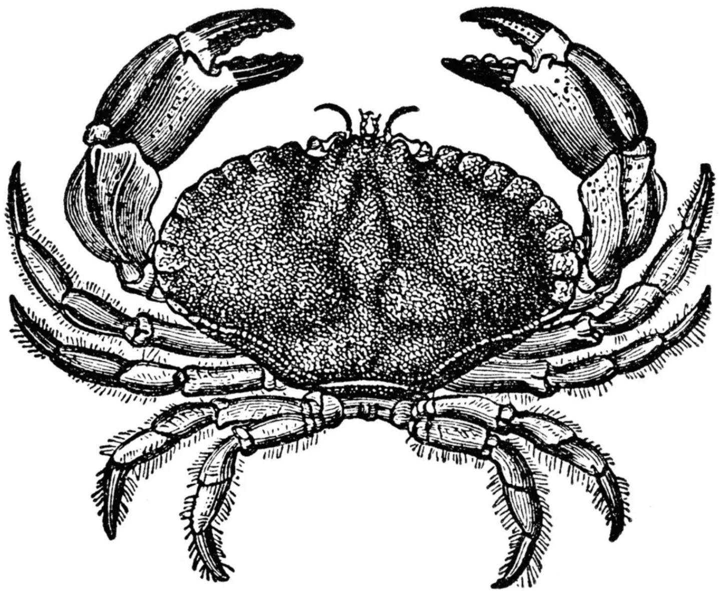
Making Sense of the Madness

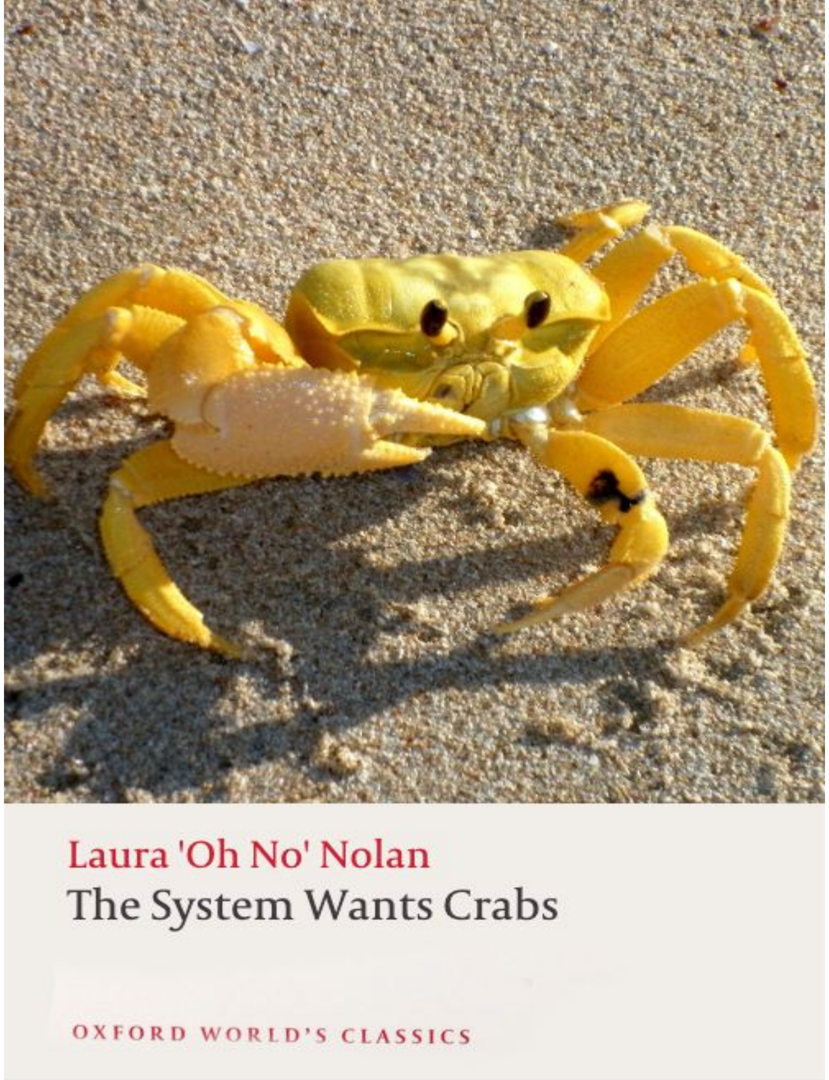


Systems Thinking

For Software Engineering

O RLY?

Laura Nolan



Laura 'Oh No' Nolan

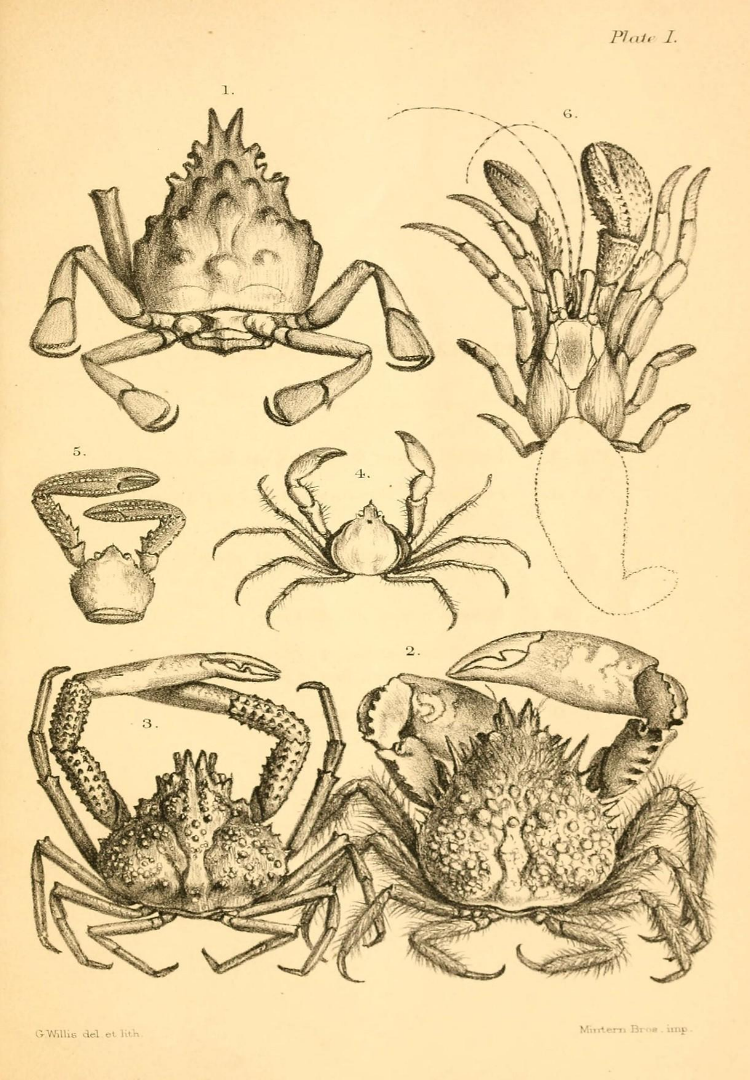
The System Wants Crabs

OXFORD WORLD'S CLASSICS

Image: Gnaraloo Turtle
Conservation Program
CC-BY SA 3.0

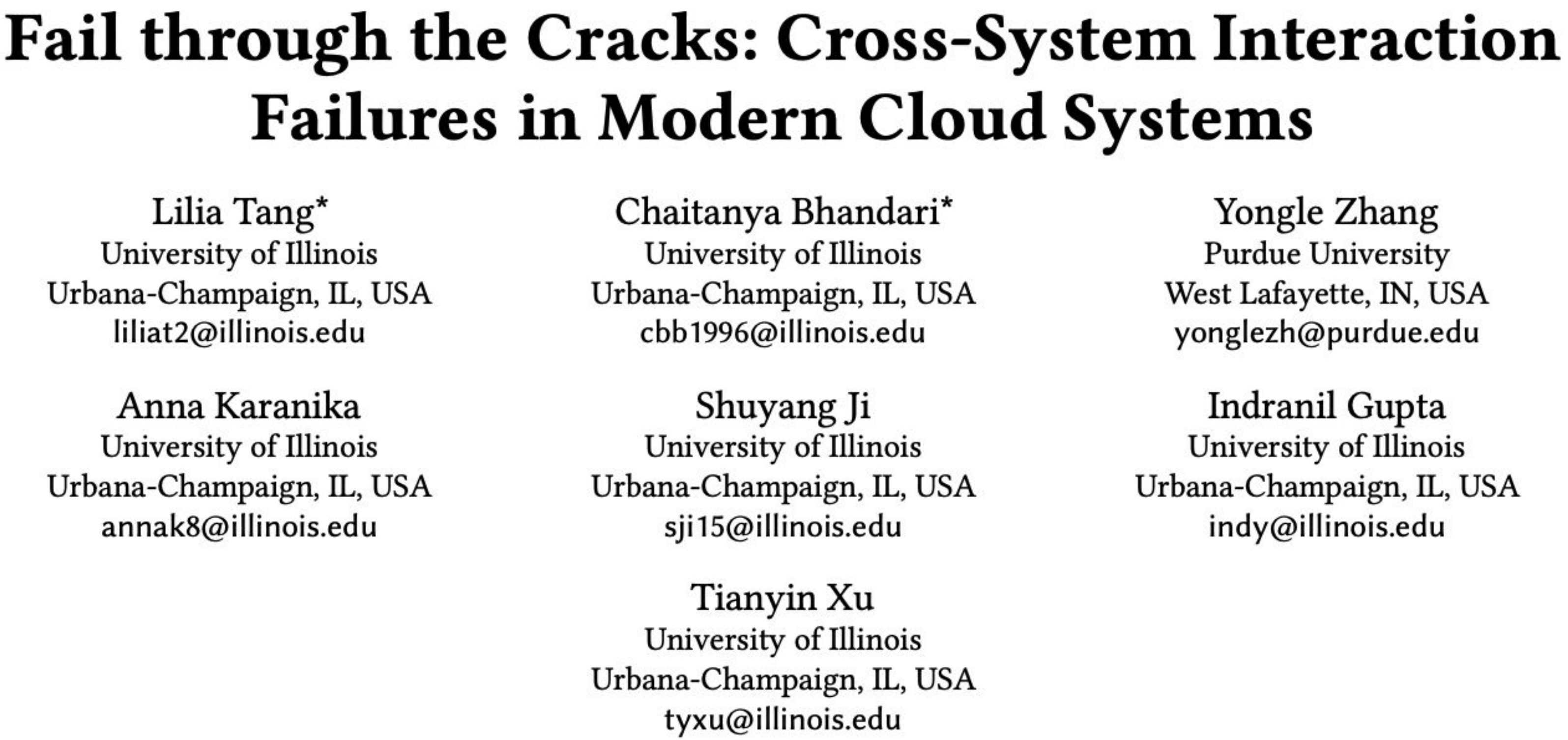
What is a System?

