Prof. Philip Koopman

Carnegie Mellon University

Electrical & Computer ENGINEERING

Safety Plans

"Adventure is just bad planning."
– Roald Amundsen

These tutorials are a simplified introduction, and are not sufficient on their own to achieve system safety. You are responsible for the safety of your system.

Safety Plan: The Big Picture for Safety

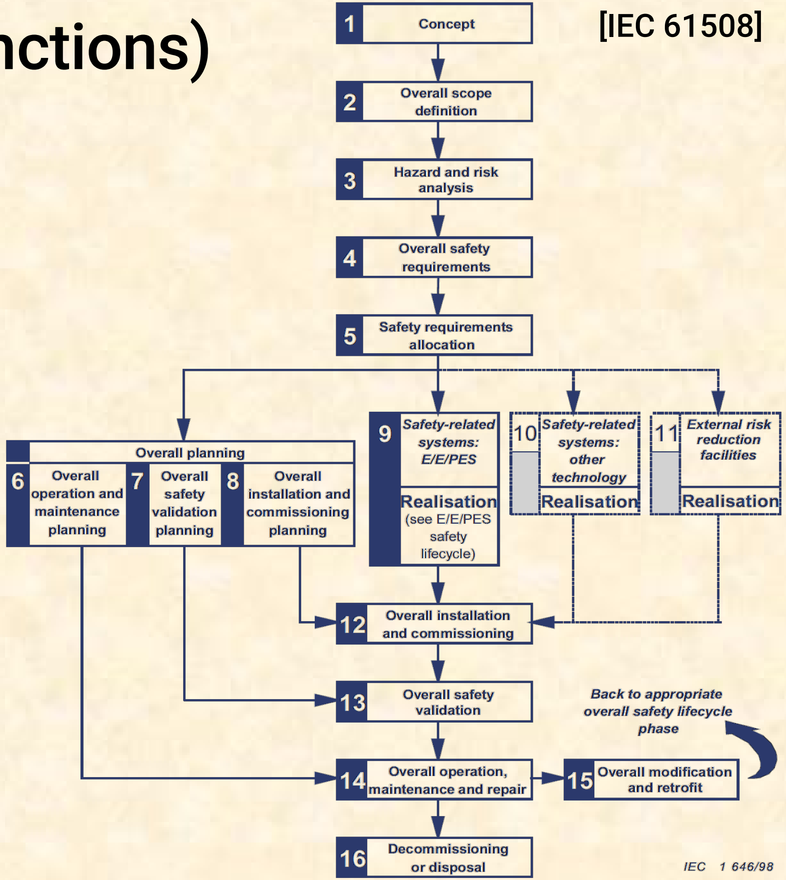
- Anti-Patterns for Safety Plans:
  - It's just a pile of unrelated documents
  - It doesn't address software integrity
  - You don't link to a relevant safety standard
  - It doesn't link to a security plan

- Safety Plan:
  - Safety Standard: pick a suitable standard
  - Hazards & Risks: hazard log, criticality analysis
  - Goals: safety strategy, safety requirements
  - Mitigation & Analysis: HAZOP, FMEA, FTA, ETA, reliability, …
  - Safety Case: safety argument

Safety Standards

- Usually "functional safety" (safety functions)
  - IEC 61508 is a generic starting point
  - Many domains have specific standards
    - ISO 26262, EN-50126/8/9, MIL-STD-882, IEC 60730, DO-178, …
- Key elements of a safety standard:
  - Method for determining risk
    - Usually Safety Integrity Level (SIL)
  - SIL determines engineering rigor
    - Analysis techniques
    - Mitigation techniques
  - Life-cycle approach to safety

[IEC 61508]



Safety Goals & Safety Requirements

- Safety Goal: top level definition of "safe"
  - Example: vehicle speed control
    - Hazard: unintended vehicle acceleration
    - Goal: engine power proportional to accel. pedal position
  - Safety strategy: how you plan to achieve goal
    - Example: correct computation AND
      engine shutdown if unintended acceleration

