Normal Accidents: A Book Report

Bill Tetzlaff

September 6, 2001

Normal Accidents

- Charles Perrow
- Princeton University Press, 1999
- ISBM 0-691-00412-9
- First published by Basic Books, 1984
- Discipline: Sociology of Organizations

What are Normal Accidents?

- Accidents that are seemingly extreemly rare, that are in fact "normal"
- Also called "system accidents"
- They are multiple failure accidents in which there are unforseen interactions that make them either worse or harder to diagnose

Some terms

- Interractive Complexity
  - Failures of two components interact in an unexpected way
- Tightly Coupled
  - Processes that are parts of a system that happen quickly and cannot be turned off or isolated
- Perrow Thesis: Tightly coupled systems with high interactive complexity will have Normal Accidents

Operator Error

- In his experience post mortums blame "operator error" 60 to 80 percent of the time
- He feels that they are scapegoated by people with 20 20 hindsight
- Mostly they are errors that are designed in to the system

Three Mile Island

- Unit Number 2 in a Nuclear Plant near Harrisburg, Pennsylvania
- March 28, 1979
- Many of us watched this unfold on the evening news for days - pretty scarey

TMI System

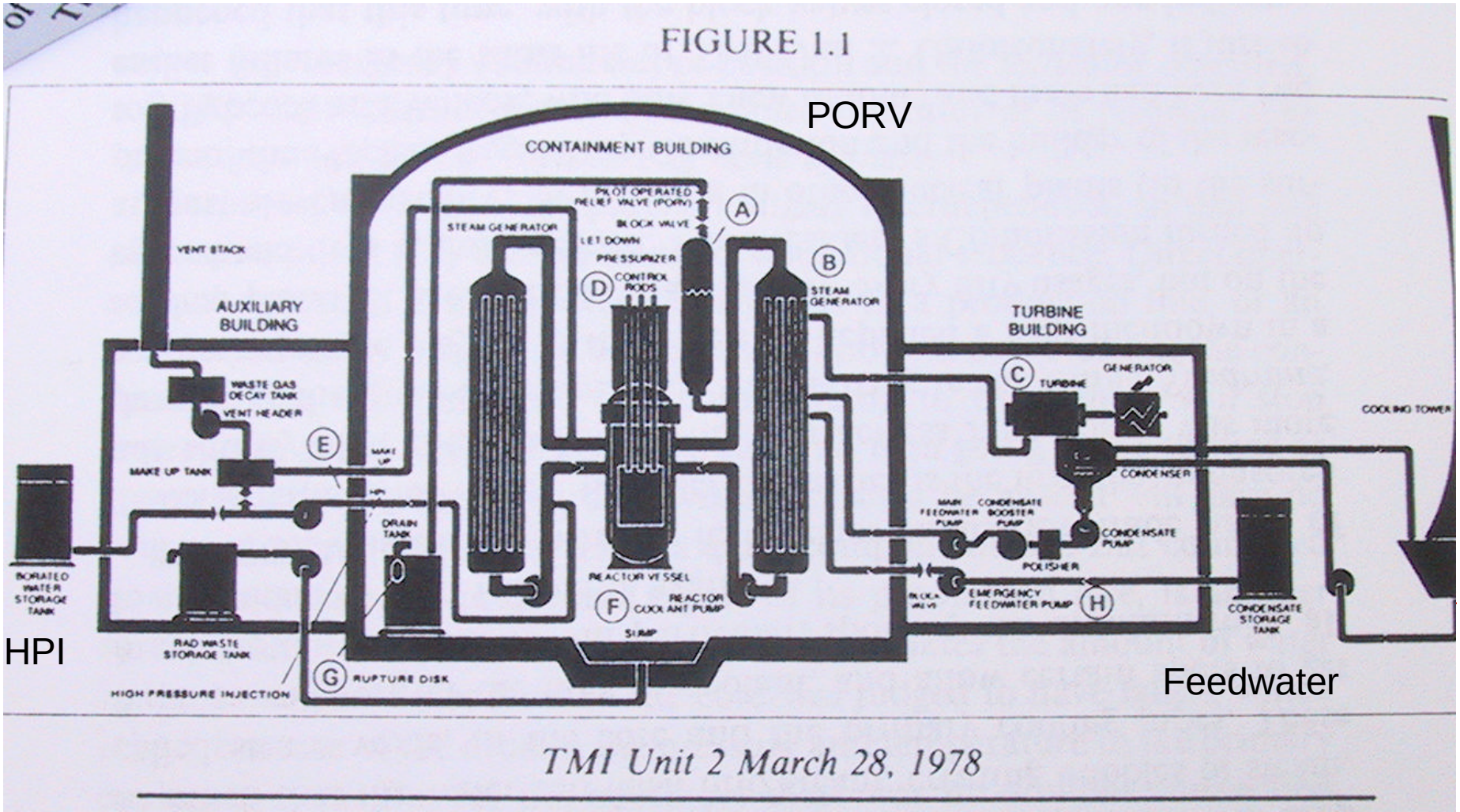


FIGURE 1.1
PORV
CONTAINMENT BUILDING
PILOT OPERATED RELIEF VALVE (PORV)
BLOCK VALVE
LET DOWN
PRESSURIZER
CONTROL RODS
STEAM GENERATOR
VENT STACK
AUXILIARY BUILDING
TURBINE BUILDING
WASTE GAS DECAY TANK
VENT HEADER
MAKE UP TANK
MAKE UP
HPI
DRAIN TANK
TURBINE
GENERATOR
CONDENSER
COOLING TOWER
MAIN FEEDWATER PUMP
CONDENSATE BOOSTER PUMP
CONDENSATE PUMP
POLISHER
BORATED WATER STORAGE TANK
REACTOR VESSEL
REACTOR COOLANT PUMP
SUMP
EMERGENCY FEEDWATER PUMP
CONDENSATE STORAGE TANK
RAD WASTE STORAGE TANK
HIGH PRESSURE INJECTION
RUPTURE DISK
A
B
C
D
E
F
G
H
HPI
Feedwater
TMI Unit 2 March 28, 1978

Cooling System

- Primary Cooling System
  - High pressure, radioactive, water circulating through the reactor.
  - Heat Exchanger transfers heat to the secondary system
- Secondary Cooling System
  - Cools the primary cooling system
  - Creates steam to run the turbines to generate electricity
  - Due to thin tubes in the turbine it must be very pure
