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.

“I cannot conceive of any vital disaster happening to this vessel. Modern shipbuilding has gone beyond that.”

– EJ Smith (Captain of the Titanic)
Safety Requirements

- **Anti-Patterns for Safety Requirements:**
  - No specifically identified safety requirements
  - All functional requirements are safety critical
  - Safety requirements can’t be validated

- **Specifying safety:**
  - Safety goals: “working” is not the same as “safe”
    - How hazards are avoided at system level
    - Can involve correctness, backup systems, failsafes, ...
    - Often what the system *does not do* is as important as what it does
  - Safety requirements:
    - More detailed safety-specific requirements allocated to subsystems
Identifying Safety-Related Requirements

- Overly-simplistic approach:
  - Start with system requirements
  - Annotate critical system requirements
  - Then, annotate supporting requirements
  - Problem: Most requirements can become critical

- Too many system components promoted to highest criticality level
  - Allocating even one critical requirement to component makes whole thing critical

Requirement Annotation Approach:

- R01. Lorem ipsum dolor sit amet, consectetur adipiscing elit.
- R02. Nam suscipit odio aliquam massa finibus, id imperdiet.
- R03. Quisque vehicula quam ut dui venenatis varius.
- R04. Nulla posuere diam ac augue bibendum, vitae laoreet.
- R05. Pellentesque aliquam sem sit amet justo porttitor.
- R06. Vestibulum scelerisque lacus ac nunc vulputate, dictum.
- R07. Ut venenatis ante in ligula efficitur, congue posuere.
- R08. Nam a nulla ultrices, tempor quam et, fringilla nisi.
- R09. Vestibulum a arcu interdum, placerat eros non, ultrices.
- R10. Ut commodo odio eu elit porttitor facilisis.
- R11. Etiam et sem eu eros congue sollicitudin.
- R13. Fusce quis magna aliquet, venenatis sem ac, rhoncus.
- R15. Cras mollis lorem vitae libero sollicitudin lobortis.
- R16. Vestibulum luctus nisi ac nibh varius congue.
- R17. Mascenae consequat augue eu venenatis euismod.
- R18. Quisque viverra felis in est ornare consectetur.
Safety Envelope Requirements Approach

- **Safety Envelope:**
  - Specify unsafe regions for safety
  - Specify safe regions for functionality
    - Deal with complex boundary via:
      - Under-approximate safe region (reduces *permissiveness*)
      - Over-approximate unsafe region
  - Trigger system safety response upon transition to unsafe region

- **Partition the requirements:**
  - Operation: functional requirements
  - Failsafe: safety requirements (safety functions)
Architecting A Safety Envelope System

**“Doer” subsystem**
- Implements normal functionality
- Allocate functional requirements to Doer

**“Checker” subsystem**
- Implements failsafes (safety functions)
- Allocate safety requirements to Checker

**Checker is entirely responsible for safety**
- Doer can be at low SIL (failure is lack of availability)
- Checker must be at high SIL (failure is unsafe)
  - Often, Checker can be much simpler than Doer
**Safety Requirements Best Practices**

- **Doer/Checker pattern**
  - Functional requirements allocated to low-SIL Doer
  - Safety requirements allocated to high-SIL Checker

- **Good safety requirements**
  - Trace to system-level safety goals
    - Orthogonal to normal functional operation if possible
  - Make safety simple to validate (test, peer review)
    - Safety testing mostly exercises the Checker box

- **Pitfalls:**
  - Tradeoff between simplicity and permissiveness
    - Doer optimality costs Checker validation effort
  - Fail-operational functions may require multiple Doer/Checker pairs
Historical Perspective: Apollo 11 Lunar Landing

[Rocket engine burning during descent to Lunar Landing]

102:38:26 Armstrong:
(With the slightest touch of urgency) Program Alarm.


102:38:30 Armstrong: (To Houston) It's a 1202.

102:38:32 Aldrin: 1202. (Pause)
[Altitude 33,500 feet.]

The 1202 program alarm is being produced by data overflow in the computer. It is not an alarm that they had seen during simulations but, as Neil [Armstrong] explained during a post-flight press conference “In simulations we have a large number of failures and we are usually spring-loaded to the abort position. And in this case in the real flight, we are spring-loaded to the land position.”

In Houston, Steve Bales, the control room's expert in the LM guidance systems, has determined that the landing will not be jeopardized by the overflow. The overflow consists of an unexpected flow of data concerning radar pointing. The computer has been programmed to recognize this data as being of secondary importance and will ignore it while it does more important computations.

[Apollo mission logs]
At the time all we had was audio; no live TV during the landing

- 11 min. clip; HBO mini-series compressed events

**Things to note:**

- Collins is in the command module
- Armstrong & Aldrin in Eagle ➔ Lunar Lander
- 1201 & 1202 alarms light up the “abort mission” warning light
  - Computer/human interface was just a bunch of digits on a display panel
  - Total of five of these alarms (three shown in the HBO version)
- At zero seconds of fuel remaining they’re supposed to abort
  - Jettison lower half/landing stage and return to orbit
  - Q: for Apollo 11, how many seconds of fuel were left when they landed?
THE INTERNET HAS ALWAYS HAD LOUD DUMB PEOPLE, BUT I'VE NEVER SEEN ANYTHING QUITE AS BAD AS THE PEOPLE WHO COMMENT ON YOUTUBE VIDEOS.

COMMENTS & RESPONSES
ROCKHOR (19 MINUTES AGO)
THIS IS SO OBVIOUSLY FAKED ITS UNBELIEVABLE, WHY R PEOPLE SO GULLIBLE?? MORONS
(REPLY)(MARK AS SPAM)

BIGMIKE133 (35 MINUTES AGO)
I'VE SEEN THE SPACE SHUTTLE IT DEFINITELY LANDED ON THE MOON DO SOME RESEARCH...
(REPLY)(MARK AS SPAM)

GUNPISTOLMAN (22 MINUTES AGO)
IF IT WAS REAL WHY IS THEIR GRAVITY? AMERICANS R SHEEP
(REPLY)(MARK AS SPAM)

CRACKMONKEY74 (17 MINUTES AGO)
U DONT THINK WE WENT TO THE MOON WHY NOT TELL LOUIS ARMSTRONG TO HIS FACE
(REPLY)(MARK AS SPAM)

SIMPLERPLAN2009 (5 MINUTES AGO)
IT WAS A SOUNDSTAGE ON MARS
(REPLY)(MARK AS SPAM)