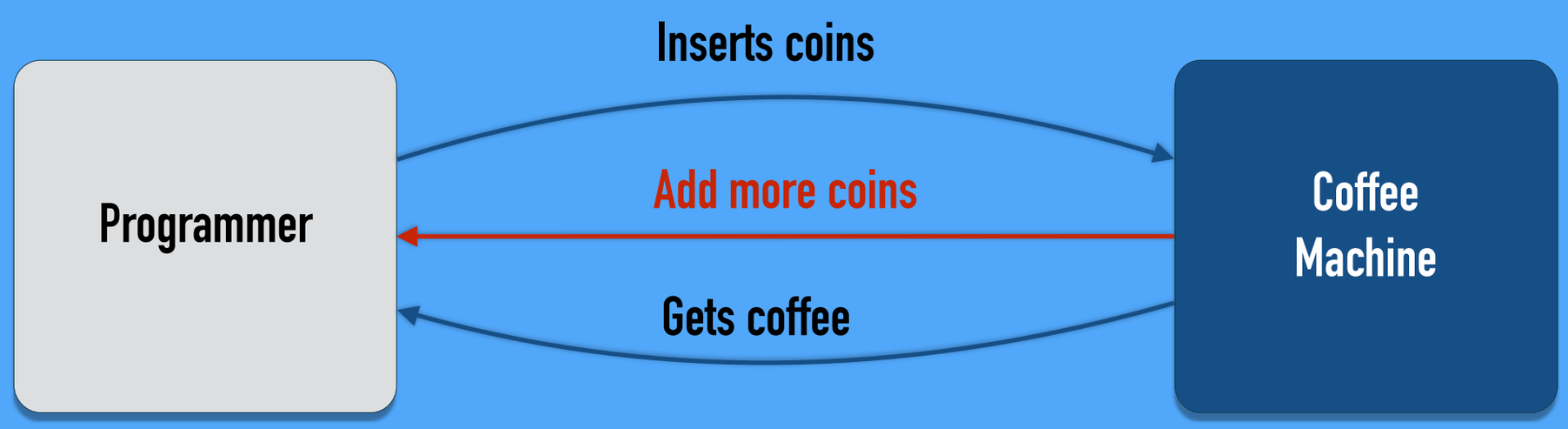
Think Vending Machine



Think Vending Machine



Think Vending Machine

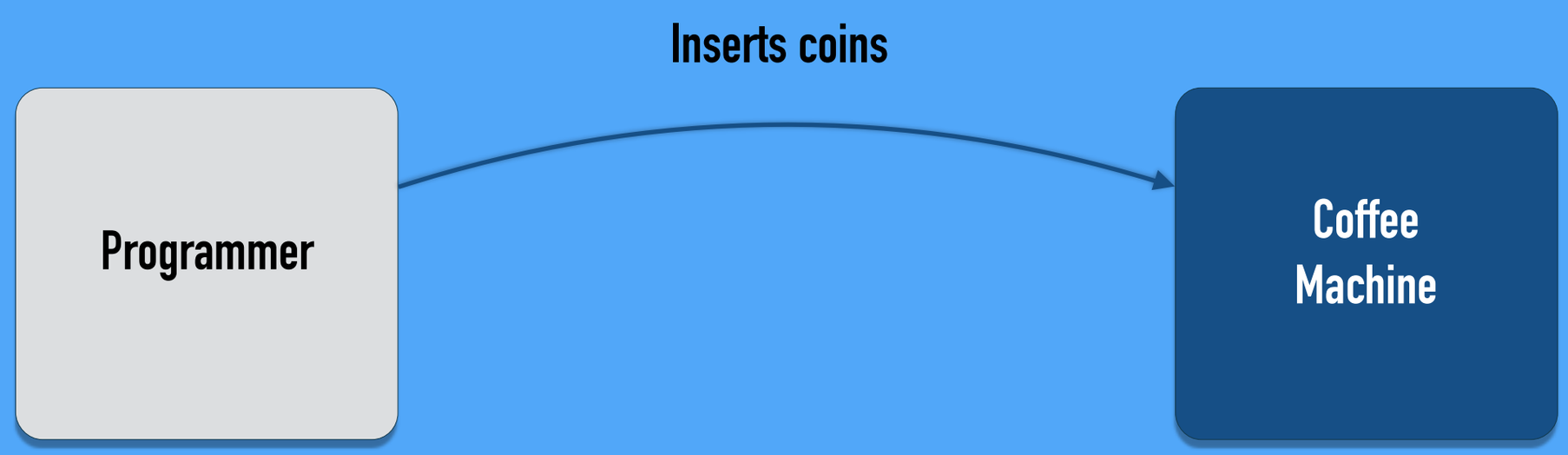


Think Vending Machine

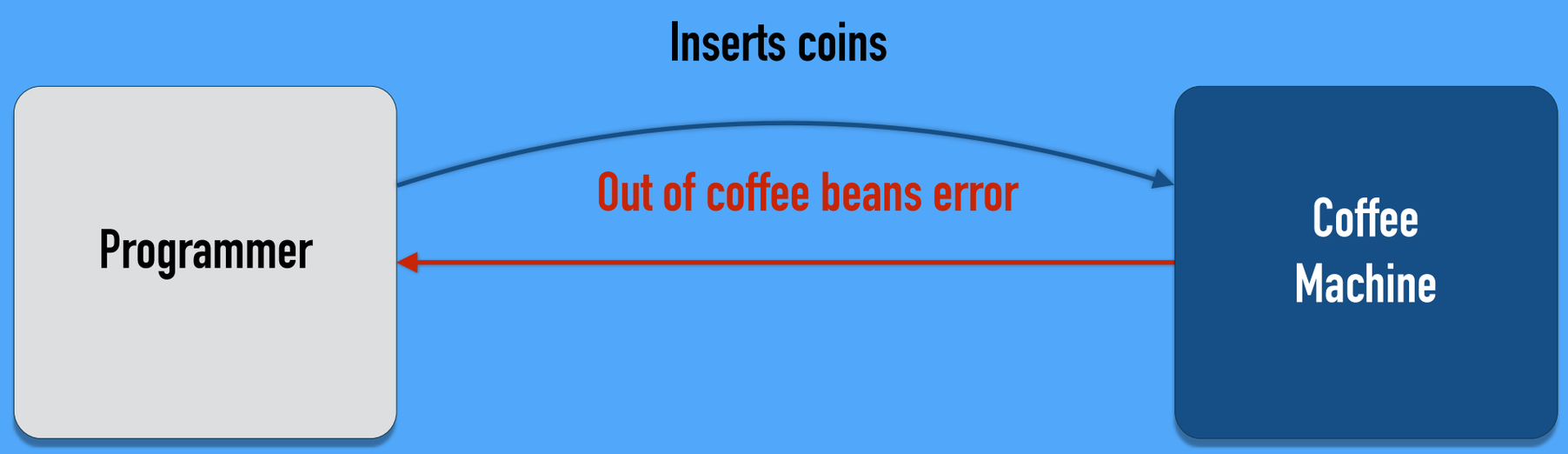
Programmer

Coffee
Machine

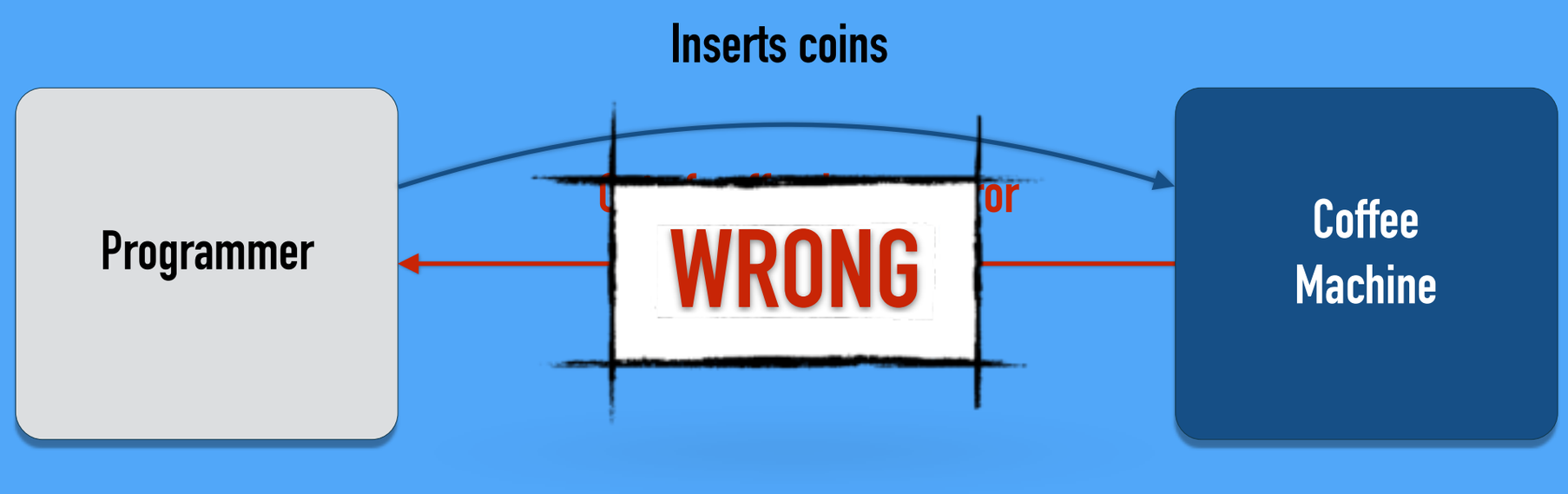
Think Vending Machine



