Notes from "Hazard Analysis Techiques for System Safety" – Clifton A. Ericson II

Definitions p. 14

Accident ≈ Mishap: "Undesirable or unexpected event". The definition gives a sense of futility, but they can be predicted and avoided.

Hazard ≈ Risk

Risk = probability x severity (p. 16)

$$P_{FAILURE} = 1.0 - e^{-\lambda T}$$

where:

T = exposure time and

λ = failure rate

Hazard: "an entity that contains only the elements necessary and sufficient to result in a mishap." (p. 17)

A Hazard has three basic components:

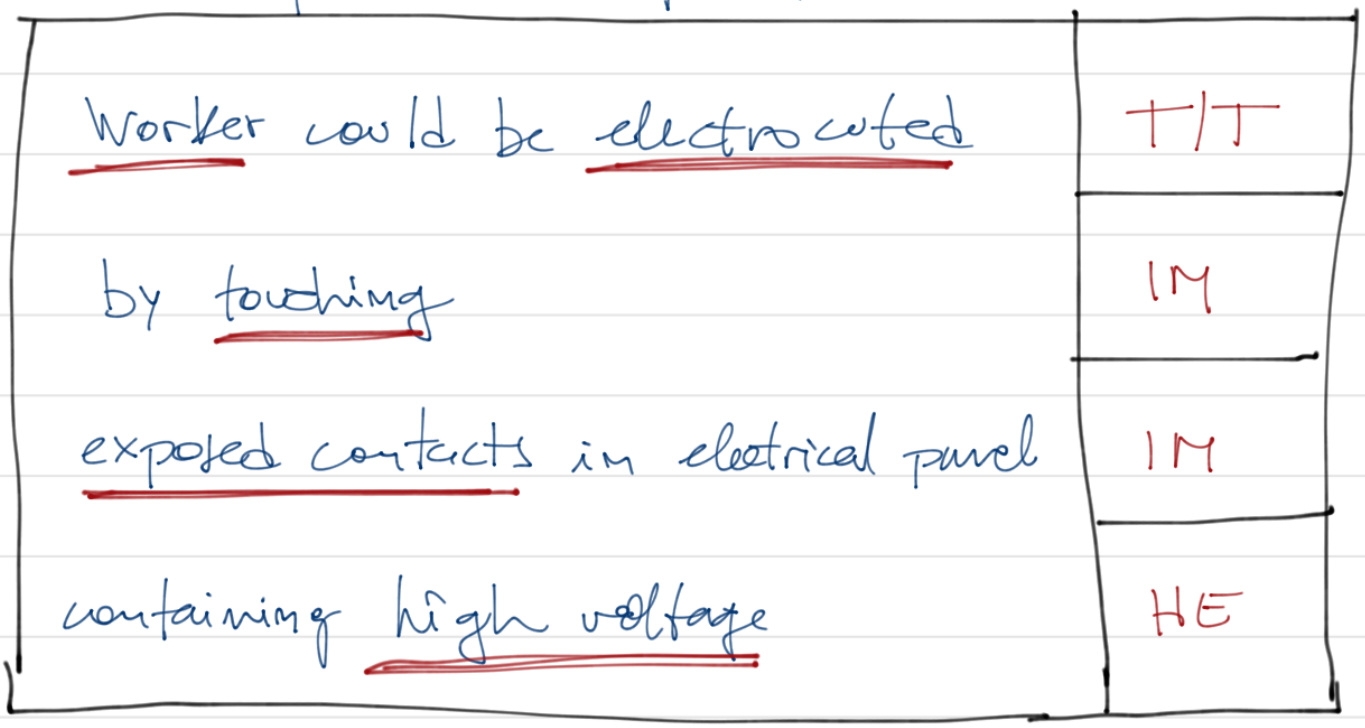
- Hazardous Element (HE)
- Initiating Mechanism (IM)
- Target and Threat (T/T)

Hazard triangle (p. 17):

Key concepts (p. 18):