- Elements or parts
- Interactions and interconnections
- In engineered systems: A function



Complex Systems

- Non-linear interactions and feedback loops
- Dynamic, have state and history
- Hard to understand and predict behaviour



Fail through the Cracks: Cross-System Interaction Failures in Modern Cloud Systems

Lilia Tang*
University of Illinois
Urbana-Champaign, IL, USA
liliat2@illinois.edu

Chaitanya Bhandari*
University of Illinois
Urbana-Champaign, IL, USA
cbb1996@illinois.edu

Yongle Zhang
Purdue University
West Lafayette, IN, USA
yonglezh@purdue.edu

Anna Karanika
University of Illinois
Urbana-Champaign, IL, USA
annak8@illinois.edu

Shuyang Ji
University of Illinois
Urbana-Champaign, IL, USA
sji15@illinois.edu

Indranil Gupta
University of Illinois
Urbana-Champaign, IL, USA
indy@illinois.edu

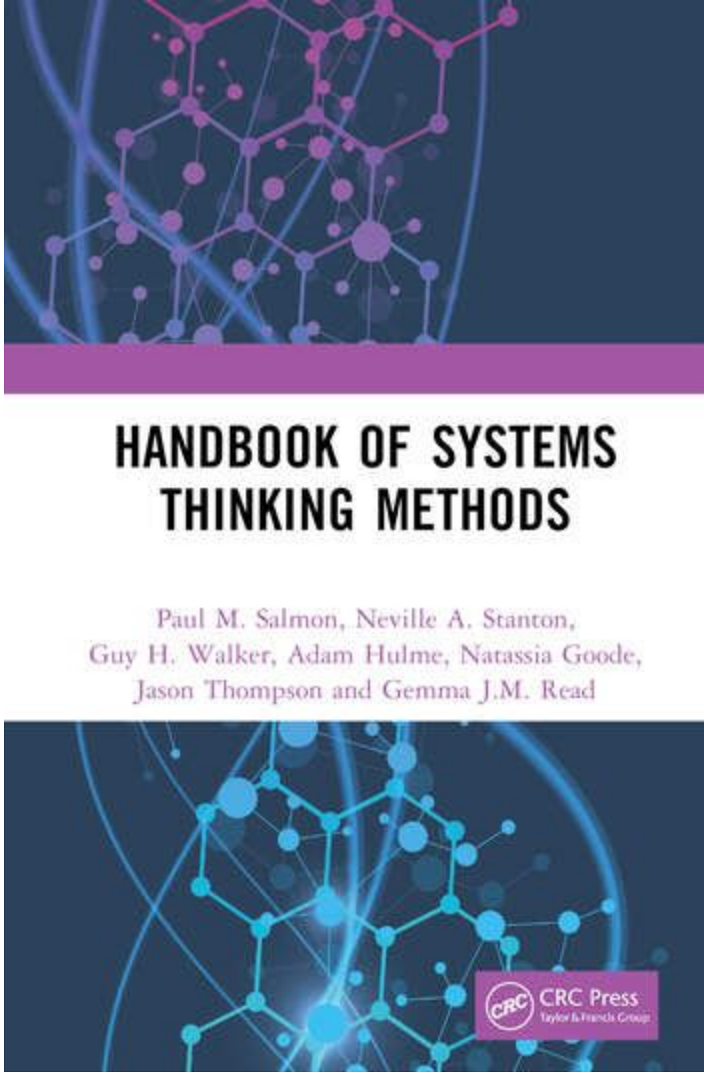
Tianyin Xu
University of Illinois
Urbana-Champaign, IL, USA
tyxu@illinois.edu

Paper at *EuroSys 23*, https://tianyin.github.io/pub/csi-failures.pdf

Systems Thinking

Tools for understanding and working with complex systems as wholes, rather than collections of parts.

Working with whole systems is what we do at Staff+ level: make them better, simpler, more reliable, more efficient.



HANDBOOK OF SYSTEMS THINKING METHODS

Paul M. Salmon, Neville A. Stanton, Guy H. Walker, Adam Hulme, Natassia Goode, Jason Thompson and Gemma J.M. Read

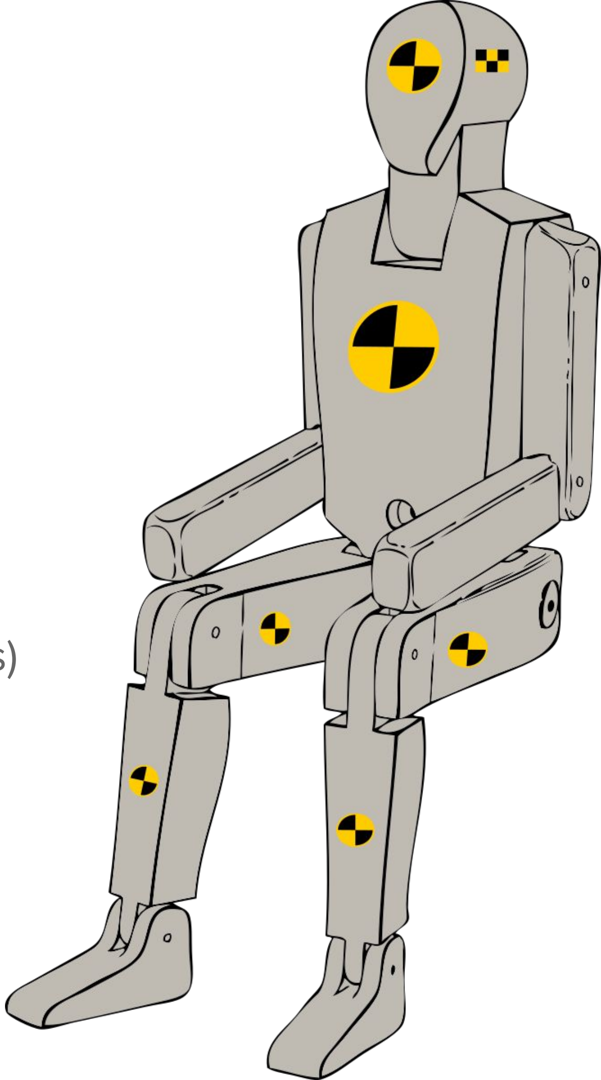
CRC Press
Taylor & Francis Group

Exploring some systems thinking tools

Energy Barriers Perspective

Prevent uncontrolled transfer of energy:

- **Prevent** build-up of harmful energy (avoid driving vehicles)
- **Reduce** amount of energy (speed limits, smaller vehicles, traffic calming)
- **Control** release of energy (install ABS, inspect tyres, straighten dangerous bends)
- **Modify** how energy is distributed (crumple zones, seatbelts)
- **Separate** potential victims from energy (build footpaths, barriers)
- **Limit** or mitigate damage to potential victims (first aid, emergency medicine, rehabilitation)



That one time Google deleted its entire CDN

- Engineer intended to decommission one rack
- CLI tool used couldn’t parse input; by default decided to delete every rack
- Deletion was almost instant - logical deletion by throwing away encryption keys

Energy Barriers Perspective: Applied to CDN deletion incident

- **Prevent:** don’t decommission CDN machines (not feasible)
- **Reduce:** ratelimit how many CDN machines can be decommissioned
- **Control:** tools should give clear feedback to operators about how many machines will be decommissioned
- **Modify:** instead of instant irrevocable logical deletion, provide a time-limited ‘undo’ function to recover keys
- **Separate:** build ‘zones’ in your infra and require a different role to be assumed to perform deletions in each zone
- **Mitigate:** build automation to rebuild CDN machines more quickly, loadshedding to protect origins