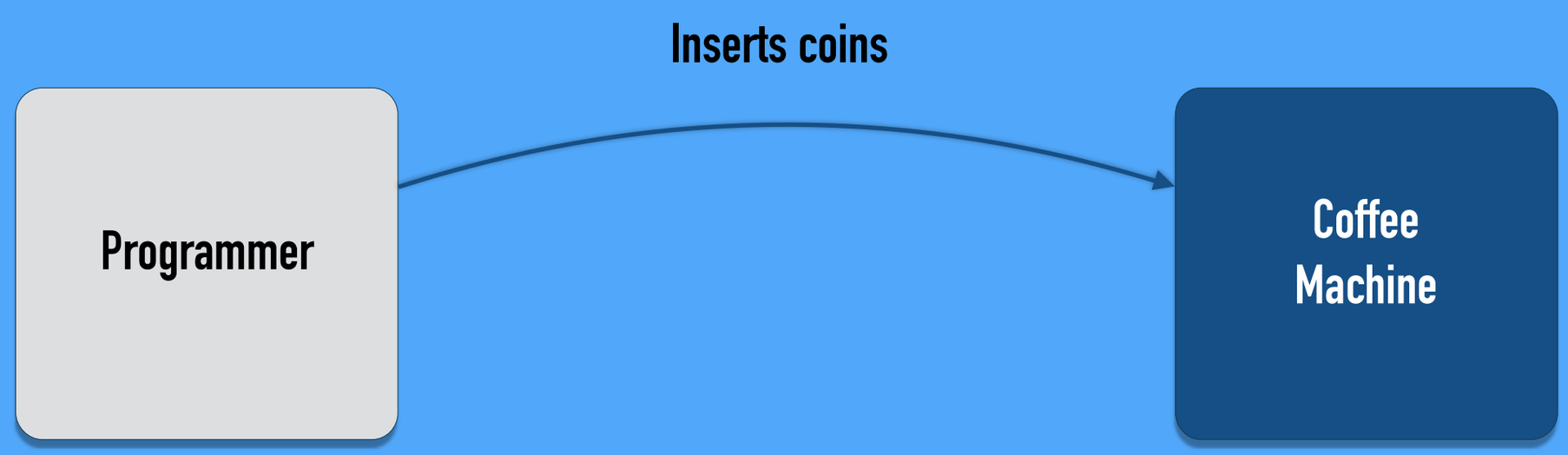
Think Vending Machine



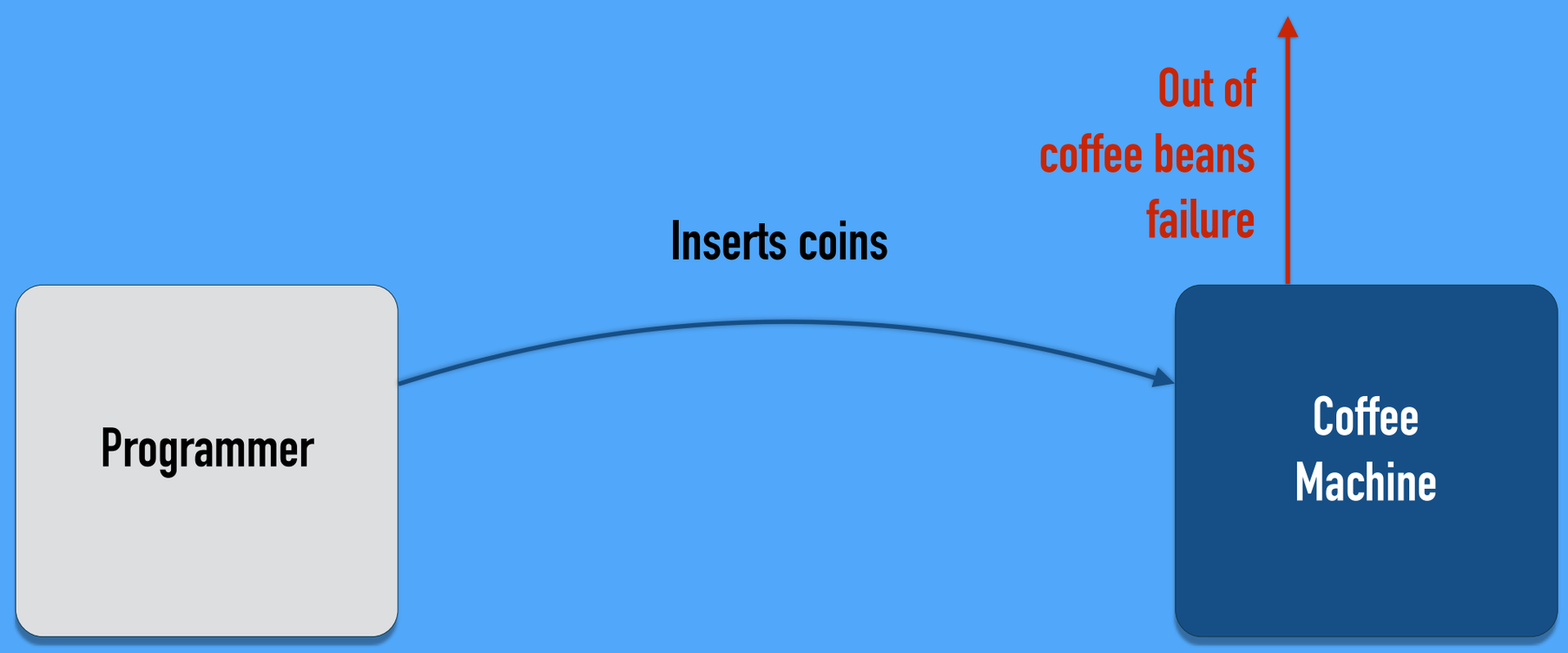
Think Vending Machine



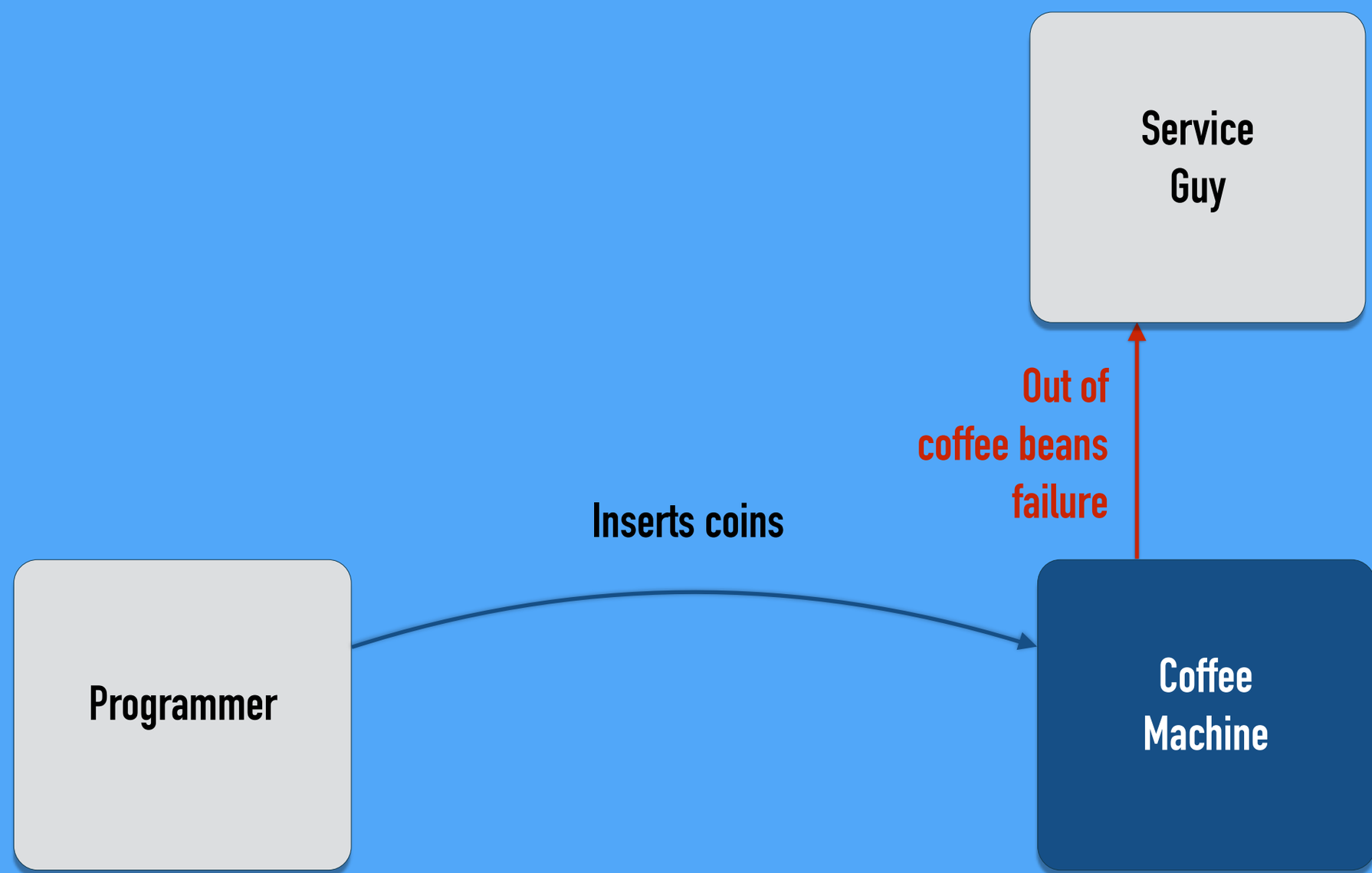
Think Vending Machine



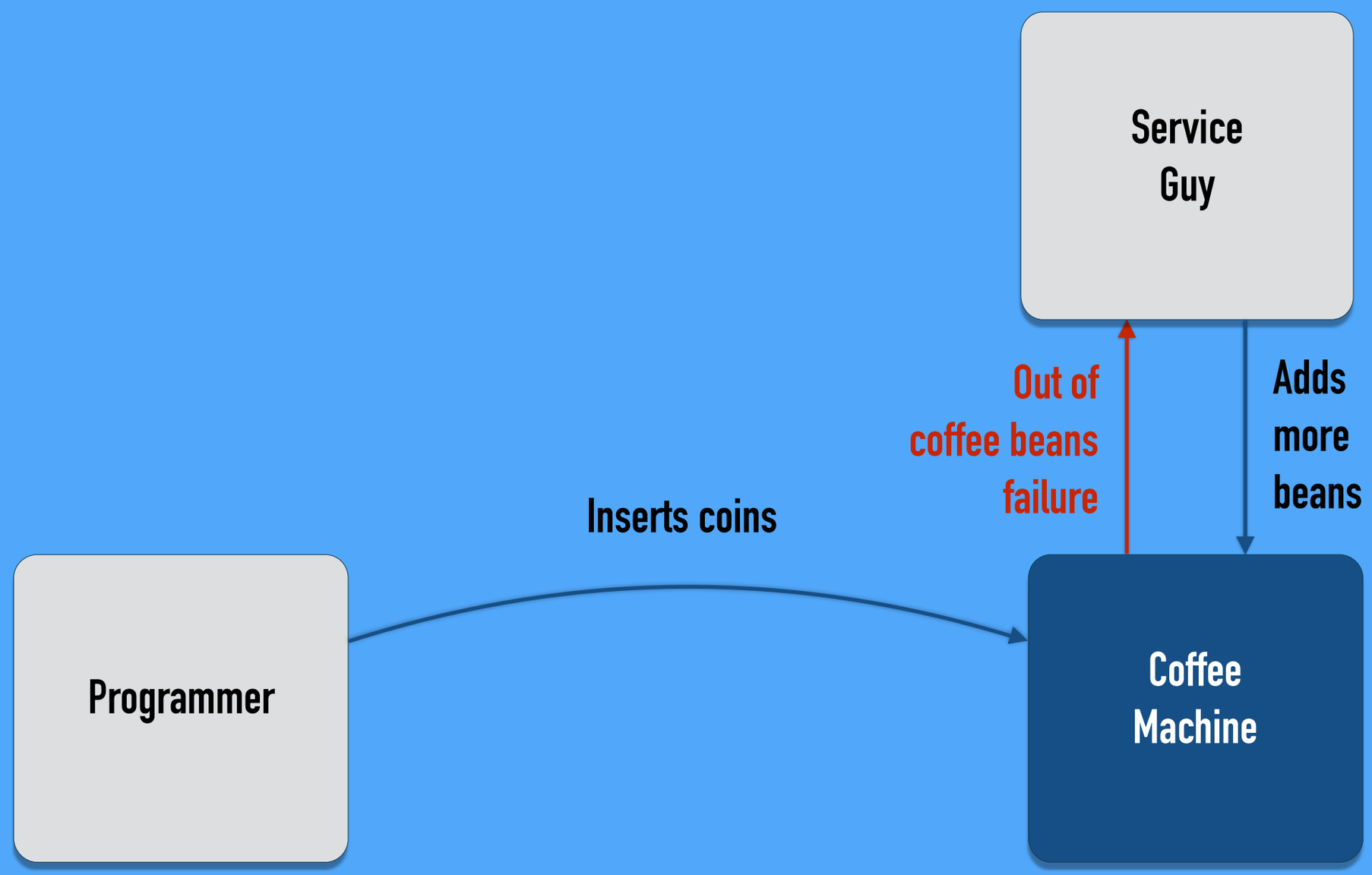
Think Vending Machine



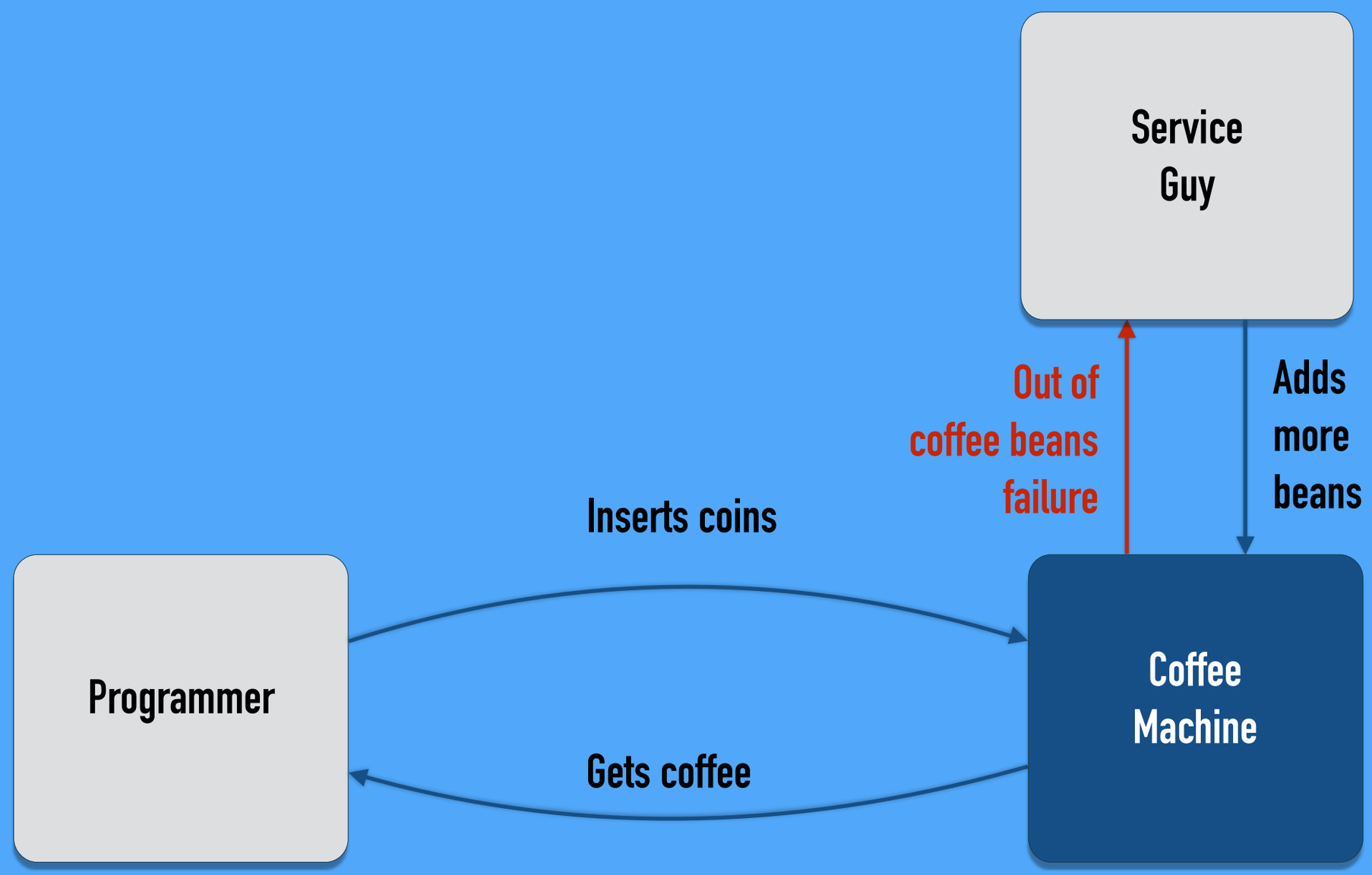
Think Vending Machine



Think Vending Machine



