The Limits of Safety

Scott D. Sagan
CISAC

May 9, 2012
Sandia National Laboratories

High Reliability Theory	*Normal Accidents Theory*
Redundancy needed to make a reliable system out of unreliable parts	**Redundancy causes three problems:** **1) Common Mode Failures** **2) Social Shirking** **3) Overcompensation**
Safety is the number one priority	**Safety is one of numerous priorities; tradeoffs constantly need to be made by planners and operators**
Trial and error learning from accidents can be effective	**Denial of responsibility, faulty reporting, and "near-accident misinterpretations" cripples learning efforts**

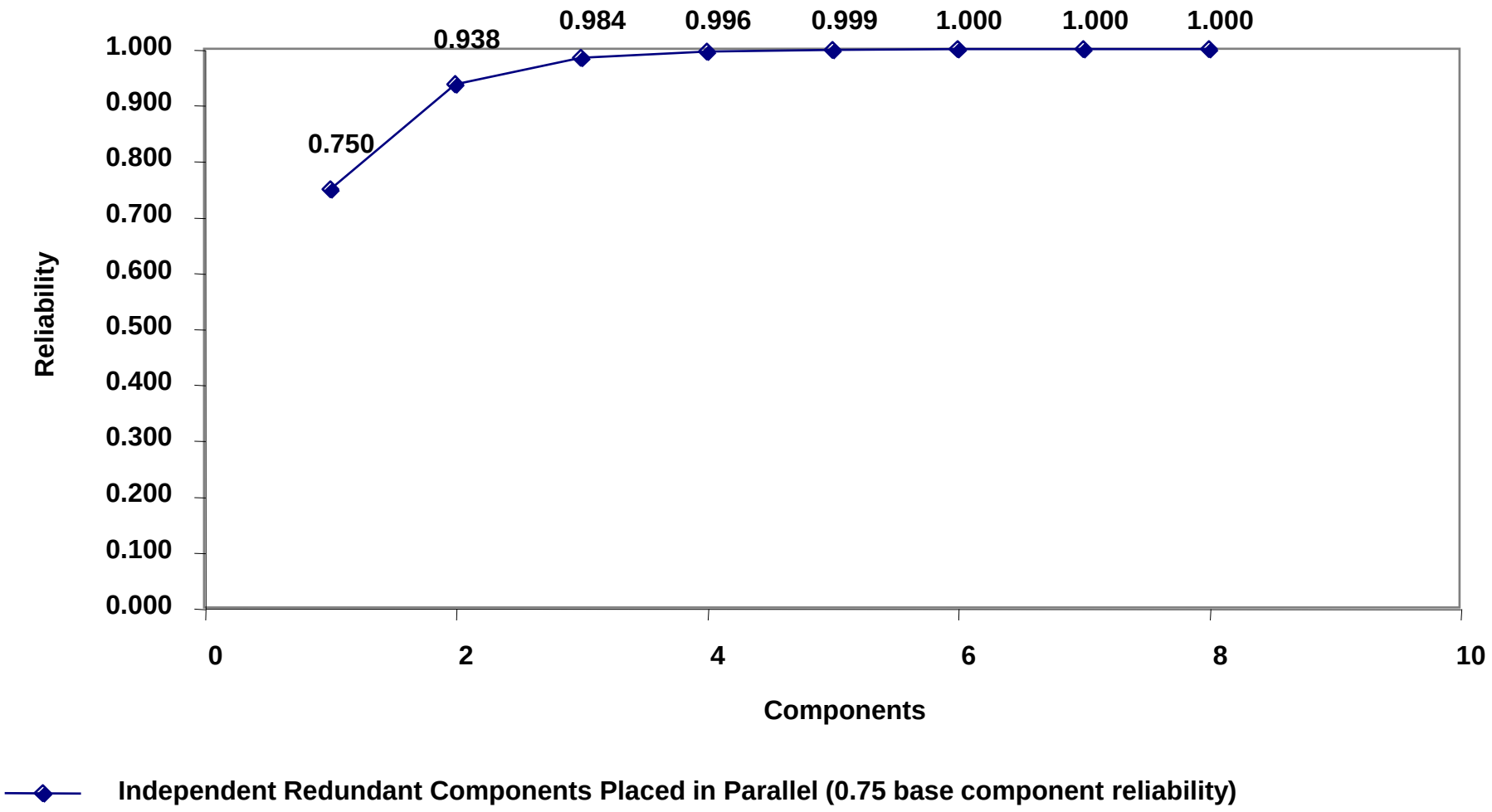
The Benefits of Redundancy

According to Jonathan Bendor, “a system’s reliability is not necessarily limited by its components’ fallibility...”

Suppose an automobile had dual breaking (sic) circuits: each circuit can stop the car, and the circuits operate independently so that if one malfunctions it does not impair the other. If the probability of either one failing is 1/10, the probability of both failing is $(1/10)^2$, or 1/100. Add a third independent circuit and the probability of the catastrophic failure of no brakes at all drops to $(1/10)^3$, or 1/1000.

(*Parallel Systems*, University of California Press, 1987: pp. 26-27.)

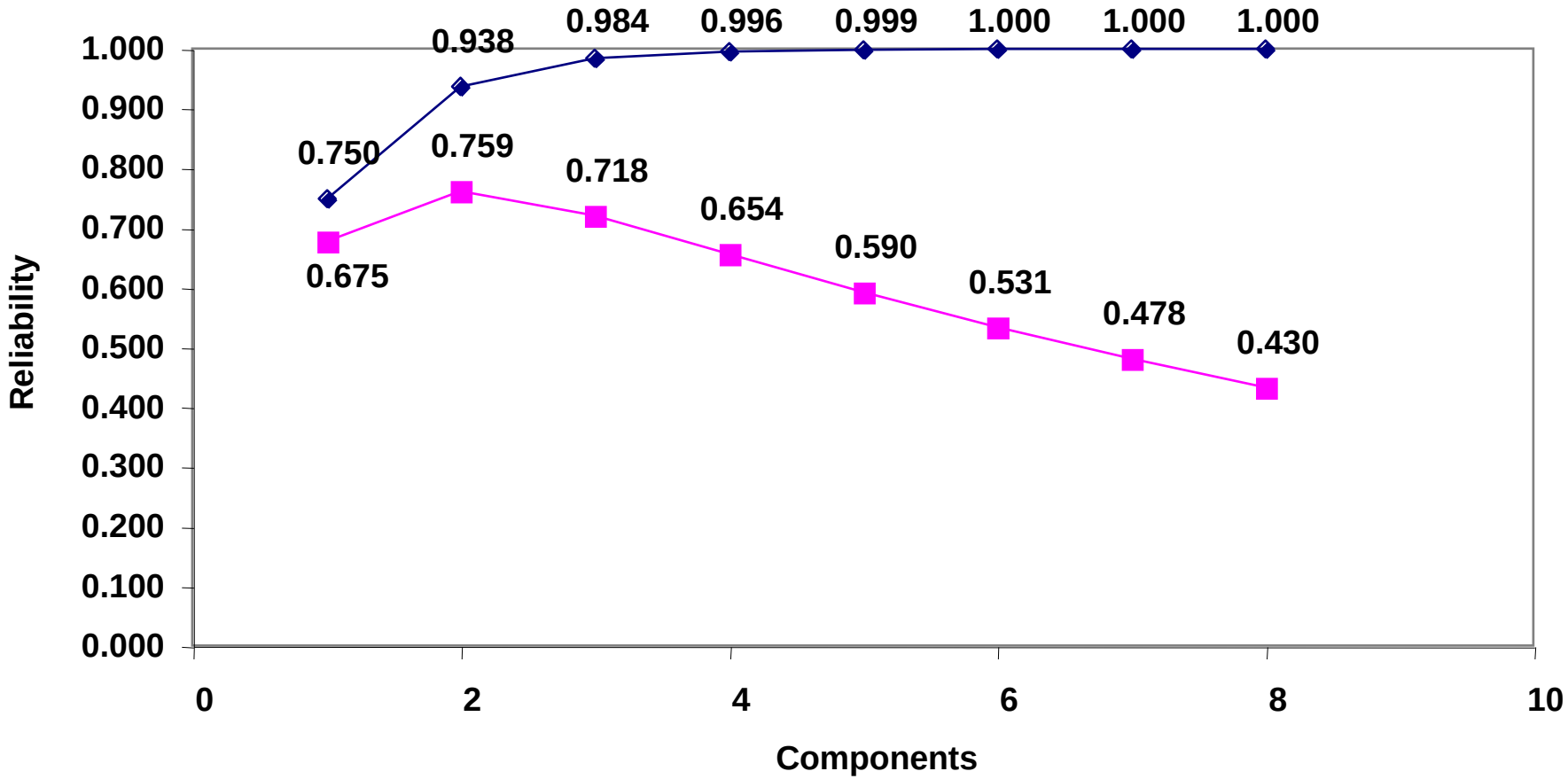
The Benefits of Redundancy



The Problem of Redundancy Problem #1: Common Mode Failures

What if redundant safety devices causes the problem?