Causal Loop Analysis

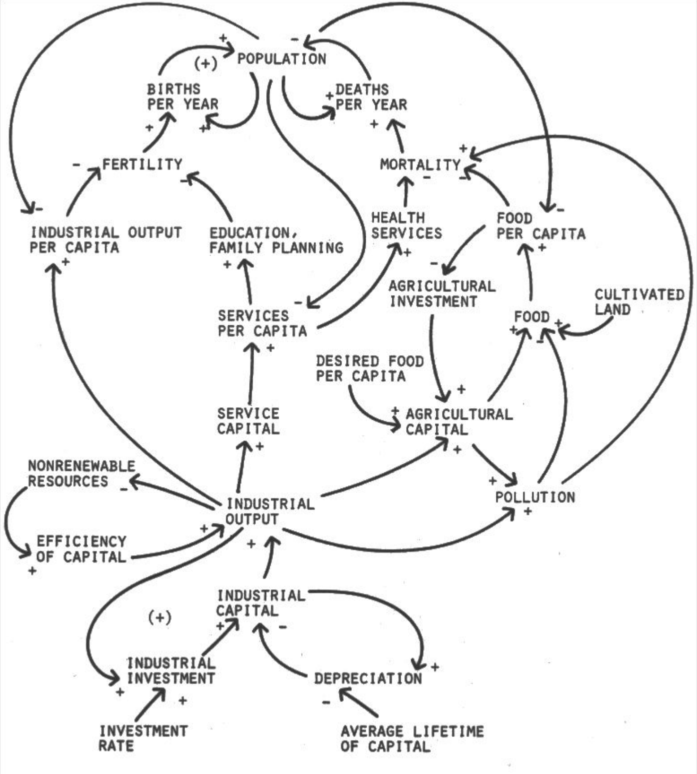
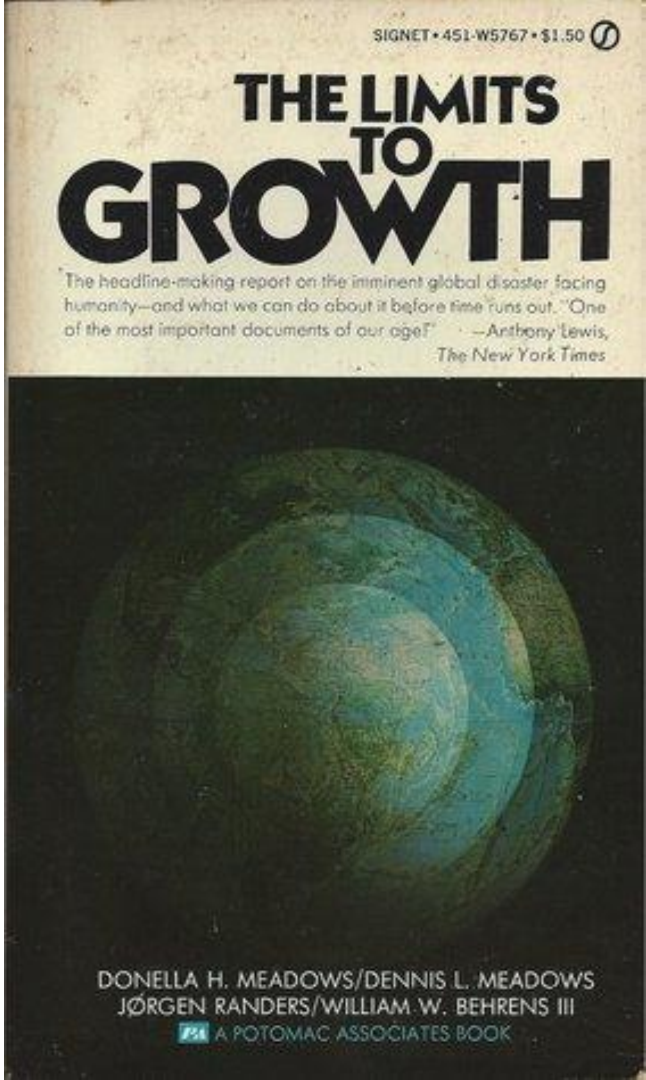
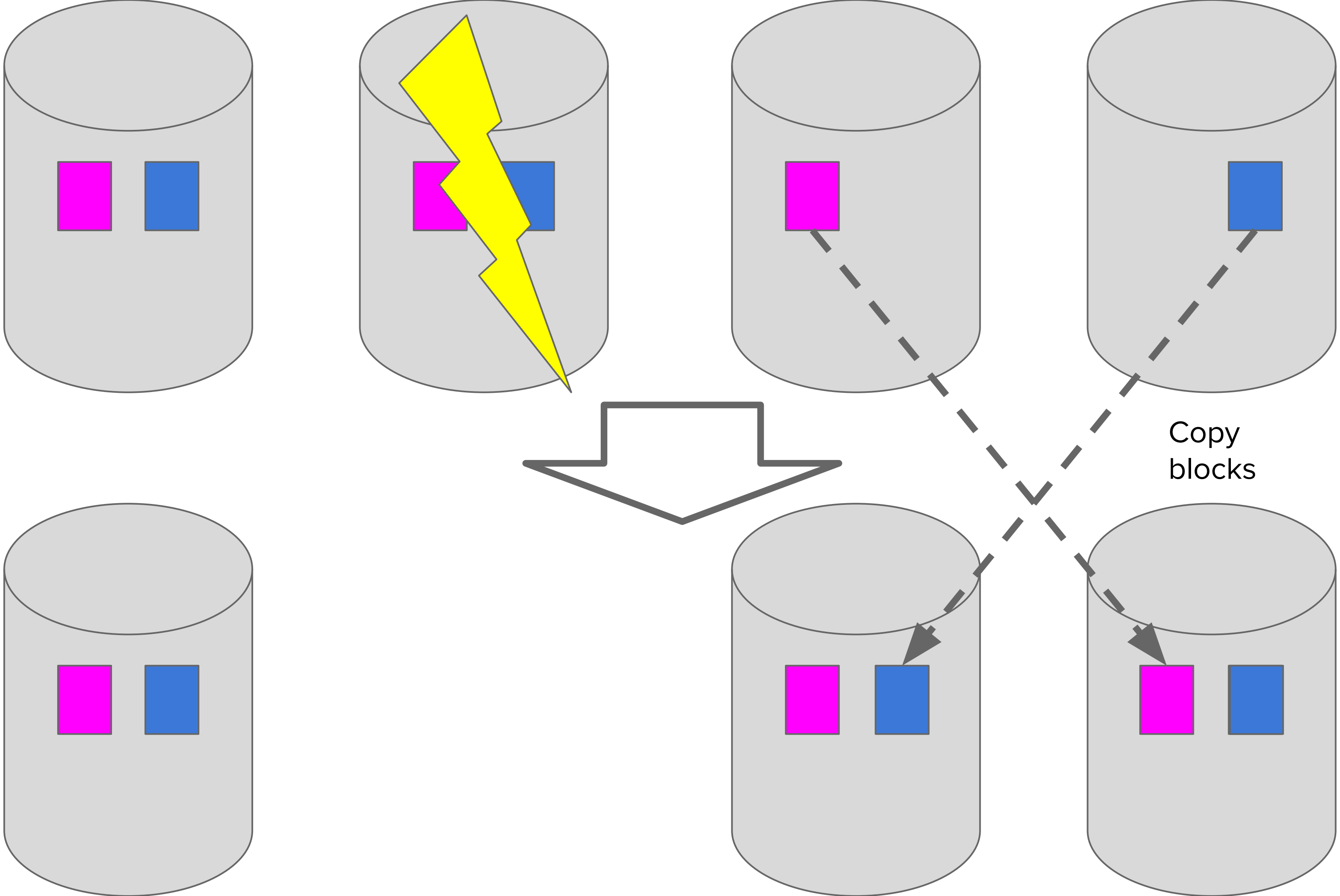


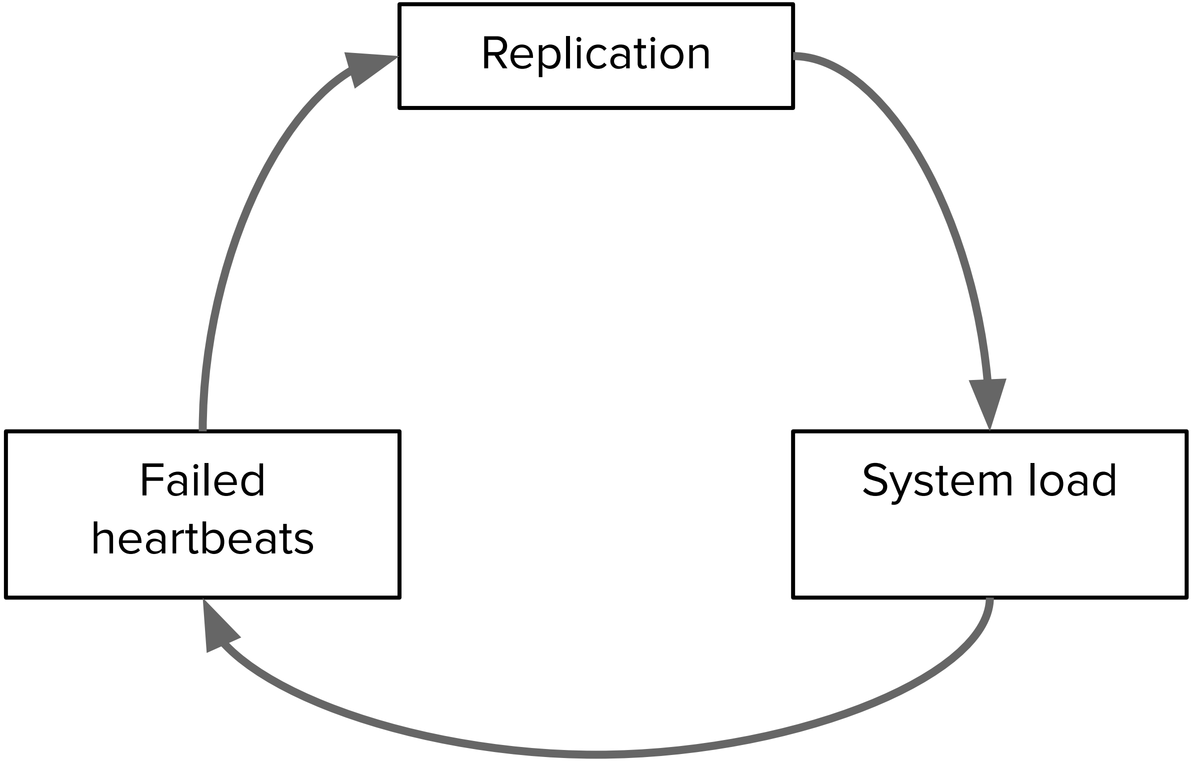
Figure 1-3 Causal-loop diagram of several important feedback loops in World3


SIGNET • 451-W5767 • $1.50
THE LIMITS TO GROWTH
"The headline-making report on the imminent global disaster facing humanity—and what we can do about it before time runs out. "One of the most important documents of our age!" —Anthony Lewis, The New York Times
DONELLA H. MEADOWS/DENNIS L. MEADOWS
JØRGEN RANDERS/WILLIAM W. BEHRENS III
A POTOMAC ASSOCIATES BOOK