Think Vending Machine

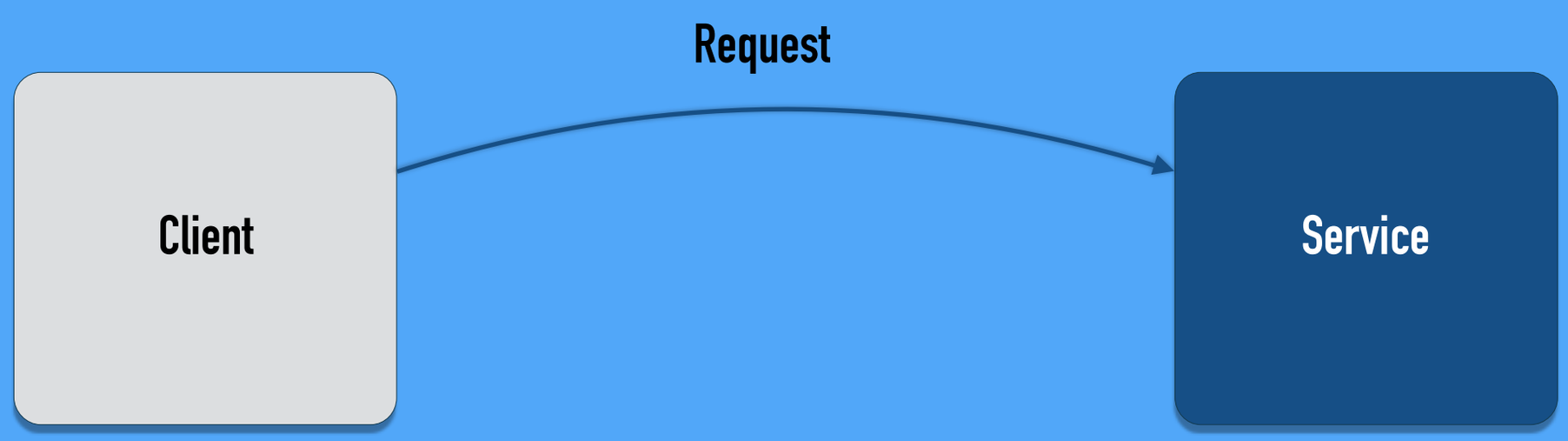


Think Vending Machine

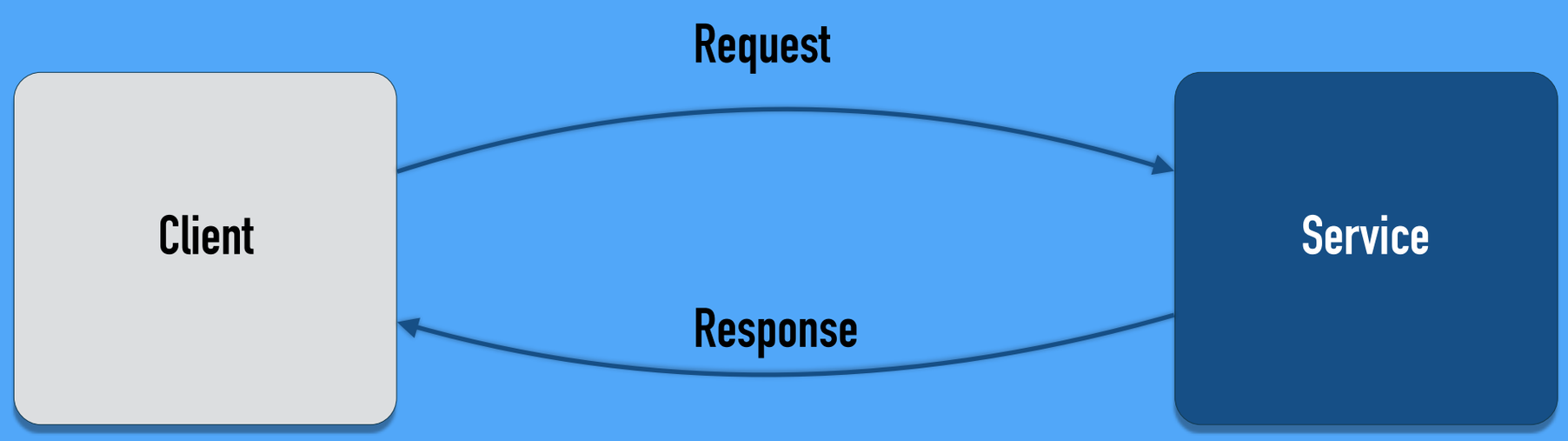
Client

Service

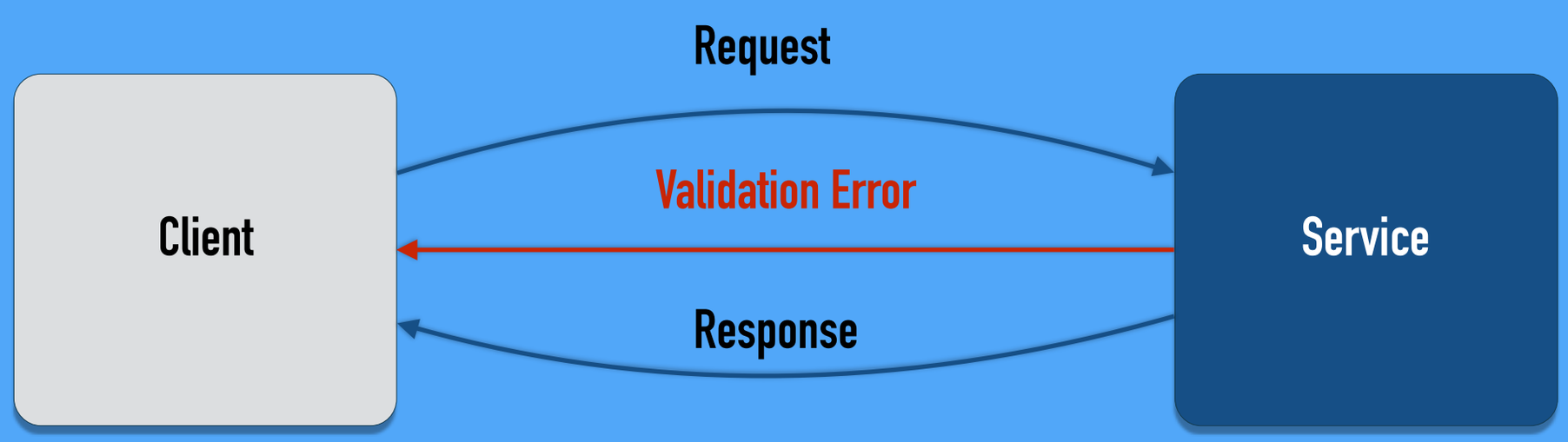
Think Vending Machine



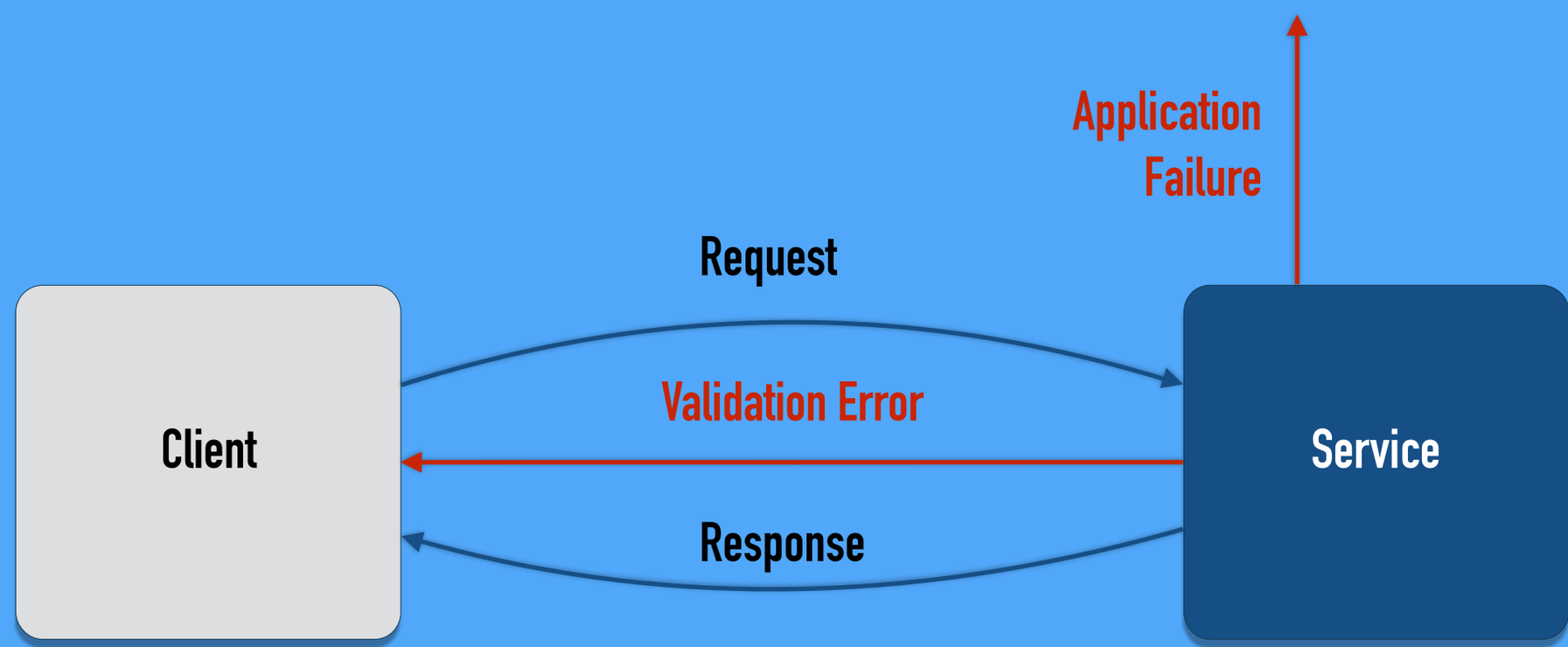
Think Vending Machine



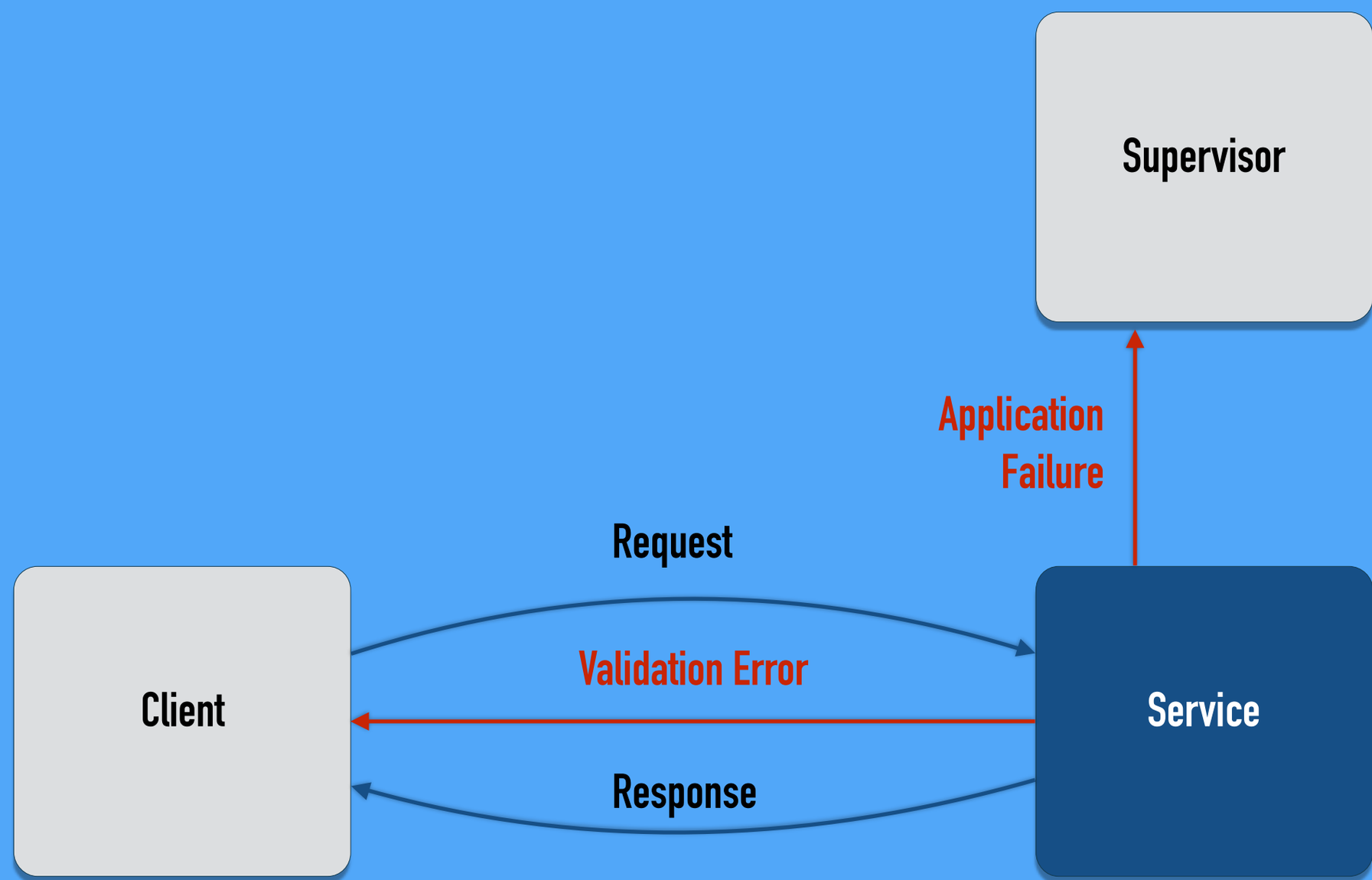