- Safety Requirements:
  - Goals at system level; requirements provide supporting detail
  - Supporting requirements generally allocated to subsystems
    - Might include functionality and fail-safe mitigation requirements
  - Examples:
    - Engine torque shall match accelerator position torque curve
    - Pedal/torque mismatch shall result in engine shutdown

FMEA: Failure Mode Effects Analysis

Carnegie Mellon University

- Idea: Start with component failure; analyze results; identify hazards

Component	Potential Failure Mode	Failure Effects	Recommended Action	Status
Resistor R2	Open	Triggers Shutdown	Use Industrial spec. component	Done
	Short	Over-current/ potential Fire	Circuit Redesign	Open
Capacitor C7	Explodes	Potential Fire	Select different component	Open

- Significant limitations for generating hazards
  - "Complex component" failures are not well behaved
    - Software fails however it wants to fail
    - Integrated circuits are usually highly coupled internally
  - Poor at representing correlated and accumulated faults
    - E.g., exploding capacitor damaging several nearby components

HAZard and Operability Analysis (HAZOP)

Carnegie Mellon University

- Hazard structured brainstorming
  - For each system requirement:
    - Modify with a guide word
    - Does the result suggest a hazard?
  - Effective starting point, but not guaranteed to find all hazards
- Examples
  - When pressure exceeds 6000 psig, relief valve shall NOT actuate.
  - System shall come to a complete stop ~~within~~ AFTER 5 seconds when emergency stop is activated.
    - Alternately: System shall come to a complete stop ~~within 5 seconds~~ LATE when emergency stop is activated.

Guide Word	Meaning
NO OR NOT	Complete negation of the design intent
MORE	Quantitative increase
LESS	Quantitative decrease
AS WELL AS	Qualitative modification/increase
PART OF	Qualitative modification/decrease
REVERSE	Logical opposite of the design intent
OTHER THAN / INSTEAD	Complete substitution
EARLY	Relative to the clock time
LATE	Relative to the clock time
BEFORE	Relating to order or sequence
AFTER	Relating to order or sequence

https://goo.gl/KTer9C

Hazards & Risks

- Hazard: a potential source of injury or damage
  - A potential cause of a mishap or loss event (people, property, financial)
- Hazard log
  - Captures hazards for a system
  - HAZOP generates some hazards
  - Others are legacy & experience
- Risk evaluation
  - Risk = Probability * Consequence
    - Typically determined via a risk table
  - Risk must be reduced to acceptable levels
    - Risk determines required SIL (e.g. “Very High” ➔ SIL 4)

Probability

Consequence

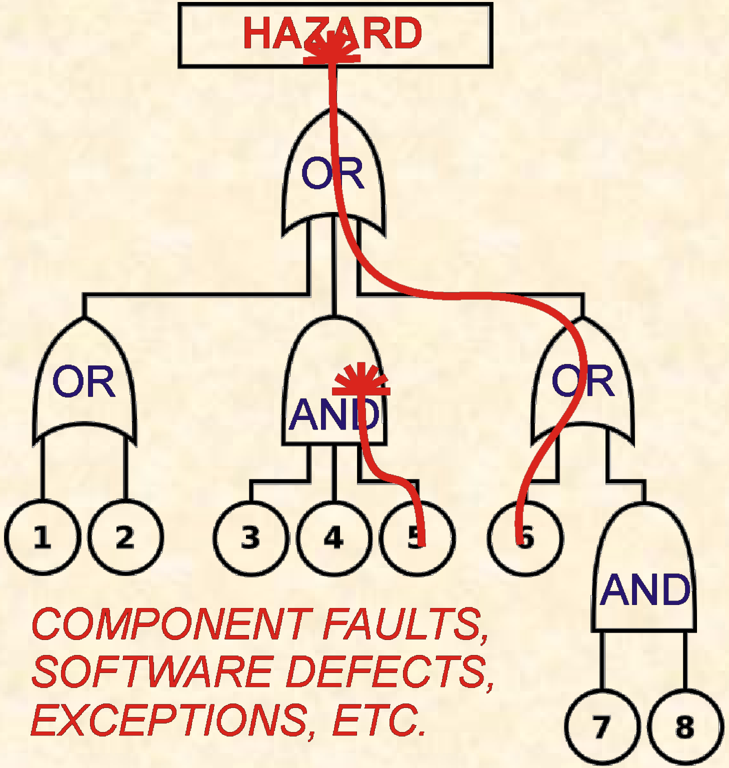
EXAMPLE RISK		Probability: Very High	High	Medium	Low	Very Low
Conse-quence	Very High	Very High	Very High	Very High	High	High
	High	Very High	High	High	Medium	Medium
	Medium	High	High	Medium	Medium	Low
	Low	High	Medium	Medium	Low	Very Low
	Very Low	Medium	Low	Low	Very Low	Very Low

