Understanding System Safety: Hazards, Controls, Inhibits, and Independence

Dr. Gerry Shaw
Senior Research Engineer
SRI International

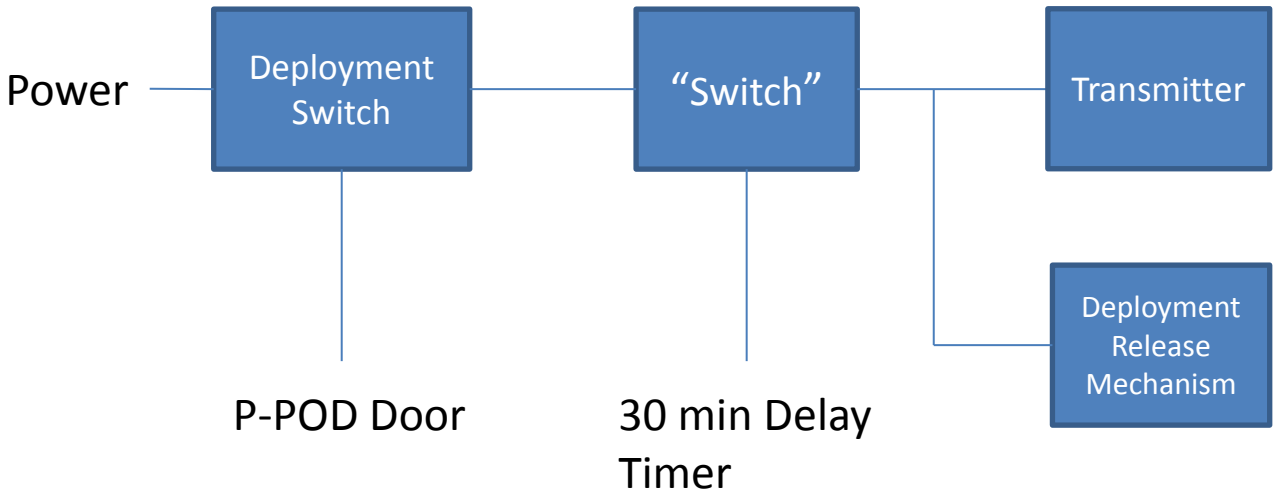
CAL POLY

SRI International

CubeSat Design Specification rev. 12 08/01/2009

- 2.3.1 No electronics shall be active during launch to prevent any electrical or RF interference with the launch vehicle and primary payloads…
- 2.3.2 The CubeSat shall include at least one deployment switch to completely turn off satellite power once actuated.
- 2.4.2 All deployables such as booms, antennas, and solar panels shall wait to deploy a minimum of 30 minutes after the CubeSat's deployment switch(es) are activated from P-POD ejection.
- 2.4.3 RF transmitters greater than 1 mW shall wait a minimum of 30 minutes after the CubeSat's deployment switch(es) are activated from P-POD ejection.

Compliant Architecture ?



Assess Hazard

Hazard Severity		Potential Consequences			Probability*					
Category		Personnel Illness/Injury	Equipment Loss ($)	Unit Downtime	Data Compromise	A	B	C	D	E
I	Catastrophic	May cause death.	> 1,000,000	> 4 months	Data is never recoverable or primary program objectives are lost.					
II	Critical	May cause severe injury or severe occupational illness.	200,000 to 1,000,000	2 weeks to 4 months	May cause repeat of test program.					
III	Marginal	May cause minor injury or minor occupational illness.	10,000 to 200,000	1 Day to 2 Weeks	May cause repeat of test period.					
IV	Negligible	Will not result in injury or occupational illness.	< 10,000	< 1 Day	May cause repeat of data point, or data may require minor manipulation or computer rerun.					

Risk Priority: Unacceptable Waiver required Operation permissible

*Probability refers to the probability that the potential consequence will occur in the life cycle of the system (test/activity/operation). Use the following list to determine the appropriate Risk Level.