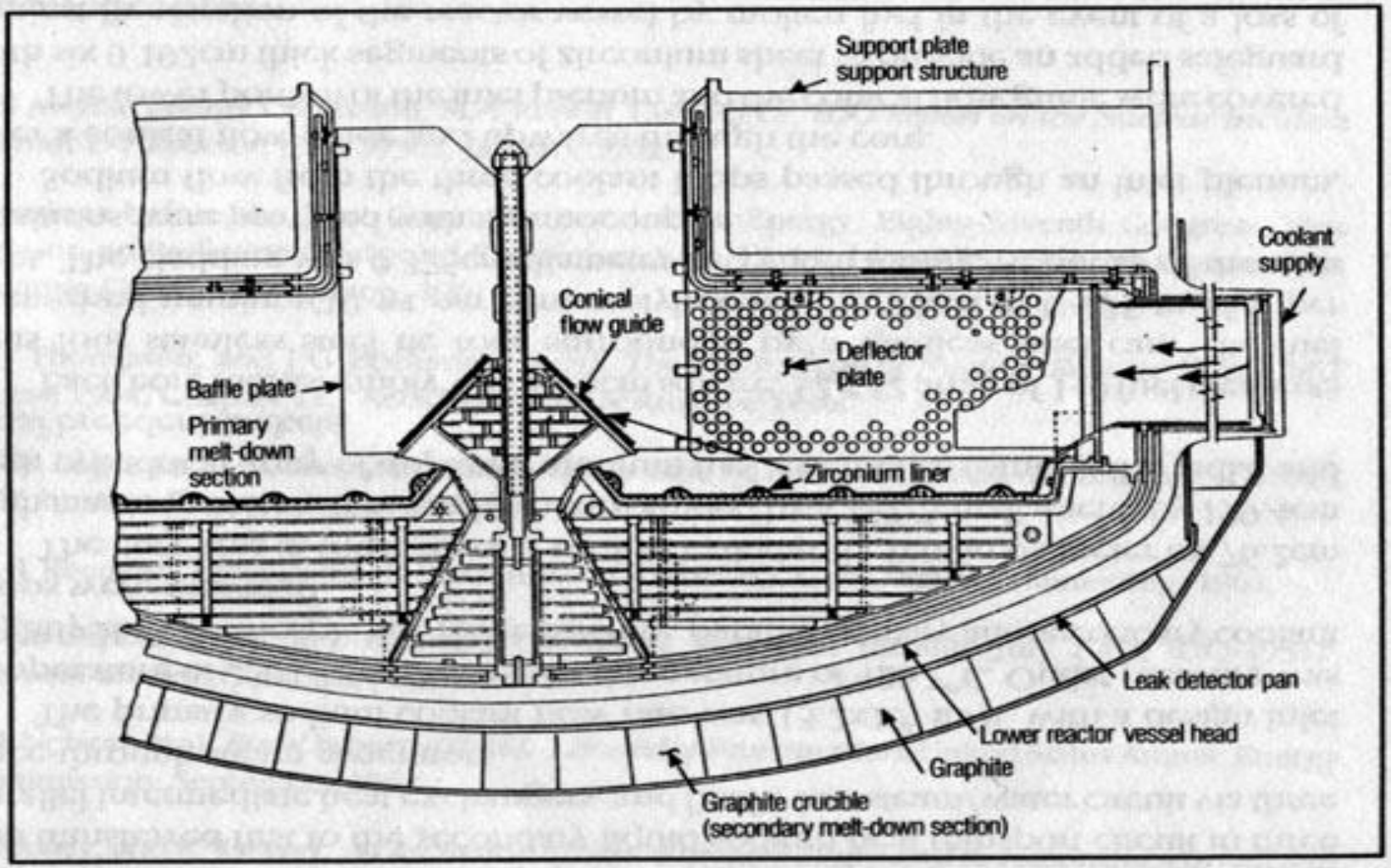
Redundant Safety Devices With Catastrophic Common-Mode Failure



Independent Redundant Components Placed in Parallel (0.75 base component reliability)

With Catastrophic Common-Mode Failure (0.75 base reliability, plus 0.10 probability of catastrophic common-mode failure in each component)

The Fermi Reactor Incident



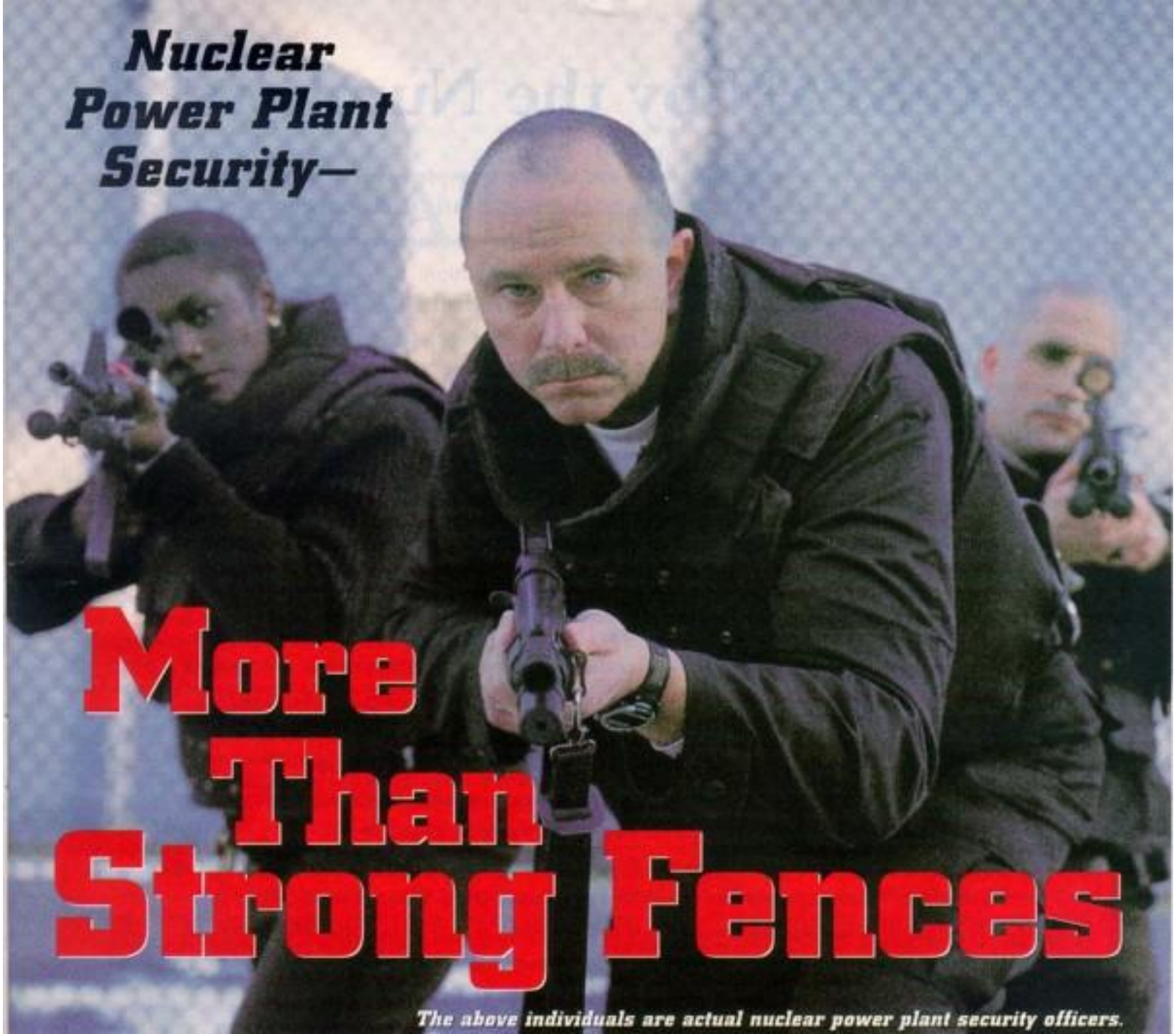
The lower portion of the Fermi 1 reactor showing the zirconium liner plates. The plates on the flow guide were added late and not recorded on the "as-built" drawings.

Indira Gandhi (1917-1984)

Sikh Golden Temple Attack, 1984

"What we did not perceive was that an attempt could be made inside the Prime Minister's house."

- Head of Secret Service



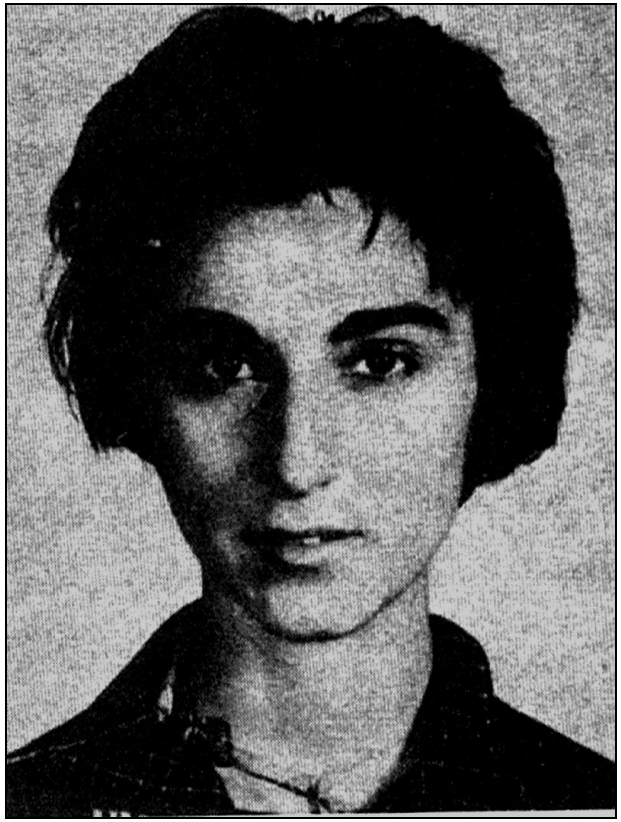
Nuclear Power Plant Security—

More Than Strong Fences

The above individuals are actual nuclear power plant security officers.