My Little Distributed Filesystem

```
replicaChecker()
    while true {
        for each block in filesystem.GetAllBlocks() {
            if block.replicasHeartbeatedOK() < minReplicas {
                block.StartCopyNewReplica()
            }
        }
    }
}
```

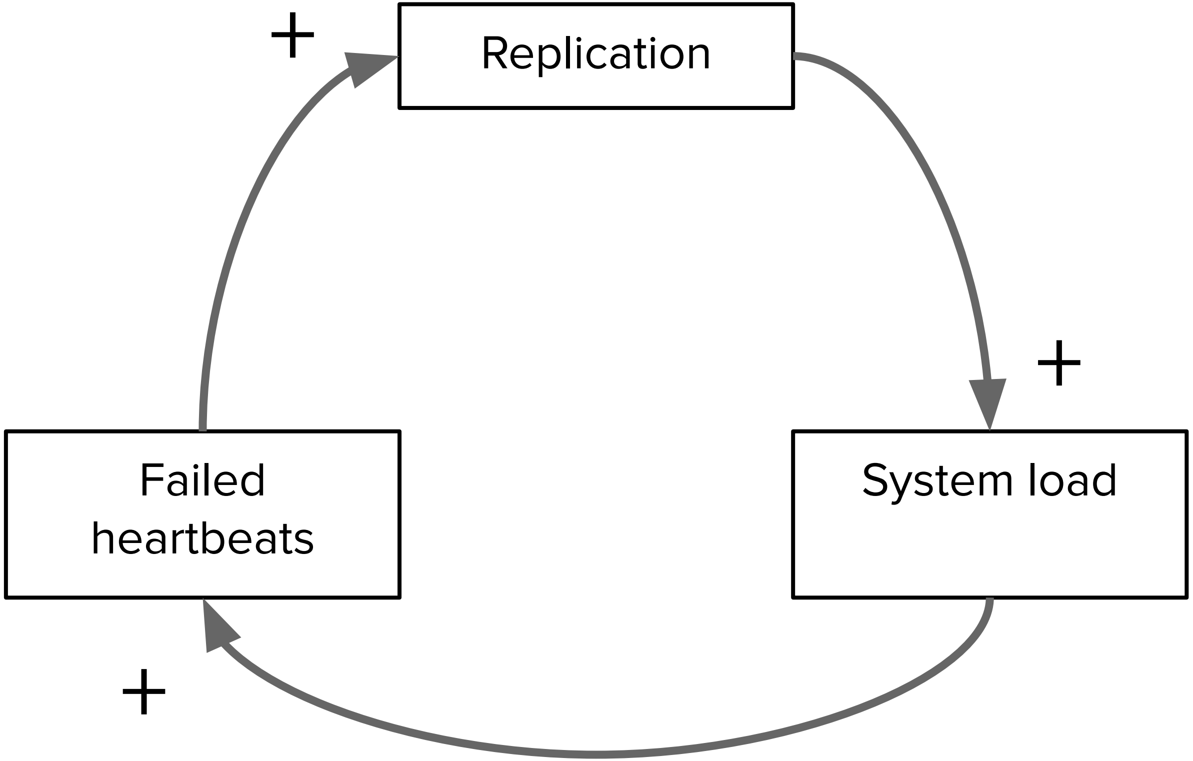

Copy
blocks

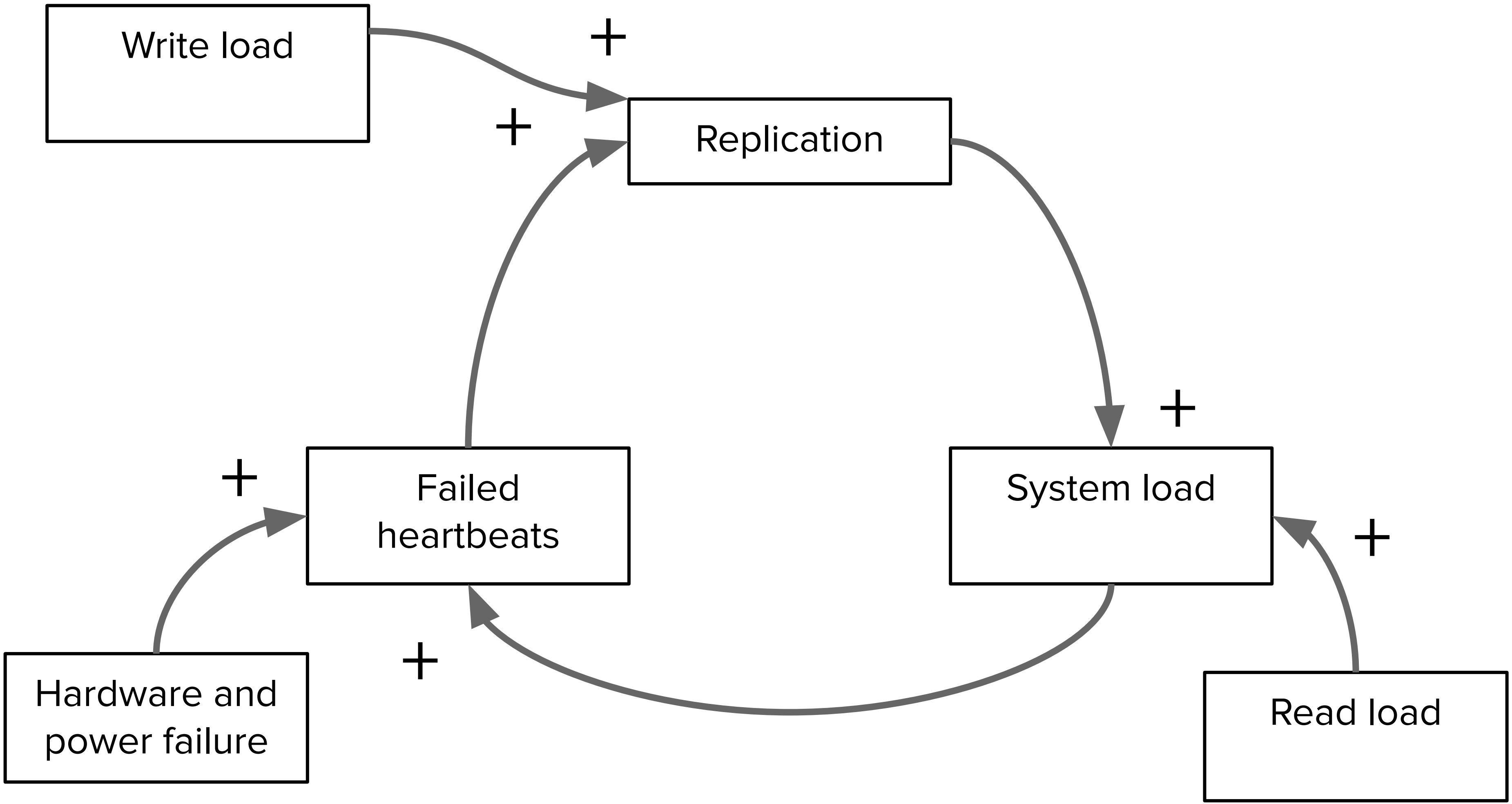


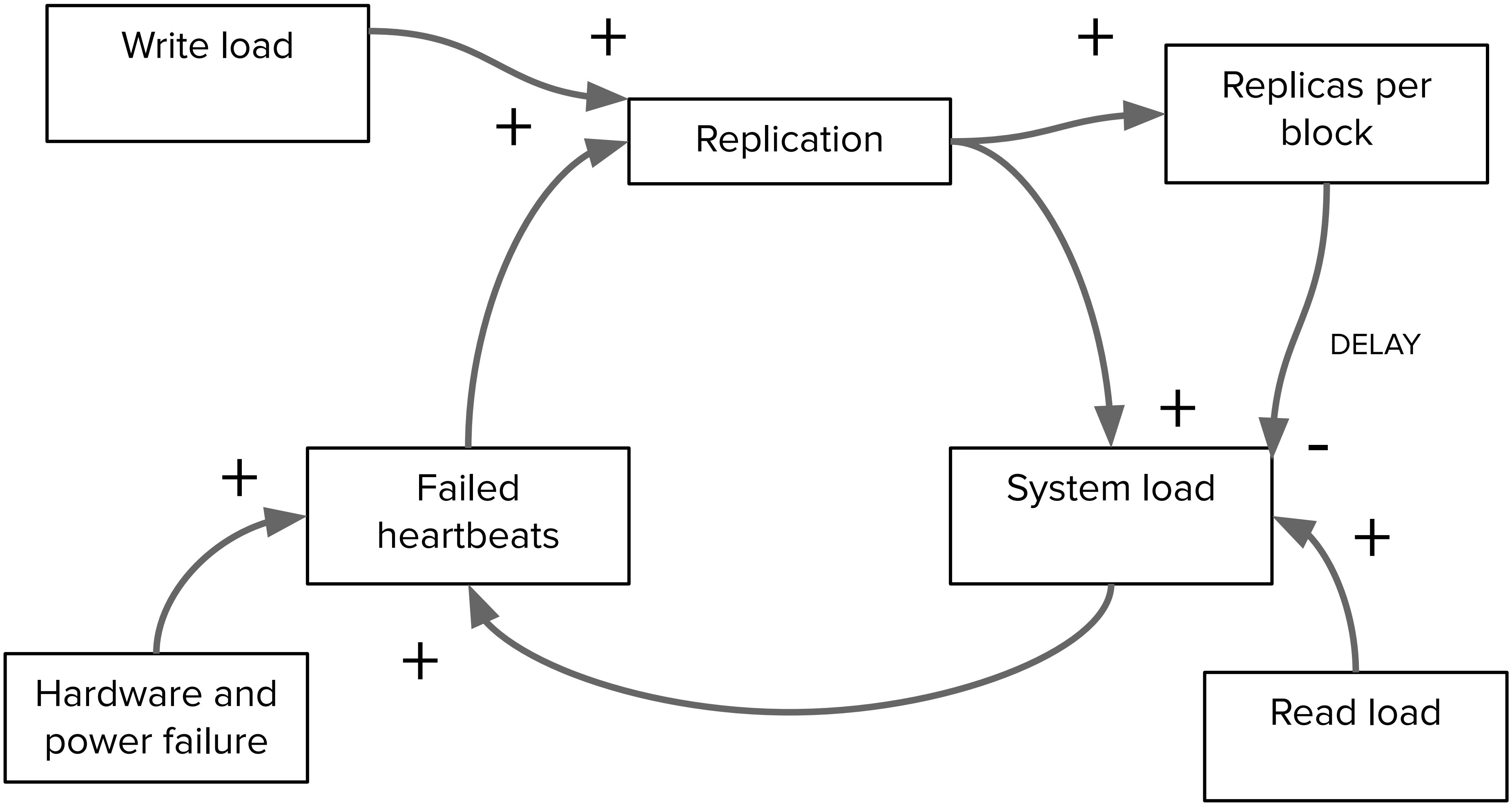
Replication

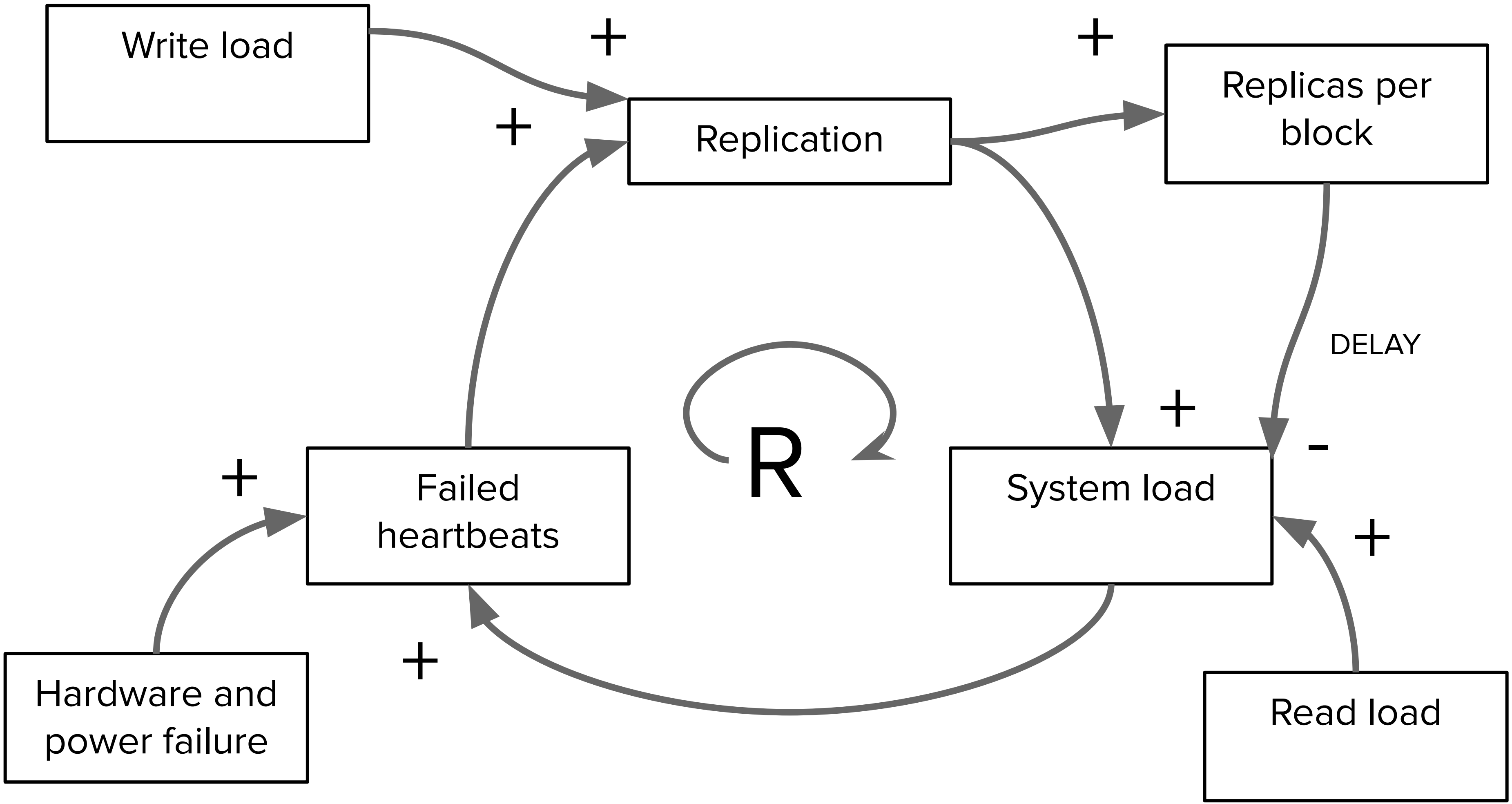