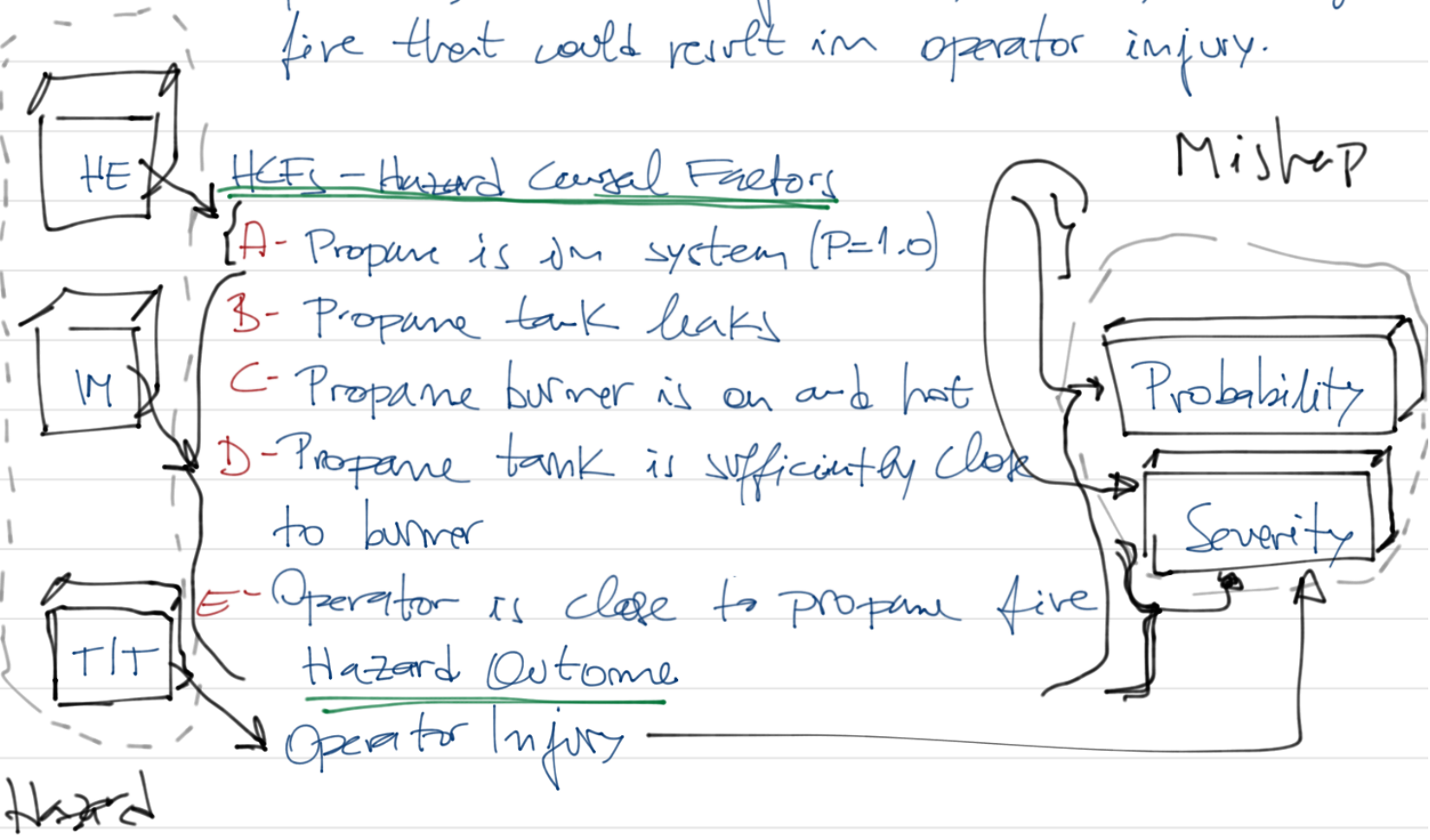
- Hazard results in mishaps;
- Hazards are (inadvertently) built into a system;
- Hazards are recognizable by their components;
- A design flaw can be a mishap waiting to happen;
- A hazard will occur according to the the hazard component involved;
- A hazard is a deterministic entity and not a random event;
- Hazards (and mishaps) are predictable and, therefore, are preventable or controllable.

Hazard components example (p. 18):



Hazard component and probability example (p. 23):

Hazard: Propane tank in barbeque unit leaks propane, which is ignited by burner, causing fire that could result in operator injury.



P(hazard) = 1.0 (it exists due to system design)

$P(\text{mishap}) = P(A) \times P(B) \times P(C) \times P(D) \times P(E)$

Recognizing Hazards (p. 23):

...

"... methodical process"

How formal methods can help us:

...

6. Key failure state questions
7. Evaluation of top-level mishaps and safety critical functions. (p. 24)

Past knowledge: hazards library?

CCFA + HAZOP(?)

Component =
  let
    NOMINAL = do → MAIN
    VIBRATION = vibration → degraded!.C → MAIN
    RF = rf → MAIN
  within [] p:{NOMINAL, VIBRATION, FF} @ P

Component may fail due to vibration, but not due to radio-frequency variation.

DDSys = || c:Cs @ c

if c won't implement one of the hazards the DDSys will deadlock, meaning the analysis wasn't complete.

HTS - Hazard Tracking System (p. 405).

CCFA: identifies only those hazards related to common causes.