Think Vending Machine



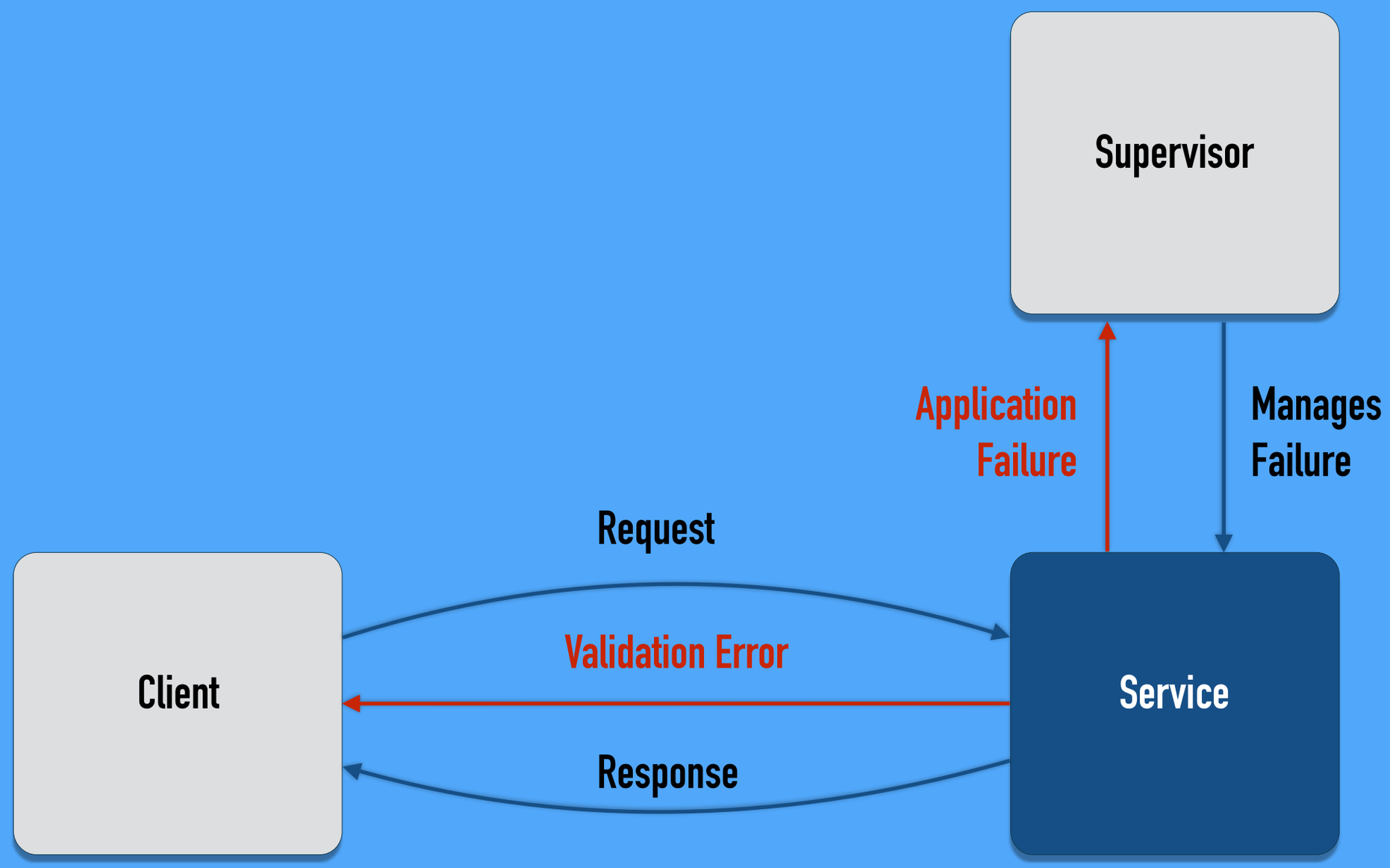
Think Vending Machine



Think Vending Machine



Think Vending Machine



Error Kernel Pattern

ONION-LAYERED STATE & FAILURE MANAGEMENT

Making reliable distributed systems in the presence of software errors - Joe Armstrong
On Erlang, State and Crashes - Jesper Louis Andersen