System load

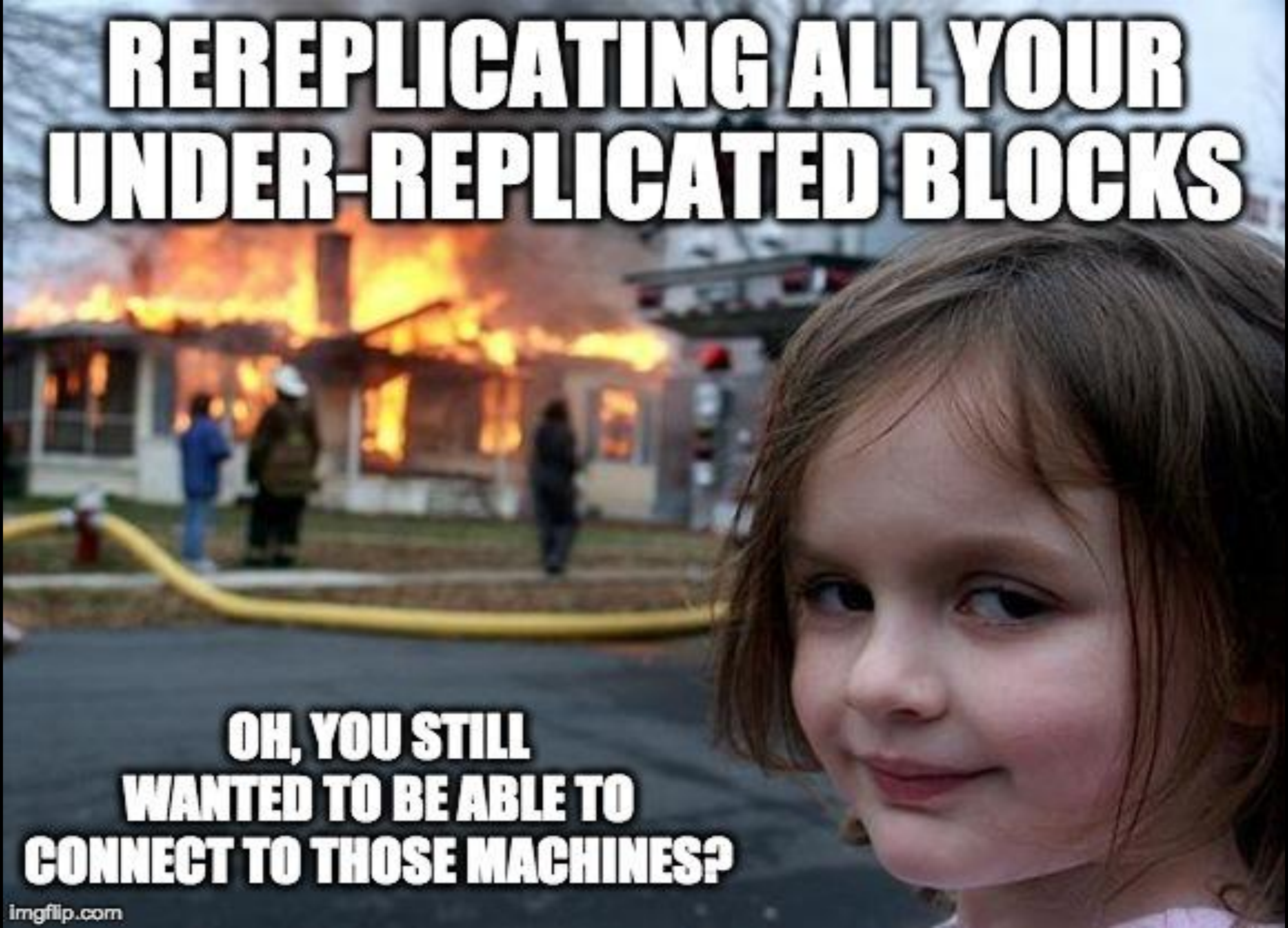
Failed heartbeats


+
Replication
+
Failed heartbeats
System load
+

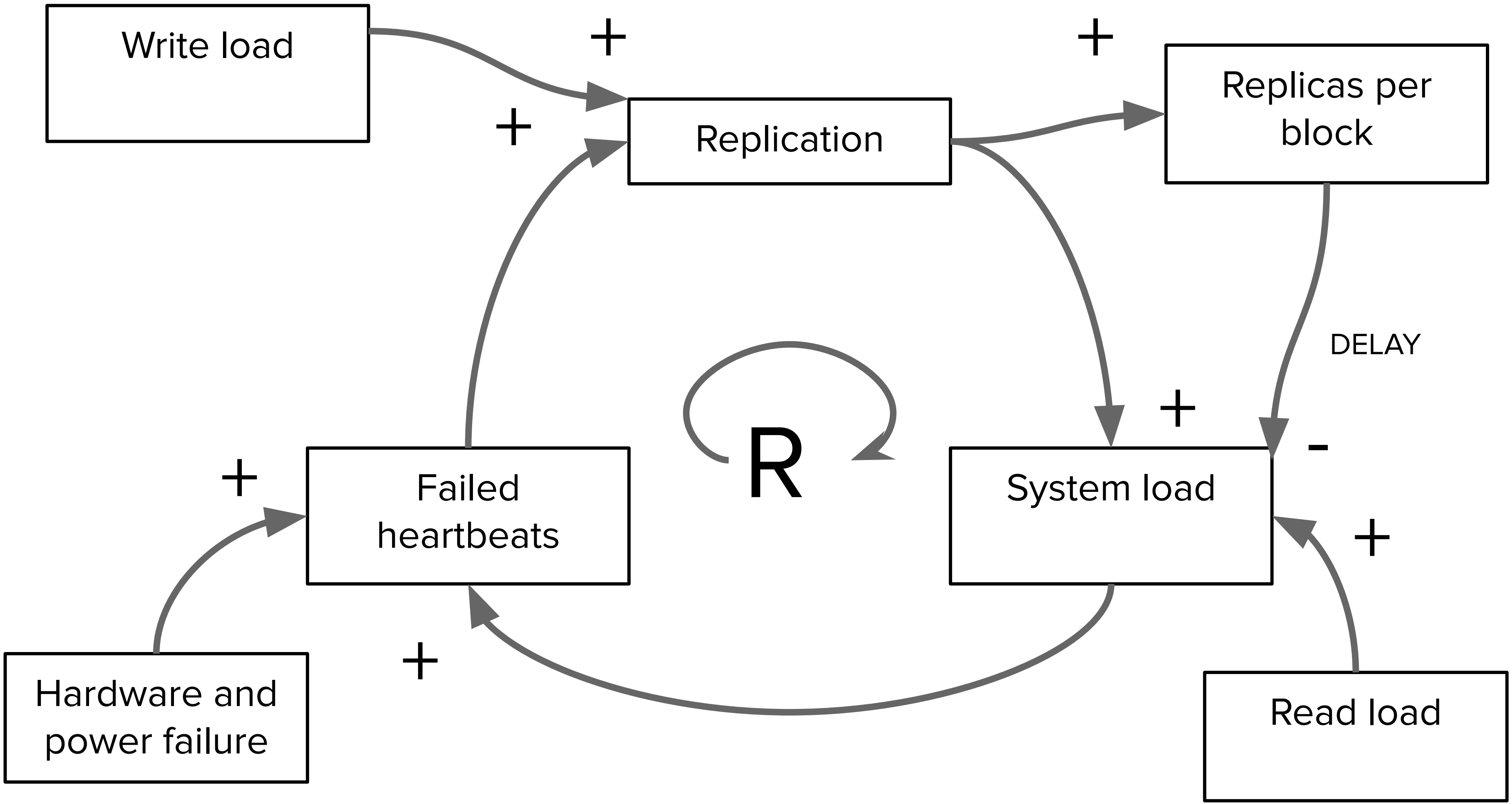

Write load
+
+
Replication
+
Failed heartbeats
System load
+
+
+
Hardware and power failure
Read load


Write load
+
+
Replication
+
Replicas per block
DELAY
+
-
Failed heartbeats
+
System load
+
+
Hardware and power failure
Read load


Write load
+
Replication
+