  - Continuously cleaned by a "polisher system"

How it started

- The polisher leaked about a cup a day of water through a seal
- Water vapor got into a pneumatic system that drives some instruments
- This water vapor interrupted pressure to two valves in the feedwater system, which caused two feedwater pumps to shut down
- Lack of flow in the secondary system triggered a safety system that shut down the turbines
- This was the first indication of trouble to the operators
- At this point the reactor still needs to be cooled - or else

Emergency feedwater takes over

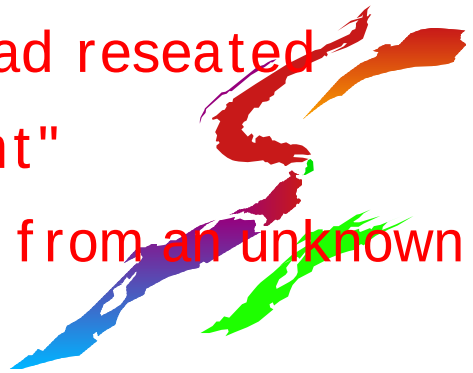
- An emergency feedwater system starts up to pump stored cold water through the secondary system to remove the accumulating heat
- The pumps were running, but valves on the pipes were incorrectly left closed from prior maintenance
  - The operators insist they were left open
  - The check lists say they were opened
- A Repair Tag on a broken indicator hung over the indicator on the control panel that indicated that the valves were closed
- Redundant pipes, redundant pumps, and redundant valves, all thwarted by having the two valves physically at the same place and miss set
- Eight minutes later they noticed they were shut
  - by then the damage was done

With no cooling the reactor got hot

- Due to overheating the reactor "scrammed" automatically
  - This shuts down the reaction
- Enough heat remains in the reactor to require a normal working cooling several days to cool off
- Without cooling the pressure goes up
- An ASU Automatic Safety Device takes over to temporarily relieve the pressure: the Pilot Operated Relief Valve (PORV)

PORV

- The PORV is supposed to vent pressure briefly, and then reclose
  - If it stays open too long liquid escapes, pressure in the reactor drops, steam forms causing voids in the water, cooling is impaired and some places get yet hotter
- Thirty-two thousand gallons of water eventually went out this unclosed valve
- There was an indication on the control panel that the message to reseat had been sent to the valve
  - However, no indication was available that it had reseated
- We are now thirteen seconds into the "transient"
  - An indicator shows that there is extra water from an unknown source

