Sisteme de Încredere
- Siguranța -

Ciprian Dobre
ciprian.dobre@cs.pub.ro

Siguranța

- Se referă la… (în timpul operării normale & anormale)
  - Controlarea unor sisteme potențial periculoase
  - Prevenirea accidentării sau omorârii unor persoane
  - Prevenirea distrugerii mediului
- Adesea văzută și ca specializare a fiabilității
  - Minimizarea apariției de defecte – în special acelora cu consecințe catastrofice

Sisteme de siguranță

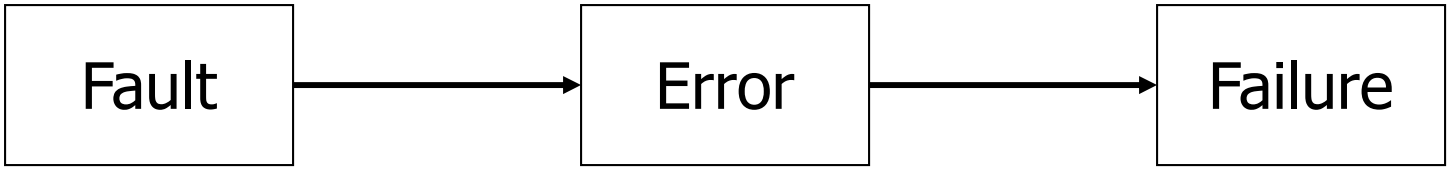
- Siguranță directă (primare):
  - Sisteme critice de siguranță
  - Chiar sistemul poate provoca daune / accidente
  - Controlul unei centrale electrice, control de zbor, etc.
- Siguranță indirectă (secundare):
  - Asistă sistemul cu implicații legate de siguranță
  - Operații asupra bazei de date, managerul de mentenanță, etc.

Lanțul de Hazarde

Hazard – Fenomenul sau situația cu potențial periculos
Incident – Apariția acelei situații de hazard
Accident - Moarte, accidentare sau pierderi rezultate în incident

Comparație

Poate vi văzut ca o instanță specifică, socio-tehnică legată de siguranță, a:



Exemple

- Hazard
  - Cablul electric este lăsat nesupravegheat
  - Tuburi de aerisire subțiri
- Incident
  - Tăietorul de iarbă taie cablul
  - Tubul de răcire se blochează
- Accident
  - Grădinarul se electrocutează
  - Core meltdown

Valoarea vieții umane

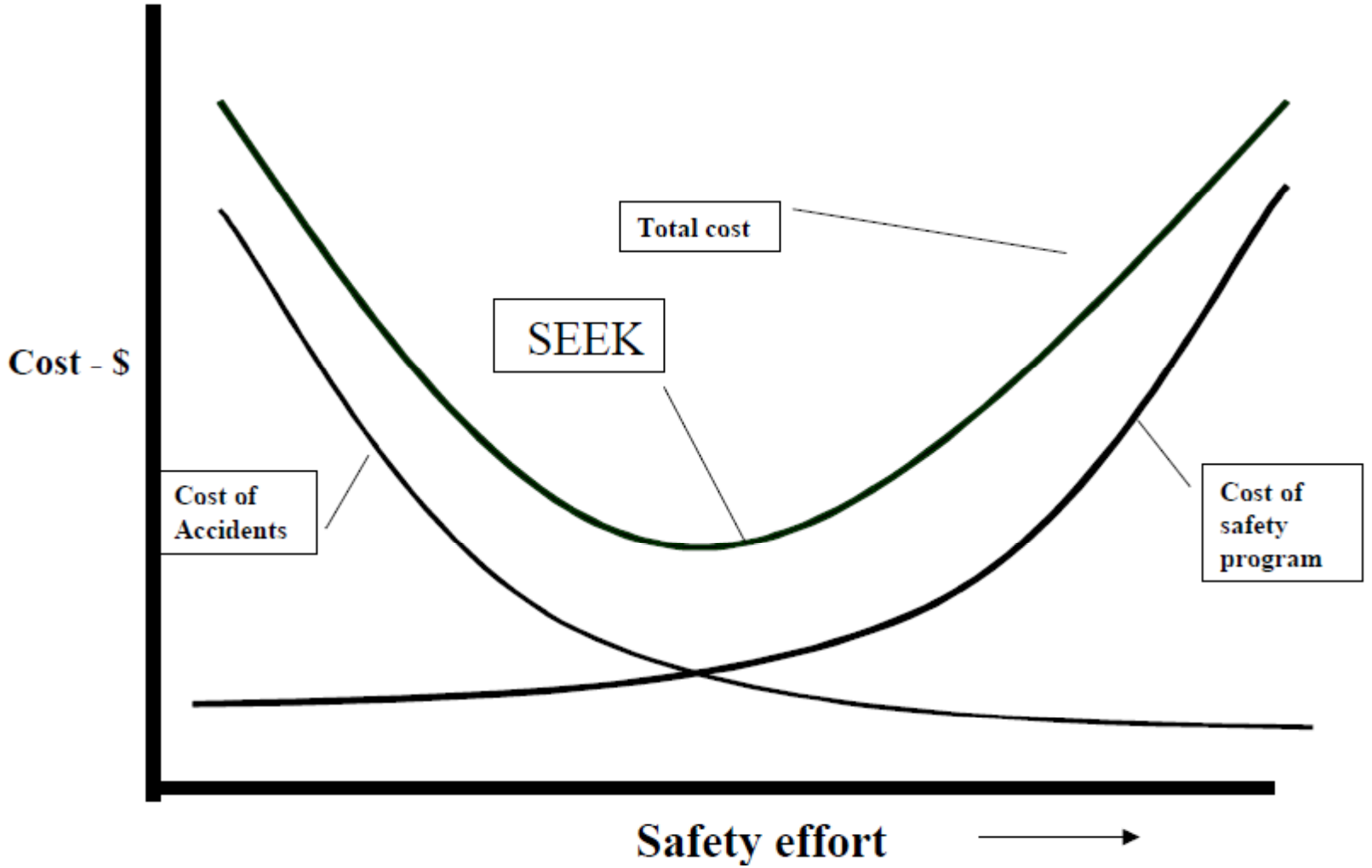
"Suntem tentați să spunem că viața umană nu are preț și că nu poate fi precupețit nici un efort pentru a o proteja. Totuși, asemenea argumente nu stau în fața logicii."

Neil Storey

Compromisul

- Trebuie pus un preț pe viață și suferință
  - Siguranța perfectă nu e posibilă
  - Fiabilitatea extrem de ridicată este scumpă
- Ajungerea la un compromis “acceptabil” între:
  - Siguranță, Practicalitate, Cost
- Multe aspecte sociale, tehnice sau politice la mijloc

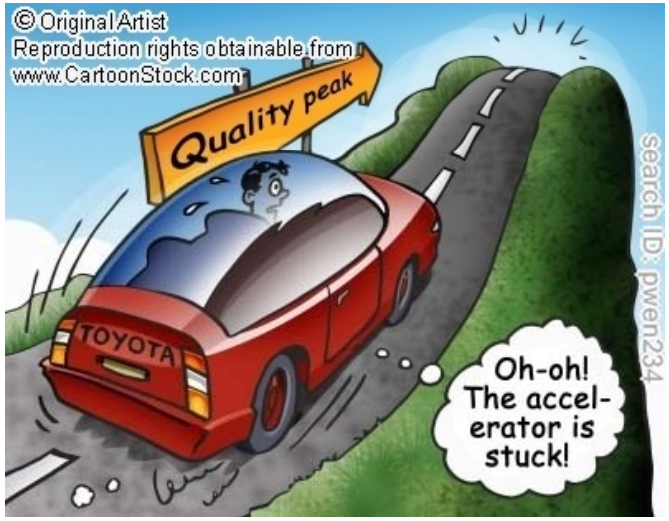
Efort siguranță vs. cost



Exemplu

"Ca și coordonator de activități de rechemare în producție, aveam următorul job: Se ia numărul de mașini aflate în circulație (A), se înmulțește cu rata probabilă a accidentelor (B), apoi cu rezultatul medierii costurilor pierdute cu diversele procese intentate (C). Dacă rezultatul (A x B x C) este mai mic decât costul rechemării în fabrică, e acceptabil."