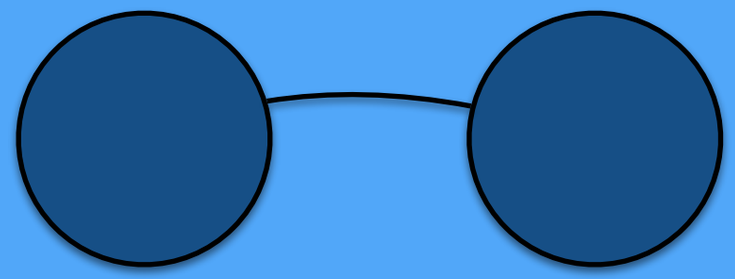
Onion Layered State Management

Client

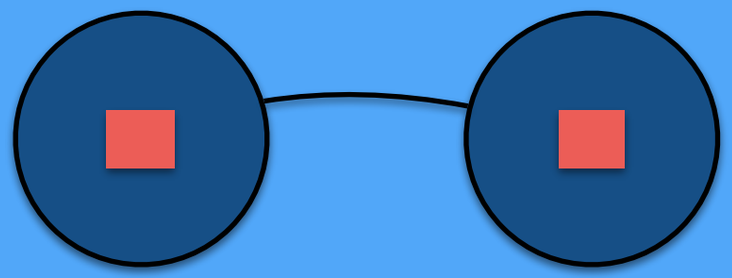
Object

Critical state that needs protection

Thread boundary



Onion Layered State Management



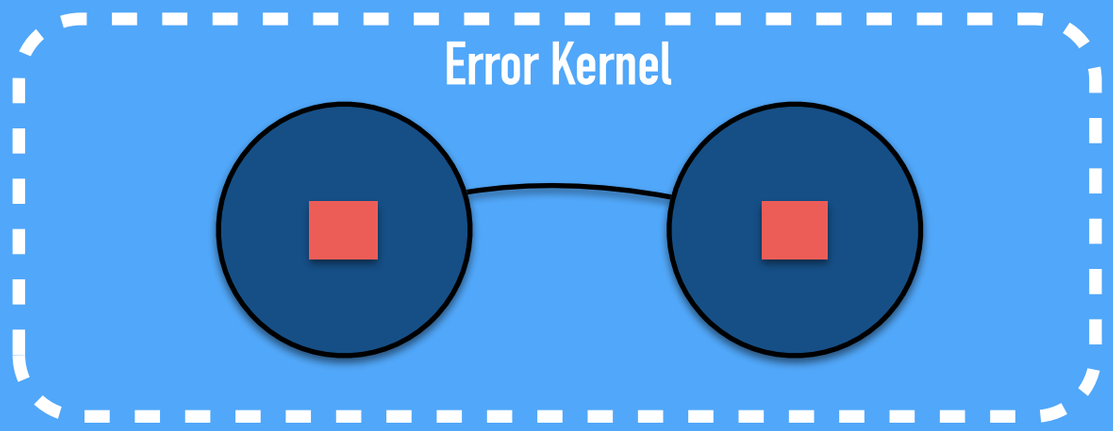
Client

Object

Critical state that needs protection

Thread boundary

Onion Layered State Management



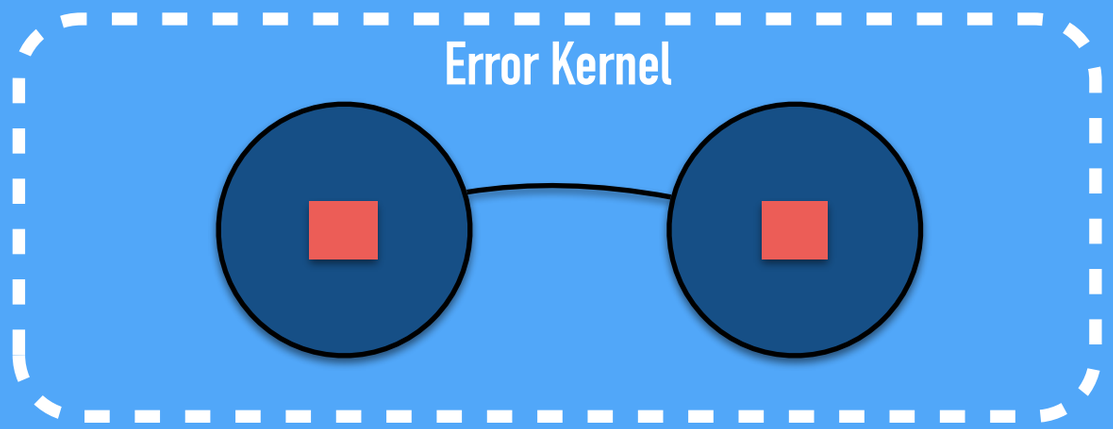
Client

Object

Critical state that needs protection

Thread boundary

Onion Layered State Management



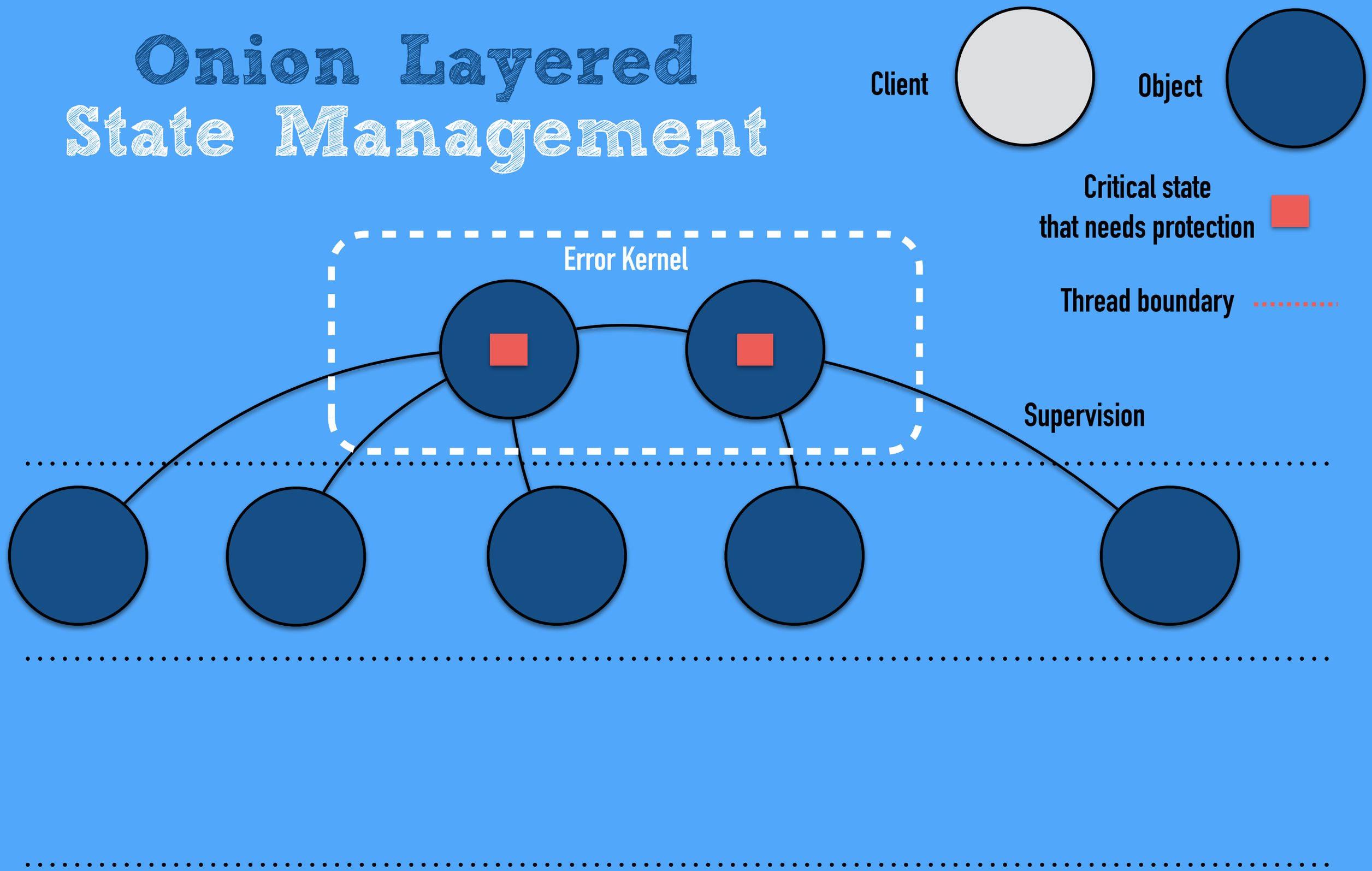
Client

Object

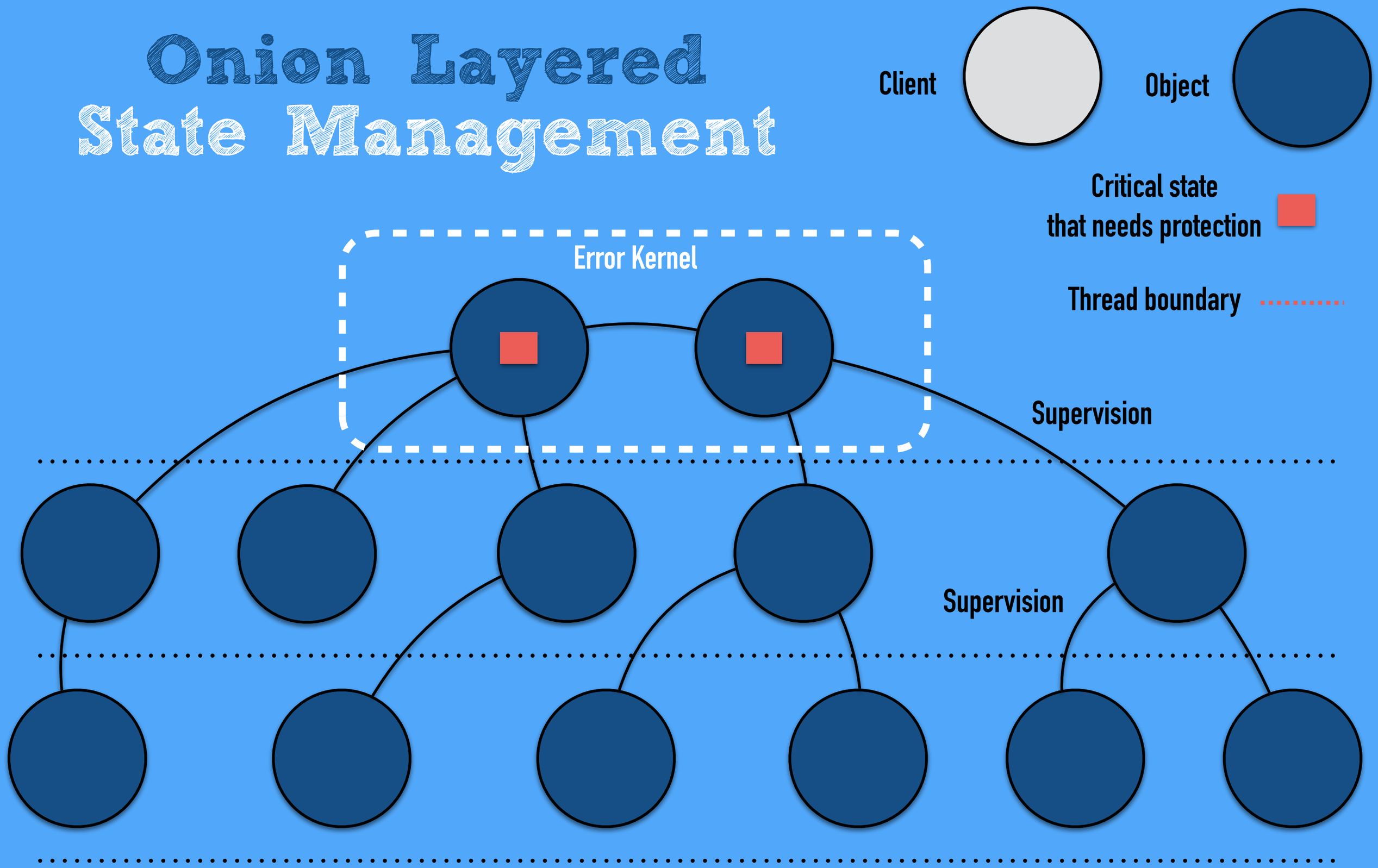
Critical state that needs protection

Thread boundary

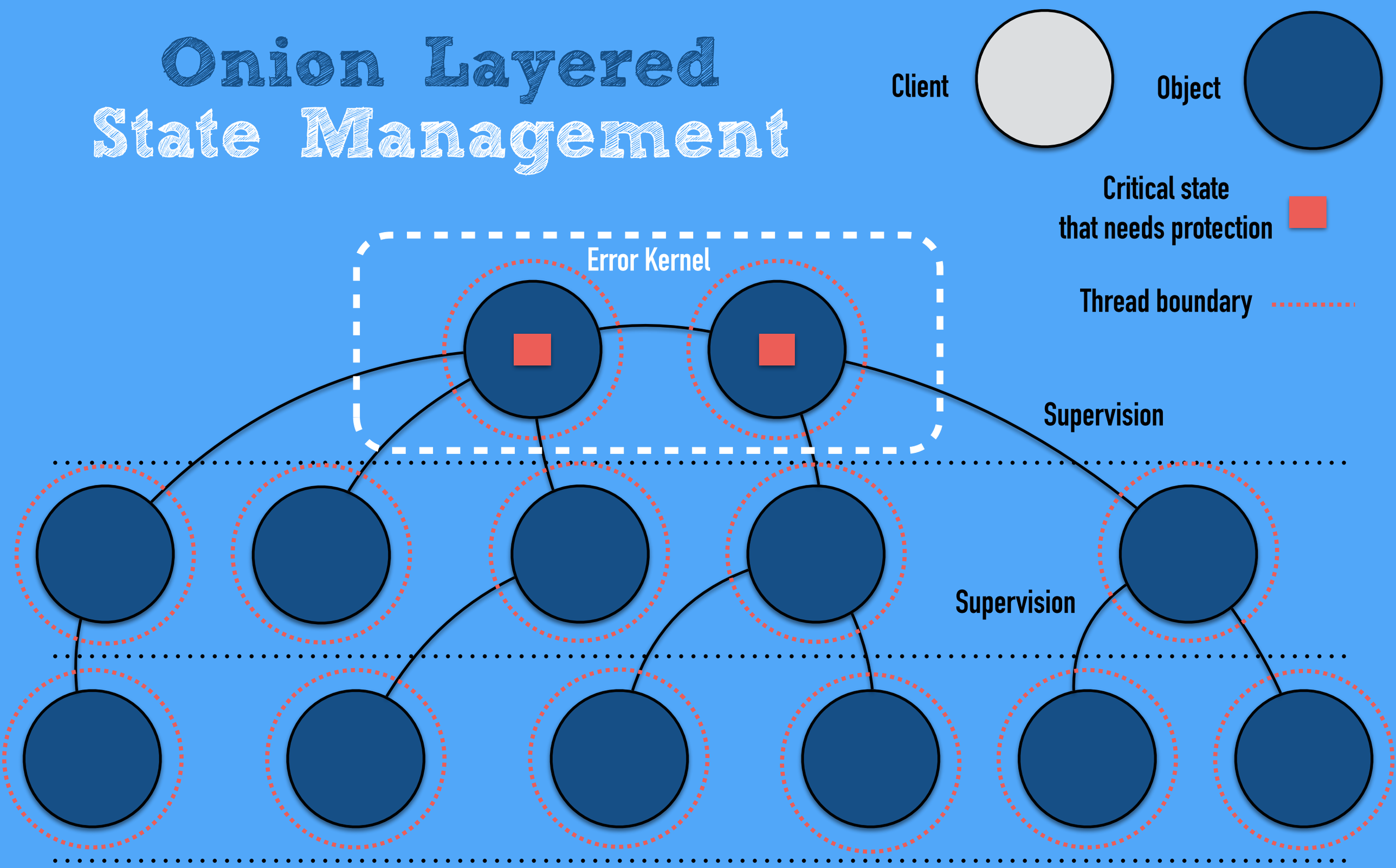
Onion Layered State Management



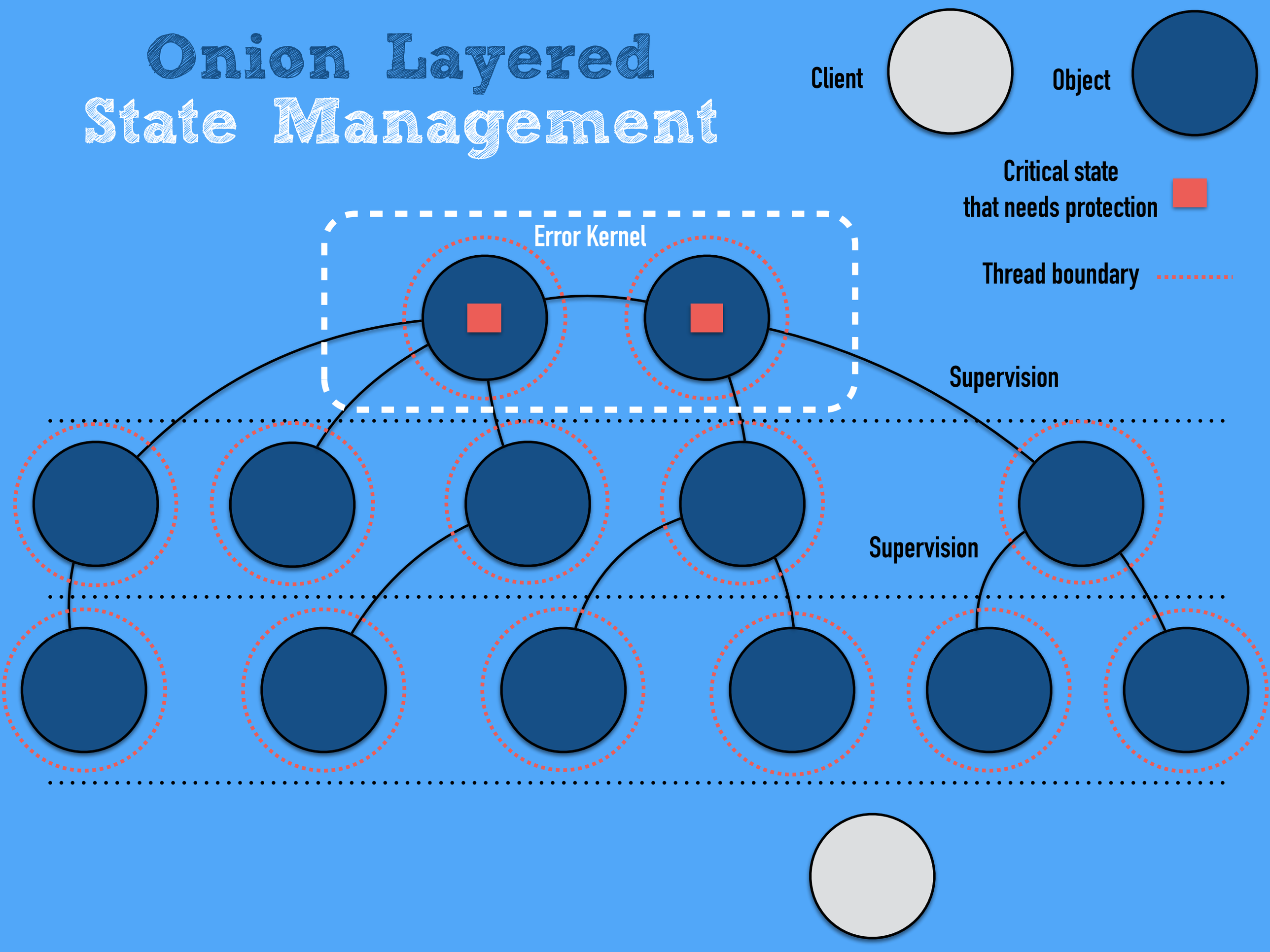
Onion Layered State Management



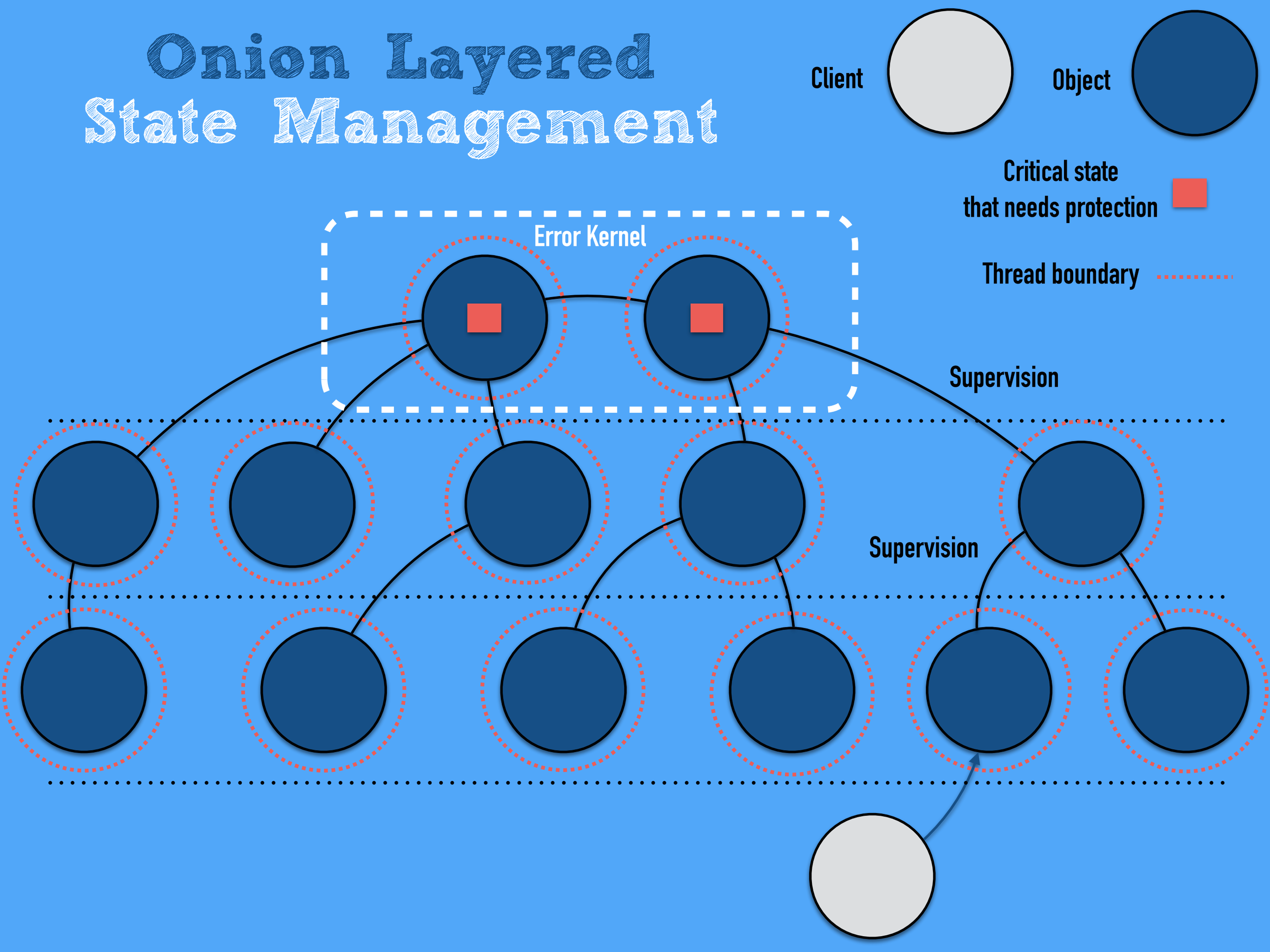
Onion Layered State Management



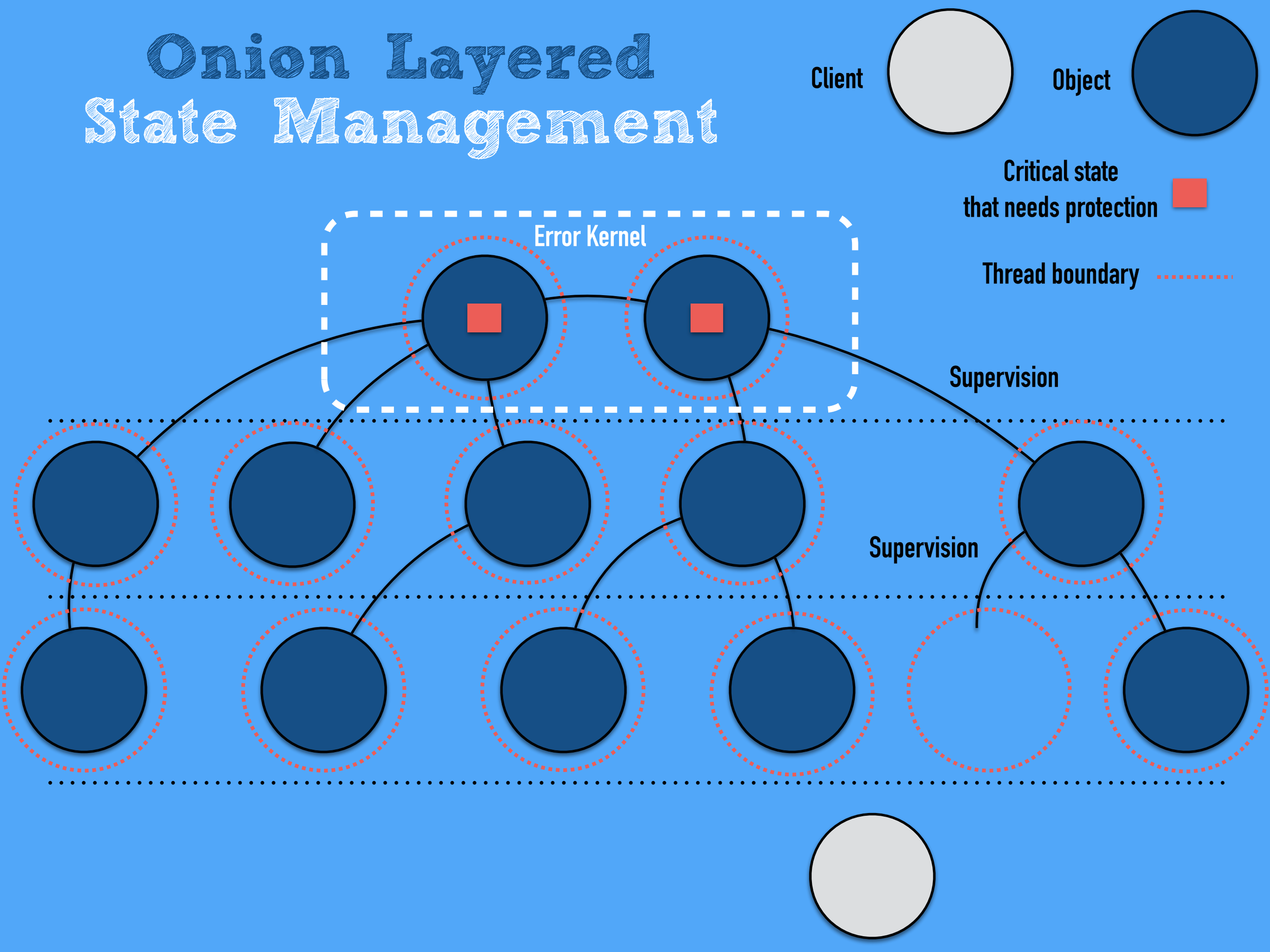
Onion Layered State Management



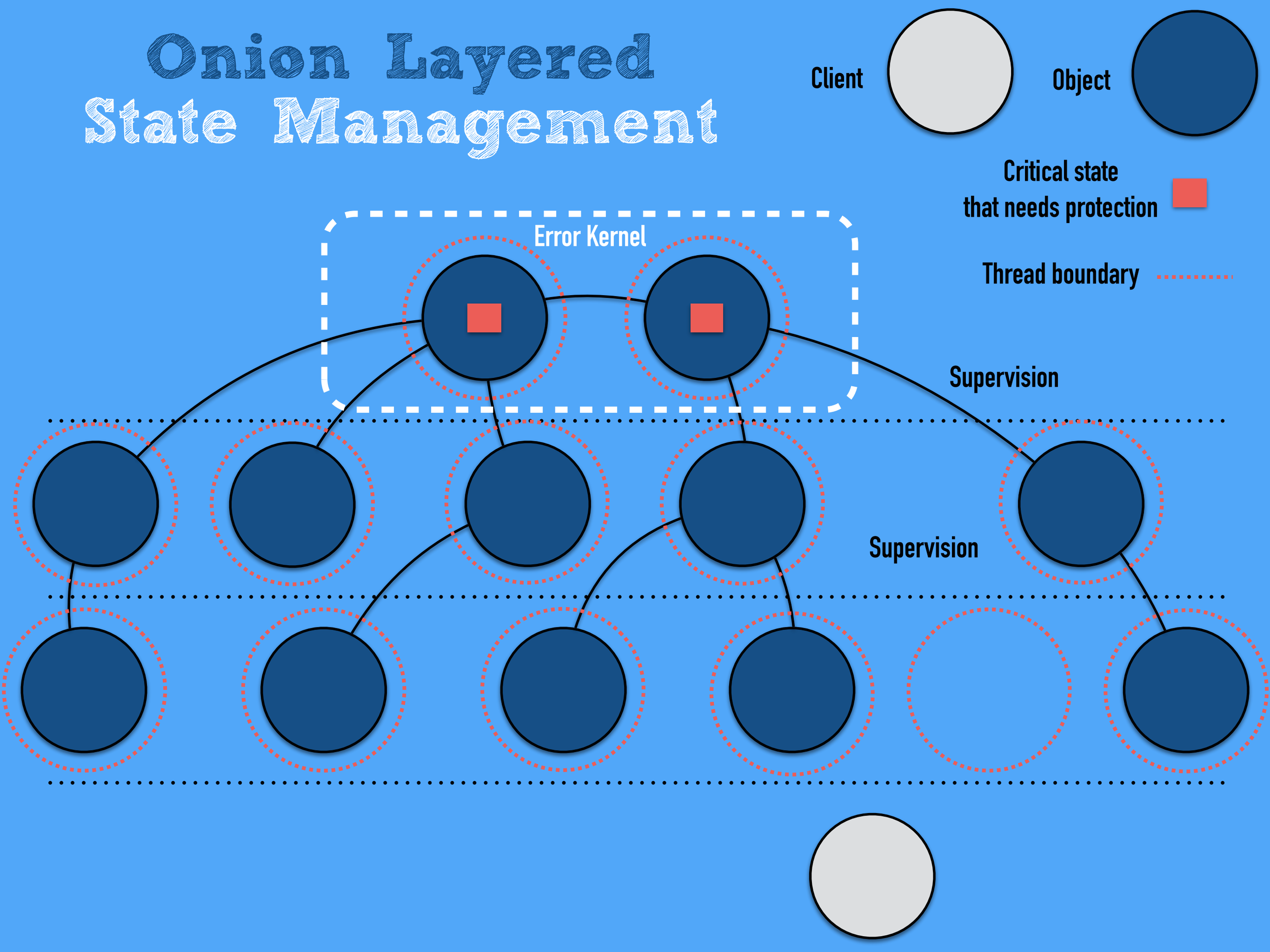
Onion Layered State Management



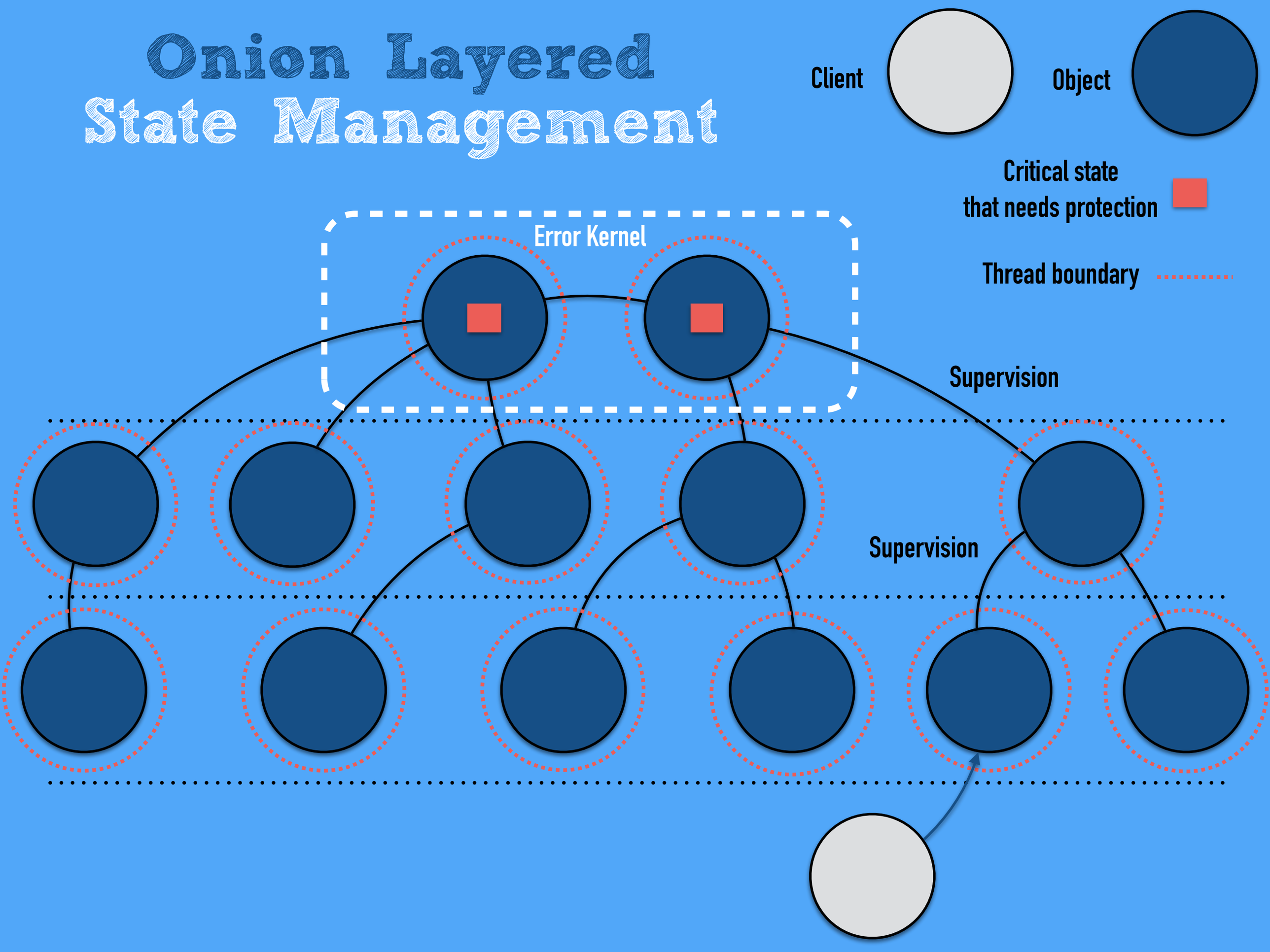
Onion Layered State Management



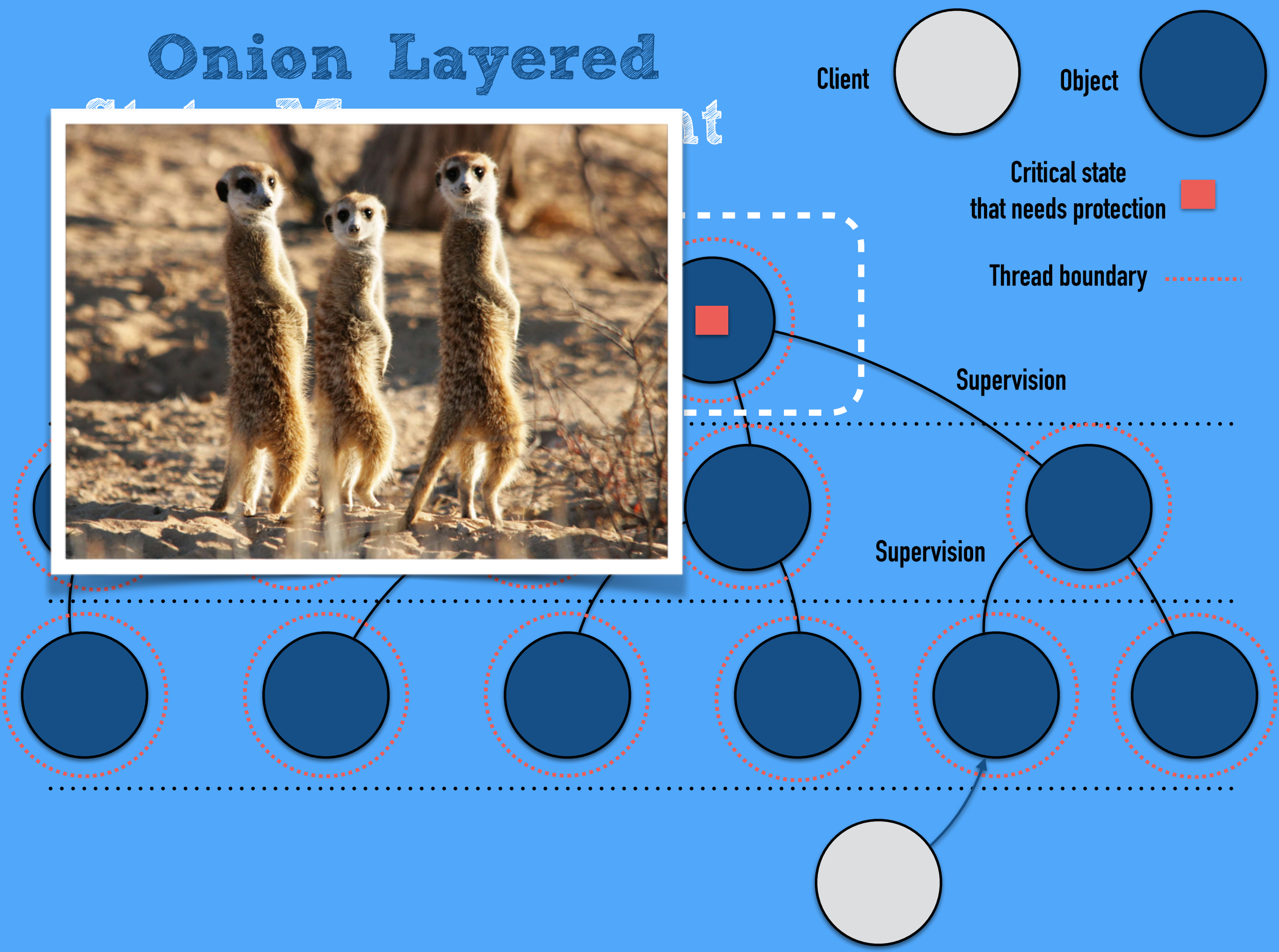
Onion Layered State Management



Onion Layered State Management



Onion Layered



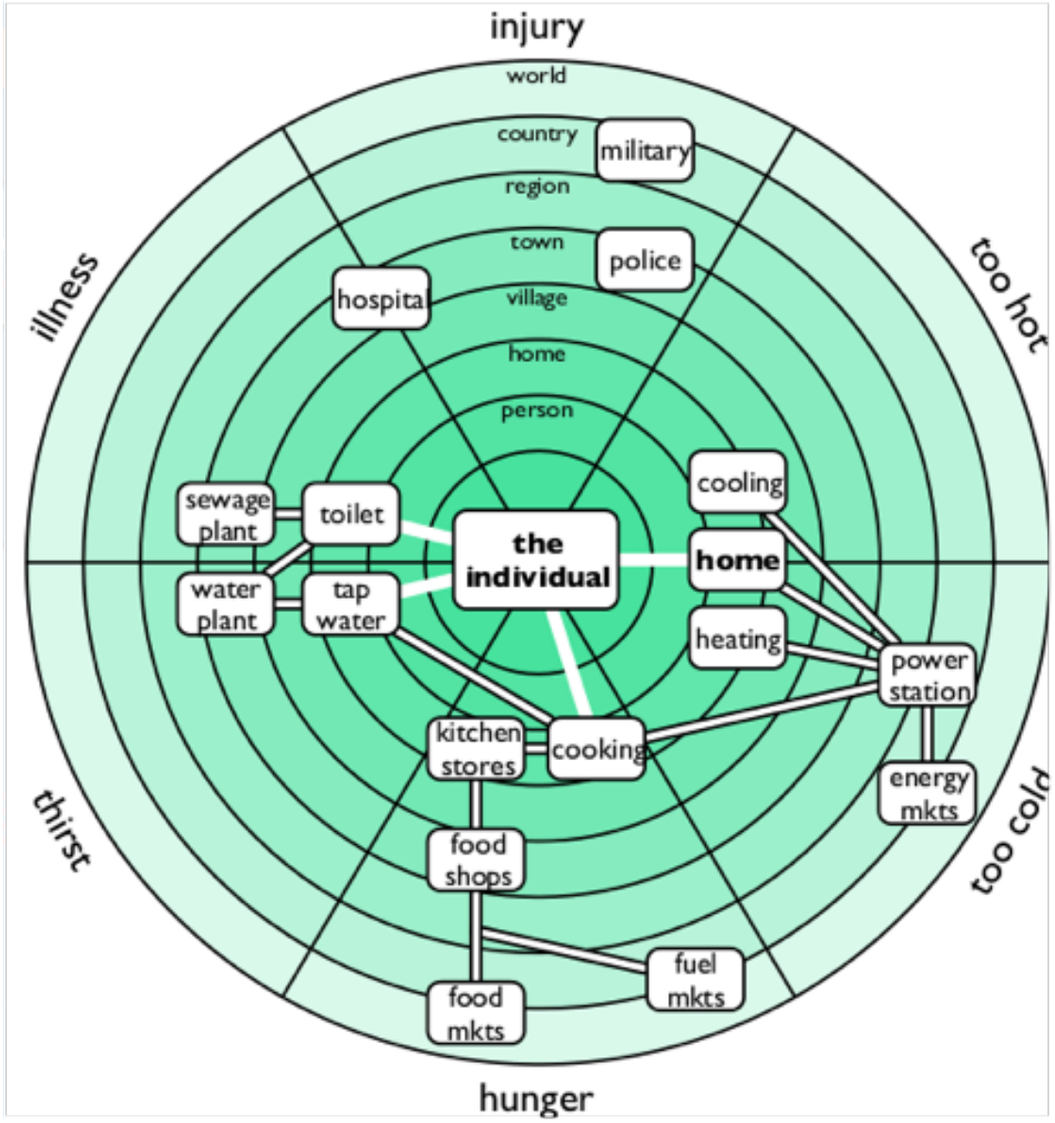
Onion Layered

Client

Object

Critical state
that needs protection

Thread boundary



Maintain Diversity and Redundancy

The Network is Reliable


The Network
is Reliable
NAT

Strong Consistency

IS THE WRONG DEFAULT

WE NEED SYSTEMS THAT ARE DECOUPLED IN