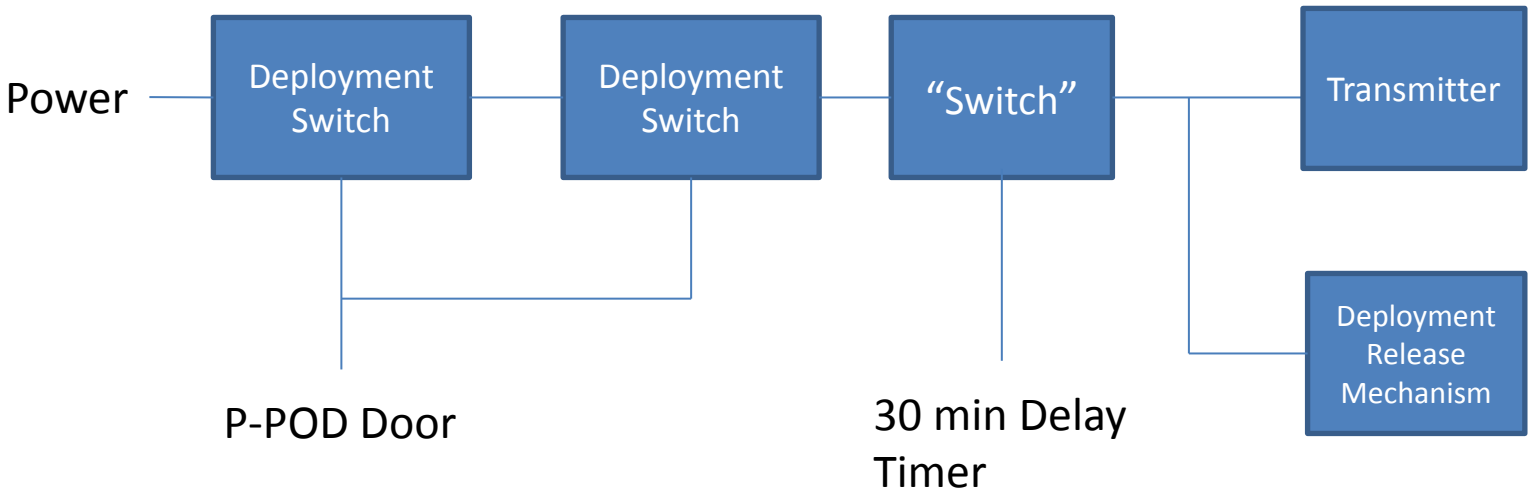
DESCRIPTION**	Threshold Level Probability Value	Specific Individual Item	Fleet or Inventory***
A Frequent	$3X10^{-1}$	Likely to occur repeatedly	Continuously experienced
	$8X10^{-2}$		
B Reasonably probable	$3X10^{-2}$	Likely to occur several times	Will occur frequently
	$8X10^{-3}$		
C Occasional	$3X10^{-3}$	Likely to occur sometime	Will occur several times
	$8X10^{-4}$		
D Remote	$3X10^{-4}$	Unlikely to occur, but possible	Unlikely, but can reasonably be expected to occur
	$8X10^{-5}$		
E Extremely Improbable	$3X10^{-5}$	Very unlikely to occur, but still possible.	Unlikely to occur, but possible

AFSPCMAN 91-710, Vol. 1, Figure 3-2

Hazard Mitigation

- Hazard Control Precedence…
  - **Change design to eliminate or minimize hazards**
    - For example: Reduce transmitter power
  - Add engineered safety features
  - **Incorporate safety devices (inhibits)**
    - For example: Introduce Inhibits
  - Provide warning devices
  - Develop procedures and training
- Inhibits
  - Physical devices that interrupt the “power path” needed to turn on a potentially hazardous device