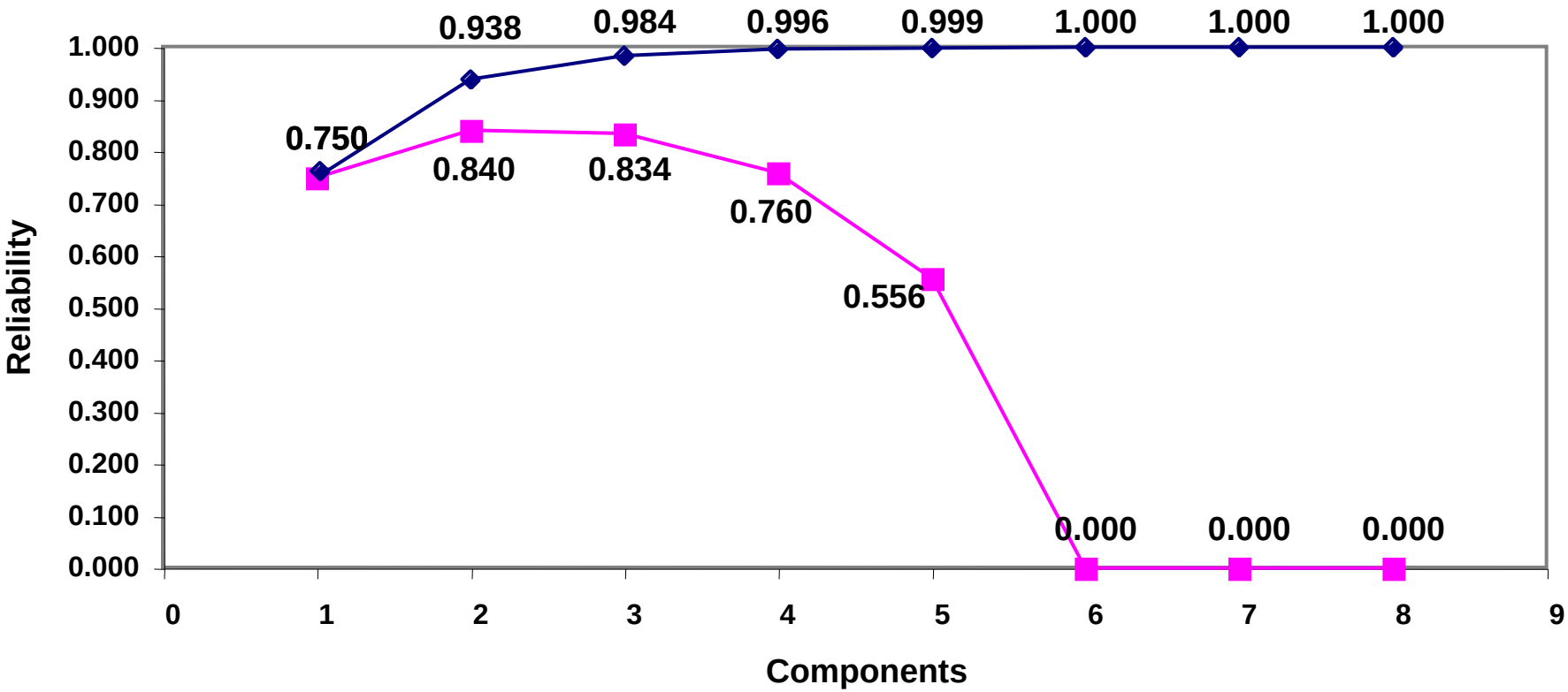
The Problem of Redundancy Problem #2: Social Shirking

What if redundant components reduce each other's reliability?



Kitty Genovese, 1964

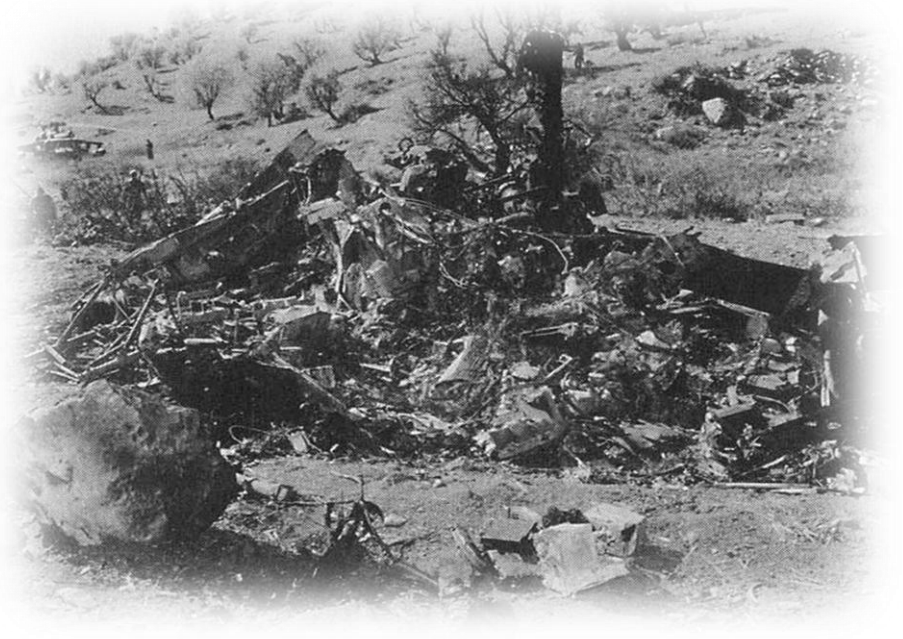
Redundant Safety Devices With Interactive Effects



Independent Redundant Components Placed in Parallel (0.75 base component reliability)

Components with Reduced Component Reliability (0.75 base component reliability, with 0.15 reduction of reliability of each component per additional component)

Friendly Fire:
US Black Hawks Over Northern Iraq, 1994

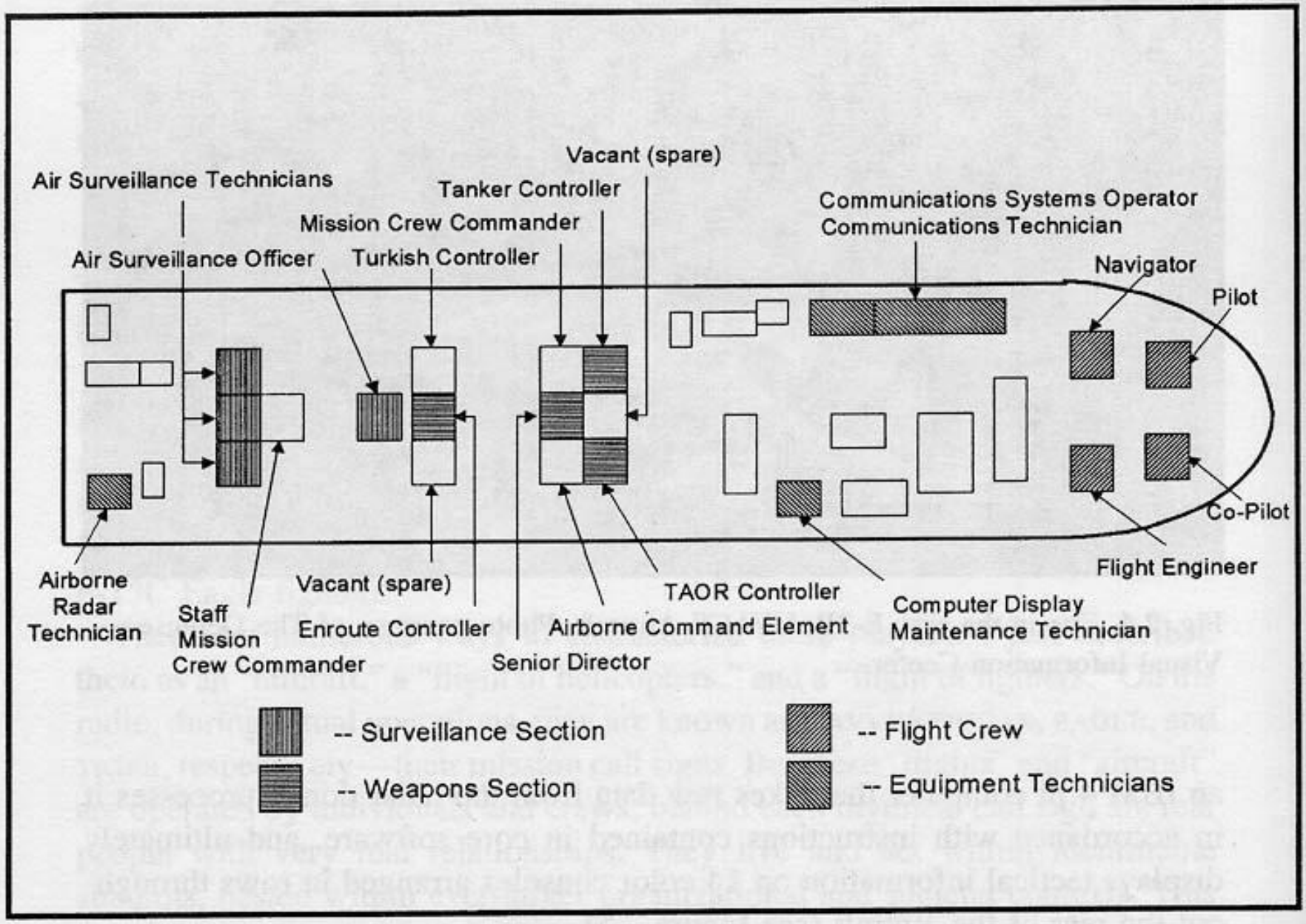


- F15 pilots mistook U.S. Black Hawks for Iraqi Hinds
- AWACS crew failed to alert F15s that the helicopters were American
- 26 peacekeepers killed

Friendly Fire: Social Shirking between the F15s

He transmitted “VID Hind, Tally Two, lead-trail.” The flight lead then transmitted, “Tiger 2, confirm Hinds?” The F-15 wingman replied, “Standby.” The wingman conducted a VID pass (approximately 2000 ft right) of the trailing helicopter, but did not confirm the identification. In response to the flight lead’s radio call, the wingman responded “Tally 2.” The wingman testified that he intended this call to indicate he saw two helicopters. The F-15 flight lead understood his wingman’s transmission to mean that he confirmed the identification. The AWACS TAOR controller said, “Copy Hinds.”