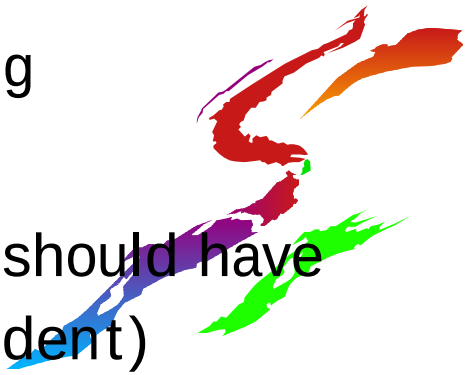


Automatic Coolant Pump Starts

- This is another automatic safety system that pumps water to cool the reactor automatically starts at 13 seconds. The second was manually started by the operator
- For three minutes it looked like the core was being cooled successfully
  - However, apparently due to the steam voids, the cooling was not happening
- The secondary steam generators were not getting water and boiled dry - at the same time water was flowing out of the primary cooling system through the stuck pressure relief valve

High Pressure Injection (HPI) Starts

- This is an automatic emergency device that forces cold water into the reactor to cool it down.
- The reactor was flooded for two minutes, and then the operators drastically cut back the flow
  - this was reguarded as the key operator error
  - what they did not realize was that the water was flowing out the PORV and the core would become uncovered
- Two dials confused the operators:
  - one said the pressure in the reactor was rising
  - the other said it was falling
- The Kemeny commission thought the operators should have realized this meant LOCA (Loss of Coolant Accident)



Conditions in the control room

- Three audible alarms are making a din
- Many of the 1,600 indicator lights are blinking
- The computer is way behind in printing out error messages
  - It turns out they can only be printed, not spooled to disk, to see the current condition they would have to purge the printer and loose potentially valuable information
- The reactor coolant pumps begin the bang and shake, due to cavitation from lack of water to pump-they are shut off

Stuck open PORV valve discovered!

- The operators checked the valve and found it open
- They closed it
  - With some trepidation since they were messing with a safety system
- The reactor core had been uncovered at this point and had partially melted
- Another 30 minutes without coolant and it would probably have been a total melt down

The Hydrogen Bubble

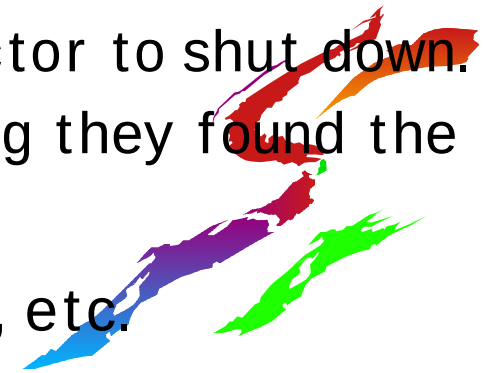
- If the cladding on the uranium pills gets too hot in the presence of water Hydrogen gas is given off
- At one point, 33 hours into the incident, there was an explosion and spiking of the instruments
- Pressure reached half the rated pressure of the containment building
  - The containment building had been significantly over engineered out of concern of being hit by an airplane from a nearby airport
  - Three years later they found the damage done in the containment building by the missiles thrown by the explosion
    - The working systems cooling and controling the reactor might have been damaged, but were not

Finally under control

- At this point the reactor eventually was cooled down
- and the investigation heated up
- In the end the operators were blamed
  - though the commission members could not agree on what the errors were

Is this typical?

- Perrow chronicles a number of other nuclear incidents, without the magnitude, but with the characteristic errors
- Indian Point Number 2
  - An indicator light is viewed as faulty, while 100,000 gallons of cold Hudson riverwater accumulate around the reactor from a broken pipe
  - Another indicator, to measure water, does not detect it because it is designed to detect hot water
  - An unrelated operator error caused the reactor to shut down. When they went into the containment building they found the 9 feet of water around the reactor
- Dresden number 2 in Chicago, Fermi in Detroit, etc.