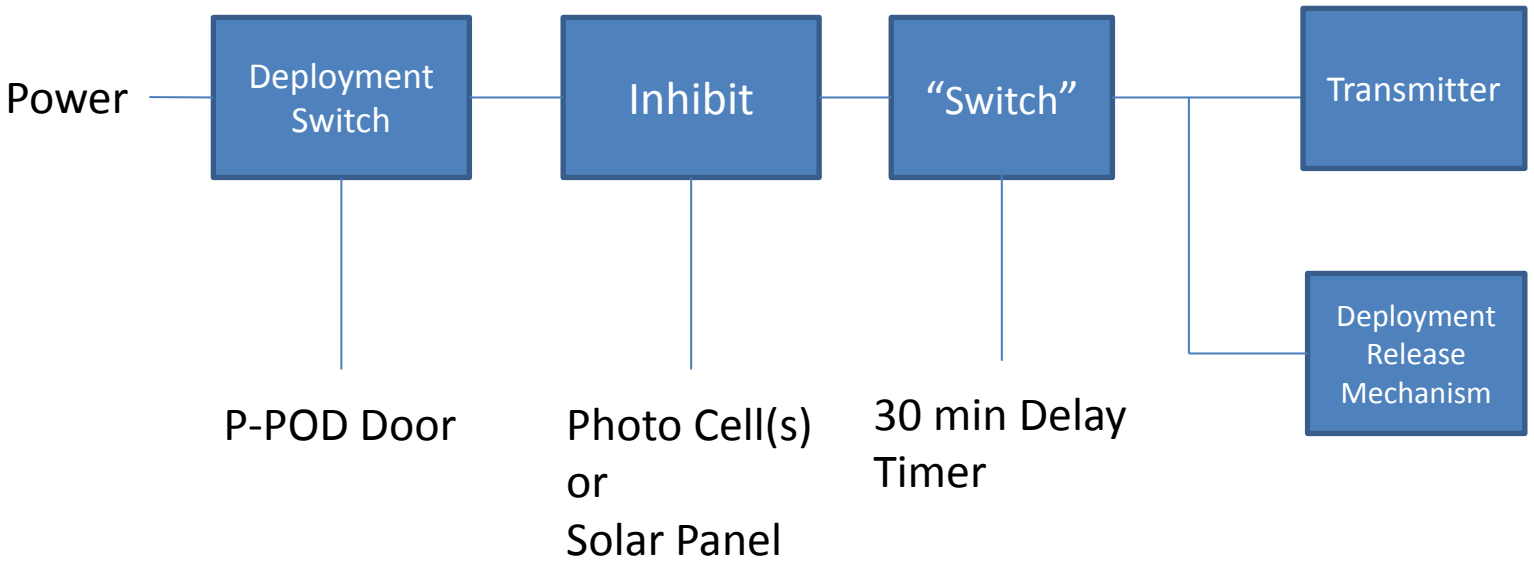
Two Series Deployment Switches



Two independent inhibits

- **Increased safety**
- **Double jeopardy for power on**

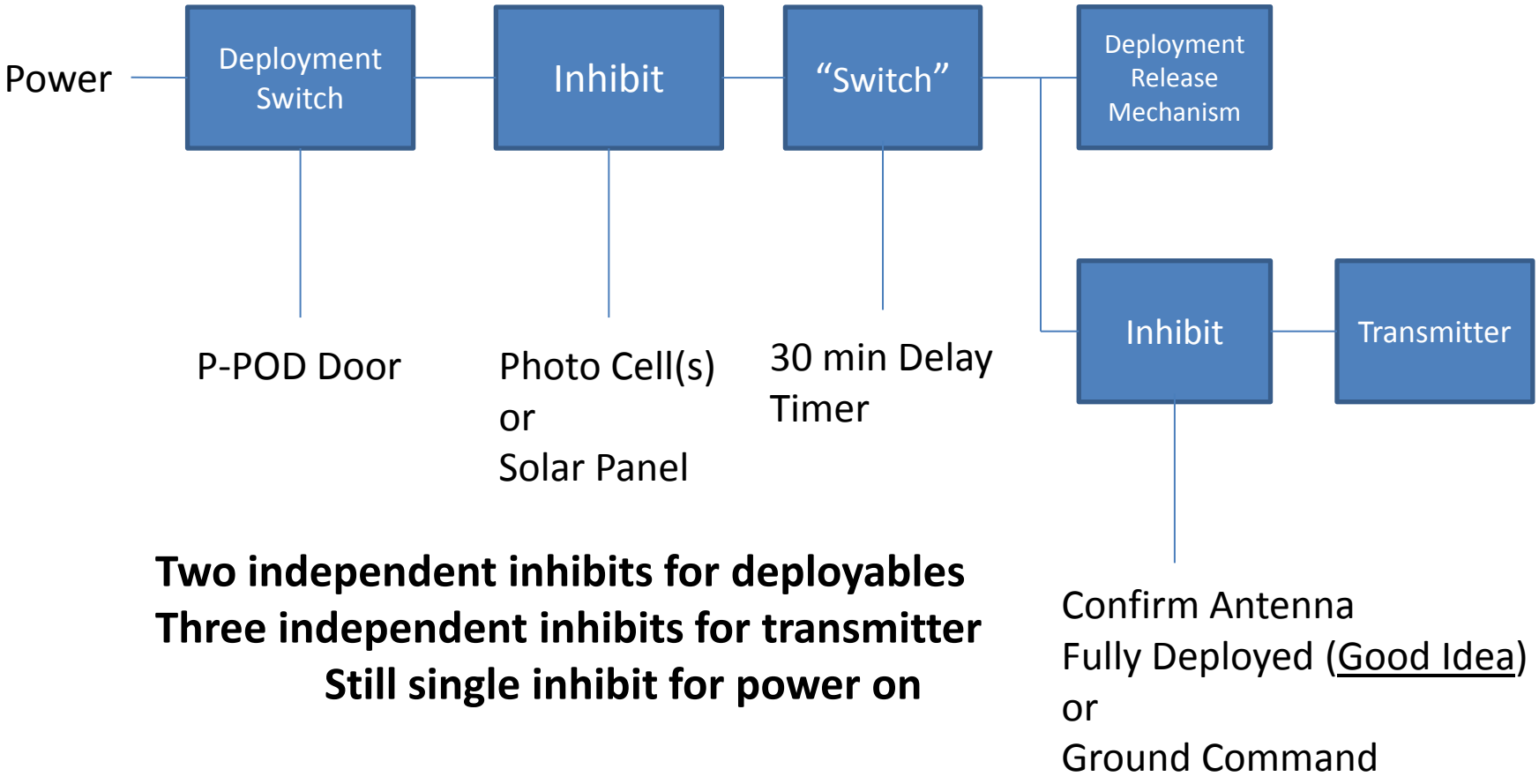
Two Series Deployment Switches



Two independent inhibits

- **Increased safety**
- **Still single inhibit for power on**

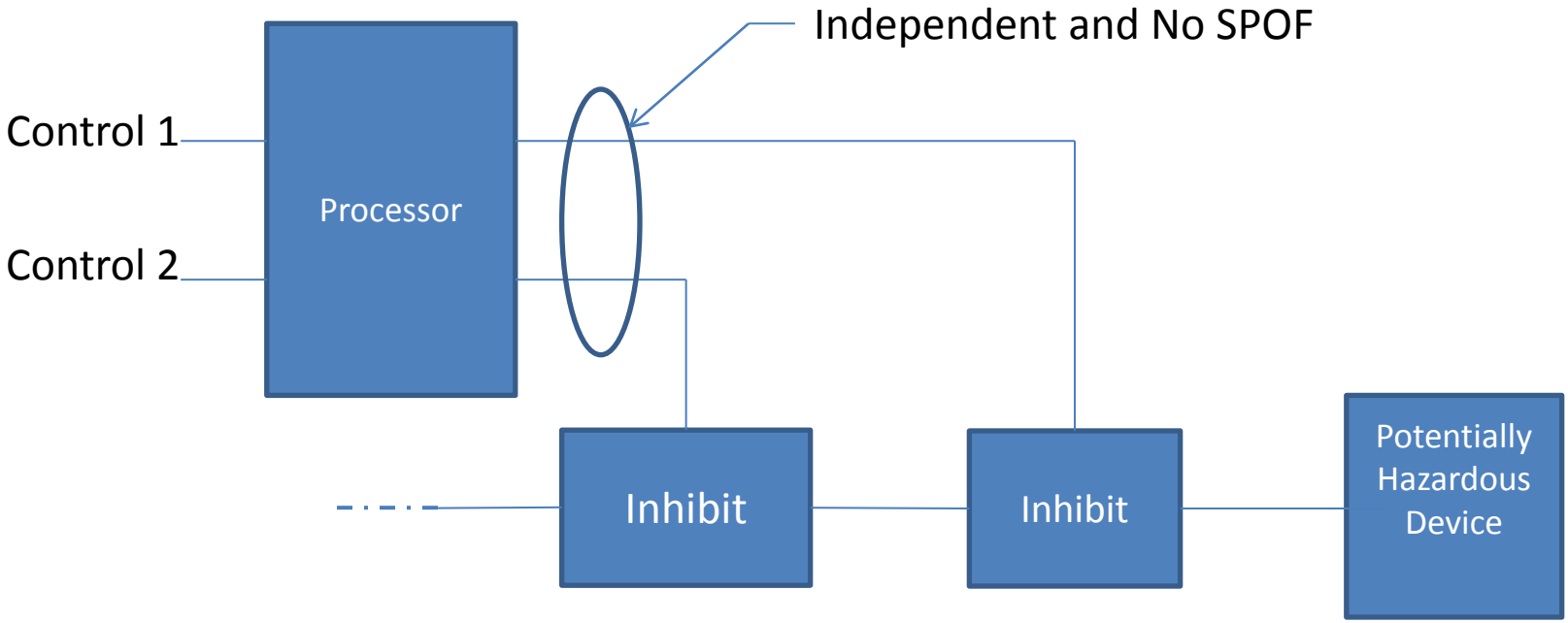
Transmitter Requires Additional Inhibit



Two independent inhibits for deployables
Three independent inhibits for transmitter
Still single inhibit for power on

No Single Point of Failure

- Multiple inhibits controlled by a single processer could have common failure mode



Summary

1. Identify hazards and causal factors using a systematic approach.

2. Assess severity and probability of hazard mishap risk.

3. Identify mitigation measures (safety design requirements).
   - Influence design, order of precedence

4. Reduce hazard risk to an acceptable level.
   - Make inhibits work for both safety and mission assurance

Contacts:

Dr. Gerry Shaw
gerald.shaw@sri.com
(805) 542-9330 x-108

Dr. Mark Tinkle
mark.tinkle@sri.com
(805) 542-9330 x-106

CAL POLY

SRI International