

**ATK Launch Systems
Crane Safety & Handling Symposium**

**Orbiter Payload Bay Bucket Hoist
Mishap... An Accident
We Should Never Forget**

Bradford P. Lytle, P.E.

November 5, 2009

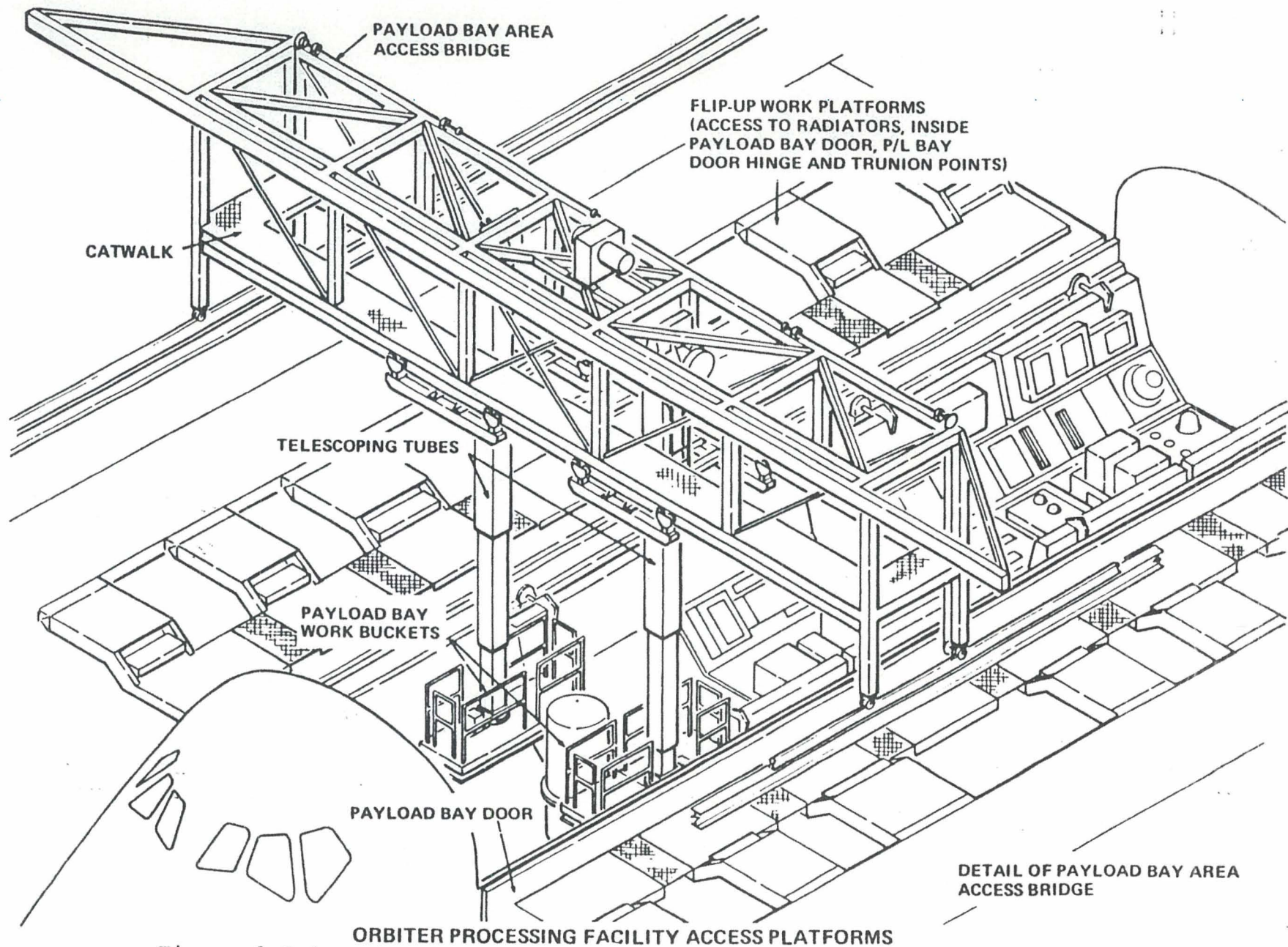
NASA Kennedy Space Center

Phone: (321) 867-8539

Email: bradford.p.lytle@nasa.gov

- Agenda
 - What happened?
 - Why did this happen?
 - Discussion on Two-Blocking
 - NASA requirements for two upper limit switches
 - Limit switch set up and testing
 - Lessons learned, how each of us could have prevented this accident.

- KSC Orbiter Processing Facility, Orbiter Payload Bay Bucket Hoist Mishap
 - March 8, 1985, during final closeout of the orbiter Discovery, a payload bay access platform fell from its stowed position.
 - This resulted in damage to the Discovery's insulating blankets and forward payload bay door.
 - A Lockheed Technician suffered a broken leg.
 - This delayed launch by approximately three weeks.



