HW #1 Hazard Analysis

Due by 10 p.m., Thursday, Feb. 13; turn in on Gradescope as a pdf

Benjamin Smith, Gurumanie Singh

1. *Hazard Identification.* (30 pts.) Lecture 2. Read 7.1 and 7.2 in the textbook. What are the hazards described for the product family of stereotactic radiosurgical systems in the article posted on Canvas?
Article
Textbook

Hazard: A system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident (loss).

Hazards are identified using the definition of an accident or loss along with additional safety criteria that may be imposed by regulatory or industry associations and practices.

Accident: An undesired or unplanned event that results in a loss, including loss of human life or human injury, property damage, environmental pollution, mission loss, etc

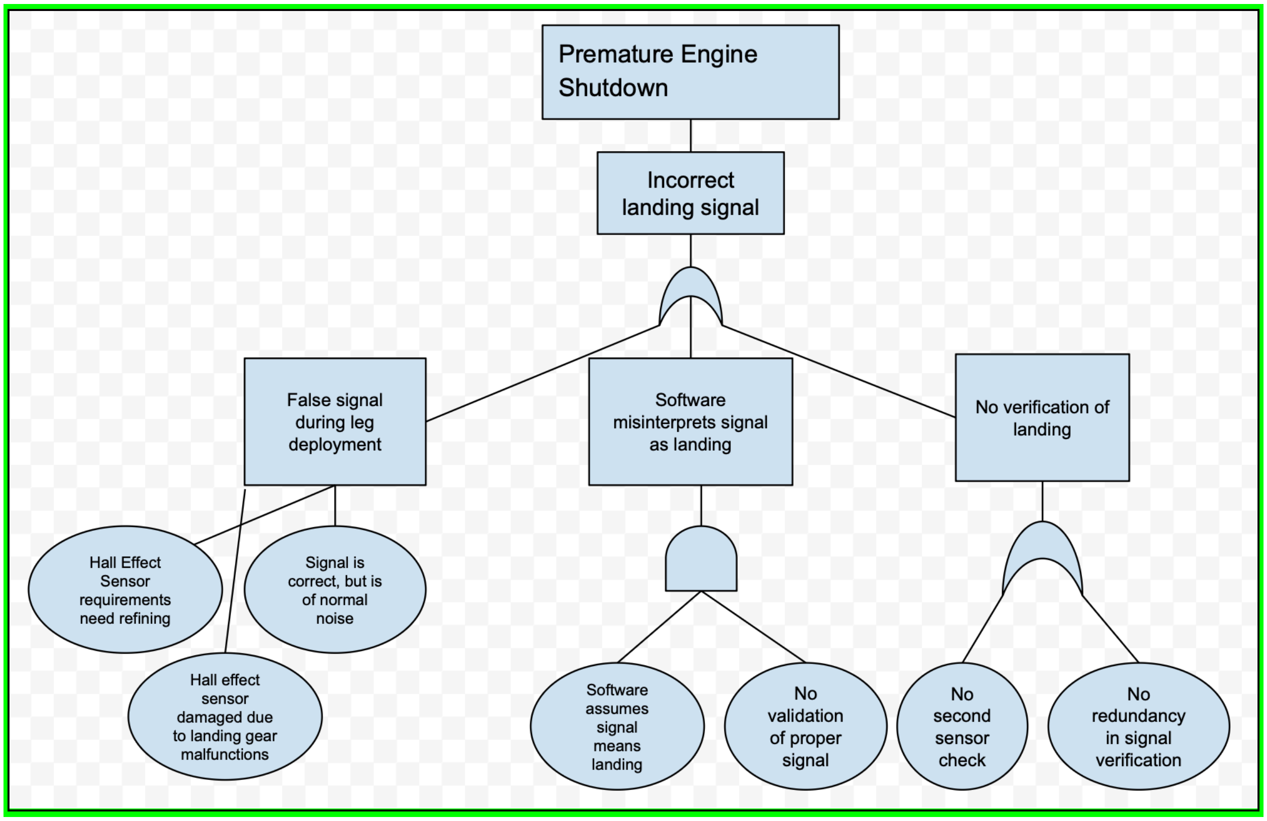
Failures can occur without resulting in a hazard and a hazard may occur without any precipitating failures.

Hazard + Environmental Conditions ⇒ Accident (Loss)

- Hazards described
    - System exposes patients or doctors to too much radiation
    - Faulty equipment allows the unwanted spillage of radiation
    - System lacks safety features to prevent/detect radiation leakage. Gives false readings.
    - Vital electronic components cant communicate with one another
    - Systems didn’t account for operator error, resulting in overexposure
    - Retrofitted, ‘mix and match’ treatment delivery systems cause potential safety flaws when coupled with user error. System doesn’t recognize certain attachments.
    - Data moving between systems that control the treatment is incorrect or corrupted.
    - Miscommunication between the computer and the metal leaves that shape the beam.
    - Treatment plan transference from one system to another
    - After treatment plan matches the doctors prescription, data is sent to a third computer that controls the linear accelerator, this information can be altered as it passes through a “chain of devices”
    - Software in the linear accelerator was built to work with specific devices, attachments used in hospitals that varied from the specifications needed a workaround to “trick” the machine.