Replicas per block
+
DELAY
R
Failed heartbeats
+
+
System load
-
+
Hardware and power failure
+
Read load



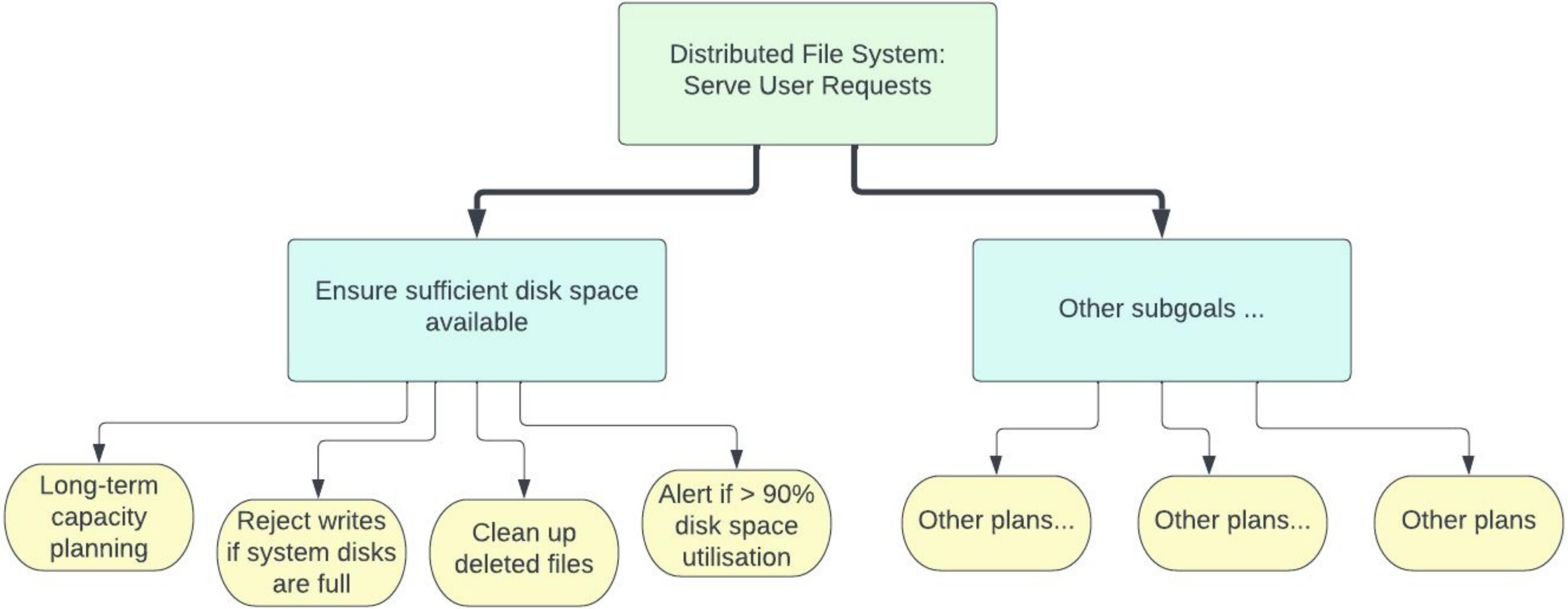
REREPLICATING ALL YOUR UNDER-REPLICATED BLOCKS
OH, YOU STILL WANTED TO BE ABLE TO CONNECT TO THOSE MACHINES?
imgflip.com

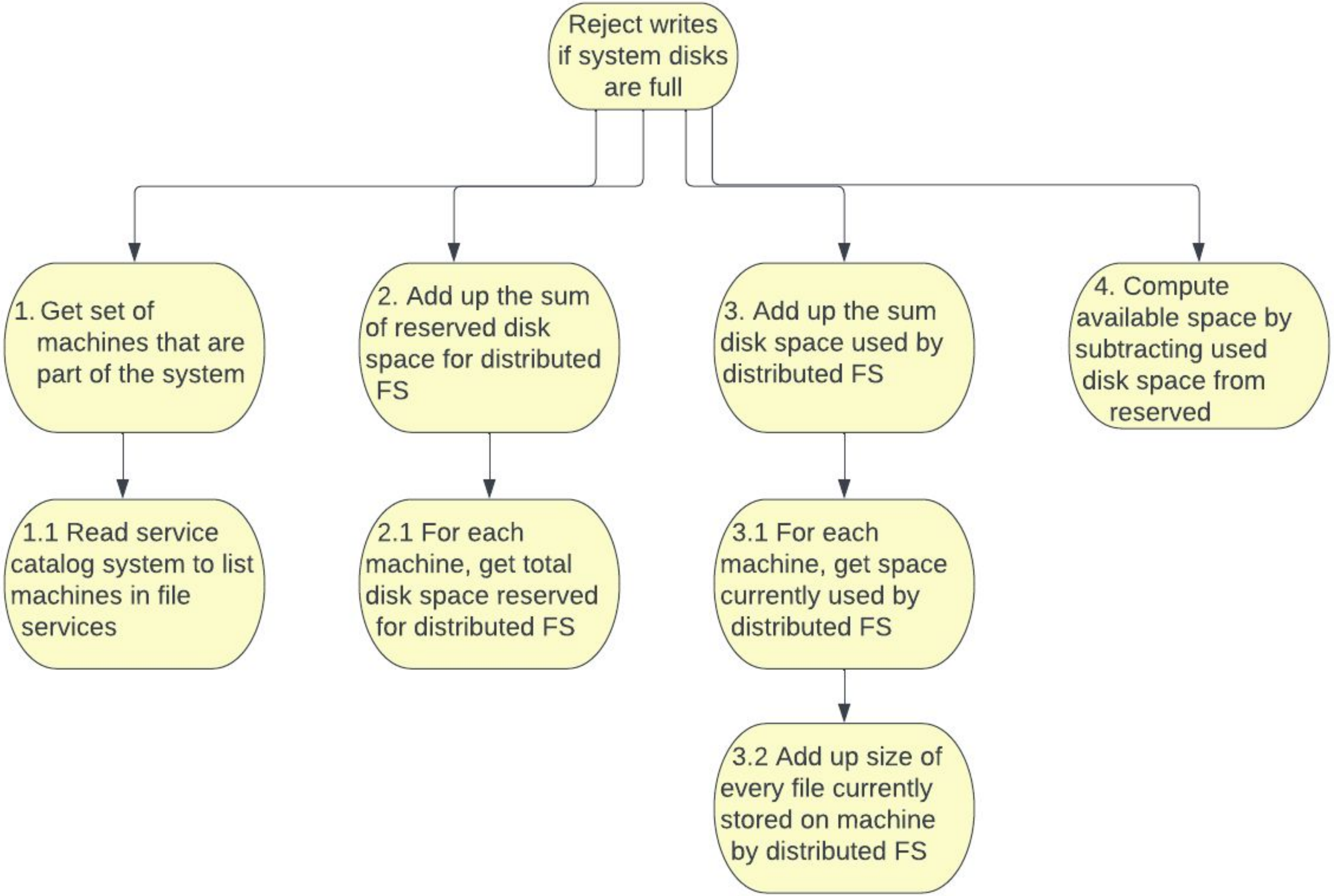


Write load
+
+
Replication
+
Replicas per block
DELAY
+
-
System load
R
+
Failed heartbeats
+
+
Read load
Hardware and power failure

