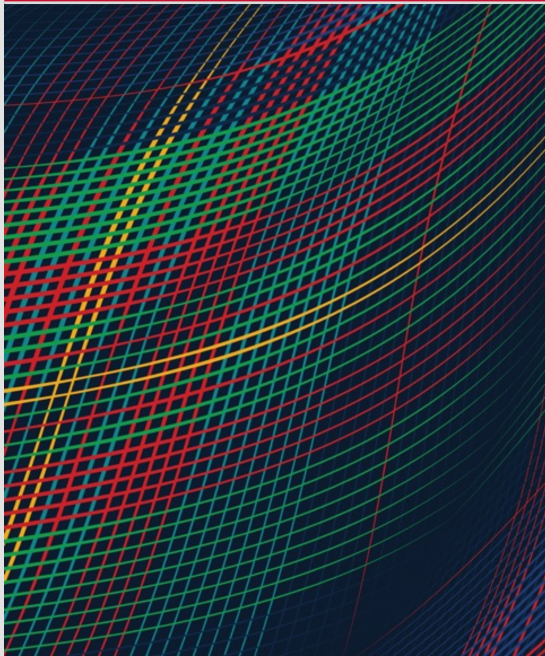
Carnegie Mellon University Software Engineering Institute

Is a Safety-First Cyber-Security Approach Feasible? Will it be Effective?

MAY 12, 2023

Sam Procter



Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM23-0475

Agenda

- Effects-Based Reasoning
- Guidewords
- Speaking the Language of Security

Is a Safety-First Cyber-Security Approach Feasible? Will it be Effective?

Effects-Based Reasoning

Carnegie Mellon University Software Engineering Institute

Effects-Based Reasoning

History and Explanation

“The CFEM organizes diverse fault categories into a cohesive framework by classifying faults according to the effect they have on the required system services rather than by targeting the source of the fault condition.”

“The customizable fault/error model for dependable distributed systems” C.J. Walter, N. Suri. Theoretical Computer Science, 2003.

“The AADL Error Library: An Operationalized Taxonomy of System Errors” Sam Procter, Peter Feiler. HILT 2018.

Usage

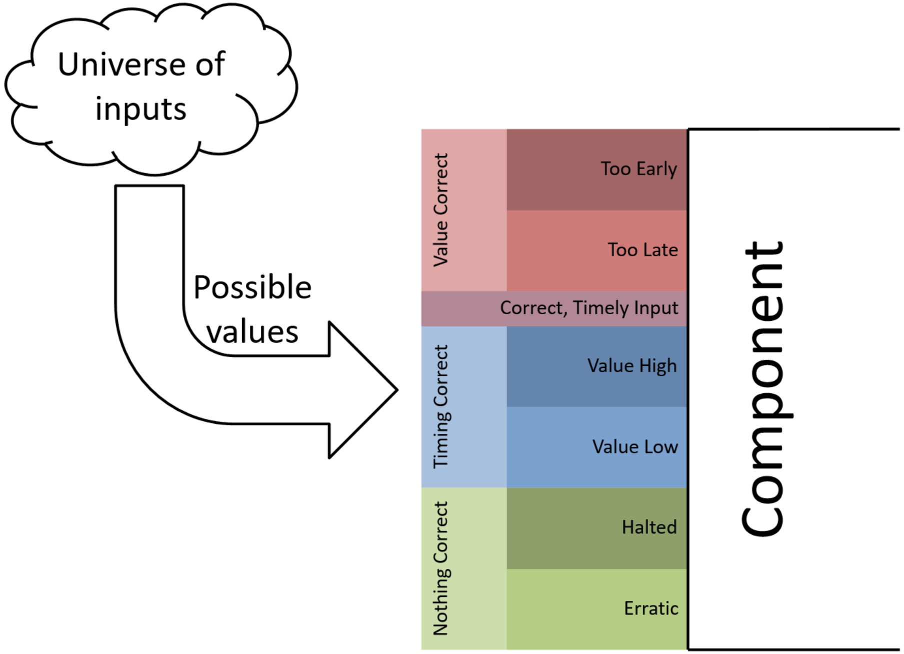
- Aligns well with top-down analyses
- Used by AADL’s EMV2 library

What

- Number of error *causes* are unbounded and may be unknowable
- Error’s *effects* are (commonly) statically determinable and tightly bounded

Effects-Based Reasoning

Error *causes* are effectively unbounded, error *effects* can be bounded



"A Development and Assurance Process for Medical Application Platform Apps" Sam Procter. PhD Dissertation, Kansas State University, 2016.

"SAFE and Secure: Deeply Integrating Security in a New Hazard Analysis" Sam Procter, Eugene Y. Vasserman, John Hatcliff. SAW 2017.