ORBITER PROCESSING FACILITY ACCESS PLATFORMS

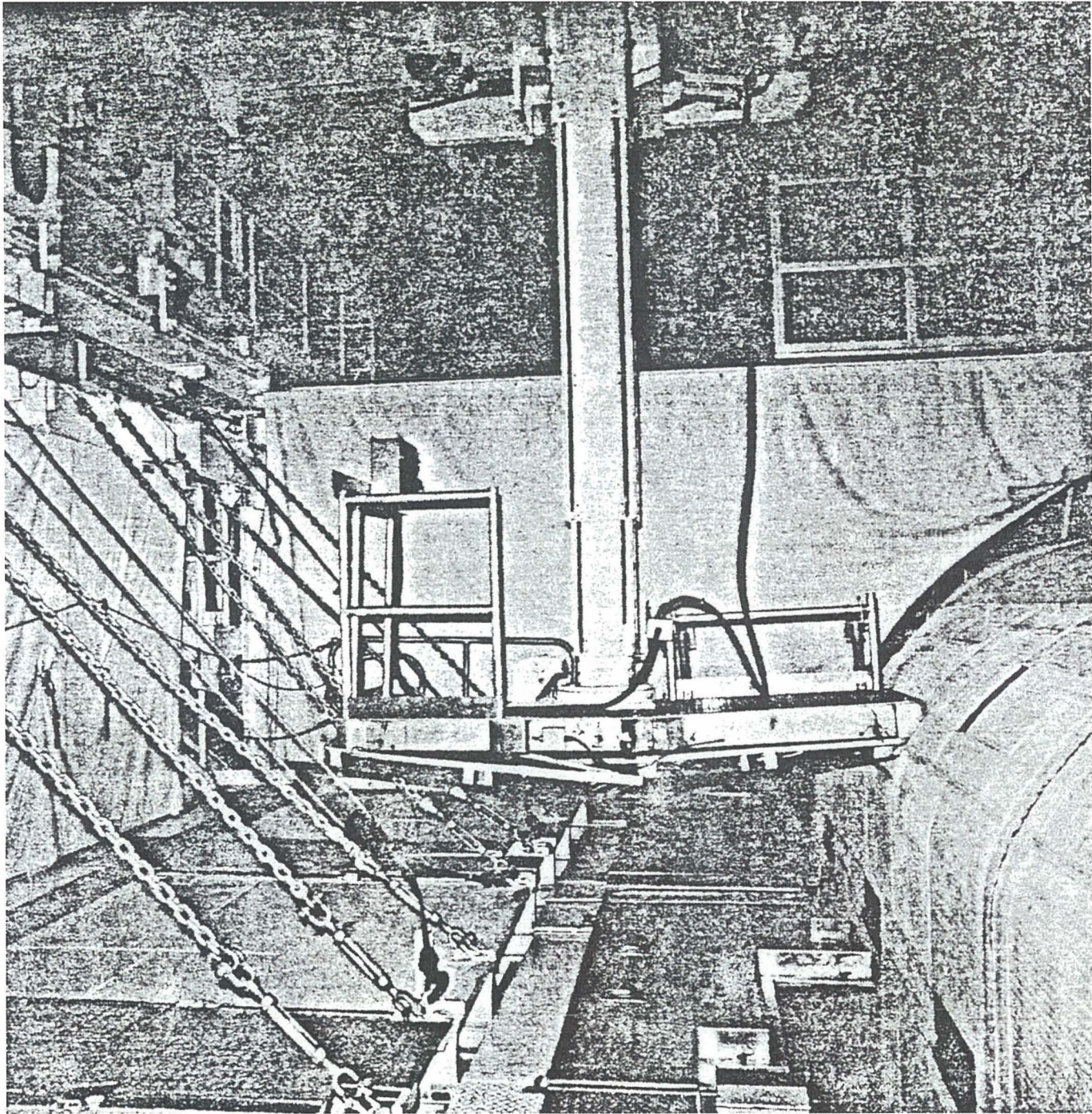
Figure 9-B-1. Sketch of OPF Access Platforms on bridge crane, upper view