Describing Systems: Hierarchical Task Analysis

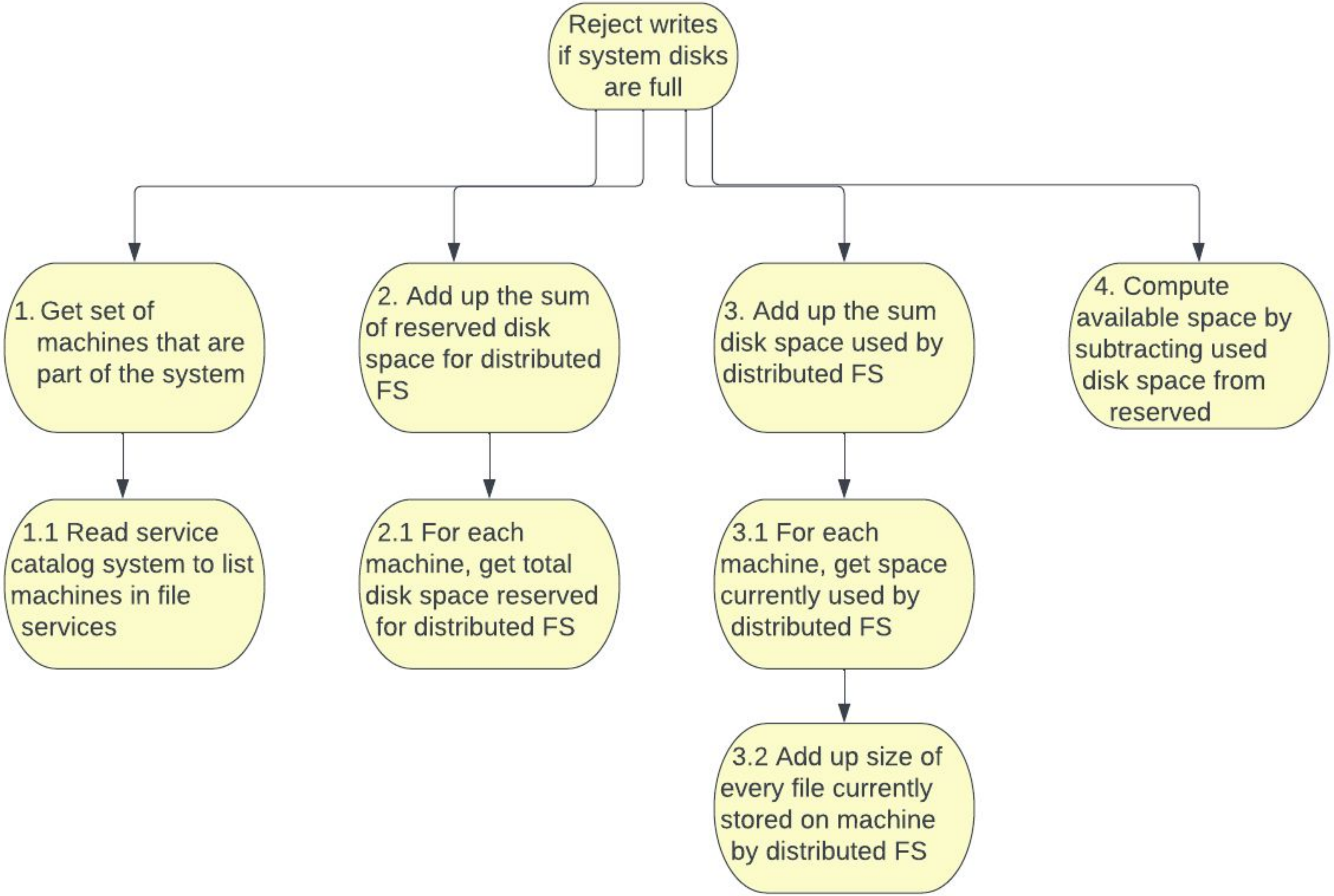
- Decompose systems into goals, subgoals, operations, and plans
- Very flexible way to describe systems, including machine and human parts
- HTA descriptions are inputs to other systems analysis techniques

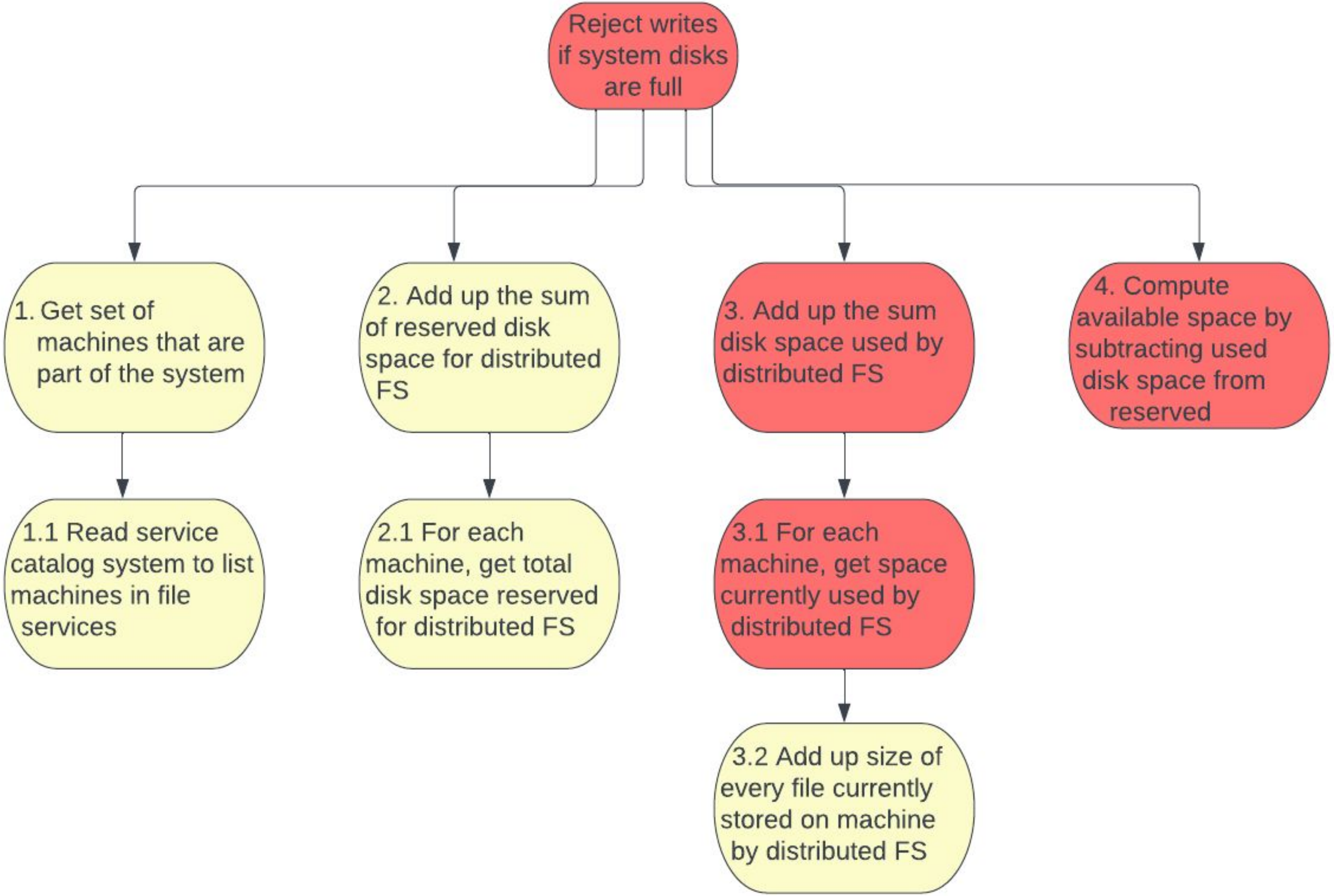

Distributed File System: Serve User Requests
Ensure sufficient disk space available
Other subgoals ...
Long-term capacity planning
Reject writes if system disks are full
Clean up deleted files
Alert if > 90% disk space utilisation
Other plans...
Other plans...
Other plans


Reject writes if system disks are full
1. Get set of machines that are part of the system
2. Add up the sum of reserved disk space for distributed FS
3. Add up the sum disk space used by distributed FS
4. Compute available space by subtracting used disk space from reserved
1.1 Read service catalog system to list machines in file services
2.1 For each machine, get total disk space reserved for distributed FS
3.1 For each machine, get space currently used by distributed FS
3.2 Add up size of every file currently stored on machine by distributed FS

EAST-BL: Event Analysis of Systemic Teamwork - Broken Links

- Starts with a HTA
- What would happen if each link were broken?
  - Not necessarily broken network connectivity: we mean inability to do the needed coordination