Friendly Fire: Social Shirking on the AWACS



Friendly Fire: Social Shirking on the AWACS

INVESTIGATOR: Who's responsible on the AWACS aircraft for going through the procedures that the General [Major General Andrus] just described in trying to, in layman's terms, identify the hits there?

MCC: *Everybody is*.

INVESTIGATOR: Who has primary responsibility?

MCC: ***I would have everybody looking at it*.**
(Andrus, 1994; TAB V-013, 49-50)

INVESTIGATOR: Would they [the weapons section] have any responsibility for the detection or electronic identification or monitoring of Aircraft other than fighters- other friendly fighters operating in that area?

MCC: It's possible… As you know, it's- *it's a team effort*. The weapons controller would-would assist in any way possible, of course. ***It is a team effort***.
(Andrus, 1994: TAB V-103, 13)

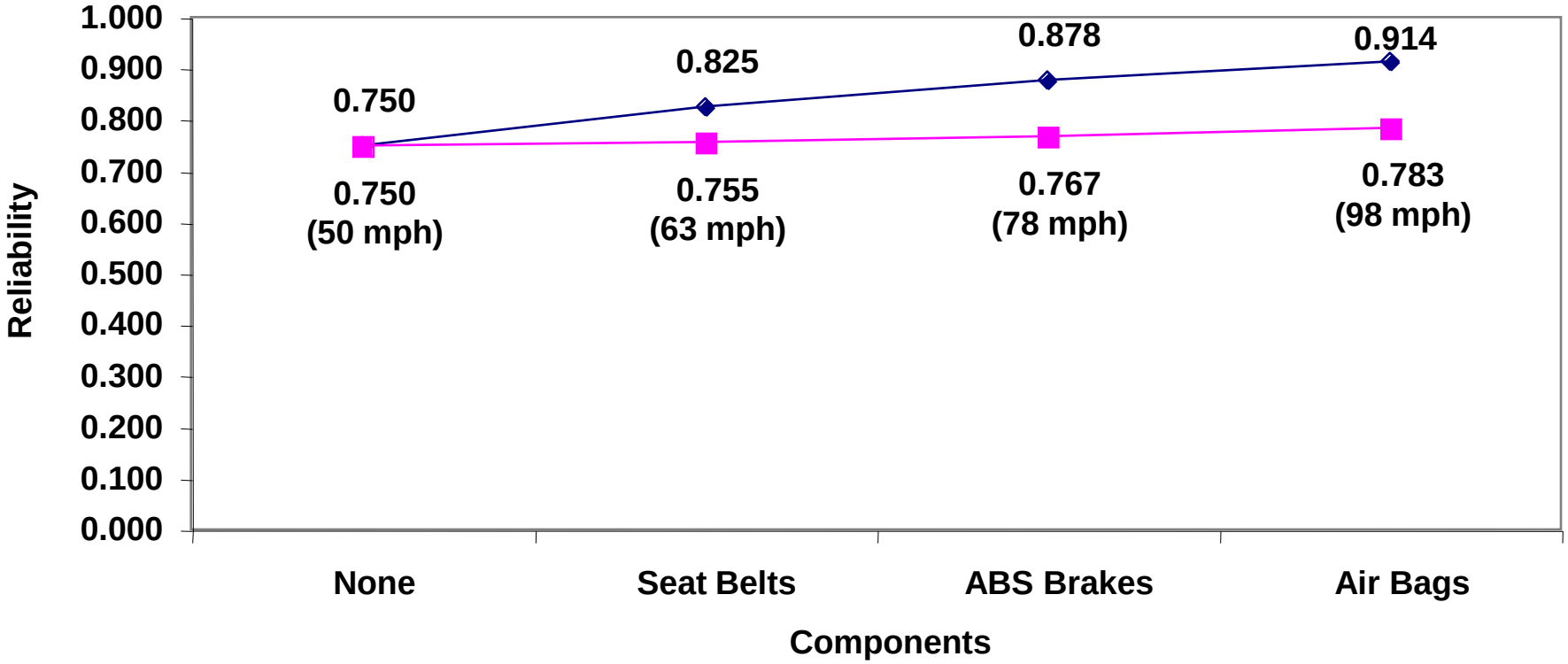
INVESTIGATOR: In the tactical area of operation on board the AWACS, who has command, control, and execution responsibilities for ATO tasked missions?

MCC: That's a- that's a very general question. The answer would be ***everybody on position on the AWACS crew***.
(Andrus, 1994:TAB V-103, 19)

The Problem of Redundancy Problem #3: Overcompensation

What if safety devices encourage operators to take more risks?

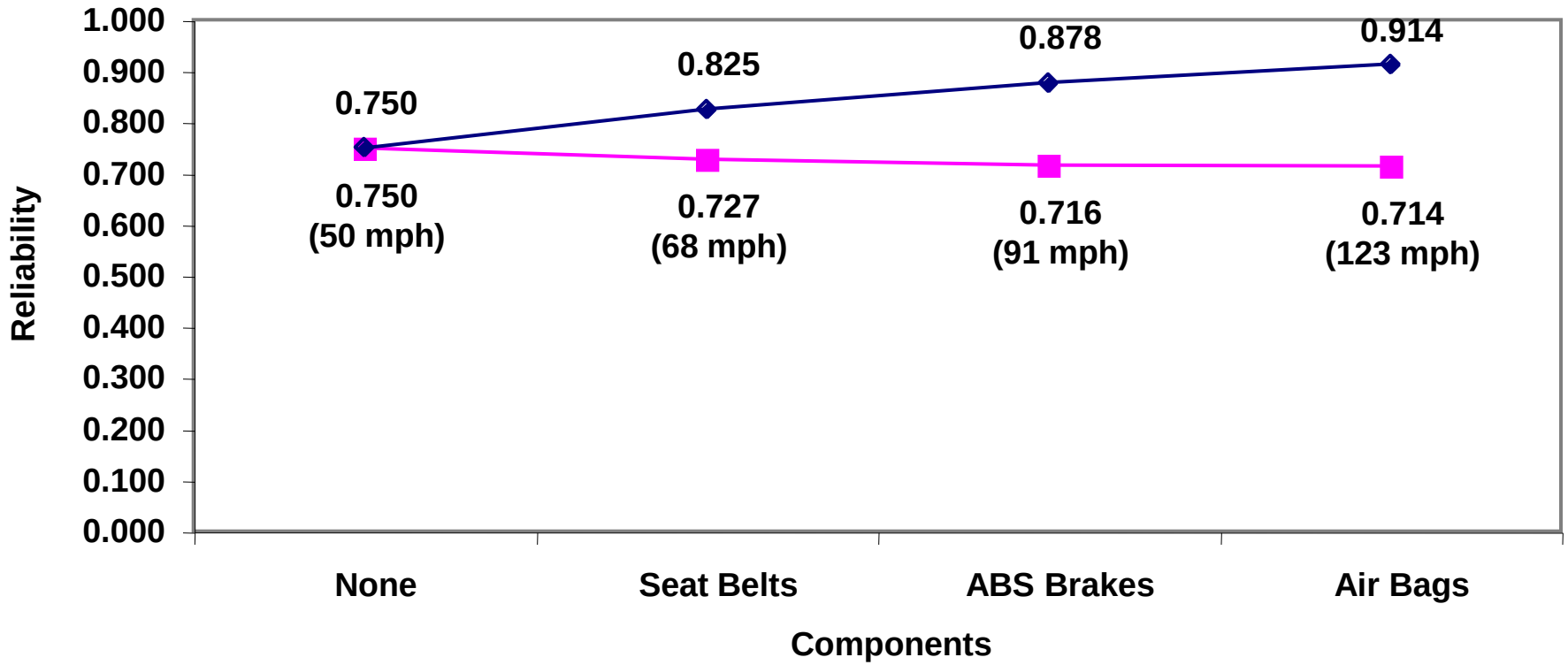
Redundant Safety Devices With Rational Compensation



Independent Redundant Components Placed in Parallel (0.25 base probability of casuality crash at 50 MPH, 0.30 safety component probability of preventing casualities)

Probability of casualty crash increasing by 0.20 per additional 25 MPH, increase in speed of 25% per additional component.