Why

- Merges safety and security concerns
  - … does it matter *why* an input is malformed?
- Reduces analysis space*
  - * barring pathological errors
- Increases compositionality / locality
  - Does it matter *who* sent malformed input?
- Reduces ambiguity
- Better aligns with formal methods
  - Provides a notion of completeness, cf "Assumption Synthesis"

"Composing Safe Systems" John Rushby. FACS 2011.

Is a Safety-First Cyber-Security Approach Feasible? Will it be Effective?

Guidewords

The Role of Guidewords

Guidewords are:

- “Baked into” many popular hazard analyses
- Fairly intuitive / don’t require a great deal of training
- Also conceivable as a taxonomy (Avižienis, Laprie) or attacker model (Dolev-Yao)

Guidewords used in hazard analysis help dictate the failure modes considered by analysts

Guideword Comparison

Concept	Avižienis et al	STPA	Dolev-Yao
Early Message	Early Arrival	Providing	Craft New & Send
Late Message	Late Arrival	Late	Delay
High Value	Value High	None*	Modify Existing
Low Value	Value Low	None*	Modify Existing
Service Stop	Halted	Fails to Provide	Drop
Babbling Idiot	Erratic	Providing	Craft New & Send
Confidentiality Violation	[In security attributes]^	None	Read

"SAFE and Secure: Deeply Integrating Security in a New Hazard Analysis" Sam Procter, Eugene Y. Vasserman, John Hatcliff. SAW 2017.

"Basic Concepts and Taxonomy of Dependable and Secure Computing" Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, Carl Landwehr. IEEE TDSC, 2004.
^ confidentiality is present as a security attribute, Procter et al used dependability attributes exclusively.

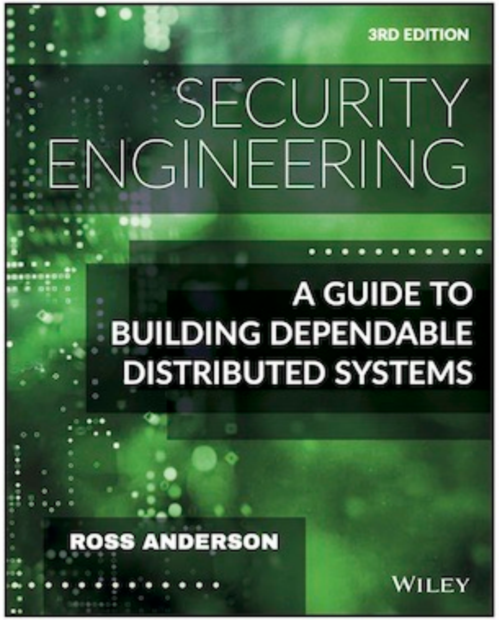
"Engineering a Safer World" Nancy Leveson, MIT Press, 2011.
** added in subsequent work*

"On the security of public key protocols" Danny Dolev, Andrew Yao. IEEE Trans on Information Theory, 1983.

Is a Safety-First Cyber-Security Approach Feasible? Will it be Effective?

Speaking the Language of Security

Speaking the Language of Security



© Wiley

“At the heart of both safety engineering and security engineering lie decisions about priorities: how much to spend on protection against what.”

It is the hierarchical structure and organization that I argue:

- Safety can offer security
- Should bind the approaches
- Safety experts should focus on when communicating with security experts

“Lessons from Safety-Critical Systems”

Principles

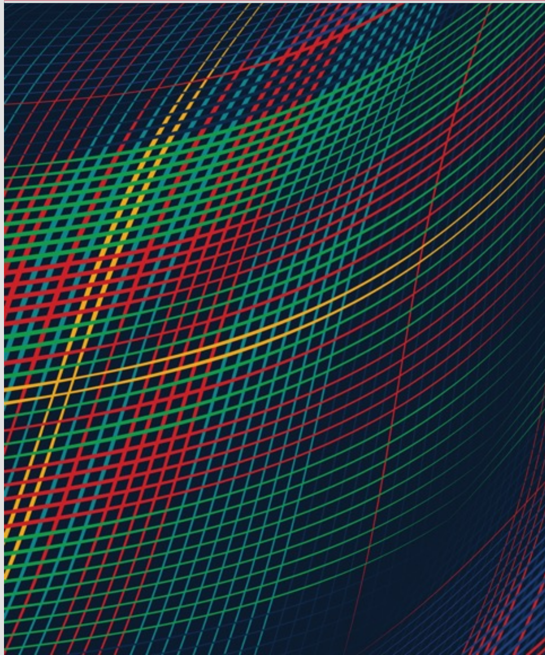
- Guide the system to a safe state when things go wrong
- In an emergency, keep the information presented simple
- Pay attention to fault masking

Safety Analyses Can…

- Identify safe states
- Present information in a human-/user-centered way
- Detect opportunities for fault masking

“Security Engineering.” Ross Anderson. 3rd Edition, Wiley.

Carnegie Mellon University Software Engineering Institute



Is a Safety-First Cyber-Security Approach Feasible? Will it be Effective?

Sam Procter

sprocter@sei.cmu.edu