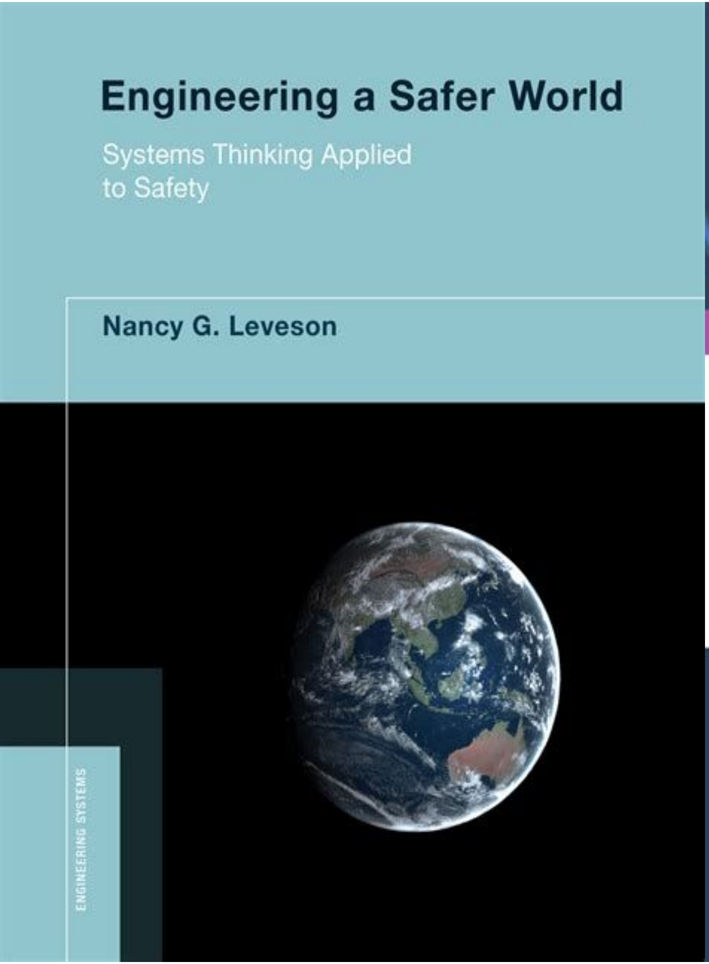

Reject writes if system disks are full
1. Get set of machines that are part of the system
2. Add up the sum of reserved disk space for distributed FS
3. Add up the sum disk space used by distributed FS
4. Compute available space by subtracting used disk space from reserved
1.1 Read service catalog system to list machines in file services
2.1 For each machine, get total disk space reserved for distributed FS
3.1 For each machine, get space currently used by distributed FS
3.2 Add up size of every file currently stored on machine by distributed FS


Reject writes if system disks are full
1. Get set of machines that are part of the system
2. Add up the sum of reserved disk space for distributed FS
3. Add up the sum disk space used by distributed FS
4. Compute available space by subtracting used disk space from reserved
1.1 Read service catalog system to list machines in file services
2.1 For each machine, get total disk space reserved for distributed FS
3.1 For each machine, get space currently used by distributed FS
3.2 Add up size of every file currently stored on machine by distributed FS

Use the tools that make the most sense for your problem

123

Image: Mstyslav Chernov
CC-BY SA 3.0

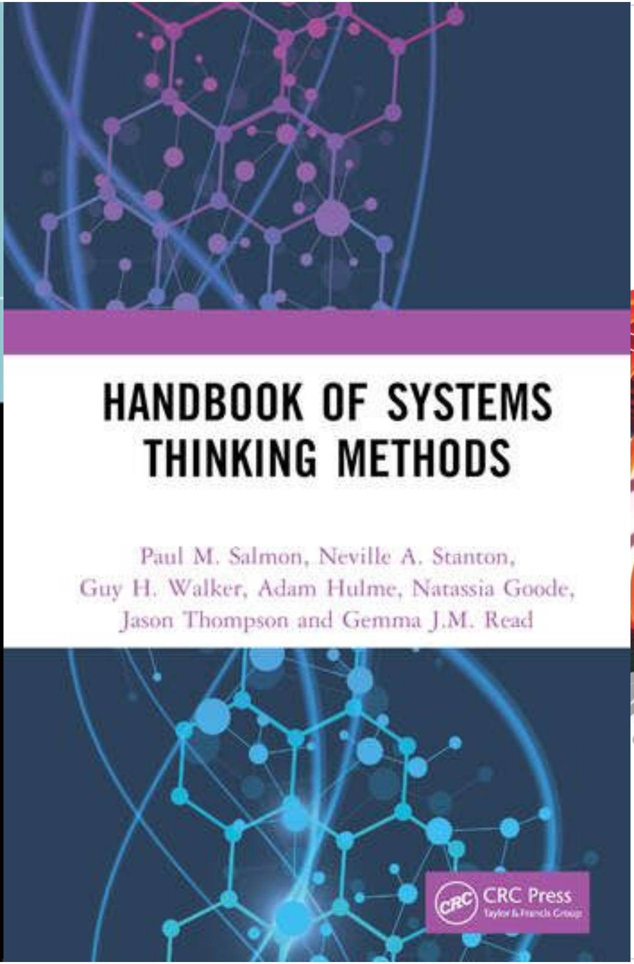


Engineering a Safer World

Systems Thinking Applied
to Safety

Nancy G. Leveson

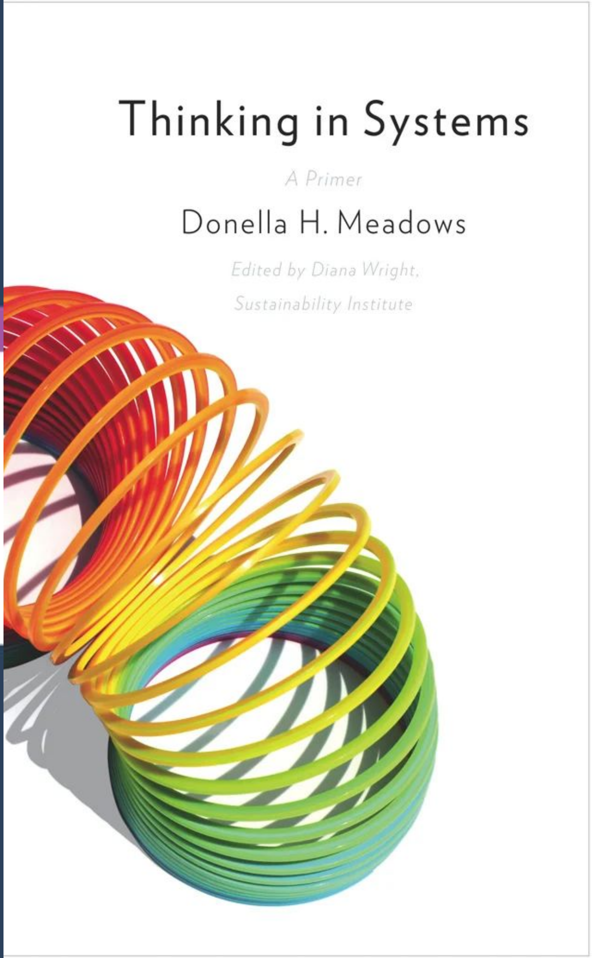
ENGINEERING SYSTEMS



HANDBOOK OF SYSTEMS
THINKING METHODS

Paul M. Salmon, Neville A. Stanton,
Guy H. Walker, Adam Hulme, Natassia Goode,
Jason Thompson and Gemma J.M. Read

CRC Press
Taylor & Francis Group



Thinking in Systems

A Primer

Donella H. Meadows

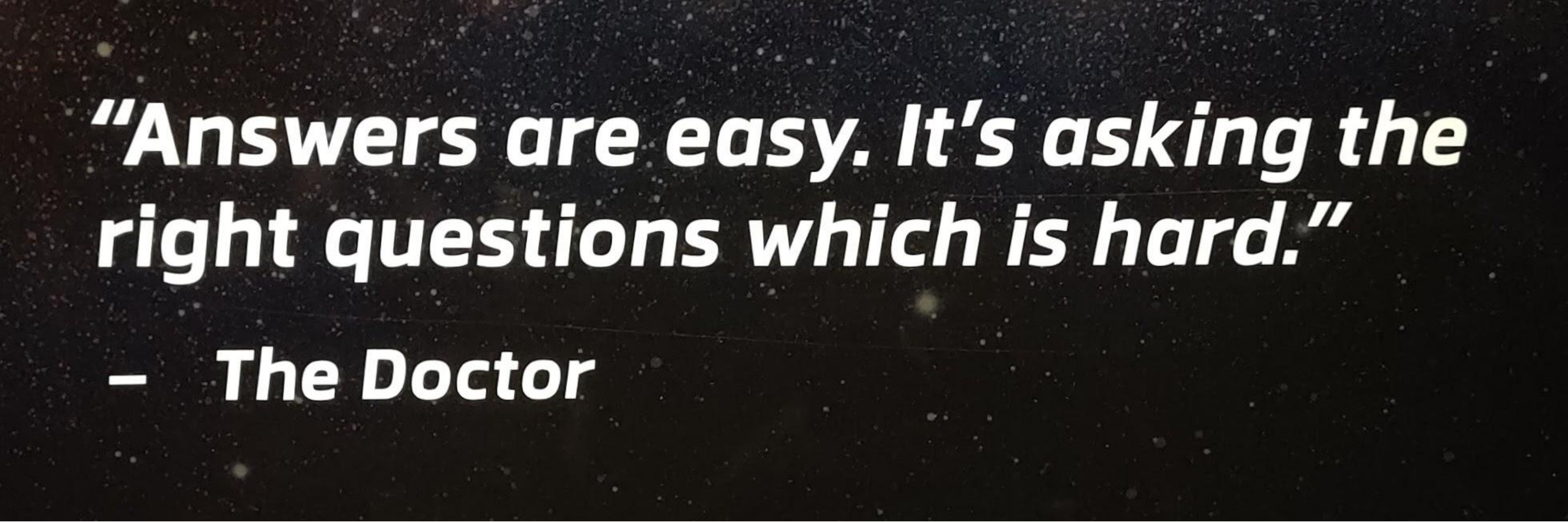
Edited by Diana Wright,
Sustainability Institute

OpenLearn Home Free courses Subjects For Study For Life Help

Free course

Mastering systems thinking in practice

Free statement of participation on completion



“Answers are easy. It’s asking the right questions which is hard.”

– The Doctor

Find me at: laura.nolan@gmail.com

For more on Stanza load management and isola

https://www.stanza.systems/contact

stanza