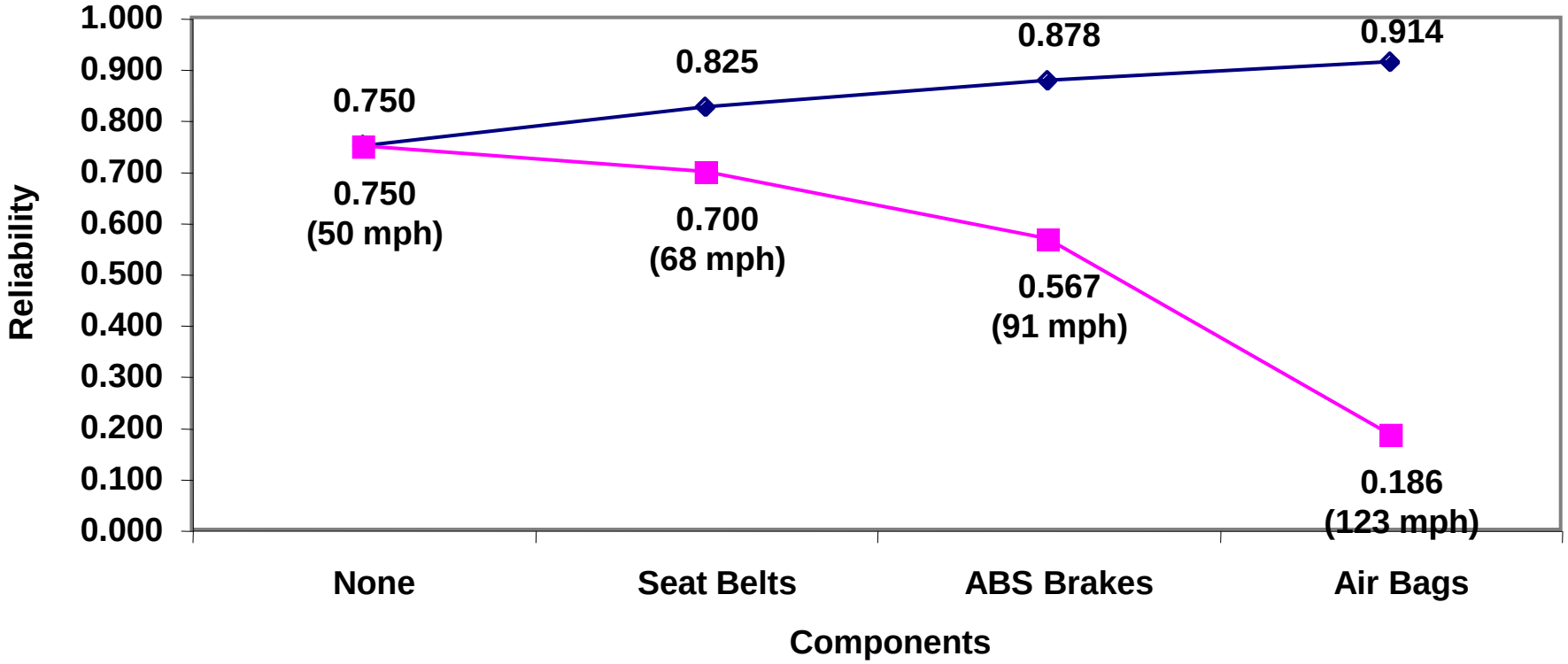
Redundant Safety Devices With Overcompensation



Independent Redundant Components Placed in Parallel (0.25 base probability of casuality crash at 50 MPH, 0.30 safety component probability of preventing casualities)

Probability of casualty crash increasing by 0.20 per additional 25 MPH, increase in speed of 35% per additional component.

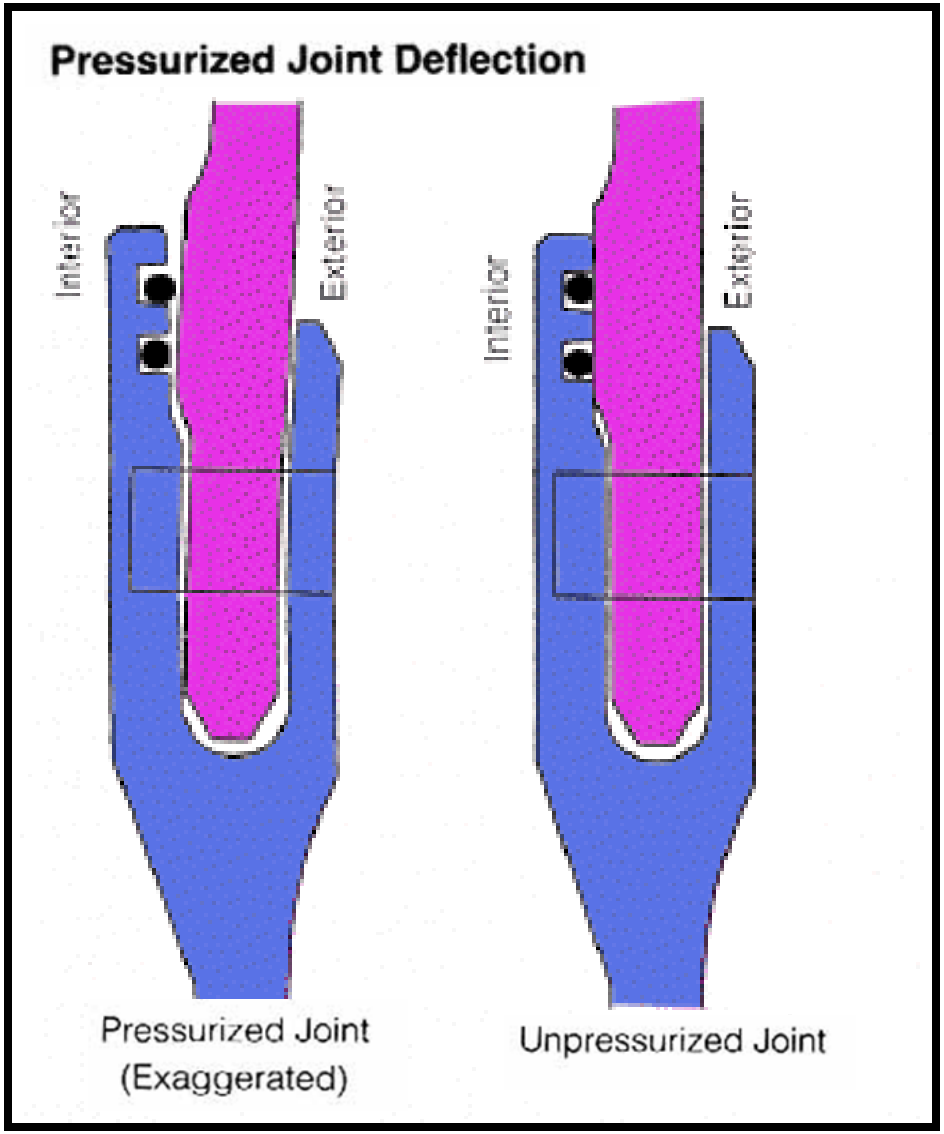
Redundant Safety Devices With Overcompensation and Reduced Component Reliability



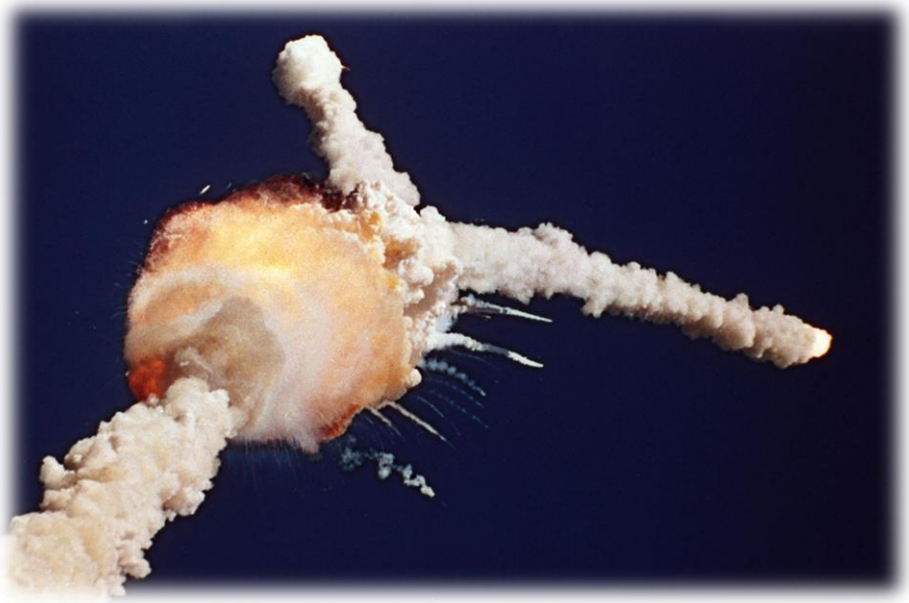
Independent Redundant Components Placed in Parallel (0.25 base probability of casuality crash at 50 MPH, 0.30 safety component probability of preventing casualities)

Probability of casualty crash increasing by 0.20 and safety component probability of preventing casualities decreasing by 0.10 per additional 25 MPH, increase in speed of 35% per additional component.

The *Challenger* Disaster



The *Challenger* Disaster



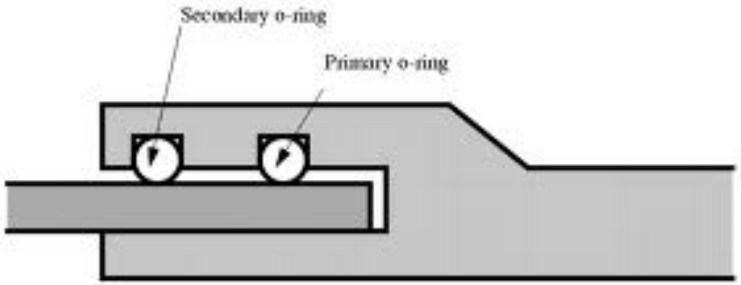
"We had faith in the tests. The data said that the primary would always push into the joint and seal... And if we didn't have a primary seal in the worst case scenario, we had faith in the secondary."