RISK

Safety Analysis & Mitigation

Carnegie Mellon University

- Failure Mode Effects Analysis (FMEA)
  - Work forward from fault to mishap
- Fault Tree Analysis (FTA)
  - Work backward from hazard to causes
  - *Strategy:* HAZOP identifies fault tree roots
- Avoid single points of failure
  - If component breaks, is system unsafe?
  - Computational elements fail in worst way
- Life-critical systems require redundancy
  - Also avoid correlated faults
  - High-SIL software techniques to avoid SW defects

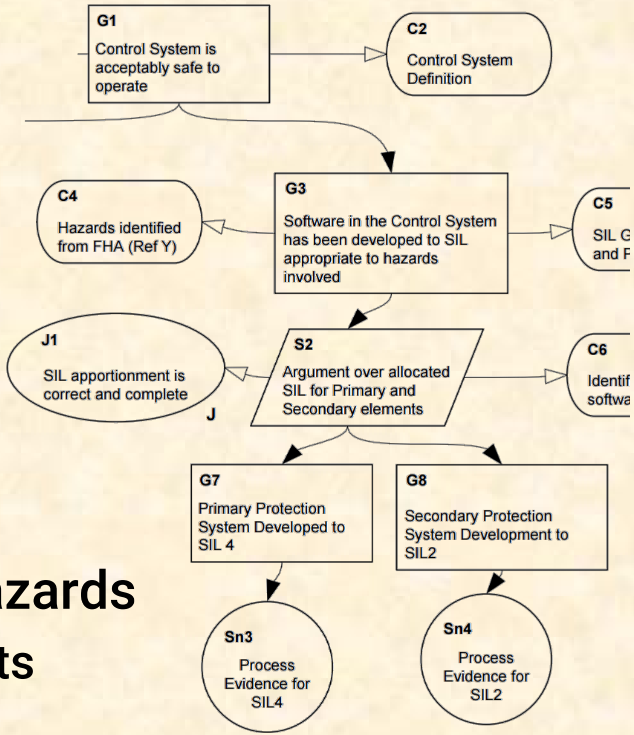


Fault Tree

Safety Case

Carnegie Mellon University

- This system is safe because:
  structured argument + evidence
- Incorporates safety plan topics:
  - Methodical identification of hazards
  - Each hazard evaluated for risk
  - Mitigation rigor determined by risk (e.g., SIL)
  - Analysis rigor determined by risk (e.g., SIL)
  - Safety requirements appropriately cover all hazards
    - Including both accidental faults & malicious faults
- Example techniques
  - Goal Structuring Notation (GSN) http://www.goalstructuringnotation.info/documents/GSN_Standard.pdf
  - Systems-Theoretic Process Analysis (STPA / Leveson)



[GSN Standard]