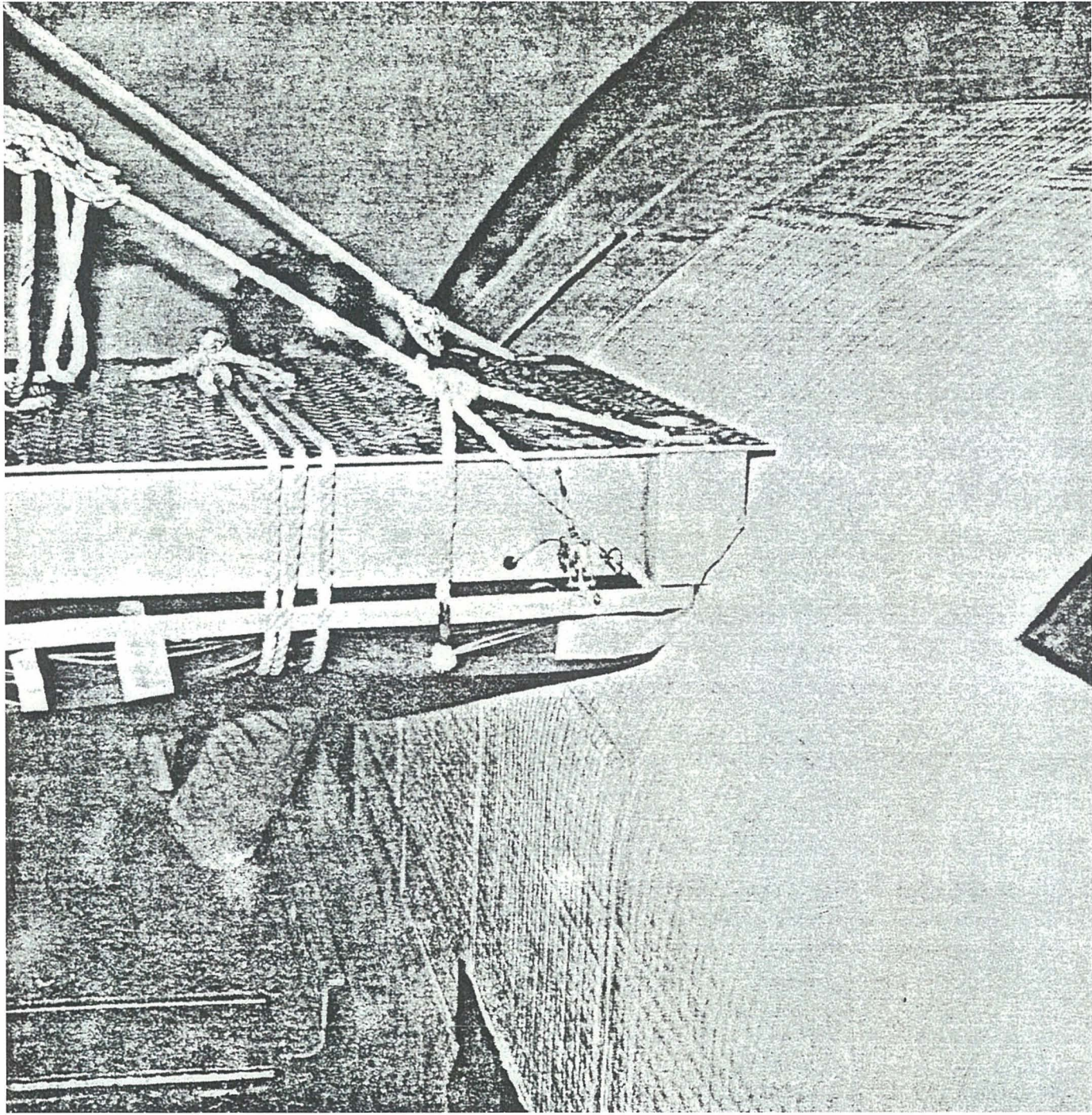


OPF Payload Bucket Hoist



OPF Payload Bucket Hoist





ENGINEERING
DEVELOPMENT
DIRECTORATE

48

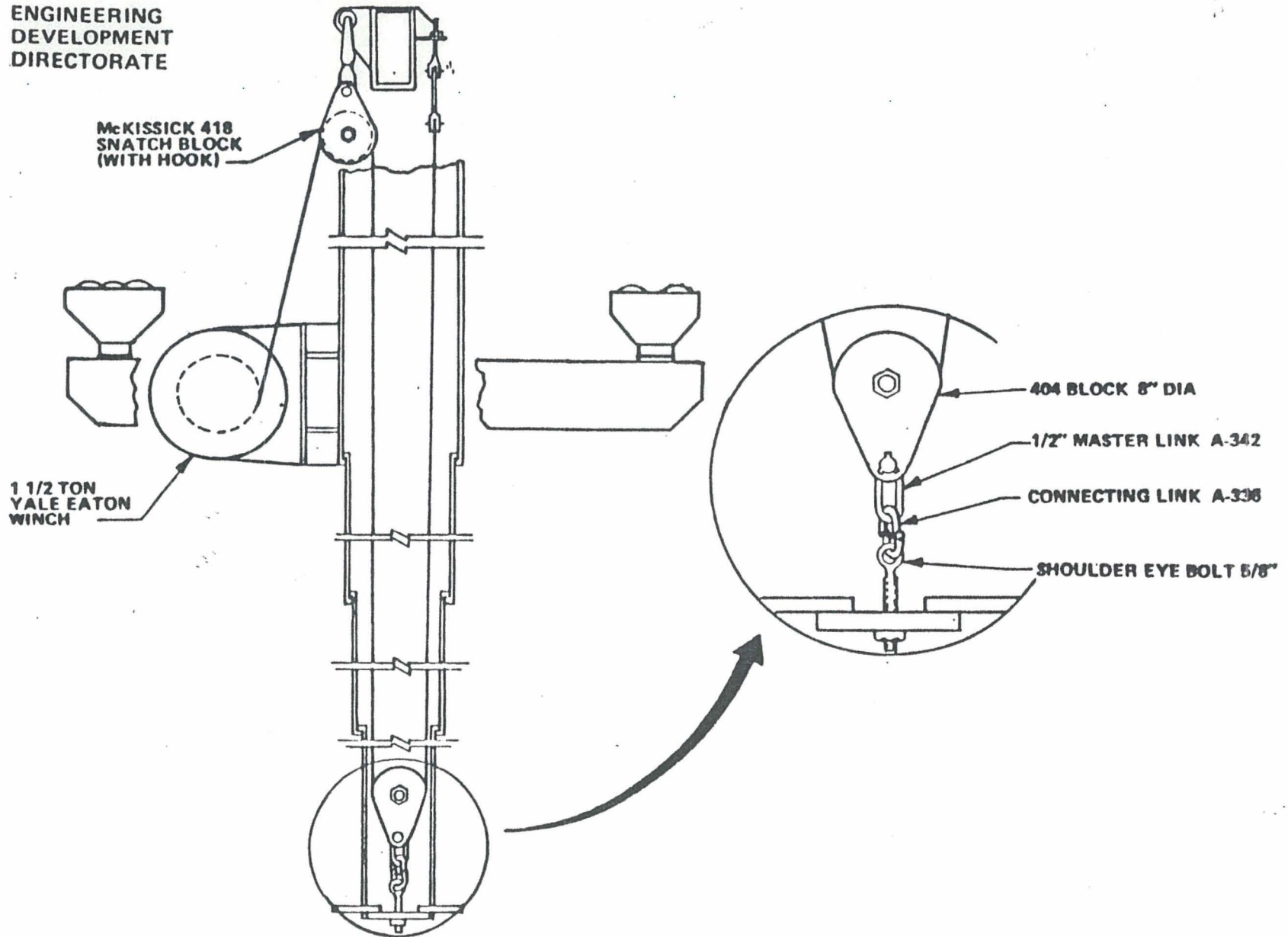


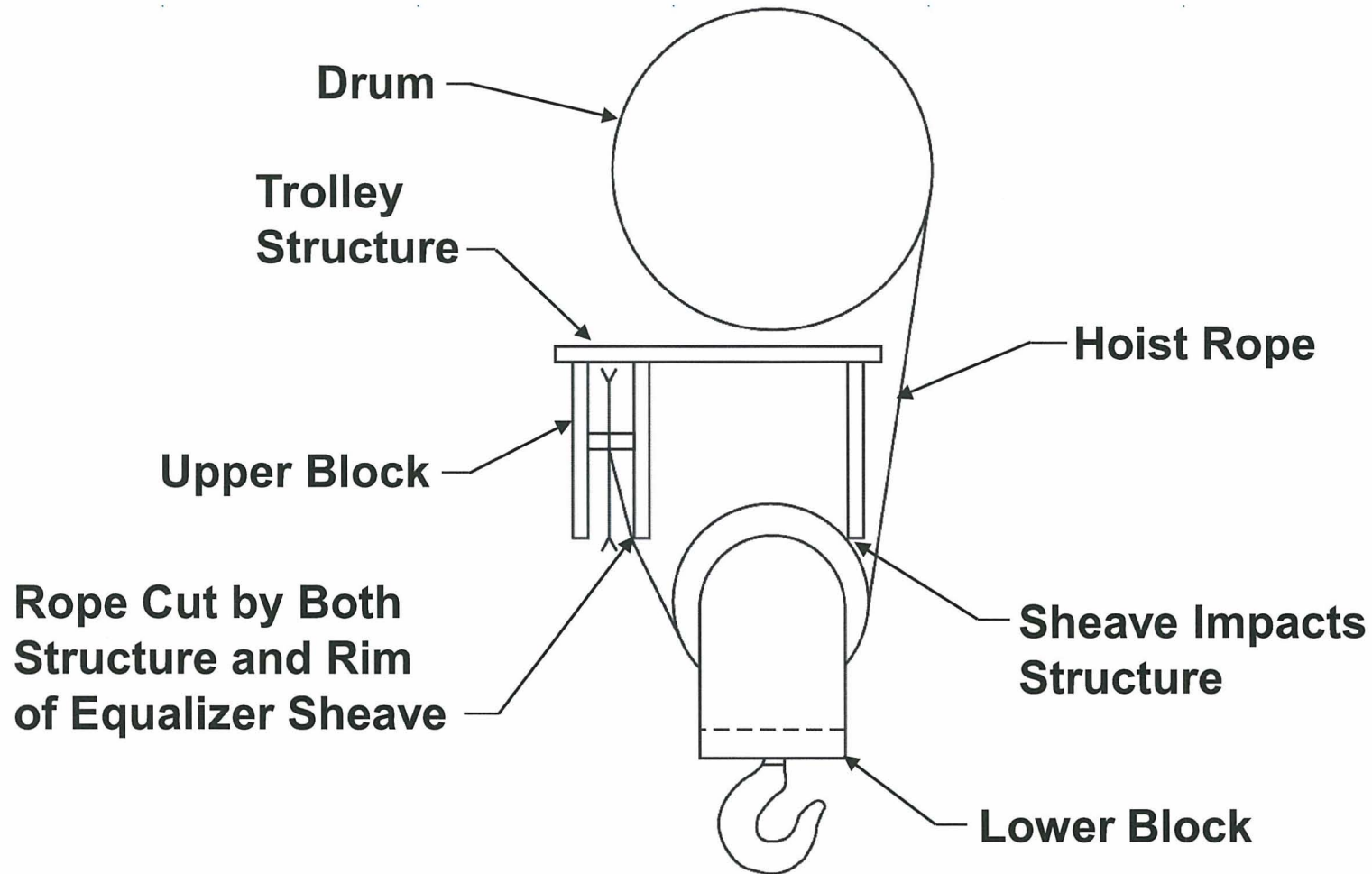
Figure 9-B-2. Side view of Access Platform hoist, cable system, and telescoping tubes