Edward Norton



Responsabilitatea Producătorului

- Pentru că moartea/accidentarea pot fi tolerate
- Manufactorul este deschis unor eventuale litigii
- Amenzi din partea agențiilor guvernamentale (ex., agenția de mediu)
- Procese civile
- Chiar încarcerarea angajaților

Apărarea Producătorului

- Demonstrează că sistemul “se potrivește scopului”
- “As Safe as Could Reasonably be Expected”
- Demonstrează lipsa de neglijență
- Furnizează avertismente (semne, etichete, disclaimere)
- Apelează la asiguratori !!!

Evaluarea siguranței

- Siguranța este greu de măsurat
  - Se bazează adesea pe nivelul de siguranță “judecat”
    - Estimează propriile noastre “nivele de conștiință”
      - De la “foarte sigur” la “foarte nesigur”
    - Contează pentru evaluări profesionale
    - Evaluare pe baza unor argumente
    - Trebuie să adreseze atât produsul, cât și procesul

Factori ce influențează judecata

- Reputația dezvoltatorilor
- Maturitatea procesului de dezvoltare
- Aderența la standarde
- Proces bine documentat de V&V:
  - Review-uri/inspecții
  - Verificare statică
  - Testare în amănunt
- Verificări formale
- Cazuri de siguranță

Cazuri de test pentru siguranță

- Justificare și apărare pentru sistem
- Nu garantează în totalitate siguranța sistemului
- Argumente pentru *indicarea* nivelului de siguranță
- Demonstrează proiectul și presupunerile făcute
- Susține “dovezi” pe baza:
  - Evaluare inginerească expertă
  - Analiza riscului probabilistică
  - Demonstrarea riscurilor și verificarea adresării acestora

Verificare prin contradicție

- Abordare sistematică & matematică
- Arată că anumite stări nesigure nu pot fi atinse în funcționare
- Arată că anumite condiții pentru hazard nu pot exista
- Focus pe un singur aspect al sistemului
- Metodă ce împrumută din mecanismele formale

Măsuri de asigurare a unui grad înalt de siguranță

- Folosirea unor metode pentru asigurarea unui grad înalt de siguranță → problematică
  - Adesea imposibil de verificat rezultatul
  - Nu se pot executa teste la limită (umană???)
- Putem construi experimente pentru evaluarea extremelor?
- Sunt oare astfel de sisteme prea riscante?
  - Dacă nu putem verifica – mai bine nu construim!

Măsuri de calcul a Severității

- Nu toate defectele au aceeași severitate
- Putem să tolerăm unele minore…
- Nivele de integritate:
  - Neglijabil: 10^{-2} la10^{-1}
  - Efect minor: 10^{-4} la 10^{-3}
  - Efect major: 10^{-6} la 10^{-5}
  - Efect de hazard: 10^{-8} la 10^{-7}
  - Efect catastrofic: 10^{-9} și mai mic
- (Propusă de fabricanții din industria aviatică civilă)

Clasificarea bazată pe consecințe

Probability (Quantitative)		1.0	10^{-3}	10^{-5}	10^{-7}	10^{-9}
Probability (Descriptive)	FAR	Probable		Improbable		Extremely Improbable
	JAR	Frequent	Reasonably Probable	Remote	Extremely Remote	Extremely Improbable
Failure condition severity classification	FAR	Minor		Major		Catastrophic
	JAR	Minor		Major	Hazardous	Catastrophic
Effect on aircraft occupants	FAR	• Does not significantly reduce airplane safety (Slight decrease in safety margins) • Crew actions well within capabilities (Slight increase in crew workload) • Some inconvenience to occupants		• Reduce capability of airplane or crew to cope with adverse operating conditions • Significant reduction in safety margins • Significant increase in crew workload *Severe Cases:* • Large reduction in safety margins • Higher workload or physical distress on crew - can't be relied upon to perform tasks accurately • Adverse effects on occupants		• Conditions which prevent continued safe flight and landing
	JAR	• Nuisance	• Operating limitations • Emergency procedures	• Significant reduction in safety margins • Difficulty for crew to cope with adverse conditions • Passenger injuries	• Large reduction in safety margins • Crew extended because of workload or environmental conditions • Serious or fatal injury to small number of occupants	• Multiple deaths, usually with loss of aircraft

Exemple de sisteme – siguranță …

Neglijabilă (10^{-2} la10^{-1}) ?

Amortizoare, șoc static

Cu efecte minore (10^{-4} la 10^{-3}) ?

Tăieturi, oase minore rupte

Cu efecte majore (10^{-6} la 10^{-5}) ?

Pierderi de membre, accidentări serioase

Hazard (10^{-8} la10^{-7}) ?

Accident auto fatal, accident cu un balon cu aer cald

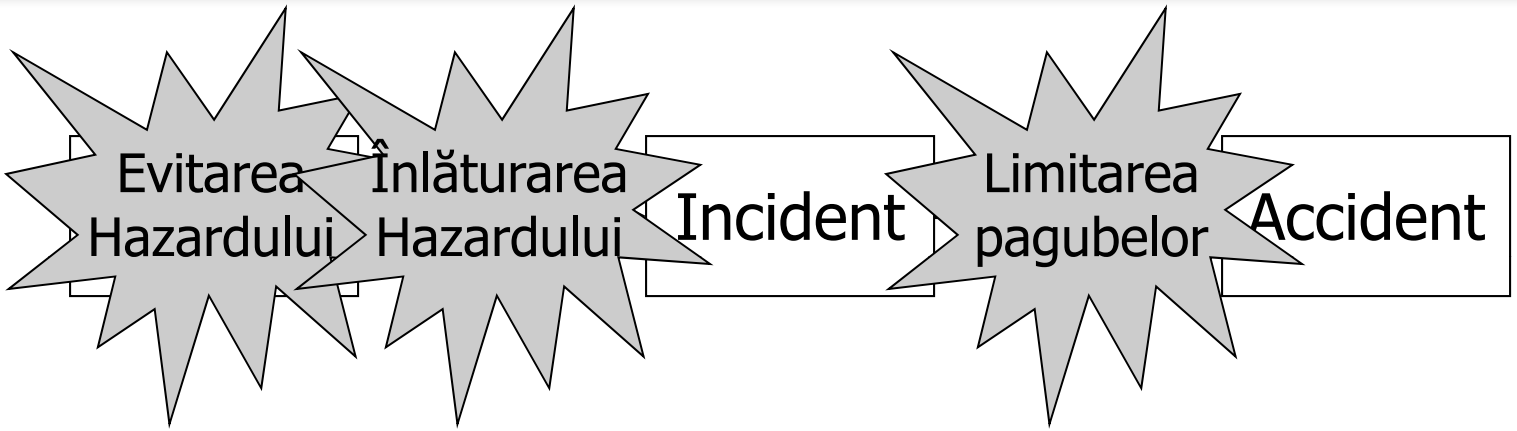
Catastrofice (10^{-9} și mai mici) ?

