



Prof. Philip Koopman

Critical Systems

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.

“Never tell me the odds!”

— Han Solo

■ Anti-Patterns for Critical Systems:

- You haven't characterized worst case failures
- You haven't assigned SILs to system hazards
- Validation plan doesn't match fleet exposure

■ Critical systems require low failure rates

- SIL = Safety Integrity Level
 - Higher level of integrity needed for higher risk

- **Safety critical:**

Loss of life, injury, environmental damage

- Special care must be taken to avoid deaths

- **Mission critical:**

Brand tarnish, financial loss, company failure

- Consider a safety critical approach

Knicht Capital Says Trading Glitch Cost It \$440 Million

By NATHANIEL POPPER AUGUST 2, 2012 9:07 AM 356 Comments

Runaway Trades Spread Turmoil Across Wall St.



Errant trades from the Knight Capital Group began hitting the New York Stock Exchange almost as soon as the opening bell rang on Wednesday. Brendan McDermid/Reuters

The [Knight Capital Group](#) announced on Thursday that it lost \$440 million when it sold all the stocks it accidentally bought Wednesday morning because a computer glitch.

<https://goo.gl/7dHOj0>

What Is The Worst Case Failure?



- Worst case might not be obvious
 - Aircraft – software can cause a crash
 - Thermostats/HVAC – software can freezing plumbing
 - Can – rarely! – also kill small children due to overheating
- Key thought experiment:
 - What's the worst that can happen if ...
 - ... your system intentionally tried to cause harm?
 - This identifies system hazards to mitigate
- Failure consequence varies, typically:
 - Multiple fatalities (e.g., plane crash)
 - Single fatality (e.g., single-vehicle car crash)
 - Severe injuries
 - Minor injuries
 - Can consider analogies for mission-critical goals

Malfunctioning heater leads to Fort Worth toddler's death



WFAA Channel 8 <https://goo.gl/rFd8qW>

Takeaway: get a baby monitor with temperature sensor

Safety Integrity Level (SIL)

■ SIL represents:

- The risk presented by a system-level hazard
- The engineering rigor applied to mitigate the risk
- The permissible residual probability after mitigation

■ Example: DO-178 (aviation flight hours)

- DAL A (Catastrophic): 10^9 hrs/failure = 114077 years
- DAL B (Hazardous): 10^7 hrs/failure = 1141 years
- DAL C (Major): 10^5 hrs/failure = 11 years
- DAL D (Minor): 10^3 hrs/failure = 42 days

■ Example: IEC 61508 (industrial controls)

- SIL 4: 10^8 hrs/dangerous failure = 11408 years
- SIL 3: 10^7 hrs/dangerous failure = 1141 years
- SIL 2: 10^6 hrs/dangerous failure = 114 years
- SIL 1: 10^5 hrs/dangerous failure = 11 years



https://en.wikipedia.org/wiki/Bhopal_disaster

1984: Bhopal Chemical Plant
Thousands of deaths
(not software related;
pre-dates IEC 61508)

<https://goo.gl/GGHWRn>

Higher SIL Invokes More Engineering Rigor

Example: IEC 61508

- HR = Highly Recommended
- R = Recommended
- NR = Not Recommended (don't do this)

SIL 1: lowest integrity level (low risk)

SIL 4: highest integrity level (unacceptable risk)

Technique/Measure*		Ref	SIL1	SIL2	SIL3	SIL4
1	Fault detection and diagnosis	C.3.1	---	R	HR	HR
2	Error detecting and correcting codes	C.3.2	R	R	R	HR
3a	Failure assertion programming	C.3.3	R	R	R	HR
3b	Safety bag techniques	C.3.4	---	R	R	R
3c	Diverse programming	C.3.5	R	R	R	HR
3d	Recovery block	C.3.6	R	R	R	R
3e	Backward recovery	C.3.7	R	R	R	R
3f	Forward recovery	C.3.8	R	R	R	R
3g	Re-try fault recovery mechanisms	C.3.9	R	R	R	HR
3h	Memorising executed cases	C.3.10	---	R	R	HR
4	Graceful degradation	C.3.11	R	R	HR	HR
5	Artificial intelligence - fault correction	C.3.12	---	NR	NR	NR
6	Dynamic reconfiguration	C.3.13	---	NR	NR	NR
7a	Structured methods including for example, JSD, MASCOT, SADT and Yourdon.	C.2.1	HR	HR	HR	HR
7b	Semi-formal methods	Table B.7	R	R	HR	HR
7c	Formal methods including for example, CCS, CSP, HOL, LOTOS, OBJ, temporal logic, VDM and Z	C.2.4	---	R	R	HR
8	Computer-aided specification tools [IEC 61508]	B.2.4	R	R	HR	HR