- While placing the platform in the full up position to stow the bucket hoist the operators were using the upper limit switch as a control stop (only one control type upper limit switch).
- The location of the limit switch set point and the mechanical configuration of telescoping tube assemblies was so close that there was little room for drift between the limit switch actuation point / hoist stop point and mechanical contact between the telescoping tube assemblies and hard structure. All 8 Payload Bucket Hoists were adjusted the same way.

Why did this Happen?

- In effect they were running the risk of two-blocking the hoist every time they used the upper limit switch to stow the bucket hoist in the full up position.
- Two blocking is about the worse thing you can do to a hoist. You only need to two block a hoist once to cause a failure and drop the load.

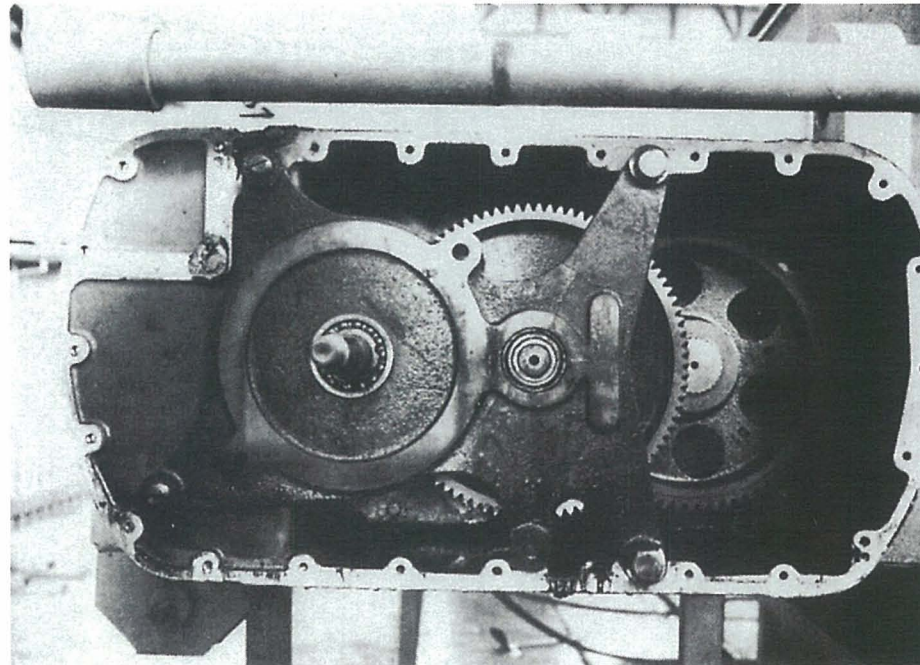
- Two-Blocking
 - Two-blocking is the result of hoisting beyond the intended safe upper limit of hook travel to the point of solid contact between the load block and the upper block or hoist/trolley structure. The usual result is immediate failure of the wire rope, due to the ropes being cut by the grooves of the drum or sheaves.



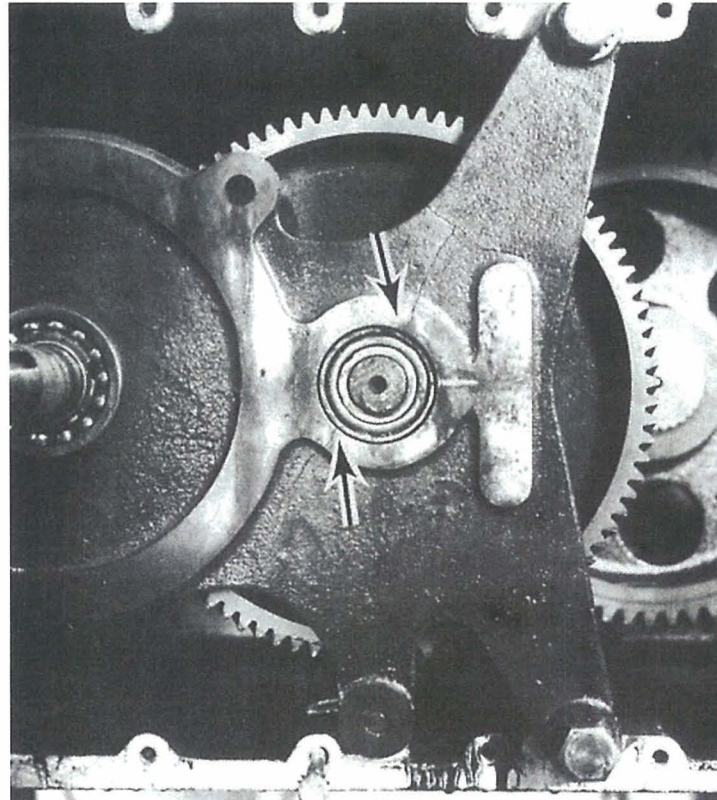
Two-Blocking

- Play the Two Block film clip.