Time and Space

Resilient Protocols

DEPEND ON

ASYNCHRONOUS COMMUNICATION

EVENTUAL CONSISTENCY

Resilient Protocols

DEPEND ON

ASYNCHRONOUS COMMUNICATION

EVENTUAL CONSISTENCY

- ARE TOLERANT TO
  - MESSAGE LOSS
  - MESSAGE REORDERING
  - MESSAGE DUPLICATION

Resilient Protocols

DEPEND ON

ASYNCHRONOUS COMMUNICATION

EVENTUAL CONSISTENCY

- ARE TOLERANT TO
  - MESSAGE LOSS
  - MESSAGE REORDERING
  - MESSAGE DUPLICATION
- EMBRACE ACID 2.0
  - ASSOCIATIVE
  - COMMUTATIVE
  - IDEMPOTENT
  - DISTRIBUTED

Testing


YOU SCHEDULED THE END OF THE TEST PHASE AFTER THE START OF THE PRODUCTION PHASE.
Dilbert.com DilbertCartoonist@gmail.com
WE'RE FEELING CONFIDENT.
5-17-11 ©2011 Scott Adams, Inc. Dist. by Universal Uclick
IT'S TOO BAD THAT BEING SMART DOESN'T COME WITH SOME SORT OF GOOD FEELING LIKE THAT.

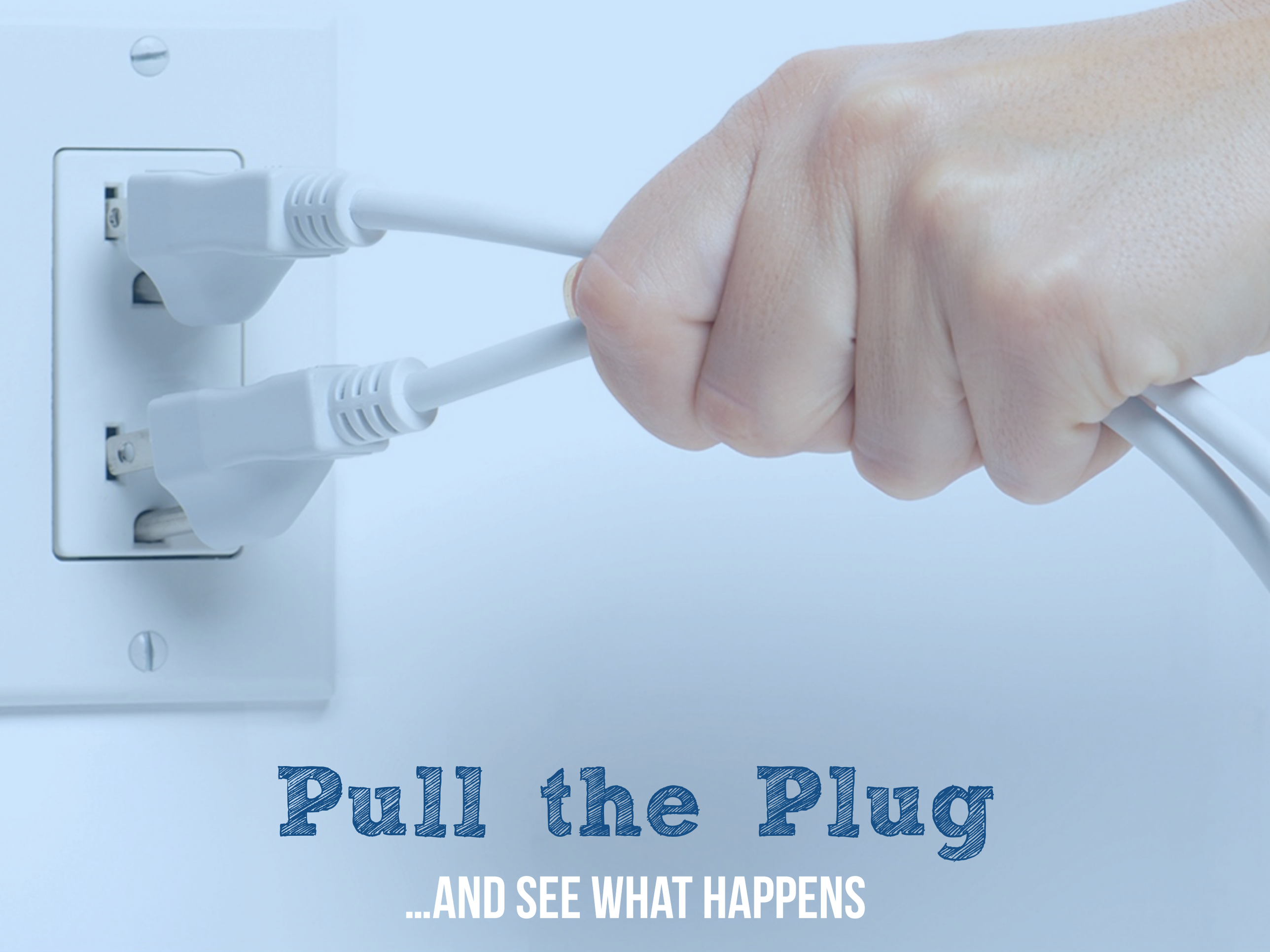
WHAT CAN WE LEARN FROM ARNOLD?

WHAT CAN WE LEARN FROM ARNOLD?

WHAT CAN WE LEARN FROM ARNOLD?

BLOW THINGS UP

Shoot Your App Down


Pull the Plug
...AND SEE WHAT HAPPENS

akka

Executive Summary

“Complex systems run in degraded mode.”

“Complex systems run as broken systems.”

- RICHARD COOK

How Complex Systems Fail - Richard Cook

Resilience is by Design

Photo courtesy of FEMA/Joselyne Augustino

Thank You

Thank You

References

- **Antifragile: Things That Gain from Disorder** - http://www.amazon.com/Antifragile-Things-that-Gain-Disorder-ebook/dp/B009K6DKTS
- **Drift into Failure** - http://www.amazon.com/Drift-into-Failure-Components-Understanding-ebook/dp/B009KOKXKY