Accident feroviar, sau nuclear

Hazarde și defecte

- Hazard-ul este văzut adesea de specialiști ca un tip specializat de “defect”
- Defecțiune de siguranță
- Perspectivă socio-tehnică lărgită
- Harzardele pot fi gestionate în manieră similară:
  - Evitarea hazardului (eq. evitarea defectelor)
  - Limitarea problemelor (eq. toleranța la defecte)

Prevenirea accidentelor



Siguranța împrumută abordări asemănătoare celor tratate la fiabilitate…

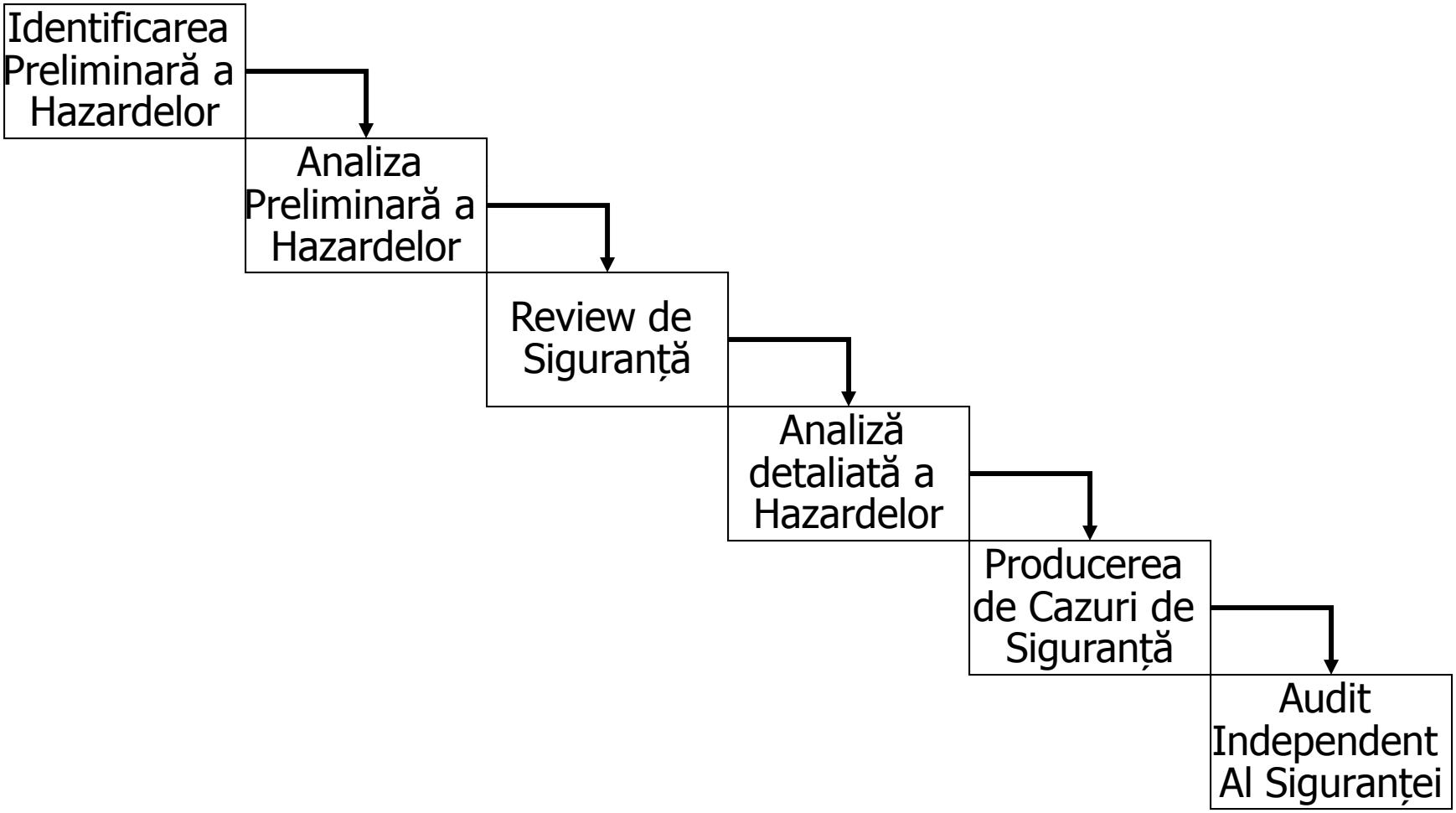
Evitarea și înlăturarea hazardelor

- Evaluări formale
- Argumentări informale
- Ciclu de dezvoltare matur și supravegheat
- Analiza hazardelor:
  - Instrumente suport
  - Liste de verificare
  - Brainstorming

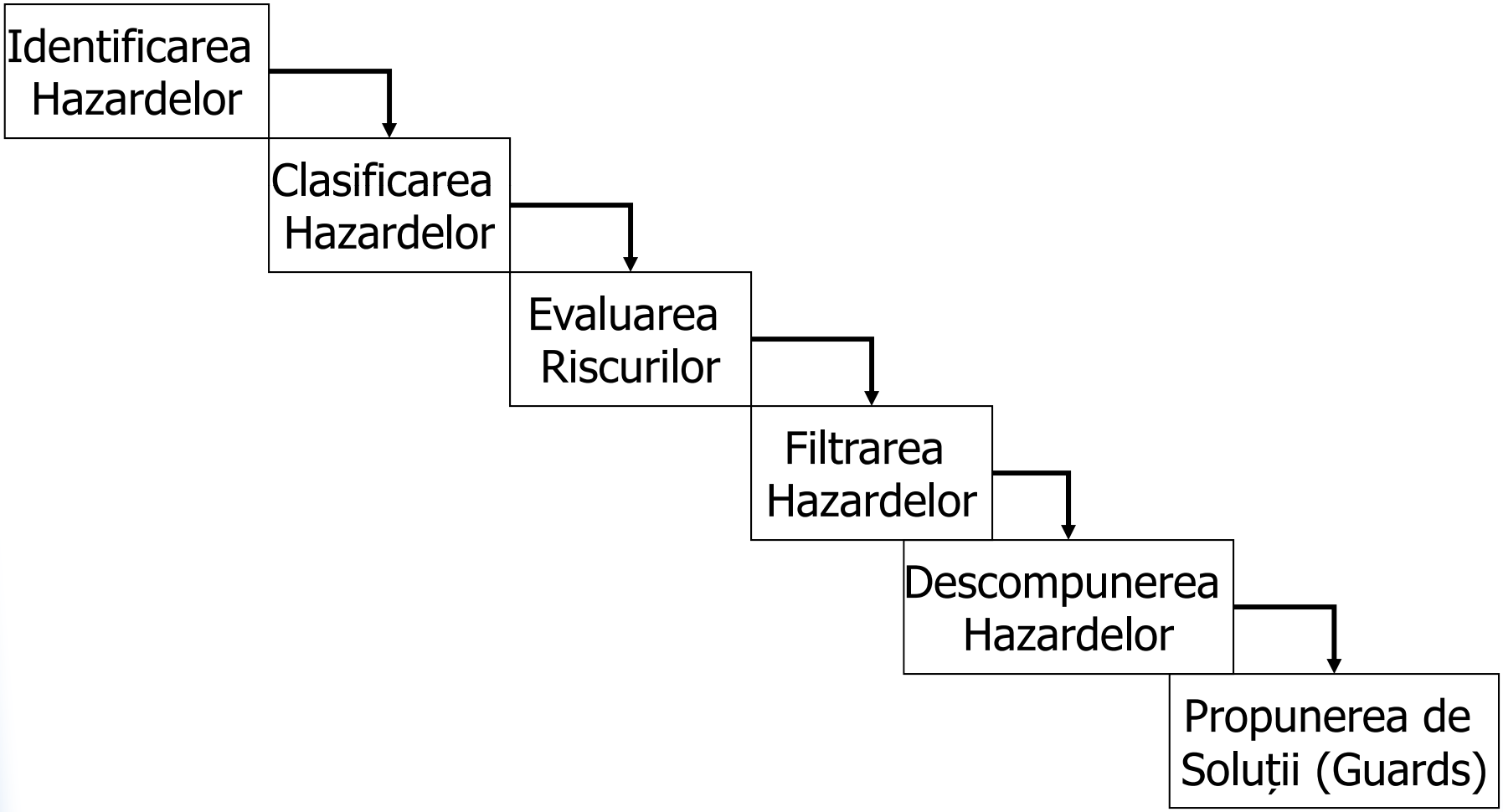
Ciclu de dezvoltare de "Siguranță"