(Vaughan, p. 105)

The *Challenger* Disaster

One of the things that we always believed, and indeed, that Thiokol had told us, was never mind blow-by of the primary because if it does that, it will only seat the secondary from the driving gas pressure. And one of the last comments that Al McDonald made before we went off the loop was, "Don't forget about the secondary, you know, there's always the secondary."

(Vaughan, p. 315)



The *Challenger* Disaster

FINAL THIOKOL LAUNCH RECOMMENDATION

MTI ASSESSMENT OF TEMPERATURE CONCERN ON SRM-25 (51L) LAUNCH

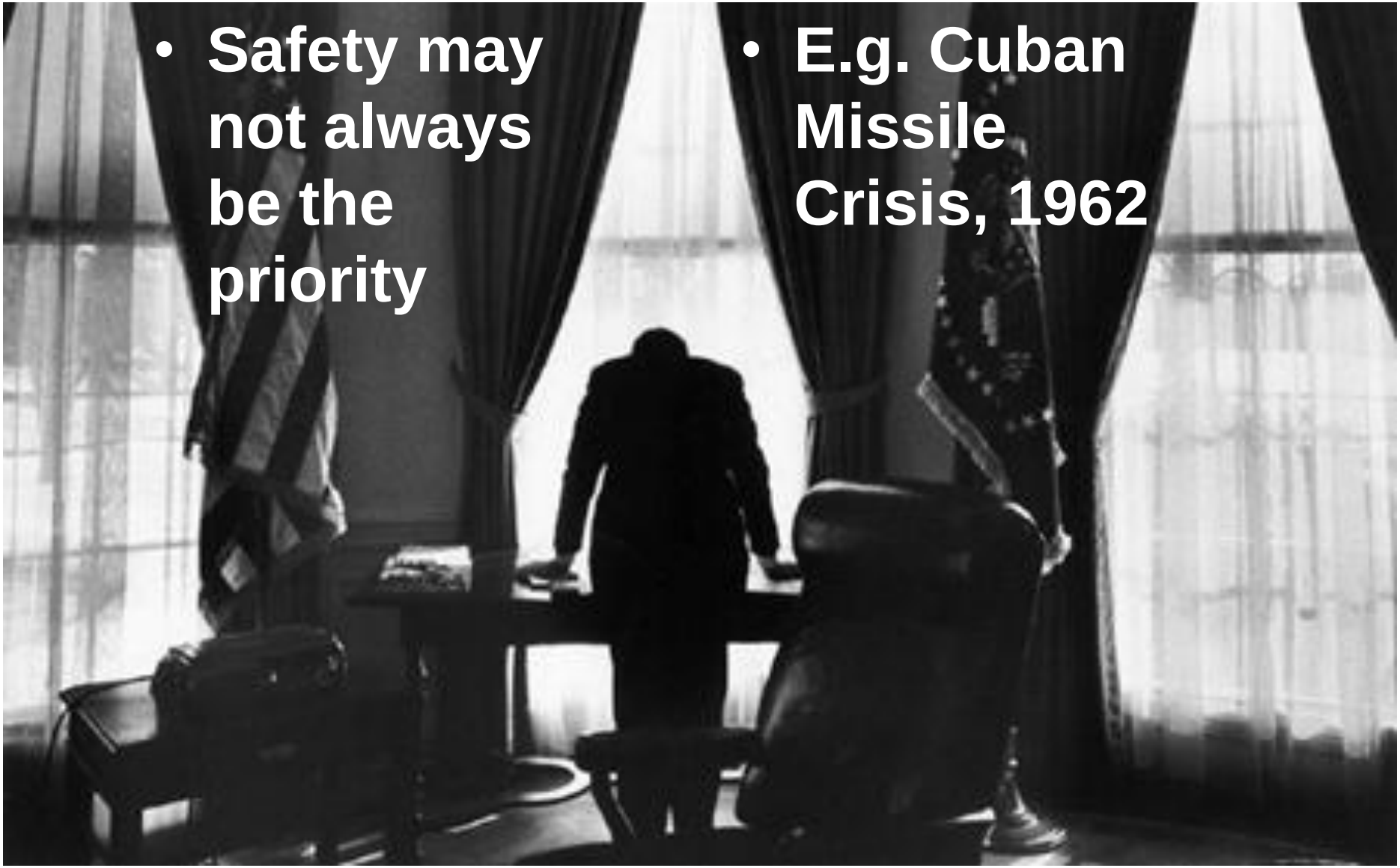
- 0 CALCULATIONS SHOW THAT SRM-25 O-RINGS WILL BE 20° COLDER THAN SRM-15 O-RINGS
- 0 TEMPERATURE DATA NOT CONCLUSIVE ON PREDICTING PRIMARY O-RING BLOW-BY
- 0 ENGINEERING ASSESSMENT IS THAT:
  - 0 COLDER O-RINGS WILL HAVE INCREASED EFFECTIVE DUROMETER ("HARDER")

0 IF THE PRIMARY SEAL DOES NOT SEAT, THE SECONDARY SEAL WILL SEAT

  - 0 DEMONSTRATED SEALING THRESHOLD IS 3 TIMES GREATER THAN 0.038" EROSION EXPERIENCED ON SRM-15
  - 0 IF THE PRIMARY SEAL DOES NOT SEAT, THE SECONDARY SEAL WILL SEAT
  - 0 PRESSURE WILL GET TO SECONDARY SEAL BEFORE THE METAL PARTS ROTATE
  - 0 O-RING PRESSURE LEAK CHECK PLACES SECONDARY SEAL IN OUTBOARD POSITION WHICH MINIMIZES SEALING TIME
- 0 MTI RECOMMENDS STS-51L LAUNCH PROCEED ON 28 JANUARY 1986
  - 0 SRM-25 WILL NOT BE SIGNIFICANTLY DIFFERENT FROM SRM-15

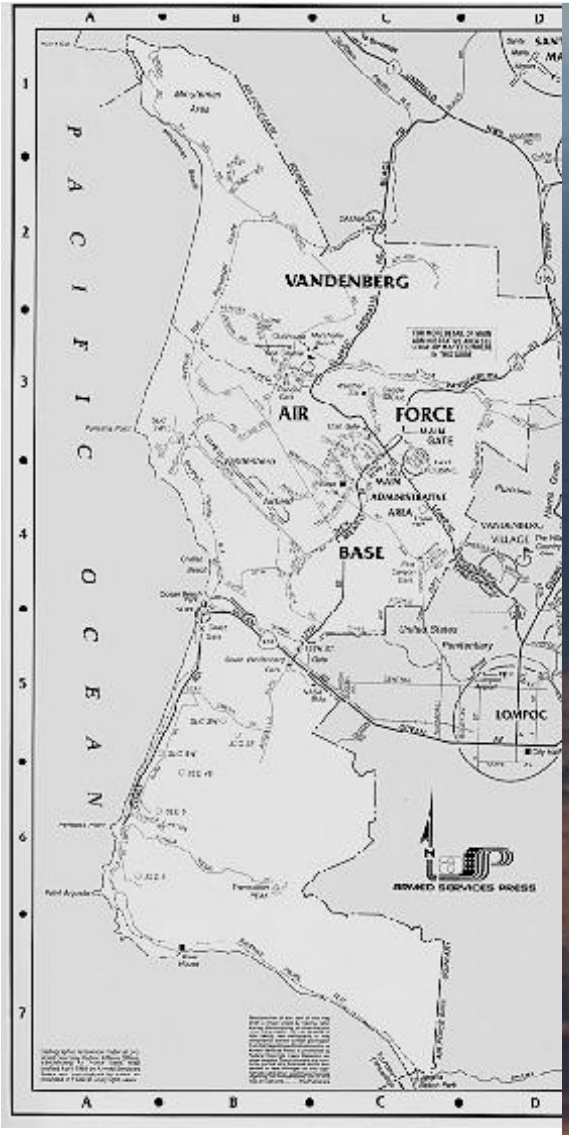
JOE C. KILMINSTER, VICE PRESIDENT
SPACE BOOSTER PROGRAMS

