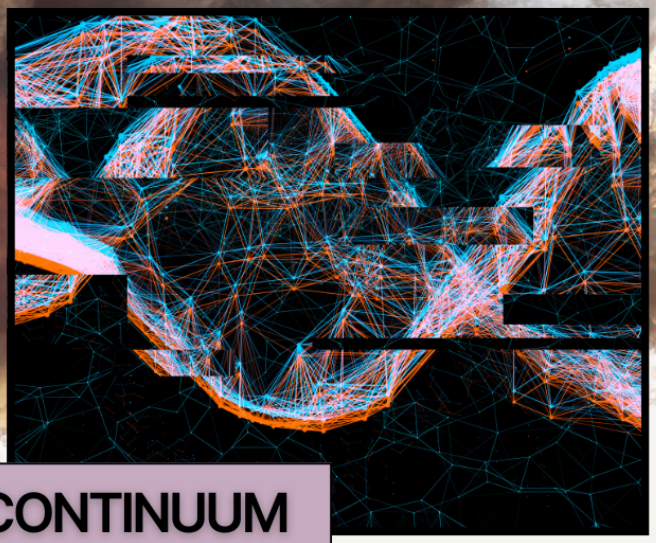
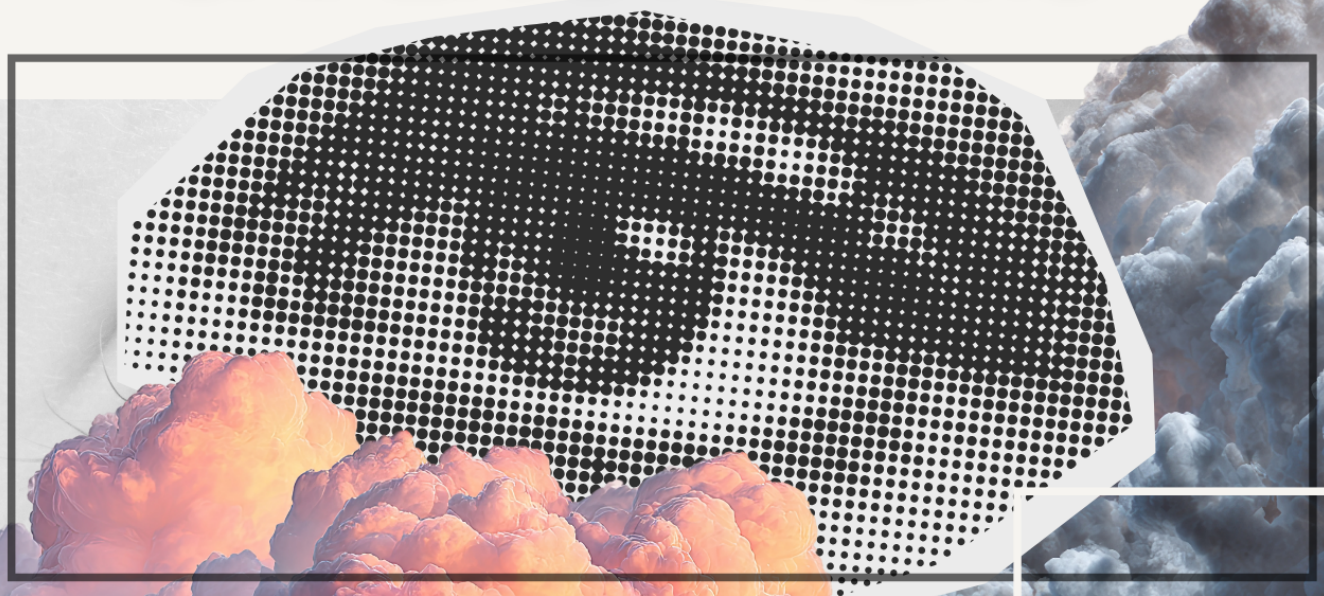


THE SAFETY CONTINUUM

FROM DRY RUN TO DIGITAL TWINS

A GUIDE TO BUILDING SAFER SYSTEMS



BOOK ONE: MECHANICS OF SAFETY

CURTIS COLLICUTT

The Safety Continuum

From Dry-Run to Digital Twins: A Guide to Building Safer Systems

---

Book One - Mechanics of Safety

By Curtis Collicutt

Table of Contents

About this Guidebook

Introduction

This series of guidebooks is intended as a practical introduction to systems safety in software operations. This discipline, “systems safety”, is concerned not only with preventing failures, but also with empathising with operations staff, software developers, system architects, and system designers, whatever their titles are, whatever work they are doing, and with helping them to make systems safer. Drawing from the invaluable work done by researchers and creators-alike in areas such as human factors and reliability, it's written for people who use and build tools to make their day-to-day work safer and better. If you design systems and the operational tools and protocols that support them, this guidebook is for you. If this guidebook allows just a single person to miss one 3AM pager notification, then it was worth it!

However, as a practical guide it's not intended to be an encyclopaedia of every existing safety model, and instead it's intended as an introduction. Rather than conducting an exhaustive search, we present a continuum: a structured approach to considering safety as an emergent property of design. This continuum ranges from simple confirmation prompts and dry runs to record-and-replay, formal verification, and adaptive self-governance. Throughout, we try to consider all major issues and caveats.

This field guide is about moving faster by being safer. Rather than providing final answers, it offers a loose framework and a shared language to help readers identify patterns that make safety visible, testable and learnable. Readers can review the continuum and make informed decisions about their next steps.

Book One: Mechanics of Safety

The Safety Continuum is a two volume series, consisting of *Book One* and *Book Two*.

In this first volume, Book One, we explore the fundamental principles of system safety and examine how safety emerges from complex software systems. Specifically, we consider how safety can be designed into systems not only through the implementation of safety mechanisms, but also by having empathy for not only ourselves, and our future selves, but others operating these complex systems. We start where most operational practitioners are: in the world of configuration, deployment and day-to-day operation. We treat safety as an operational property that emerges from the human-in-the-loop mechanism created and implemented by designing systems and tools with safety in mind.

Book One covers the following areas. Note that these sections will be covered more in detail as to their contents in this guidebook.

Safety Continuum Level	Sections
0-7	Planning and Execution
8-10	Simulation and Rehearsal

Book Two proceeds into more advanced and autonomous safety (levels 11 through 18).

Safety Continuum Level	Sections
11-14	Verification and Resilience
15-18	Scale, Autonomy, and Meta-level Governance