- Analiza hazardelor
- Gestiunea hazardelor (logare, tracing)
- Engineri specializați în probleme de siguranță
- Folosirea extensivă a review-urilor de siguranță
- Certificarea siguranței
- Management detaliat al configurației

Ciclu de dezvoltare de siguranță



Procesul de analiză al hazardelor



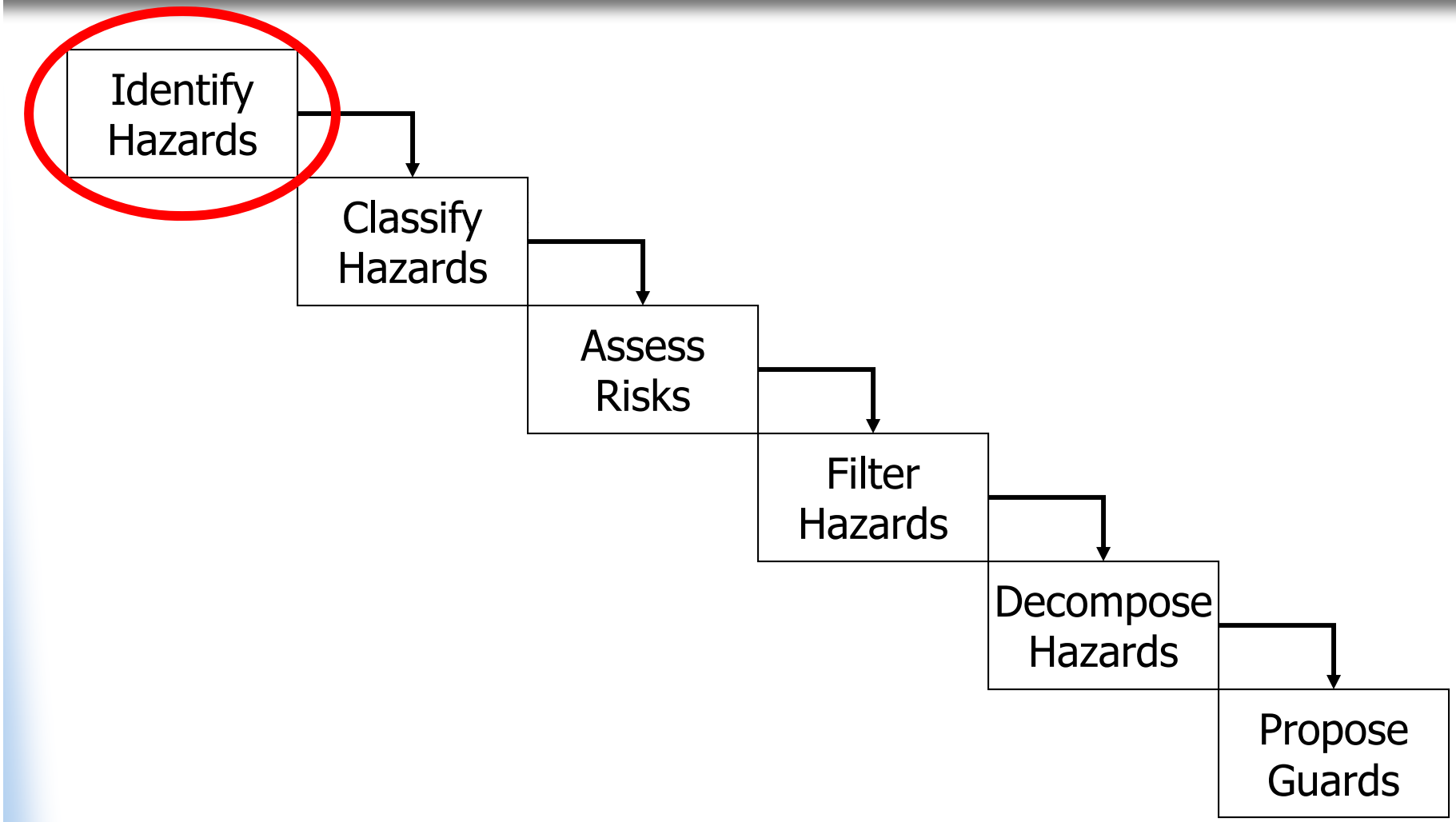
Colaborare în procesul de analiză a hazardelor

- Dezvoltatori
- Experți ai domeniului
- Experți în siguranță
- Manageri
- Utilizatori finali
- Organisme de control
- Organizații de certificare

Analiza de Hazard

- Lungă și consumatoare de timp
- Dificilă și complexă
- Costisitoare
- Susceptibilă la omisiuni și erori
- Estimarea probabilităților și severității hazardelor este greu de făcut

Procesul de Analiză a Hazardelor



Identificarea Hazardelor

- Identificarea tuturor posibilelor hazarde
  - Adesea sunt multe posibile hazarde ce pot apărea
  - Greu de identificat toate hazardele
  - Potențial pentru interacțiunea hazardelor

Majoritatea accidentelor se datorează mai multor hazarde/incidente (Perrow 1984)

Mecanisme pentru Identificare

- Introspecția
- Group brainstorming
- Studii pe cazuri cheie
- Instrumente suport
- Liste de verificare

Analiza HazOp

- Suport pentru cooperare între experți
- Ajută la acoperirea diferenței “culturale”
- “Suport de gândire” sistematic
- Prompt pentru operatorii umani
- Entități și fenomene
- “Lucruri rele” dependente de domeniu
- Toate combinațiile sunt considerate

Concepte HazOp

1. Intenție – cum ar trebui să funcționeze sistemul
2. Cuvânt de ghidare – abstractizează “lucrurile rele”
3. Parametru – entitate sau fenomen modificabil
4. Deviație – operație neintenționate (2 x 3)
5. Cauză – cauza deviației
6. Consecință – rezultatul deviației
7. Acțiune sugerată – previne deviația

Exemplu de analiză HazOp

- Producerea unei “căni cu ceai”