Safety Tradeoffs



- Safety may not always be the priority
- E.g. Cuban Missile Crisis, 1962

Safety Tradeoffs: The Vandenberg ICBM launch, October 1962



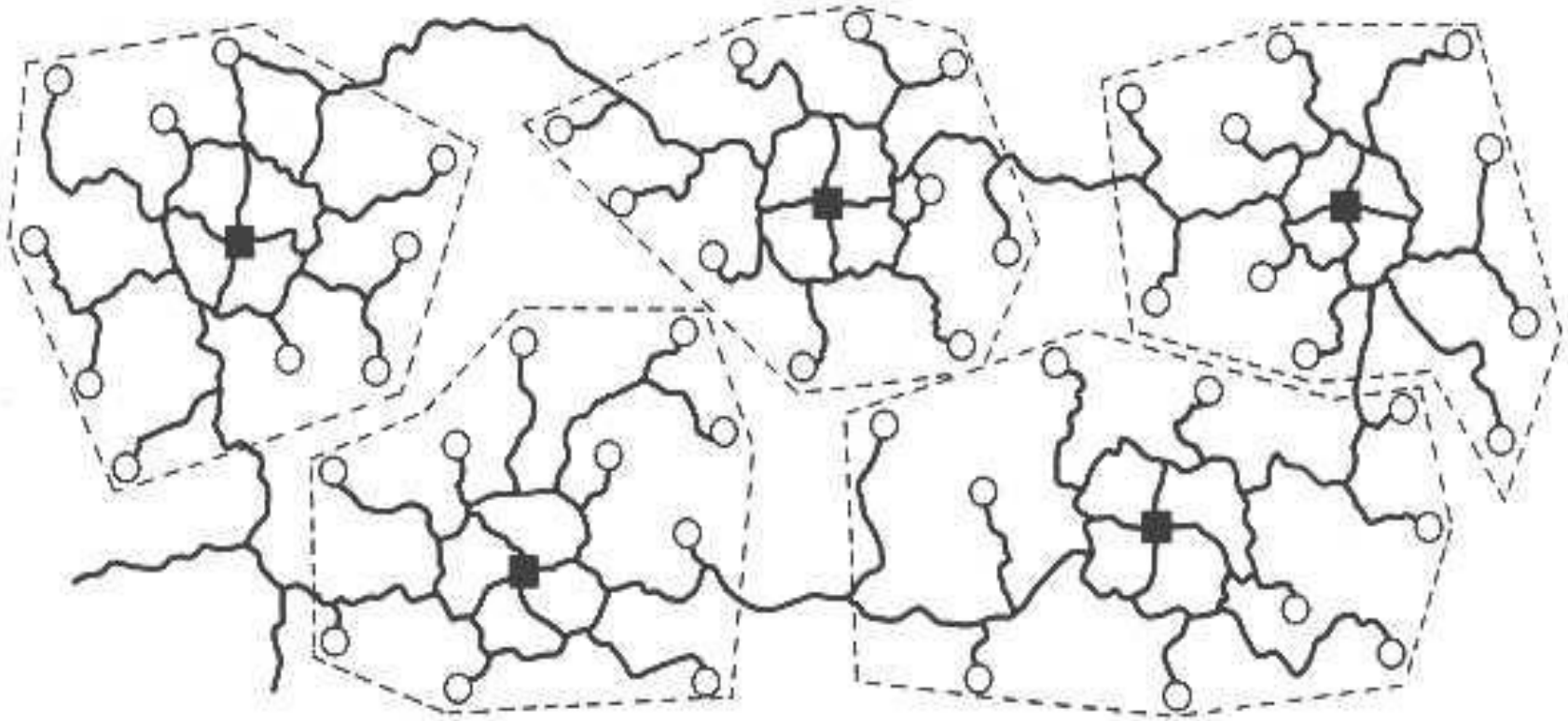
Barriers to Learning

1. Cover-ups

2. Ambiguity of near-accidents

NORAD
Cheyenne Mountain
Colorado Springs, CO

Cover-ups: Malmstrom Minutemen Incident

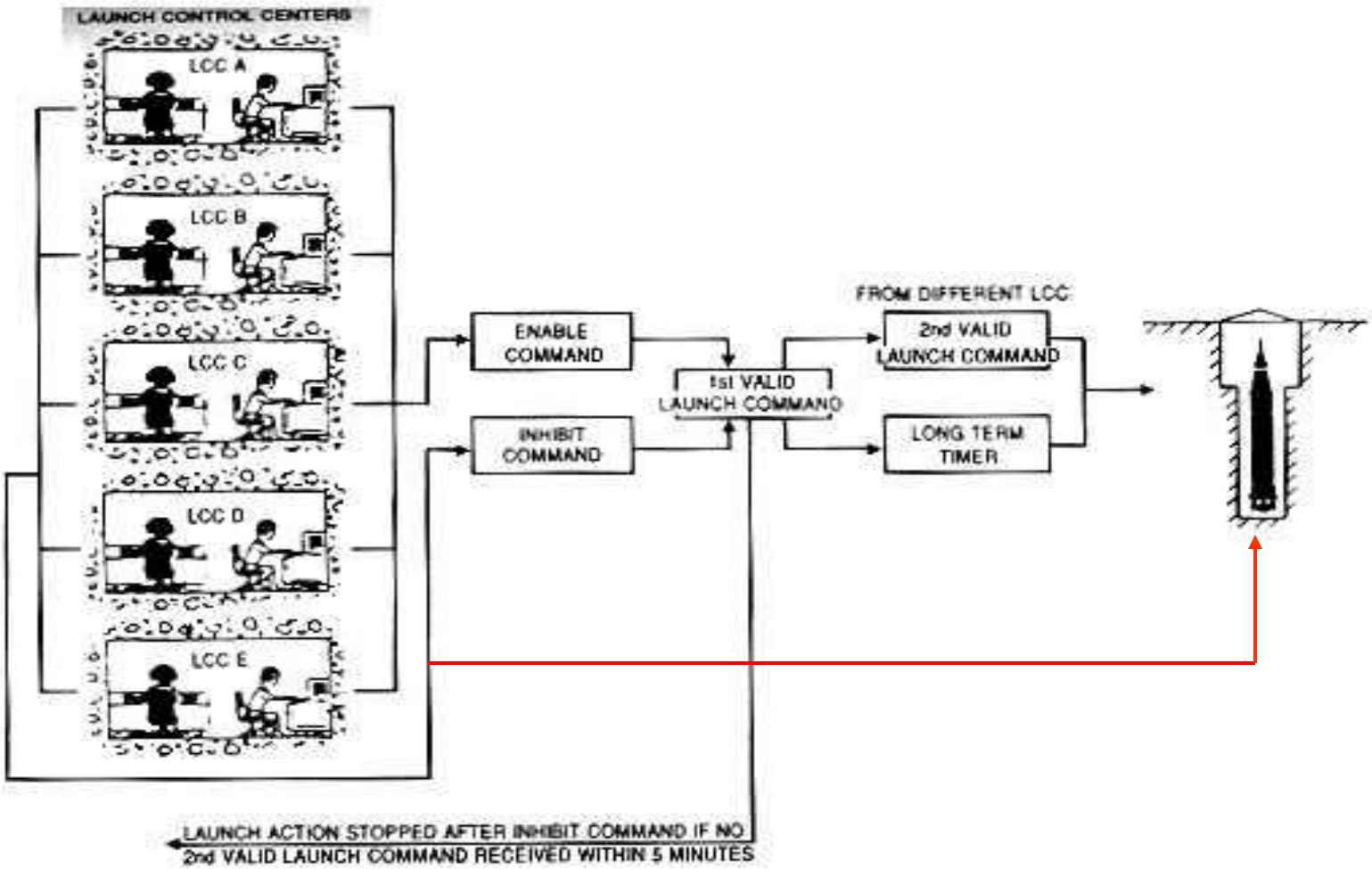


TYPICAL SQUADRON LAYOUT

- Launch Control Center
- Launch Facility (ICBM)
- Flight Location
- Hardened Cable Route

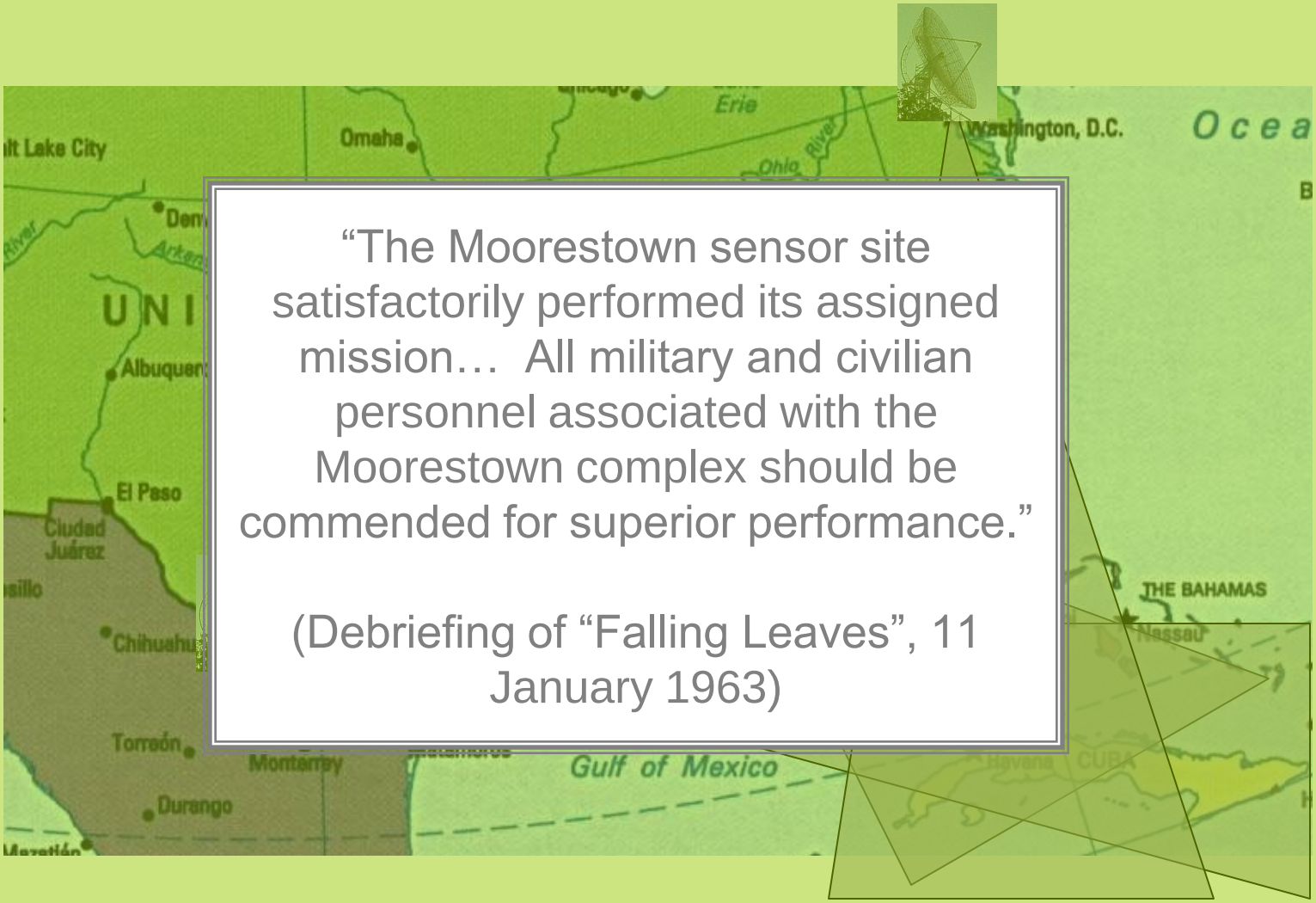
- Five Flights per Squadron each containing ten ICBM's and one Launch Control Center
- Minimum distance between sites – four nautical miles