Common characteristics

- The whole system is never all up and working as designed
  - thus it is hard to understand
- When things start to fail the system is even harder to understand
- Safety systems are not always working
  - some are down, and known to be
  - some are accidentally turned off
  - some are not set properly
  - others fail to work when needed
- There are often not direct indicators of what is happening
  - operators figure it out indirectly

Defense in Depth

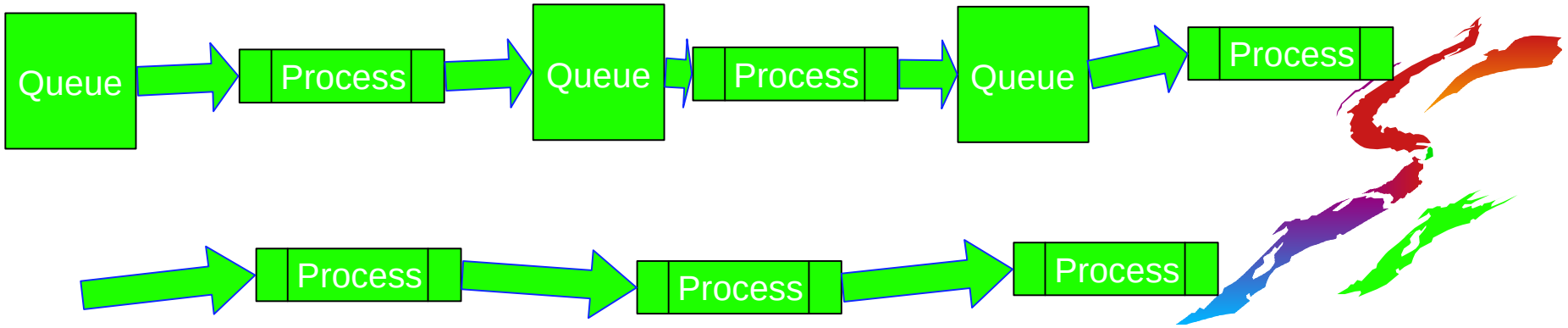
- Nuclear power systems are as safe as they are because of defense in depth
  - Many levels of systems and containment
  - Ultimately the containment building is supposed to contain a meltdown
    - (Early Russian reactors did not have them)
  - The containment building has negative pressure, so even if cracked, air will not escape

Some Definitions:

- Coupling
  - Tight
    - direct and immediate connection and interaction between components
  - Loose
    - slack or buffering between components
- Interactions, and transformation processes
  - Linear
    - orderly step by step with only interactions with adjacent steps, easy isolation of components
  - Complex
    - many connections and interrelationships