Fleet Exposure & Probability

■ Bigger fleets have increased exposure

- 250 Million US vehicles @ 1 hour/day
= $2.5 * 10^8$ hrs/day exposure
- If “unlikely” failures happen every million hours...
that's: $2.5 * 10^8$ hrs / 10^6 hrs per event
→ 250 events every day
- This is why 10^8 to 10^{10} hrs is a typical goal

■ Hardware components fail at $\sim 10^5$ - 10^6 hrs

- Need two independently failing components to get to 10^9 hours!
 - This motivates redundancy for life-critical applications (SIL 3 & SIL 4)

■ For mission-critical systems, consider:

- Fleet exposure = # units * operational hours/unit
- Number of acceptable failures
- Compute failure rate = failures / hours; pick an appropriate SIL



Lime halts scooter service in Switzerland after possible software glitch throws users off mid-ride

Ingrid Lunden @ingridlunden / 23 hours ago

<https://techcrunch.com/2019/01/12/lime-scooters-switzerland-bumps/>

Comment

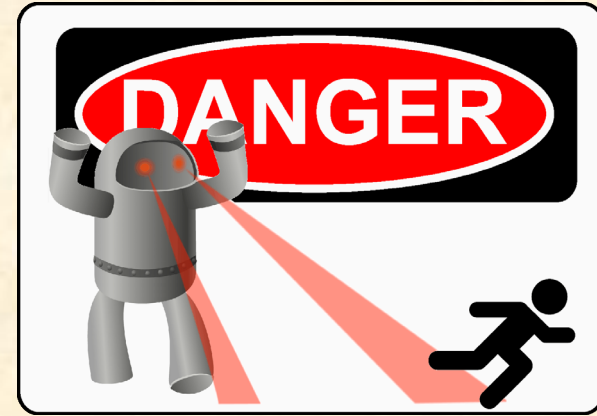


<https://www.li.me/second-street/safety-update-february-2019>

“Recently we detected a bug in the firmware of our scooter fleet that under rare circumstances could cause sudden excessive braking during use.”

Best Practices For Critical Systems

- Characterize worst case failure scenarios
 - Assign SIL based on relevant safety standard
 - Use engineering rigor for software SIL
 - Use redundancy for ultra-low failure rates
 - Consider fleet exposure, not just single unit

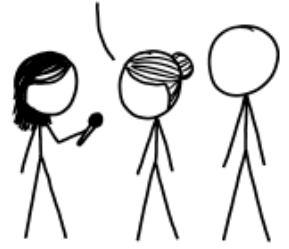


- Pitfalls:

- Software redundancy is difficult, and diversity is usually impracticable
- Designer's intuition about "realistic" faults usually optimistic
 - At 10^{-9} /hr, random chance is a close approximation of a malicious adversary
- Going through the motions not enough for SIL-based process

ASKING AIRCRAFT DESIGNERS ABOUT AIRPLANE SAFETY:

NOTHING IS EVER FOOLPROOF, BUT MODERN AIRLINERS ARE INCREDIBLY RESILIENT. FLYING IS THE SAFEST WAY TO TRAVEL.



ASKING BUILDING ENGINEERS ABOUT ELEVATOR SAFETY:

ELEVATORS ARE PROTECTED BY MULTIPLE TRIED-AND-TESTED FAILSAFE MECHANISMS. THEY'RE NEARLY INCAPABLE OF FALLING.



ASKING SOFTWARE ENGINEERS ABOUT COMPUTERIZED VOTING:

THAT'S TERRIFYING.



WAIT, REALLY?

DON'T TRUST VOTING SOFTWARE. AND DON'T LISTEN TO ANYONE WHO TELLS YOU IT'S SAFE.

WHY?

I DON'T QUITE KNOW HOW TO PUT THIS, BUT OUR ENTIRE FIELD IS BAD AT WHAT WE DO, AND IF YOU RELY ON US, EVERYONE WILL DIE.



THEY SAY THEY'VE FIXED IT WITH SOMETHING CALLED "BLOCKCHAIN."

AAAAA!!!

WHATEVER THEY SOLD YOU, DON'T TOUCH IT. BURY IT IN THE DESERT. WEAR GLOVES.



<https://xkcd.com/2030/>