

Roadmap to Secure Data Centers

Steve Comer and Dr. William “Dollar” Young, PhD

March 26, 2026



GLOBAL AND EMERGING RISKS

Applying STPA: Security Strategy & Conceptual Engineering in the Real World (Building Blocks)

Leveson & Young

viewpoints

DOI:10.1145/2556938 William Young and Nancy G. Leveson

Inside Risks
An Integrated Approach to Safety and Security Based on Systems Theory
Applying a more powerful new safety methodology to security risks.

Control room of a nuclear power plant.

The Relationship Between Safety and Security
Practitioners have traditionally treated safety and security as different system properties. Both communities generally work in isolation using their respective vocabulary and frameworks. Safety experts see their role as preventing issues due to unintentional actions by benevolent actors. Security experts see their role as preventing losses due to intentional actions by malevolent actors. The key difference is the intent of the actor that produced the loss event. It may never be possible to determine this intent—but if the majority of our energy and analysis is refocused on building better loss prevention strategies (regardless of actor intent), then it may not matter. We are not suggesting that intent need not be considered, only that the problem can be reframed as a general loss prevention problem that focuses on the aspects of the problem (such as the system design) that we have control over rather than immediately jumping to

FEBRUARY 2014 VOL. 37 NO. 2 COMMUNICATIONS OF THE ACM 31

Hillman

A Systems-Theoretic Approach to Design of Early Concepts for Novel, Complex Systems in Aerospace
by
Alexander P. Hillman
Major, United States Air Force

B.S. Economics, The United States Air Force Academy, 2011
M.S. Operations Research, Air Force Institute of Technology, 2013
M.S. Systems Engineering, Air Force Institute of Technology, 2016
M.S. Flight Test Engineering, U.S. Air Force Test Pilot School, 2017
M.A. Military Operational Air & Sciences, Air University, 2021

Submitted to the Department of Aeronautics and Astronautics in Partial Fulfillment of the Requirements for the Degree of
DOCTOR OF PHILOSOPHY IN AERONAUTICS AND ASTRONAUTICS
at the
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
NOVEMBER 2024

©2024 Alexander P. Hillman. All rights reserved.
The author hereby grants to MIT a non-exclusive, worldwide, irrevocable, exclusive license to exercise any and all rights under copyright, including to reproduce, process, distribute, and publicly display copies of the thesis, or release the thesis under an open-access license.

Author: Alexander P. Hillman
Department of Aeronautics and Astronautics
21 November, 2024

Certified by:
Nancy G. Leveson
Jerome C. Hunsaker Professor in Aeronautics and Astronautics
Thesis Committee Chair

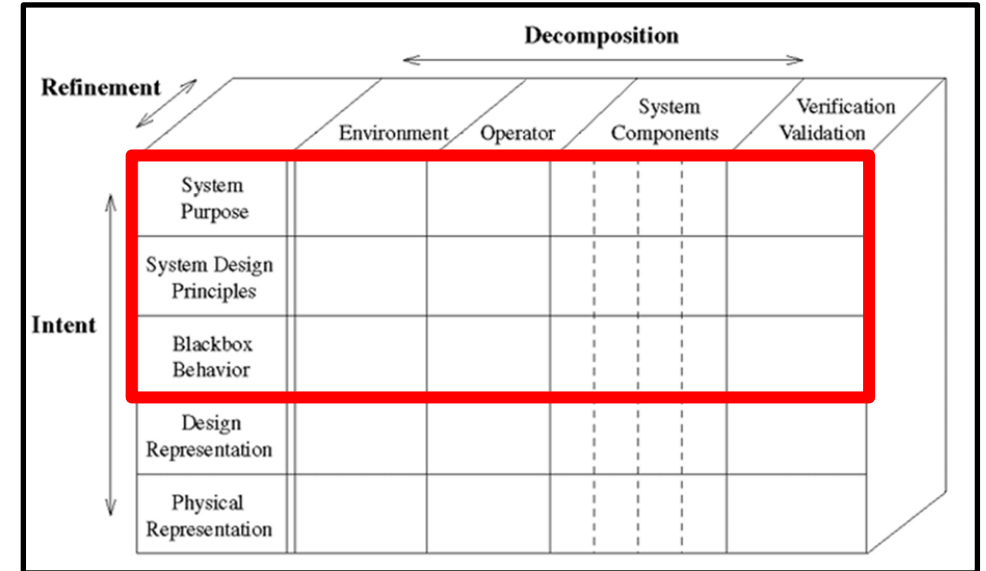
Sheila M. E. Wildall
Institute Professor Emerita, Department of Aeronautics and Astronautics
Thesis Committee Member