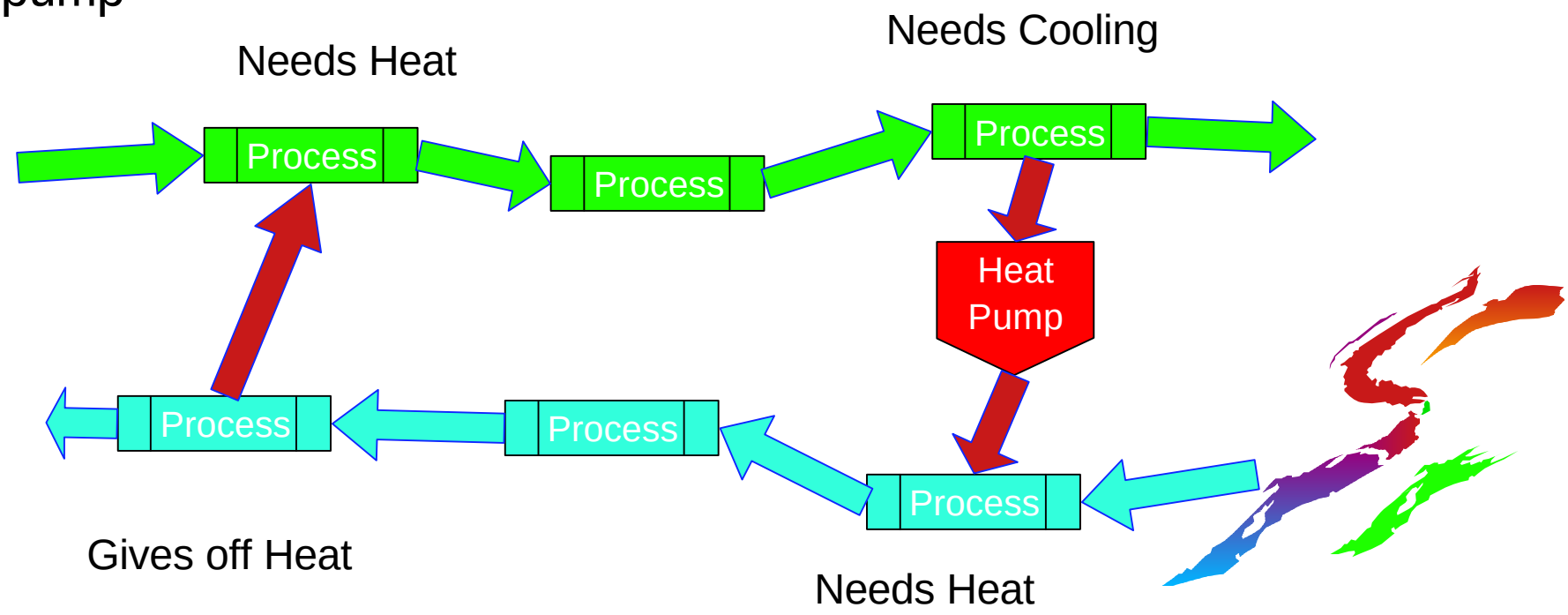
Assembly Line of workstations

- Loose and linear
  - assuming that there is space to store work in progress between workstations
- Tight and linear
  - assuming something like automobile assembly where the frame moves by and there is only so much time to add in each item
  - Bread baking