- Two Blocking (continued)
 - The electric motor can produce high torque in a fraction of a second.
 - A DC motor can produce 180% of rated motor torque.
 - An AC motor can produce 275% of rated motor torque.
 - we are assuming the hoist motor is not oversized.
 - During the two block event two things happen at the instant the upper and lower block impact.
 - First the motor torque increases abruptly, secondly the rotational inertia of the hoist motor adds to the motor torque.
 - If the wire rope does not fail something else will. Perhaps damage will be hidden (in a coupling or gear reducer).
 - Commercial hoist machinery is not designed to withstand the loads created during two blocking.



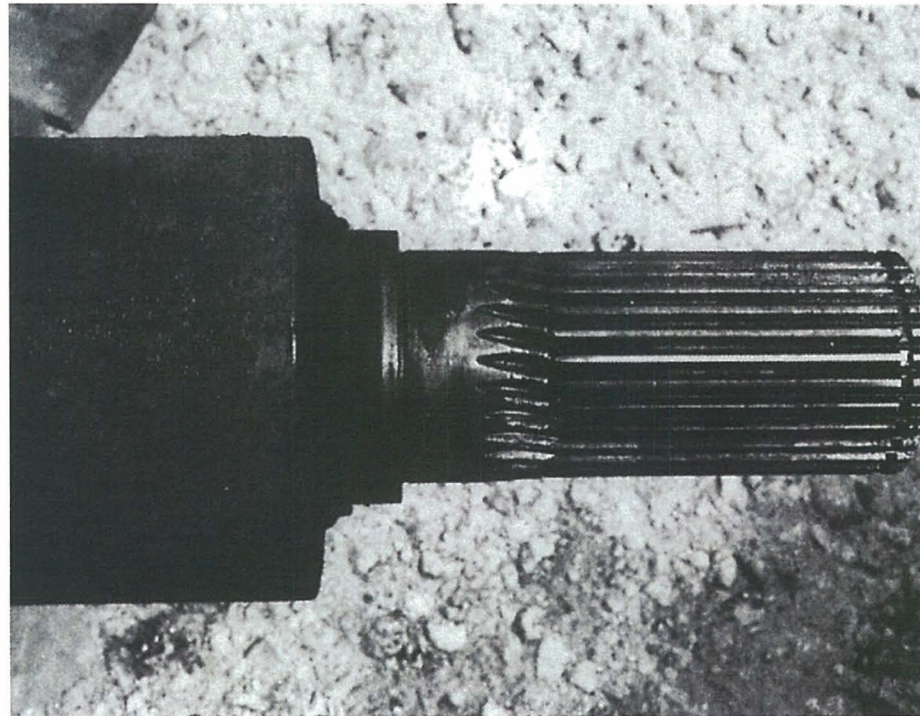
Gear Box Depicting the Spider Plate and Relative Position of the Spider in the Gear Box



Cracks Around the Shaft and Bearing



Spider Plate Removed From the Gear Box



**Drum Shaft Spline Depicting the Deformation Found
After the Spider Failure**

- The bucket hoist has two fully redundant attachment points to the telescoping tubes and a length of wire rope (that would act like a spring between the attachment point and the wire rope drum).
- This redundant design appears to provide unparalleled strength and safety, i.e. two separate load paths.
- However, two blocking is so severe the redundant load paths and the high design margins does not provide protection against the loads imposed from two blocking!