John P. Thomas
Research Engineer, Department of Aeronautics and Astronautics
Thesis Committee Member

William E. Young
PhD, Colonel, U.S. Air Force (Retired)
Thesis Committee Member

Accepted by:
Jonathan P. How
R. C. Maclaurin Professor of Aeronautics and Astronautics Chair
Graduate Program Committee

Leveson

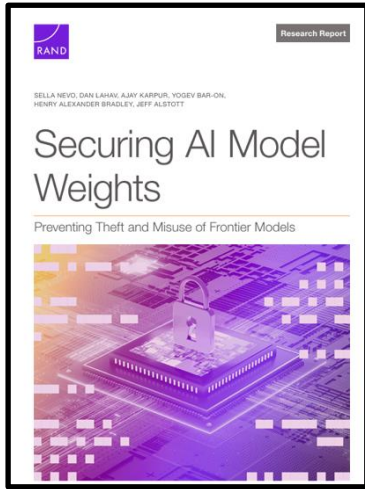


- “Strategy” for Security
- Loss-Driven Engineering

- System-Theoretic Concept Development (STCD)

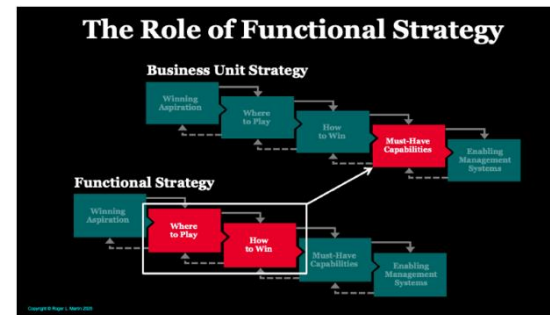
- Intent Specification

Our Challenge: Secure an AI Data Center Against Loss from Nation-State Threat Actor



- Mission vs protection
- Trades

System Availability
Stack & Connectivity
Design Approach
Material Flow
Human Presence



Tactics

- Threat First
- Technical Controls-based
- Design Choice Assessment

Strategy

- Goals and Losses First
- Socio-Technical Constraints
- Design Choice Guidance (Proactive)

Our Approach

- What we did
 - 1: Process steps + generic architecture
 - 2: Aggressive pruning of unnecessary steps and features
 - 3: Define controller behavior and required constraints
 - Refine; repeat

- Detailed trades

<u>Topic</u>	<u>Decision</u>
• System Availability	Delay-tolerant, intermittent
• Stack & Connectivity	Fixed software, no networking
• Design Approach	Custom, special-purpose
• Material Flow	Restricted physical inputs
• Human Presence	Minimal on-site presence

Insights

- C-Suite Executive
 - Align on strategy to create options and resolve tensions, save money and execute quickly (2 days vs 2 months)
- Chief Engineer
 - Possible to balance conflicting security and usability demands
 - Unlocking top three levels of IntentSpec enabled architecture-agnostic design choices (data center as “factory”)
- Security Practitioner
 - “General purpose + controls” approach has limited upside
 - Resolved security debates with user needs in context (long-wire)
- Overall
 - Generalized but accurate refinement only possible with SMEs
 - Significant STPA process off-roading requires a facilitator

Questions?

Executive feedback:

“Why STPA? It's a research methodology that enables us to get from security goals and assumptions to concrete plans and assurances more systematically and effectively than other methodologies I've seen.”

“This is a novel, effective approach and a unique application of relevant tools.”

Steve Comer
scomer@rand.org

Dr. William “Dollar” Young, PhD
william.young@scasdconsulting.com



GLOBAL AND EMERGING RISKS