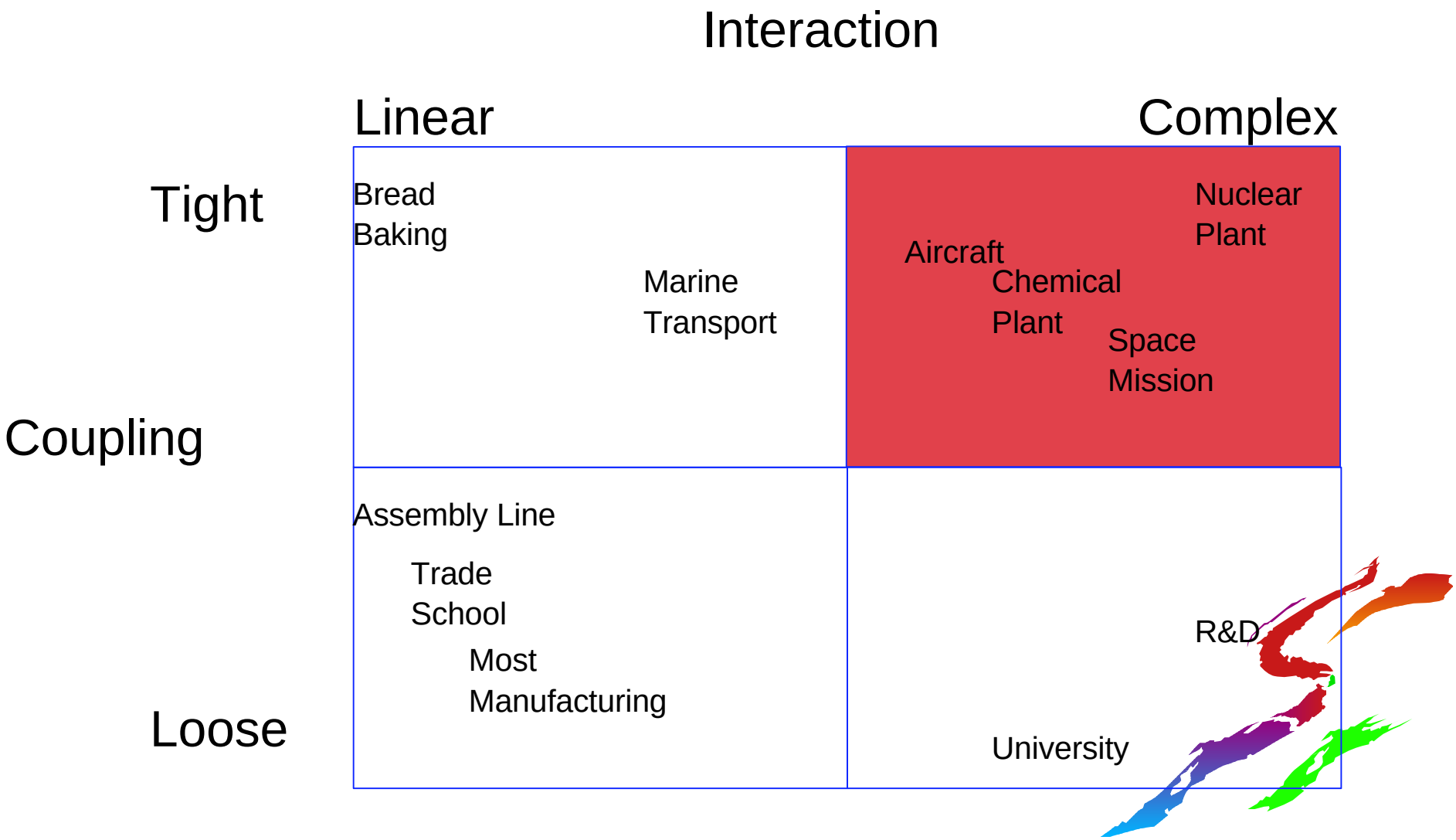


Chemical Plant

- Tight and complex
- Heat given off by one process is used to heat a step of another by transfering the heat
- One step is cooled and another is heated by a heat pump



Interactions and coupling



Air Transportation

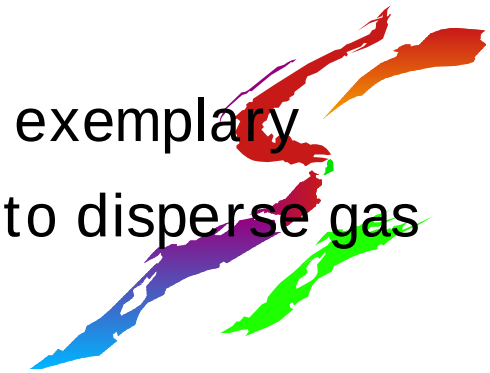
- Structuraly favors safety
  - Industry elites, regulatory elites, politicians fly
  - Lots of independendent redundant equipment
  - Pilot Co-pilot relationship
    - They talk a lot and agree
    - If they are wrong, they are both wrong
  - Cockpit automation
    - "the burning question... is not how much a man can work but how little"

Air Transportation becoming less coupled

- Built in buffers
  - spacing
  - ability to be late
  - abort takeoff or landing
  - planes can move in three dimensions
- Restricted air space
- flight lanes by type of aircraft
- Less use of voice communication
  - aircraft reports altitude all the time
- Technology is primarily improving throughput

Chemical Plants

- Bhopal: December 1984
  - Nothing complex, just component failure
- Declining profits
  - operations crew cut in half
  - maintenance crew cut in half
- "it takes the right combination of circumstances to produce a catastrophe"
  - No warning, no evacuation plan, no alarms, people asleep nearby, light wind in the right direction
- Similar plant at Institute West Virginia-OSHA exemplary
- August 11, 1985 - West Virginia-weather right to disperse gas
  - OSHA "accident waiting to happen"