ENGINEERING
DEVELOPMENT
DIRECTORATE

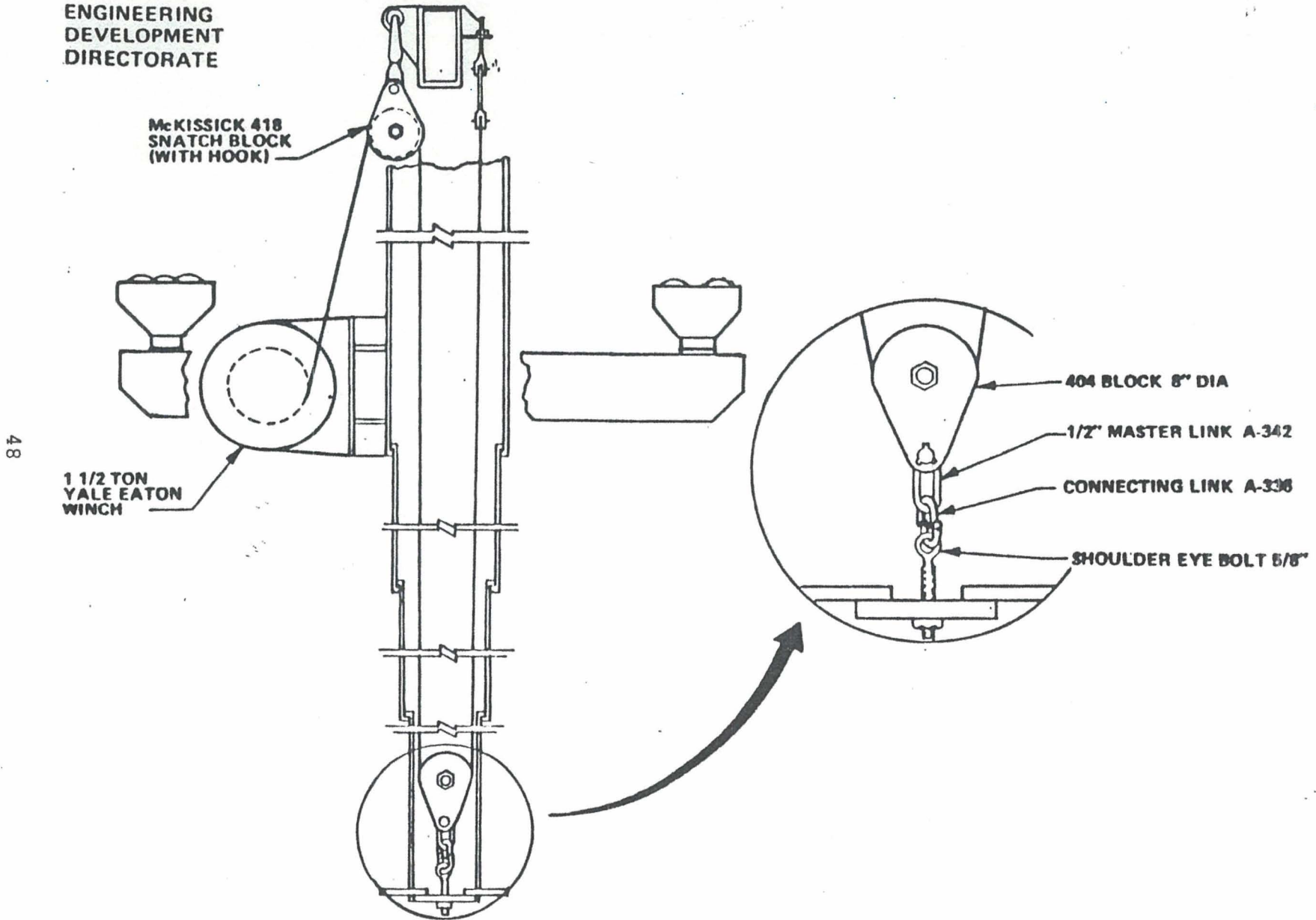


Figure 9-B-2. Side view of Access Platform hoist, cable system, and telescoping tubes

- The operators were “just barely” two blocking the hoist every time they stowed the bucket.
 - Before the accident... inspection of the 10 inch telescoping tubes revealed evidence of metal to metal contact on the supporting structure. Apparently no action was taken by the inspectors.
 - Before the accident... The actuator arm on the hoist limit switch broke. The Bucket Hoist was Locked Out / Tagged Out until repairs could be made.
 - The operators were confused about the type of Lock Out / Tag Out imposed on the equipment and they operated the unit anyway.

- Before the accident... The Training / Certification course “OPF / High Bay Bridge Bucket Operator Certification “ taught all operators to use the upper limit switch as an operating control during stow operations. Approximately 200 people were certified to operate these units.
- After the accident... all buckets hoist were inspected, of the 8 bucket hoists 7 showed signs of damage as demonstrated by elongated or cracked master links (the accident was going to happen, it could have happened on any payload bucket it was just a matter of time...)

- The NASA Safety Standard NASA-STD-8719.9 requires two upper limit switches. This is to prevent two blocking.
- The switches should be electrically independent such that a common electrical failure cannot render both switches inoperable.
 - Usually the first switch is a “control” limit switch arranged to stop hoisting but allow lowering.
 - The second limit switch is a “power” limit switch arranged to remove power from the hoist. This switch will stop all hoist motion (sometimes shut down the crane). This is our last chance to prevent Two Block!