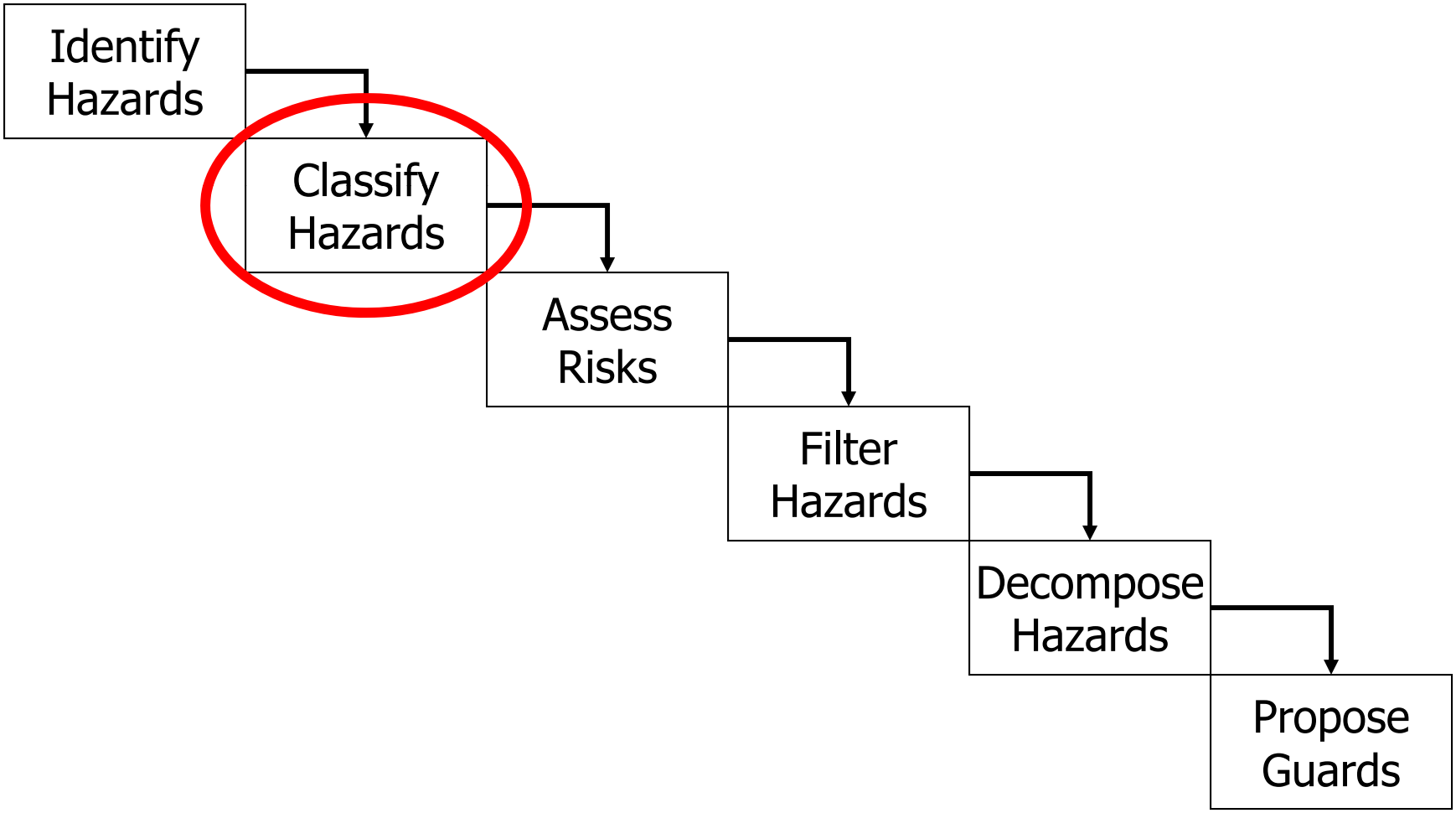
Parametrii:
- Frunze de ceai
- Căldură
- Apă
- Zahăr
- Lapte
- Scaun confortabil

Cuvinte de ghidare:
- Mai mult
- Mai puțin
- La fel ca și
- Altfel cât
- Mai devreme
- Mai târziu

Deviații posibile

- Mai multe frunze de ceai – prea puternic
- Mai puțină căldură – infuzare slabă, ceai rece
- Lapte pus prea târziu – (ceaiul mai întâi) distrugerea proteinelor
- Mai mult zahăr – prea dulce
- Altceva decât scaun confortabil – experiență ruinată

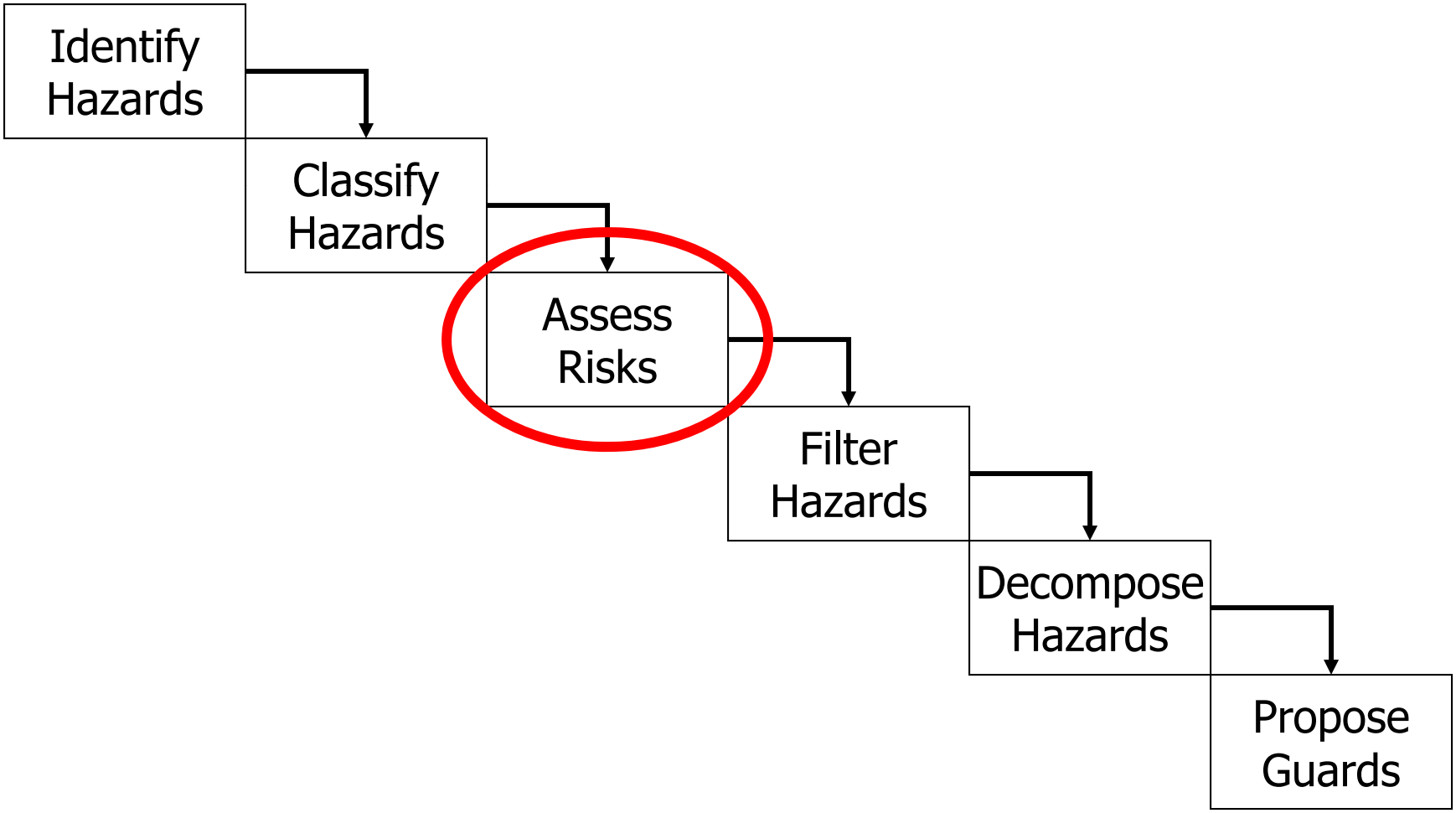
Procesul de analiză a Hazardelor



Clasificarea hazardelor

- Natura stricăciunii (ex., toxic)
- Exemplul fiind etichetarea containerelor de marfă
- Probabilitatea de stricare/defectare
- Severitatea defectului

Hazard analysis process



Evaluarea riscurilor

- Produce valori pentru riscurile calculate
- Se consideră acceptabilitatea riscului:
  - Intolerabil
  - As Low As Reasonably Practical (ALARP)
  - Acceptabil
- Se consideră o serie de factori socio-politici
- + costul prevenirii
- Ajută la deciderea acțiunii ce trebuie luată