2. *FTA & Software Fault Tree Analysis (SFTA).* (35 pts.) Lecture 3. Perform and turn in the Software Fault Tree Analysis for the Mars Polar Lander software, taking as your root hazard the "Premature Engine Shutdown" that caused the spacecraft to crash on Mars. Note that you are doing only the software part of the larger system's fault tree. Page 8 of the textbook gives an overview of the accident; however, you will need the more detailed information about the software logic, found in the excerpt of the public Accident Report that's posted on Canvas (Section 7.7.2). (See Syllabus or 1st lecture for how to download textbook chapters for free.)
Excerpt
Textbook
Lecture 3

FTA DRAWING


Premature Engine Shutdown
Incorrect landing signal
False signal during leg deployment
Software misinterprets signal as landing
No verification of landing
Hall Effect Sensor requirements need refining
Signal is correct, but is of normal noise
Hall effect sensor damaged due to landing gear malfunctions
Software assumes signal means landing
No validation of proper signal
No second sensor check
No redundancy in signal verification

3. *FMECA & Software Failure Modes, Effects and Criticality Analysis (SFMECA)*. (35 pts.) Lecture 4. Perform a SFMECA on the Infant Incubator system described as follows:

The system being specified is the Thermostat of an Incubator. An incubator provides controlled temperature, humidity, and oxygen (if necessary) for an infant in a hospital. Incubators are used extensively in Neonatal Intensive Care Units for the care of premature infants.
The purpose of the Thermostat is to maintain the air temperature of an Incubator within a desired range. It senses the Current Temperature of the Incubator and turns the Heat Source on and off to warm the air as needed. If the temperature falls too far below or rises too far above the Desired Temperature Range, it activates an Alarm to alert the Nurse. The system allows the Nurse to set the Desired Temperature Range and to set the Alarm Temperature Range outside

the Desired Temperature Range of which the alarm should be activated. [Adapted from DOT, 2009].
Lecture 4

(a) Create and turn in a **Data Table** for the data item “Alarm activation command” with 4 entries in the Failure Mode column: ***Absent*** **data**, ***Incorrect*** **data, *Timing* of Data Wrong, *Duplicate* data**.

Data Table:

Data item	**Data failure mode (fault type)**	**Description**	**Effect**	**Criticality**	**Mitigating Actions**
Alarm Activation Command	***Absent Data***	Closed / Blocked sensor vent in thermostat. Source of data is being blocked which disallows sensors to make accurate decisions and activate the alarm.	**Local**: alarm doesn’t sound **System**: system doesn’t alert nurse **Global**: infant exposed to harmful environment	severe	Cleaning the areas near the sensor in a timely manner / Ensuring sensor vents are not closed. Add redundant sensors and periodic system self checks. Maybe an alarm if no command received in set time.
Alarm Activation Command	***Incorrect data***	Hot / Cold source (ex. Candle) near thermostat causing it to read abnormal temperature compared to room	**Local**: Thermostat increases / decreases temperature in room drastically to counteract abnormal temperature read from sensor. This causes the alarm triggers incorrectly or fails to trigger **System**: Temperature in the room is too high /	Severe	Warning label on thermostat which states that there should not be hot / cold source items placed nearby Validation checks on inputs, cross checks with current temp

			low. This could cause Incorrect actions to be taken by the nurse **Global**: Premature infants in ICU may develop hypothermia / overheating		readings, data logs
Alarm Activation Command	***Timing of data wrong***	Alarm activated too late / early due to communication between sensor and alarm system	**Local**: Thermostat turns heat on / off too late and Alarm triggers at wrong time **System**: Temperature in the room is too high / low. Nurse not alerted on time. **Global**: Harm to infant from bad incubator conditions	severe	Redundant mechanisms, real time synchronization, timers
Alarm Activation Command	***Duplicate data***	Alarm activation command sent multiple times from either multiple sensors, or calculation issues. Possibly when not needed anymore.	**Local**: Software continues looping data thinking temperature is optimal. It could also cause the alarm to trigger repeatedly. **System**: Room temperature too high / low. Might cause confusion. Might cause boy who cried wolf scenario **Global**: Repeated false/real alarms could lead to delayed response to issues	medium	Data deduplication systems to make sure the same command isn’t sent multiple times

(b) Create an **Event Table** for the event “Heat Source turns OFF” with 4 entries in the Failure Mode column: ***Halt/Abnormal Termination, Omission, Incorrect Logic/Event, Timing/Order.*** (See posted slides for explanation.)

Event Table:

Event	**Event failure mode (fault type)**	**Description**	**Effect. (may want to split into 3 columns)**	**Criticality**	**Mitigating Actions (could get rid of this column)**
Heat Source turns OFF	***Halt / abnormal termination***	System crashes, or heat source fails permanently	Premature infants in ICU may develop hypothermia or worse.	high	Fail safe design, regular system diagnostic checks. Default to off on failure
Heat Source turns OFF	***Omission***	Heat source fails to turn off causing overheating in the room.	Infants exposed to harmful environment within incubation chamber	severe	Redundant temp sensors, emergency power cutoff
Heat Source turns OFF	***Incorrect logic/event***	Thermostat sensor miscalculates temperature and turns off	Heating turns off too early / too late	high	Sensor input validations, system checks, logs
Heat Source turns OFF	***Timing/order***	Heat source turns off to early/late, or gets sequence wrong with other components somehow	Unstable temperatures for infant	medium	Real time monitoring, heat regulation, maintenance alerts