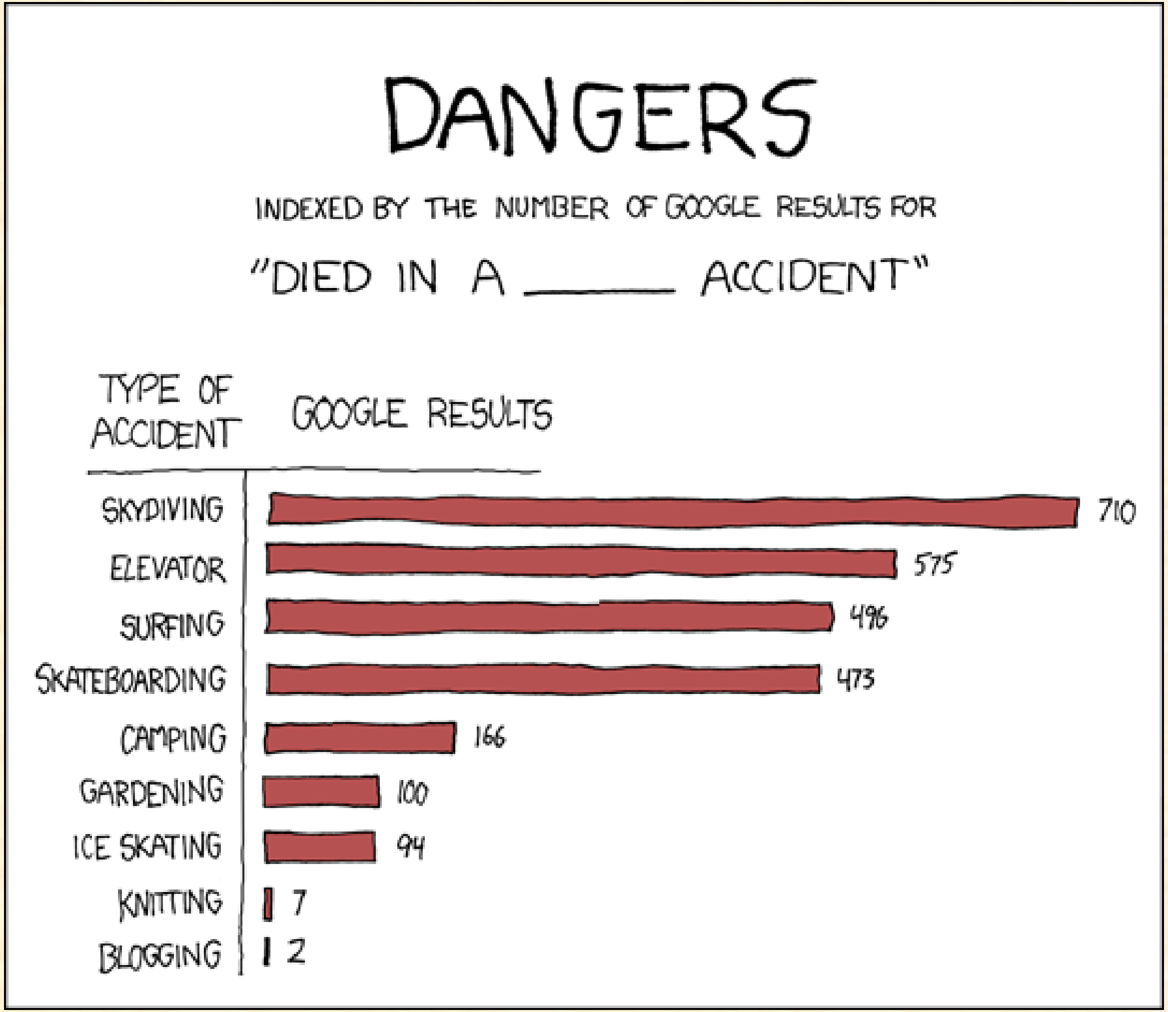
Best Practices For Safety Plans

Carnegie Mellon University

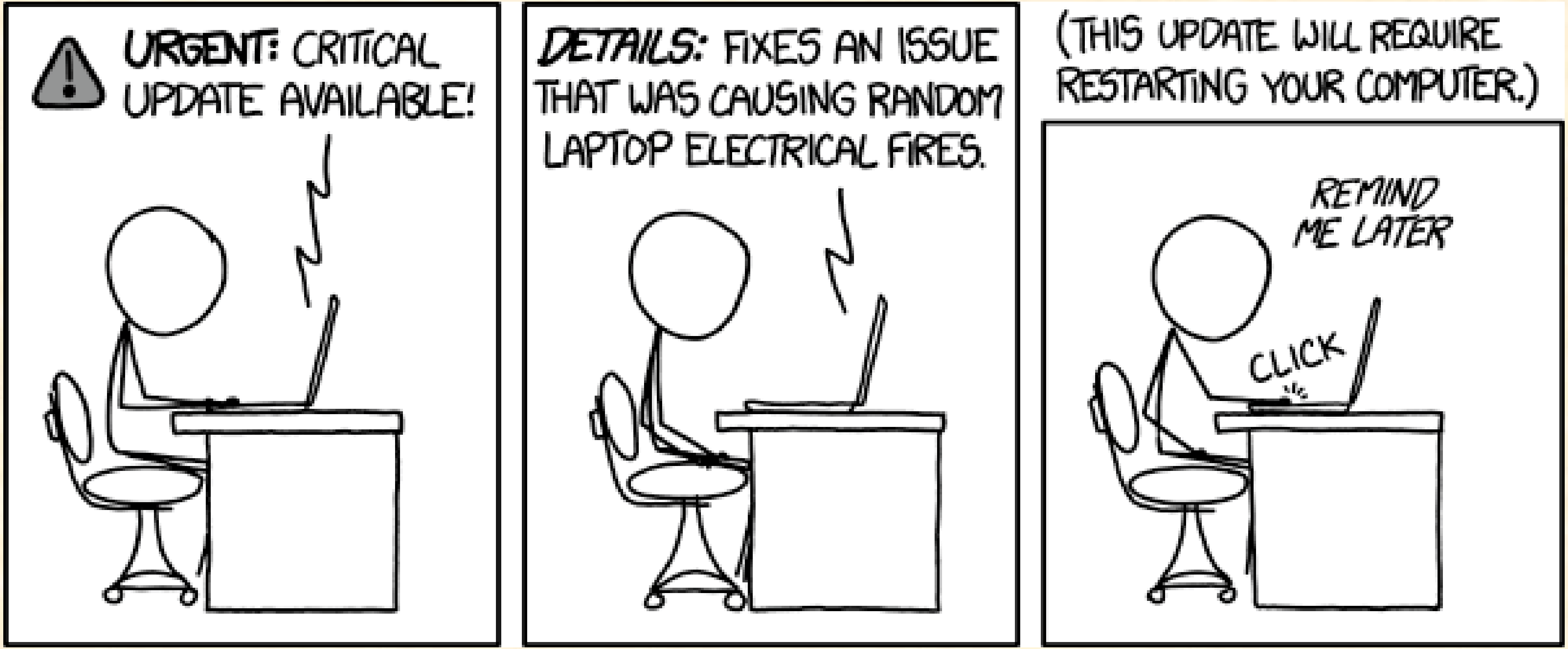
- A written Safety Plan including:
  - Hazards + risks
  - Safety goals + requirements
  - Safety analysis + Mitigation
  - Following a safety standard
  - Resulting in a *written* safety case
  - Independent audit of safety case

https://www.flickr.com/photos/jurvetson/1118807

- Pitfalls:
  - Software safety usually stems from rigorous SIL engineering
  - FMEA can miss correlated & multipoint faults – must use FTA
  - Need to include safety caused by security attacks



https://xkcd.com/369/



https://xkcd.com/1328/