Fenomenul riscului

- Riscul reprezintă un fenomen straniu
- Dependent de o gândire poate ilogică
- Dependent de presiuni politice și sociale
- Riscul *perceput* poate adesea diferi de riscul *real*

Percepția riscului

- Accident grav, multe fatalități = impact mare
- Accident minor, puține fatalități = impact mic
- Chiar dacă sunt multe accidente minore la un moment dat
- Numărul total de victime rezultat nu este atât de important !!!
- Ce omoară mai mulți oameni: Avioanele sau măgarii?
  - 2004… 9000 decese cauzate de măgari față de … 172 accidente aviatice soldate cu doar 771 de decese

Riscuri stranii

- Accident de tren – multe decese
- Reacție publică
- Guvernul este imediat supus unei presiuni publice
- Se introduc noi sisteme de protecție feroviară
- Se reduc vitezele legale permise pentru deplasarea trenurilor, cresc prețurile biletelor
- Mai mulți pasageri aleg în aceste condiții mașina ca mijloc de deplasare
- Dar mașinile sunt mai puțin sigure decât trenurile
- Deci mai mulți oameni ajung în final să decedeze decât dacă guvernul nu ar fi făcut nimic și ar fi ignorat accidentul !!!

Calcularea riscului

- Probabilitatea de apariție a hazardului (apariție)
- Probabilitatea de apariție a incidentelor (conversie)
- Probabilitatea de apariție a accidentelor (completare)
- Severitatea hazardului (paguba în cel mai rău caz)

Hazard risk =

haz_prob x incident_prob x accident_prob x haz_sev

Dimensiuni ale riscului

- Probabilitate – valoare sau scală numerică :
  - Frecvent, Probabil, Ocazional, Puțin probabil, Improbabil, Incredibil (N.B. – nimic nu este însă imposibil!)
- Severitate – valoarea sau scală numerică:
  - Catastrofic, de Hazard, Major, Minor, Neglijabil, Nici un efect
- Risc – numeric (decese / an) sau scală:
  - Intolerabil, Nedorit, Tolerabil, Neglijabil

Întrebări despre estimarea riscului

Identificați potențialele accidente rezultate în urma următoarelor situații și estimați riscurile percepute și reale:

- Condusul pe A1 pe zăpadă
- Zborul cu un avion Concorde
- Plimbare în rollercoaster
- A fi un student la Master

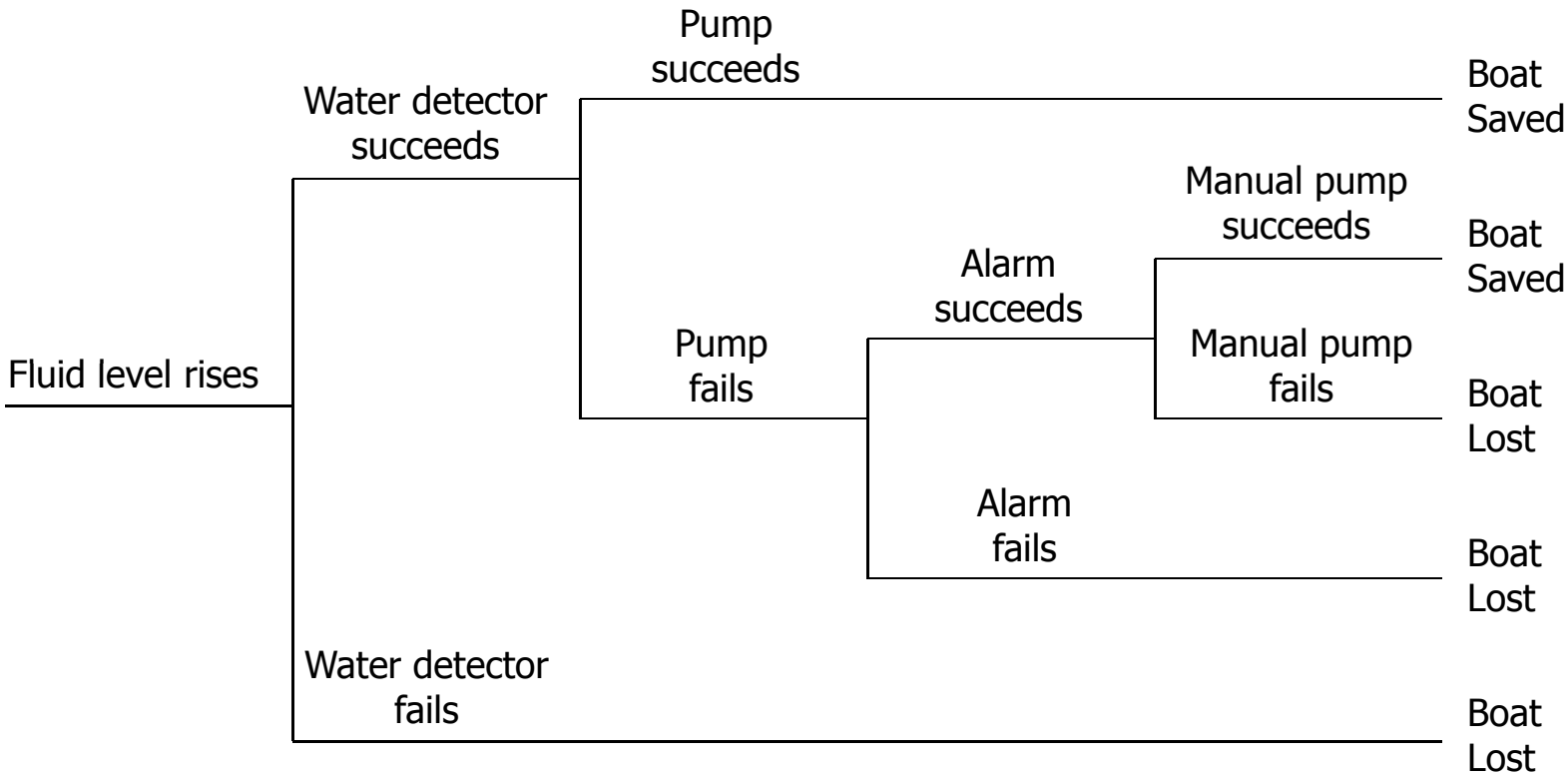
Analiza arborelui de evenimente

- Cum contribuie hazardele la accidente
- Interacțiuni între hazarde și evenimente
- Efecte combinate ale hazardelor
- Ajută la reflecția asupra a ceea ce s-ar putea întâmpla
- La bază probabilitatea de apariție a hazardelor și a unor evenimente
- Calculează probabilitatea unui accident
- Folosit în evaluarea riscului