Cover-ups: Malmstrom Minutemen Incident



2.3 Command and Control Launch Sequences (FY 1978 Authorization for Military Procurement . . . Committee on Armed Services hearings, 95th Congress, 1st sess., part 10, p. 6845.)

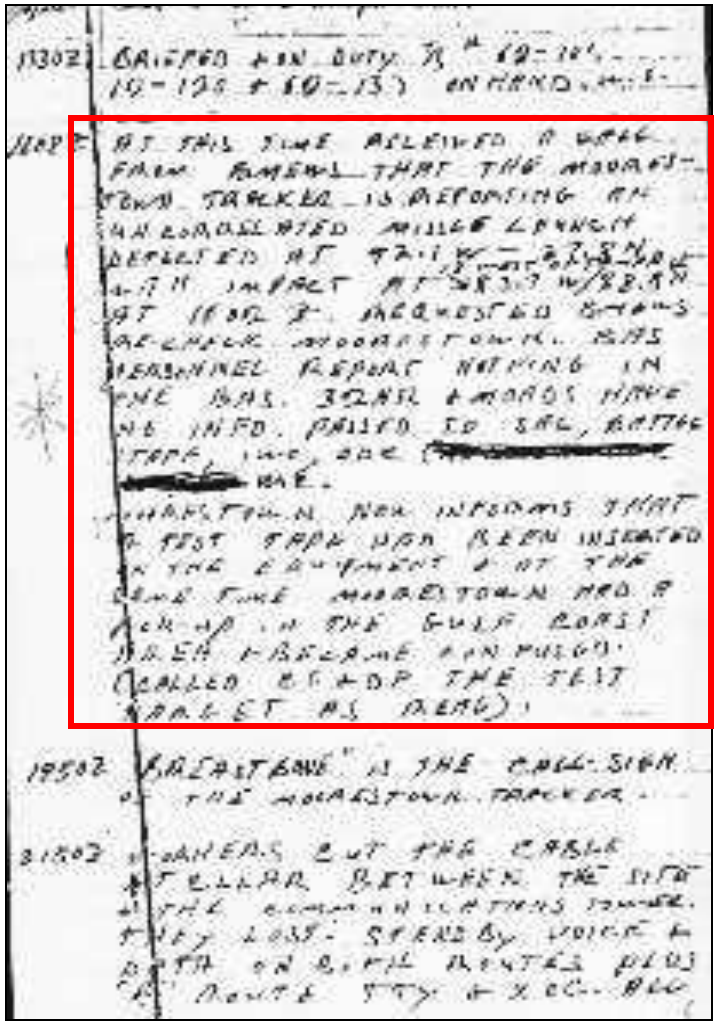
Failure to Learn: “Falling Leaves”

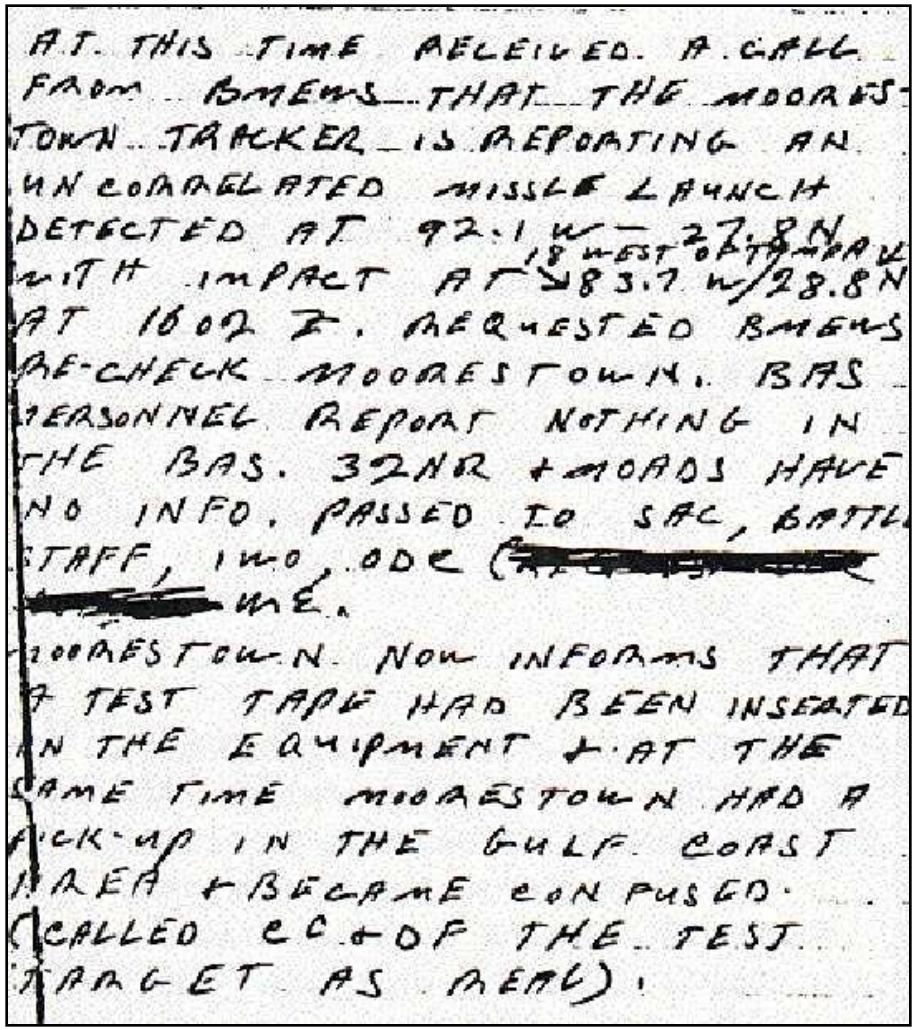


“The Moorestown sensor site satisfactorily performed its assigned mission… All military and civilian personnel associated with the Moorestown complex should be commended for superior performance.”

(Debriefing of “Falling Leaves”, 11 January 1963)

Failure to Learn: “Falling Leaves”





AT THIS TIME RECEIVED A CALL
FROM BMEWS THAT THE MOORES-
TOWN TRACKER IS REPORTING AN
UNCORRELATED MISSLE LAUNCH
DETECTED AT 92.1 W — 27.8 N
WITH IMPACT AT 83.7 W/28.8 N
AT 1602 Z. REQUESTED BMEWS
RE-CHECK MOORESTOWN. BAS
PERSONNEL REPORT NOTHING IN
THE BAS. 32NR + MORDS HAVE
NO INFO. PASSED TO SAC, BATTLE
STAFF, IWO, ODC ([redacted]
[redacted] ME.
MOORESTOWN NOW INFORMS THAT
A TEST TAPE HAD BEEN INSERTED
IN THE EQUIPMENT + AT THE
SAME TIME MOORESTOWN HAD A
PICK-UP IN THE GULF COAST
AREA + BECAME CONFUSED.
(CALLED CC + OF THE TEST
TARGET AS REAL).

Combat Operations Center Log, October 28, 1962

Failure to Learn: NORAD 1979

Failure to Learn: NORAD 1979

November 9, 1979

8:50am MST

- Exercise tape accidentally inserted into a computer
- Simulated full-scale Soviet nuclear attack

Failure to Learn: NORAD 1979

November 9, 1979

8:50am MST

- Interceptor force alerted
- At least ten interceptor aircraft launched
- President's "Doomsday Plane" launched

Continued Risk of Accidents: 2007 Minot AFB Incident

- W-80 nuclear warhead accidentally loaded onto aircraft.
- Organizational failings: Pylons of nuclear-alert missiles were identified with a paper taped to the side. In Minot case, these markings were not visible.
- No Fire Resistant Pits to limit plutonium dispersal. Air transport of warheads without FRPs is prohibited, as is refueling or starting an aircraft with weapons nearby.

B-52H departing Minot AFB

2007 Minot AFB Incident: Fire on Plane Protocol

Nuclear Payload:

1. Ditch payload in uninhabited area
2. Find safe place to land

Non-nuclear Payload:

1. Find safe place to land

Conclusions

- Future NWS will not make the same mistakes as we did during the Cold War—*they will make their own mistakes*
- Vicarious learning must improve if all NWS are to avoid repeating mistakes
- Full understanding of the inherent organizational limits of safety provides more support for nuclear disarmament

U.S.
5102
AIR FO