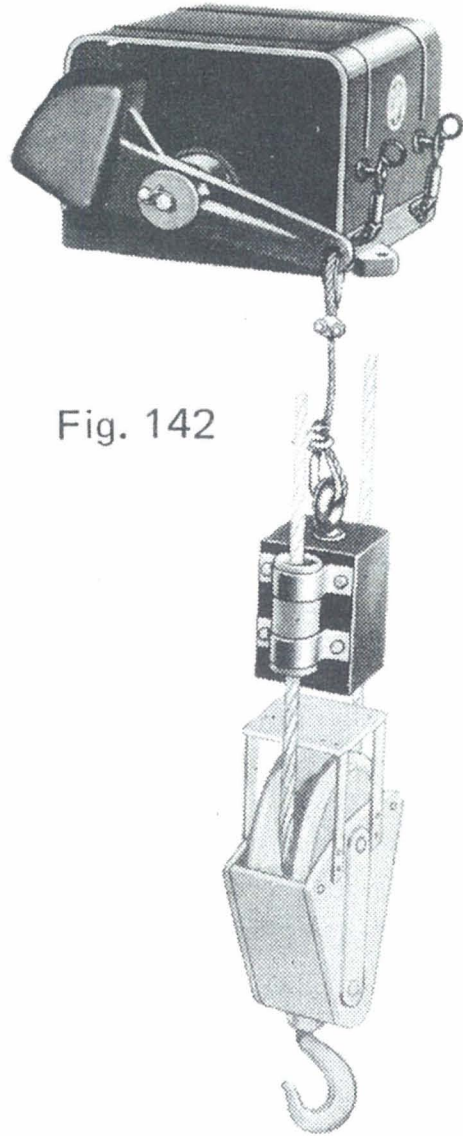


Fig. 142

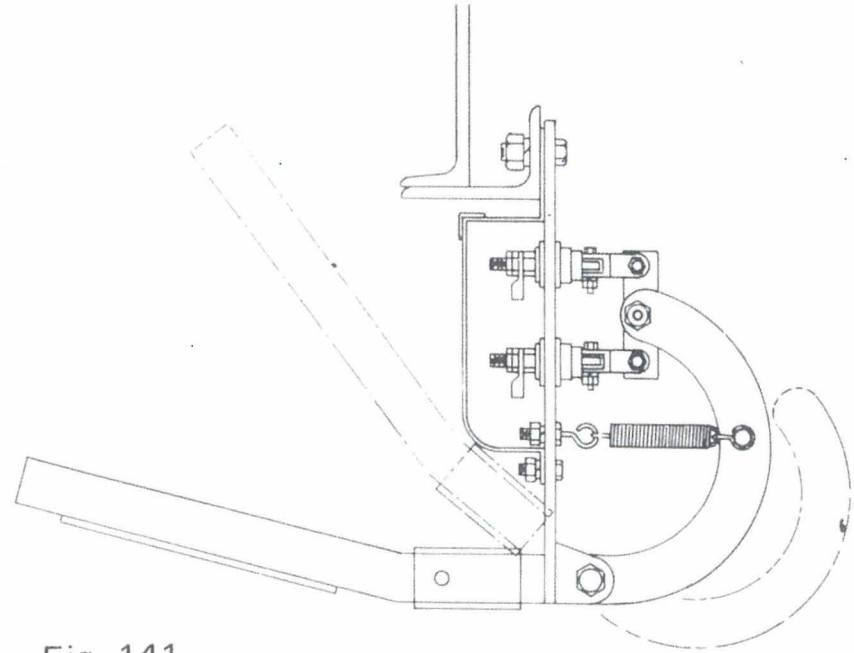
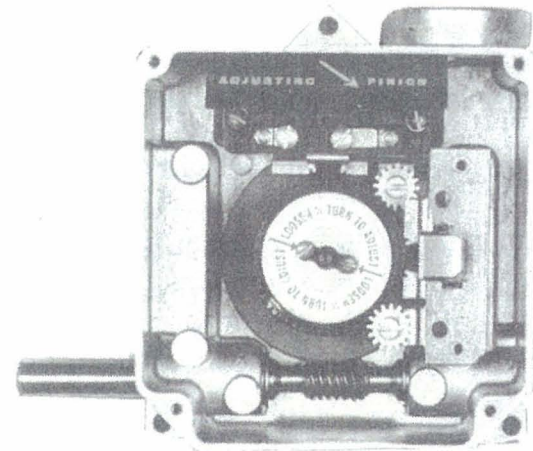
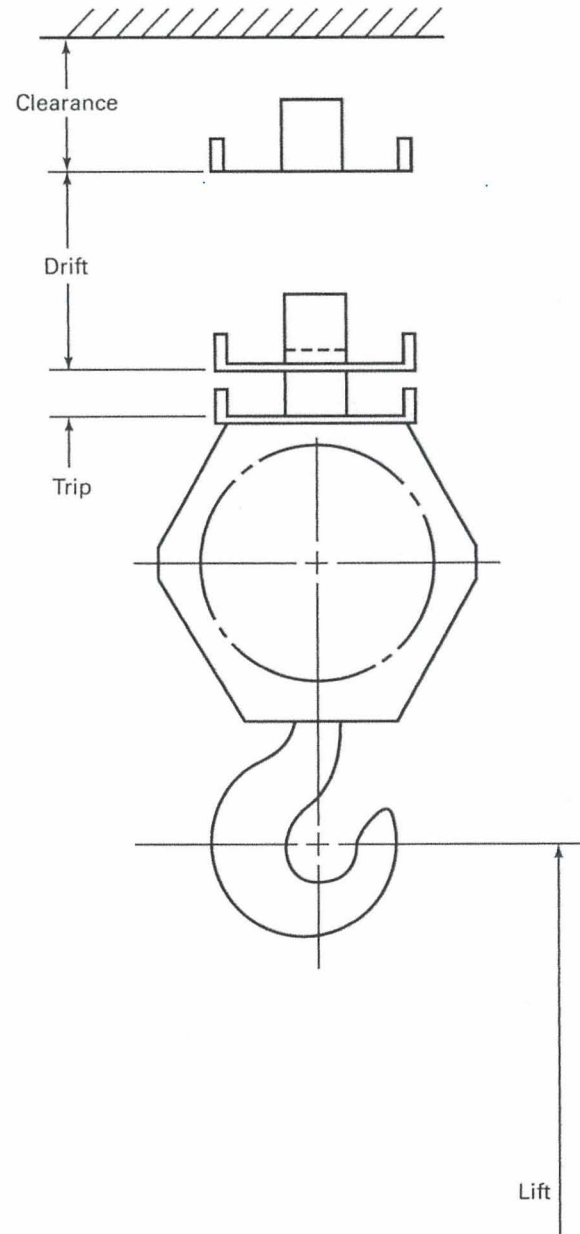
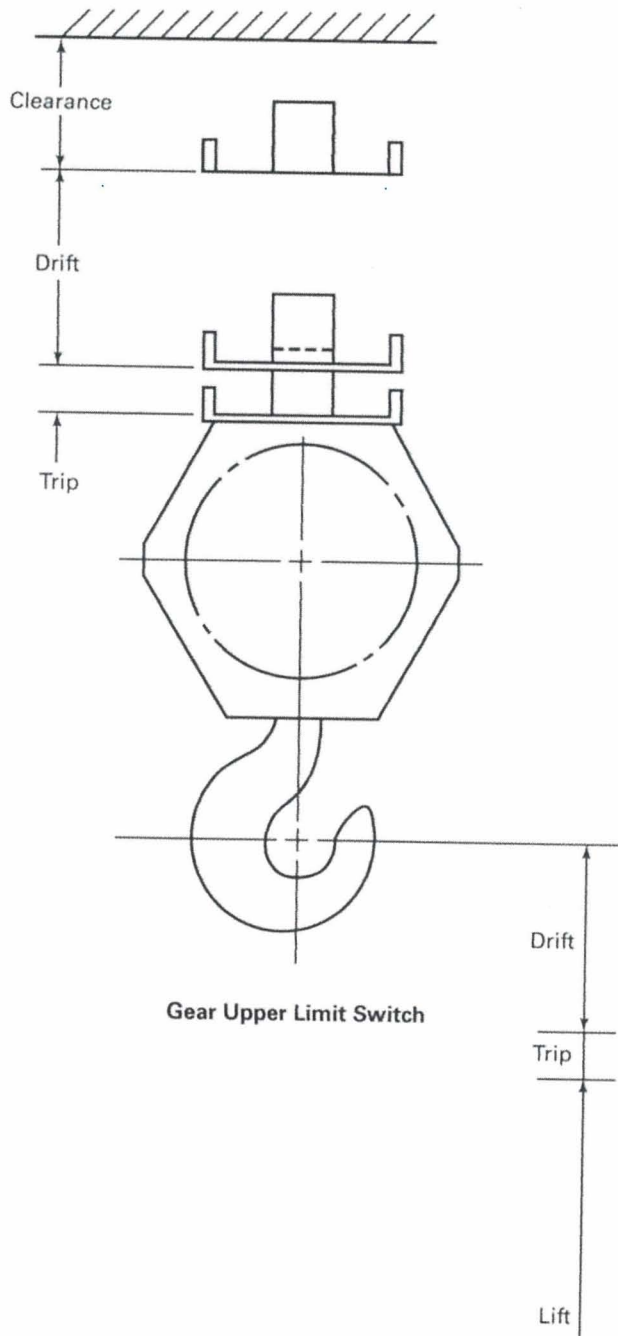


Fig. 141



- The failure of one switch is always backed up by the second switch. This is a fundamental design philosophy.
- Also the power upper limit switch usually a weight operated switch is very simple in design and should always work (but they have been known to fail).
- The actuation or set point of the limit switch is very important.



- Note in the figure... Each limit switch needs adequate space between their set points
 - They must have a distance to trip the switch
 - They must have adequate distance to allow for drift
 - And finally they must have adequate clearance between the each switch.
- Adequate space is necessary between the two switches and between the final switch and two blocking.