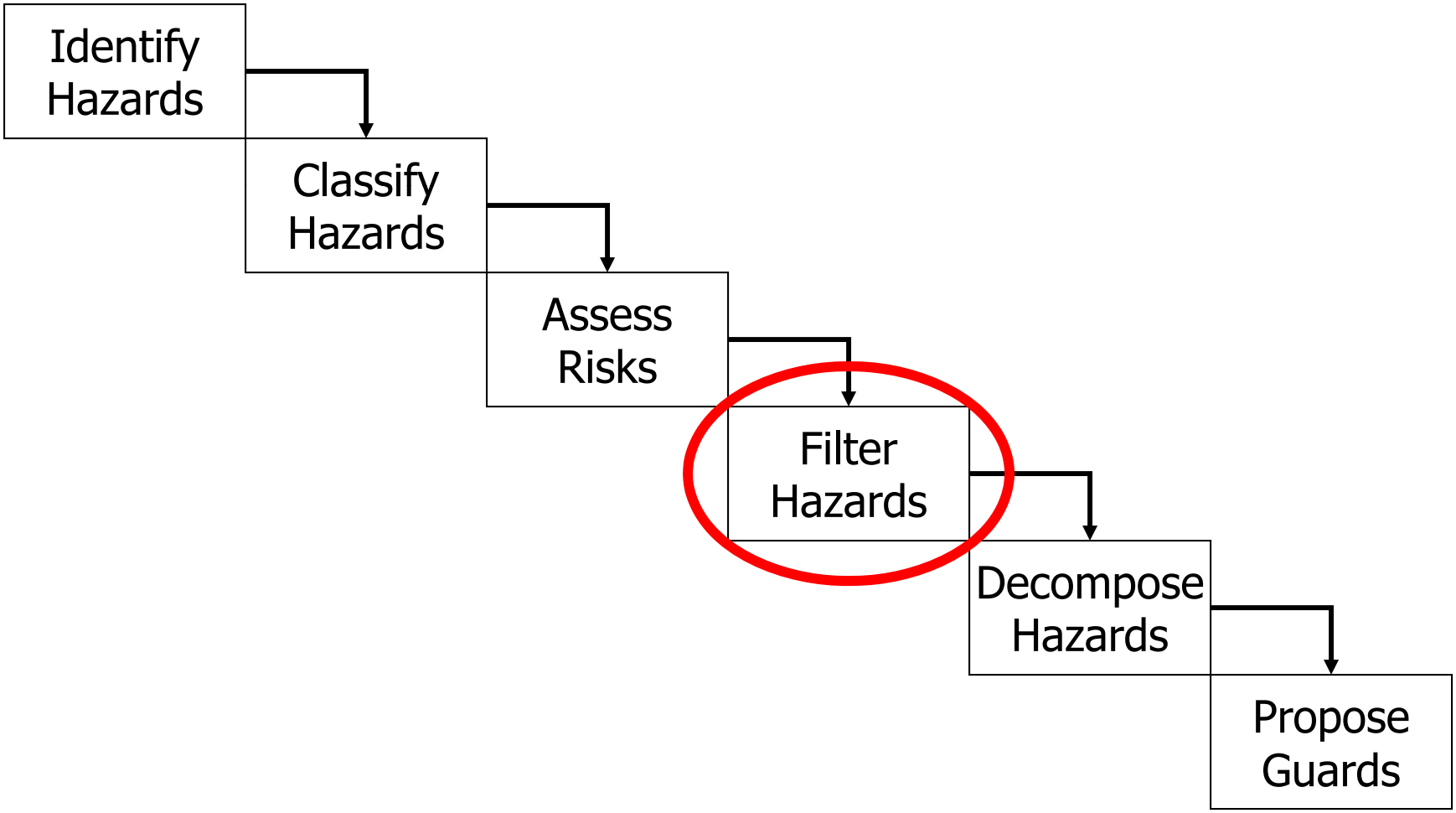
Exemplu

- Barcă cu coca neetanșă
- Sistem de detecție a apei de mare
- Pompă automată
- Alarmă de detecție a defectării pompei
- Nivel de alarmă
- Pompă manuală disponibilă

Analiză bazată pe arbore de evenimente



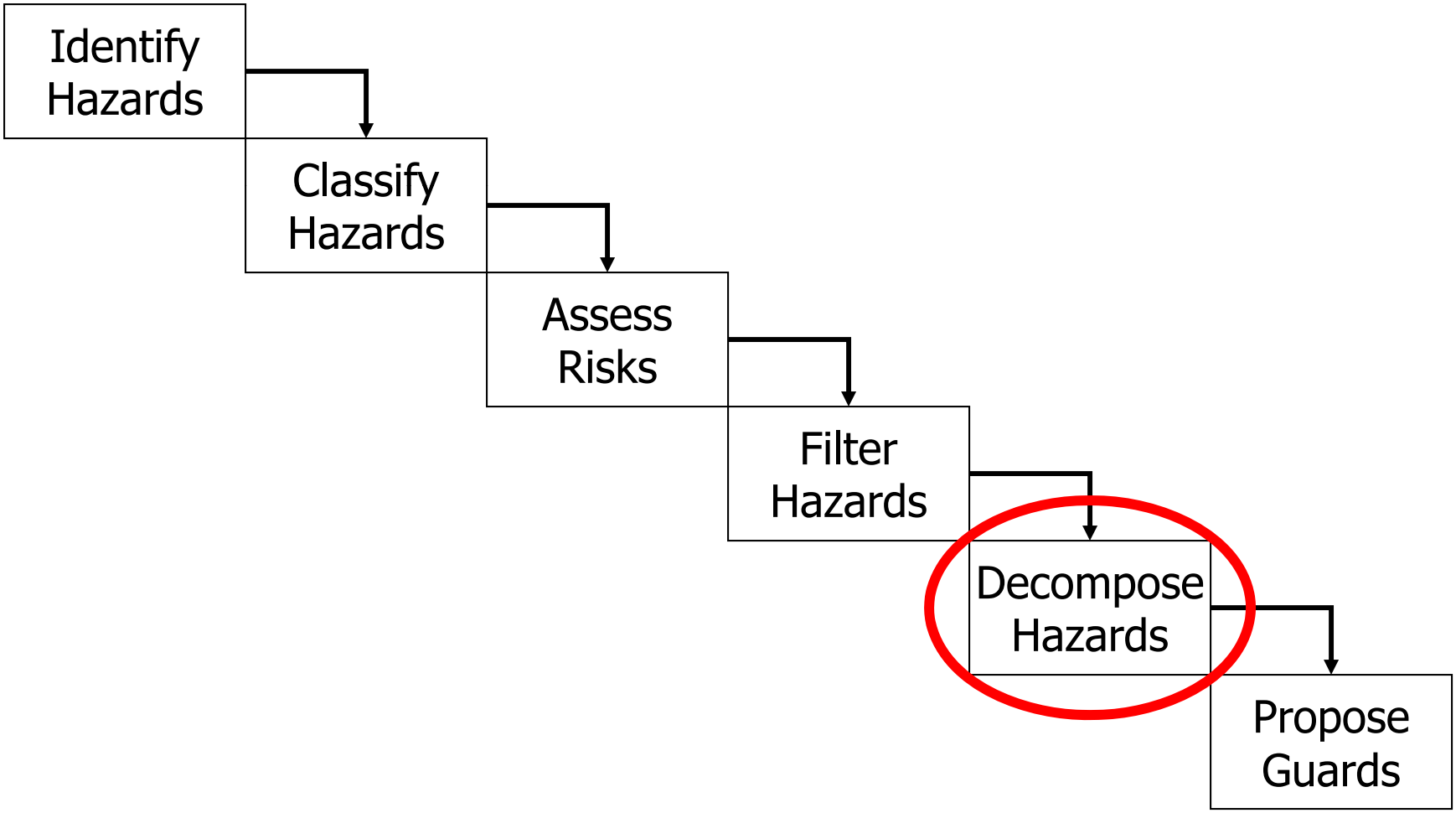
Procesul de analiză a hazardelor



Filtrarea hazardelor

- Minimizează setul de hazarde supuse analizei
- Înlătură hazardele imposibile
- Înlătură hazardele “mult” improbabile
- Înlătură hazardele cu risc scăzut
- Păstrează înregistrări ale hazardelor înlăturate
- Se reține cele raționale pentru a fi înlăturate