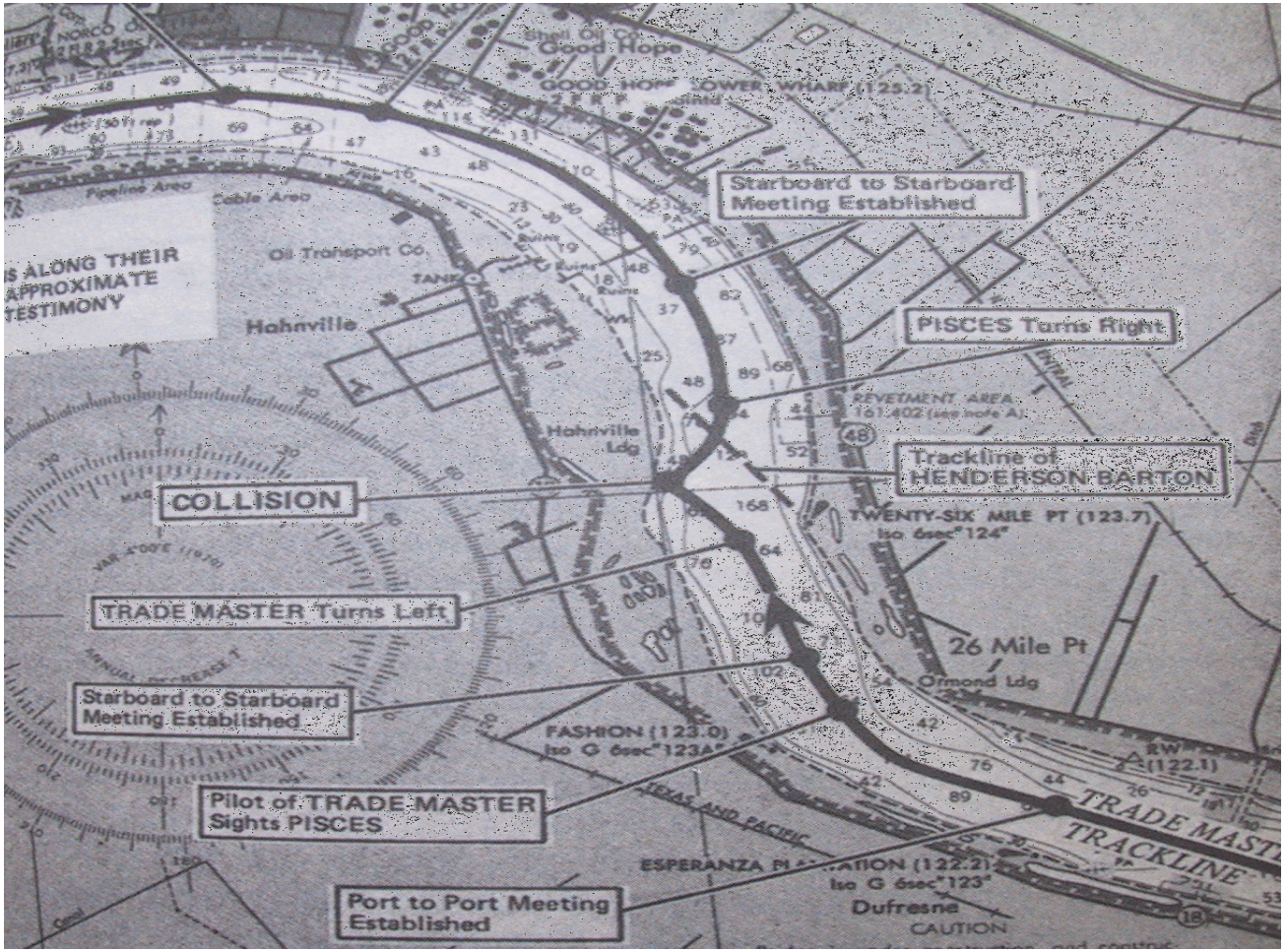
Marine Accidents

- Structurally encourages accidents
  - no high profile riders, Senators don't travel on freighters
  - risk is easily accepted as part of tradition of the sea
  - emphasis on throughput
  - poor maintenance
  - safety systems not turned on or not working
  - The captain is god
    - The mate stands by silently while they ground
- Technology improvements all go to throughput
  - no reduction in accidents
- Lots of interesting sea stories, but not terribly relevant to us

Marine Accidents - Passing in rivers

- Passing on rivers is a big problem
  - Pilots agree by radio about port to port or starboard to starboard
  - Classical one bit agreement problem
  - Gets more complex because convoys form
  - Poor radio discipline
  - A missed message and they hit each other