- **How Complex Systems Fail** - http://web.mit.edu/2.75/resources/random/How%20Complex%20Systems%20Fail.pdf
- **Leverage Points: Places to Intervene in a System** - http://www.donellameadows.org/archives/leverage-points-places-to-intervene-in-a-system/
- **Going Solid: A Model of System Dynamics and Consequences for Patient Safety** - http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1743994/
- **Resilience in Complex Adaptive Systems: Operating at the Edge of Failure** - https://www.youtube.com/watch?v=PGLYEDpNu60
- **Dealing in Security** - http://resiliencemaps.org/files/Dealing_in_Security.July2010.en.pdf
- **What is resilience? An introduction to social-ecological research** - http://www.stockholmresilience.org/download/18.10119fc11455d3c557d6d21/1398172490555/SU_SRC_whatisresilience_sidaApril2014.pdf
- **Applying resilience thinking: Seven principles for building resilience in social-ecological systems** - http://www.stockholmresilience.org/download/18.10119fc11455d3c557d6928/1398150799790/SRC+Applying+Resilience+final.pdf
- **Puppies! Now that I've got your attention, Complexity Theory** - https://www.ted.com/talks/nicolas_perony_puppies_now_that_i_ve_got_your_attention_complexity_theory
- **How Bacteria Becomes Resistant** - http://www.abc.net.au/science/slab/antibiotics/resistance.htm
- **Towards Resilient Architectures: Biology Lessons** - http://www.metropolismag.com/Point-of-View/March-2013/Toward-Resilient-Architectures-1-Biology-Lessons/