- The two switches complement each other. They provide an additional layer of protection... in the event one switch fails.
- The switches are of different types and they perform a different function. If the geared limit switch fails you know something is wrong.
 - If you approach the control limit switch and the crane shuts down you know the control switch has failed.
 - Also the control switch should be tested at the start of each operation to assure it's functioning properly.

- If the geared limit switch does not work during “start of operation testing” (and you move into the power limit switch), the power limit switch will shut down the crane and you are stuck! You cannot move until the power limit switch is reset. This is telling you something... you almost two-blocked! This is how you know something is wrong and it forces the operator to notify engineering. The geared limit is not working correctly and needs immediate attention (your operation must stop until this switch is fixed)!
- The power switch should be tested periodically to assure it’s functioning. It’s simple design assures its operation (at least most of the time).

- You should never use a limit switch as an operational control.
- The safety standards are very explicit about the upper limit switch design, setup and testing requirements. These requirements are there for good reason. Two blocking is the most devastating and unforgiving accident that can occur on a hoist. That is what these limit switches are for, its up to us to assure they are in place and functioning correctly.

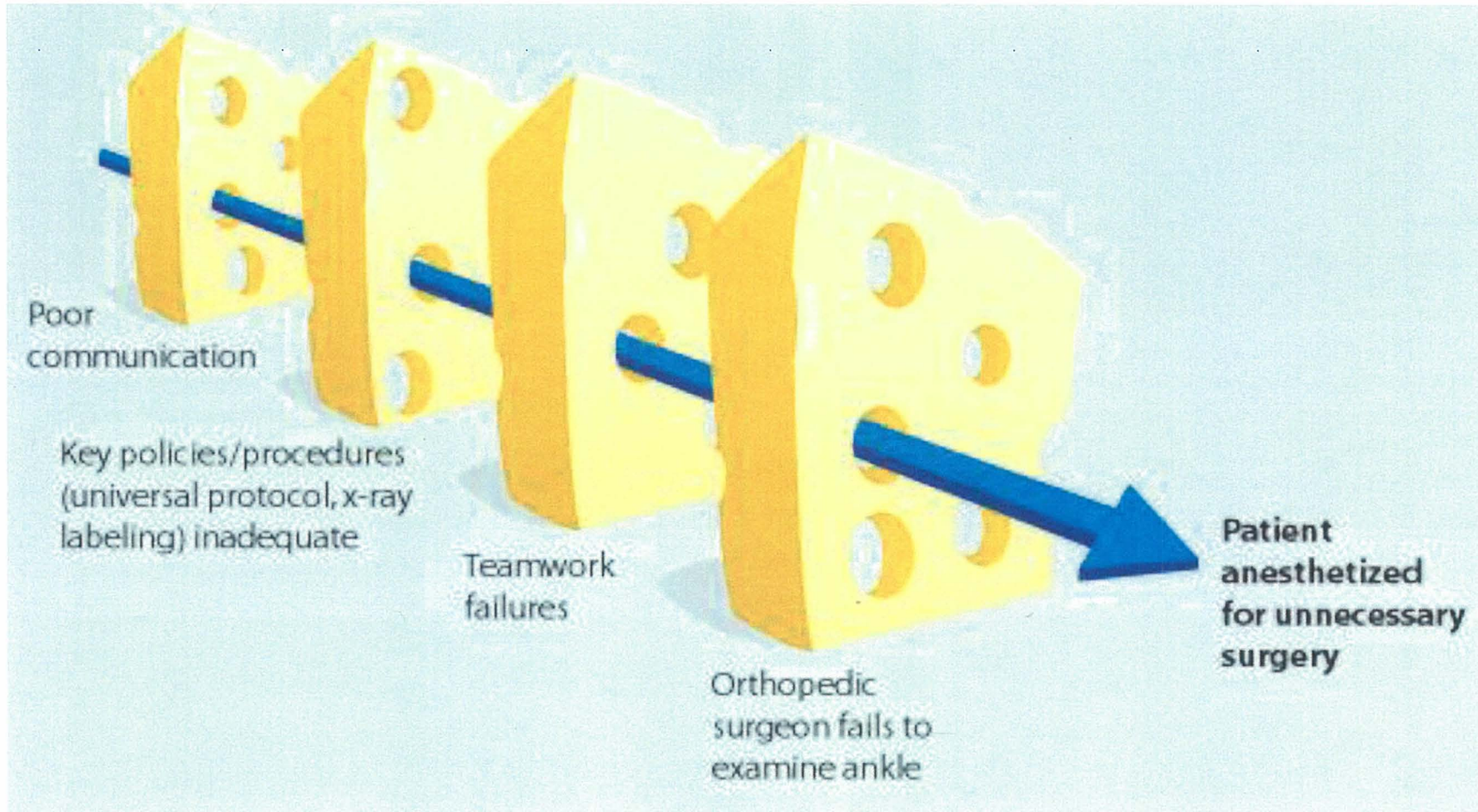
- How many things went wrong?
- Poor design,
 - We had one limit switch.
 - Not enough headroom to allow for clearance between the limit switch trip point and two blocking.
 - Poor system testing, proper limit switch set up and adjustment simply not done.
 - Reliability Engineering did not identify the violation of the NASA Safety Standard.
 - Poor operator training, 200 operators trained to use the upper limit as an operating control.

- Crane inspectors noticed evidence of metal to metal contact of telescoping tubes with supporting structure (did they understand how dangerous this is?).
- Poor operational controls, there was confusion about the meaning of the lock out / tag out (the unit was operated anyway).

Did I forget something?

- This accident could have been prevented by a lot of people, engineers, techs, basically everyone involved with this equipment.
 - Design engineering
 - Reliability engineering
 - Crane training personnel
 - Crane inspectors
 - Crane operators
- Everyone along the way made mistakes and an accident resulted.

- I like to think that every person and every aspect of an operation forms part of a system made up of “Many Layers Protection” to assure successful and safe completion of a job.
- The “Swiss Cheese Model” describes these layers of protection the best. There are many layers of protection. No one layer is perfect or full proof, this is depicted by the holes in the Swiss Cheese.



Swiss Cheese Model

Many Layers of Protection

- How many layers of protection can we think of?
 - Training
 - Institutional support
 - Empowering the work force
 - Proper system design
 - Adherence to NASA and industry standards
 - Rigorous system testing
 - Proper system inspection and periodic testing
- The crane savvy tech is the most important layer of protection we have!
- No one layer of protection is perfect but together **we can avoid accidents.**