Pisces and Trade Master



NORAD

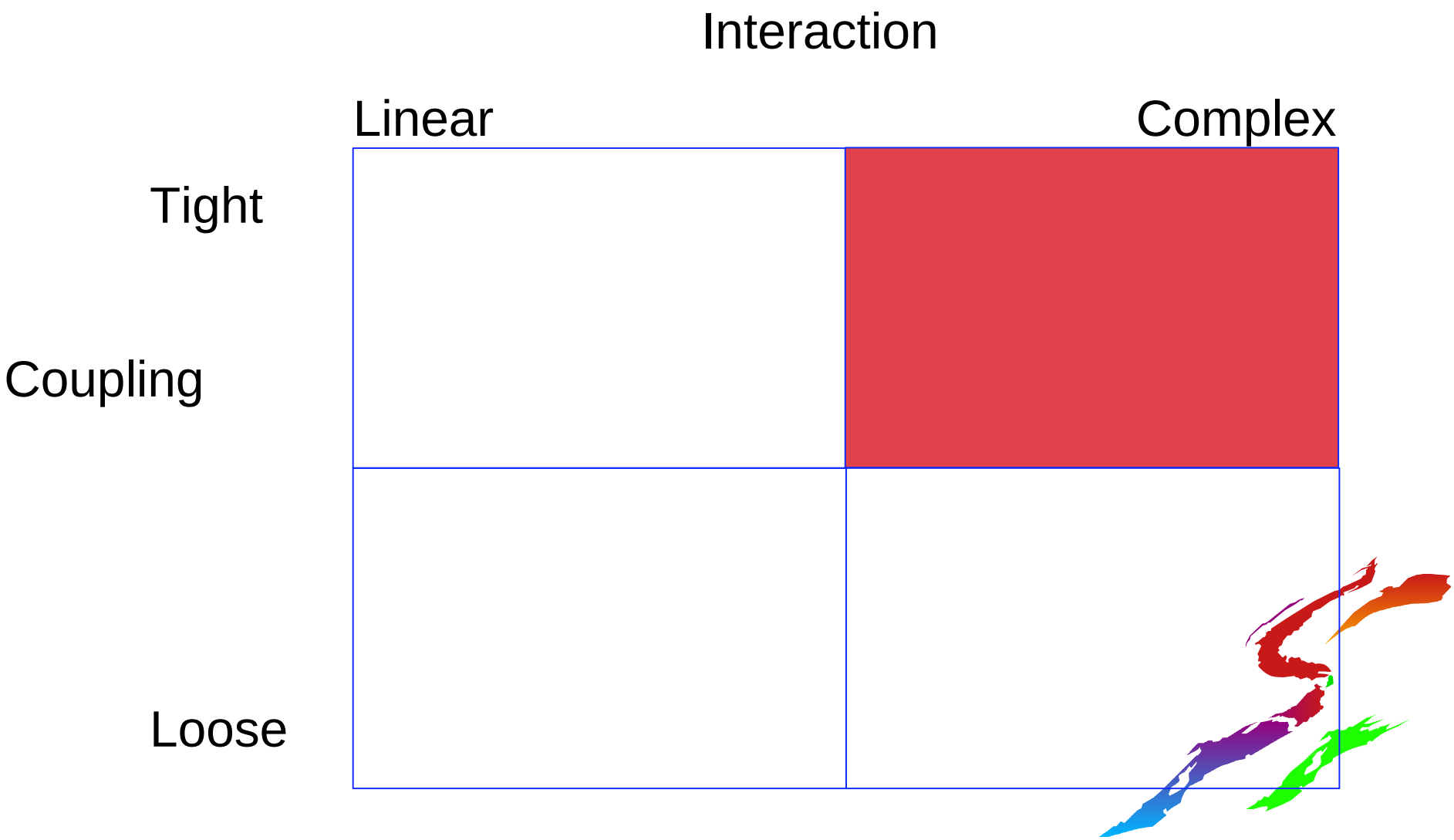
- Cheyenne Mountain Colorado
- Early warning command center
- When something goes "off" a "missile display conference" is called
  - In 1979 there were 1544
  - In first half 1980, there were 2159
- They tollerate lots of false positives to eliminate false negatives
- Two major unconnected systems
  - Satellites pick up launch
  - Radar picks up incoming flight
    - First Alaska, second North Dakota

Common Threads I found

- Multiple errors are commonplace
  - birthday paradox
- Complex systems are never actually fulling working or working properly
  - some things are known and some not
    - lights and sensors not working
  - they become hard to understand
- Backup and automatic safety systems
  - not all working properly, only some known
  - not fully or regularly tested
- Indirect measurements or no measurements
  - hard to figure out the state in an emergency
    - POV open, but told to close, is the core uncovered?
- Tendancy to blame the Operator

Place these systems:

- micro processor thermostat
- multiprogramming and multiprocessing many applications on one OS
- Single server groved for one application
- Operating system
- The internet


Interaction
Linear
Complex
Tight
Coupling
Loose

High Confidence Computing Questions?

- Are there "system accidents" in computing?
- How does defense in depth relate to computing systems?
- What computing systems are "complex?" and what are "linear?"
- Can computing systems be made more "linear?"
- What computing systems have "tight" coupling and "loose" coupling
- How can computing systems be designed to have more "loose" coupling?
- Storage overlay
- Tendancy to use single purpose servers

Promising References

- Levenson, Nancy, 1995, Safeware: System Safety and Computers, New York, Addison Wesley
- Neumann, Peter G, 1999, "Risk Digest," www.comp.risks
- Rushby, John, 1994, "Critical System Properties: Survey and Taxonomy," Reliability Engineering and System Safety, 43:189-210
- Reliable Software through Composite Design, Glenford Myers, 1975

Finish