- **Crash-Only Software** - https://www.usenix.org/legacy/events/hotos03/tech/full_papers/candea/candea.pdf
- **Recursive Restartability: Turning the Reboot Sledgehammer into a Scalpel** - http://roc.cs.berkeley.edu/papers/recursive_restartability.pdf
- **Out of the Tar Pit** - http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.93.8928
- **Bulkhead Pattern** - http://skife.org/architecture/fault-tolerance/2009/12/31/bulkheads.html
- **Making Reliable Distributed Systems in the Presence of Software Errors** - http://www.erlang.org/download/armstrong_thesis_2003.pdf
- **On Erlang, State and Crashes** - http://jlouisramblings.blogspot.be/2010/11/on-erlang-state-and-crashes.html
- **Akka Supervision** - http://doc.akka.io/docs/akka/snapshot/general/supervision.html
- **Release It!: Design and Deploy Production-Ready Software** - https://pragprog.com/book/mnee/release-it
- **Hystrix** - https://github.com/Netflix/Hystrix
- **Akka Circuit Breaker** - http://doc.akka.io/docs/akka/snapshot/common/circuitbreaker.html
- **Reactive Streams** - http://reactive-streams.org
- **Akka Streams** - http://doc.akka.io/docs/akka-stream-and-http-experimental/1.0/scala/stream-introduction.html
- **RxJava** - https://github.com/ReactiveX/RxJava
- **Feedback Control for Computer Systems** - http://www.amazon.com/Feedback-Control-Computer-Systems-Philipp/dp/1449361692
- **Simian Army** - https://github.com/Netflix/SimianArmy
- **Gatling** - http://gatling.io
- **Akka MultiNode Testing** - http://doc.akka.io/docs/akka/snapshot/dev/multi-node-testing.html

Q&A