Procesul de analiză a hazardelor



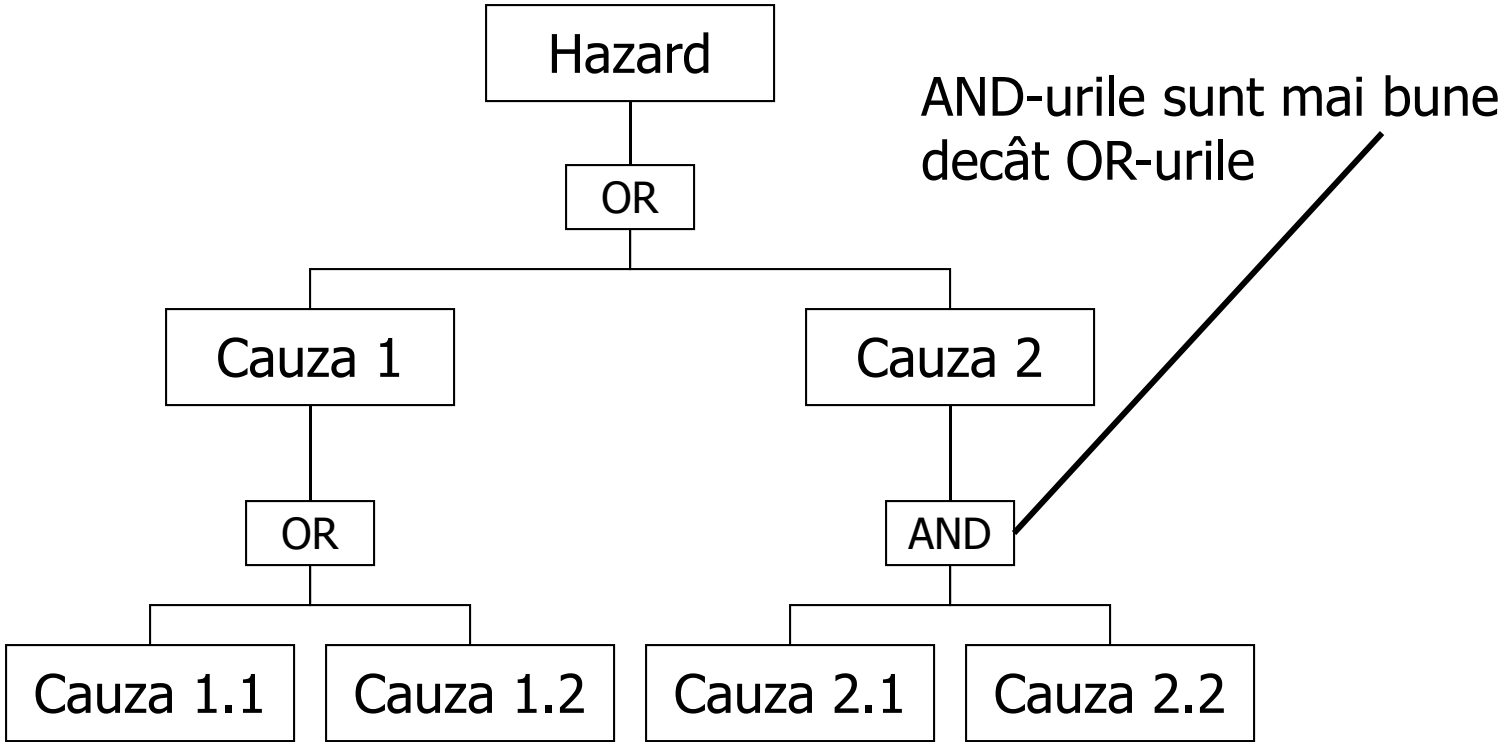
Descompunerea hazardelor

- Se identifică cauzele fiecărui hazard
- Adesea o combinație de mai mulți factori conduc la un hazard
- Un singur hazard poate avea mai multe cauze
- Esențial înțelegerea fiecărui hazard

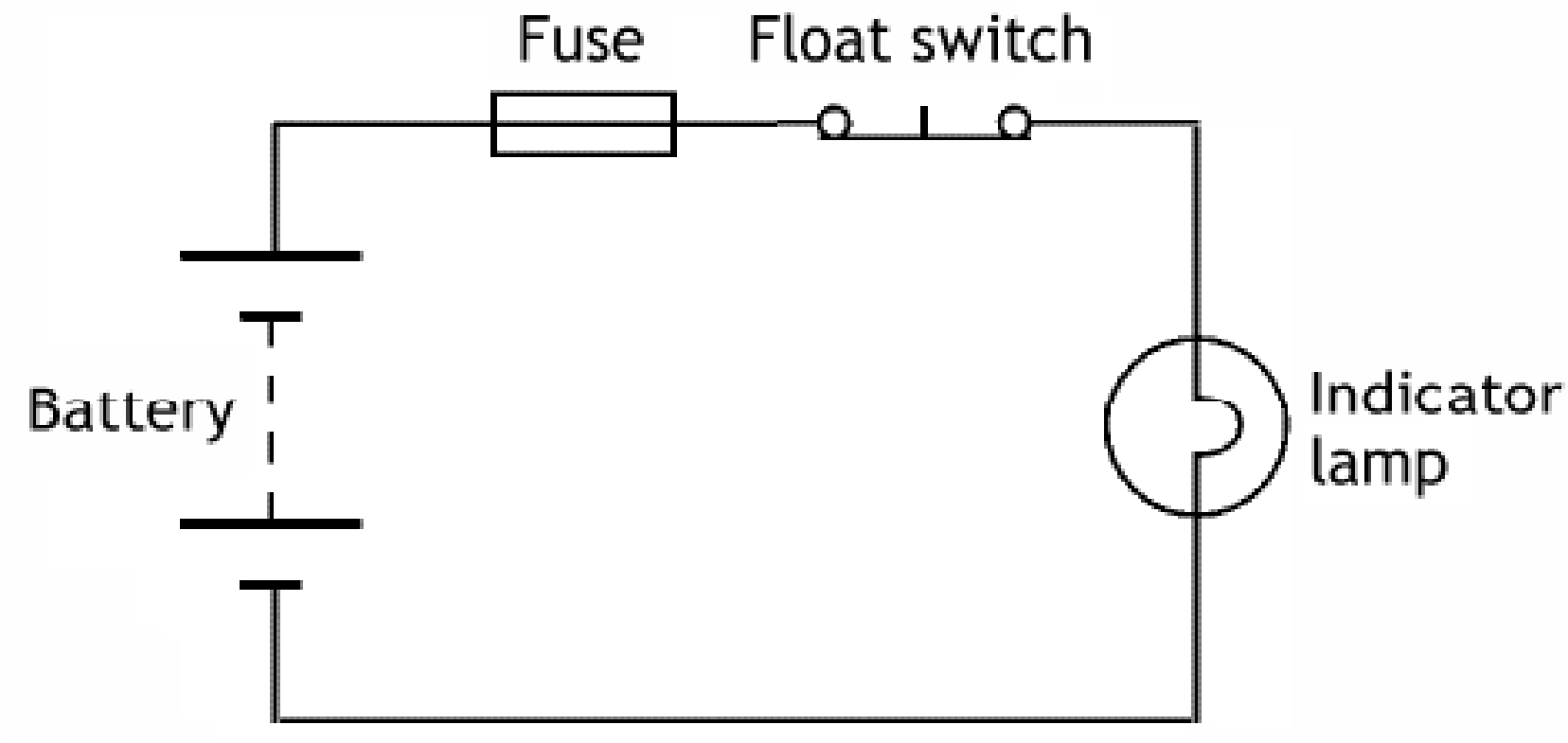
Analiza bazată pe arborele de defecte

- Documentarea sistematică a hazardelor
- Poate utiliza probabilitățile de apariție a diverselor evenimente
- Tabele cu probabilitățile asociate unor defecte sunt disponibile pentru componente mai comune
- Se calculează probabilitatea de apariție a unui hazard
- Tinde să conducă la producerea unor arbori de mari dimensiuni
- Evoluează de-a lungul procesului de analiză

Analiza bazată pe arborele de defecte

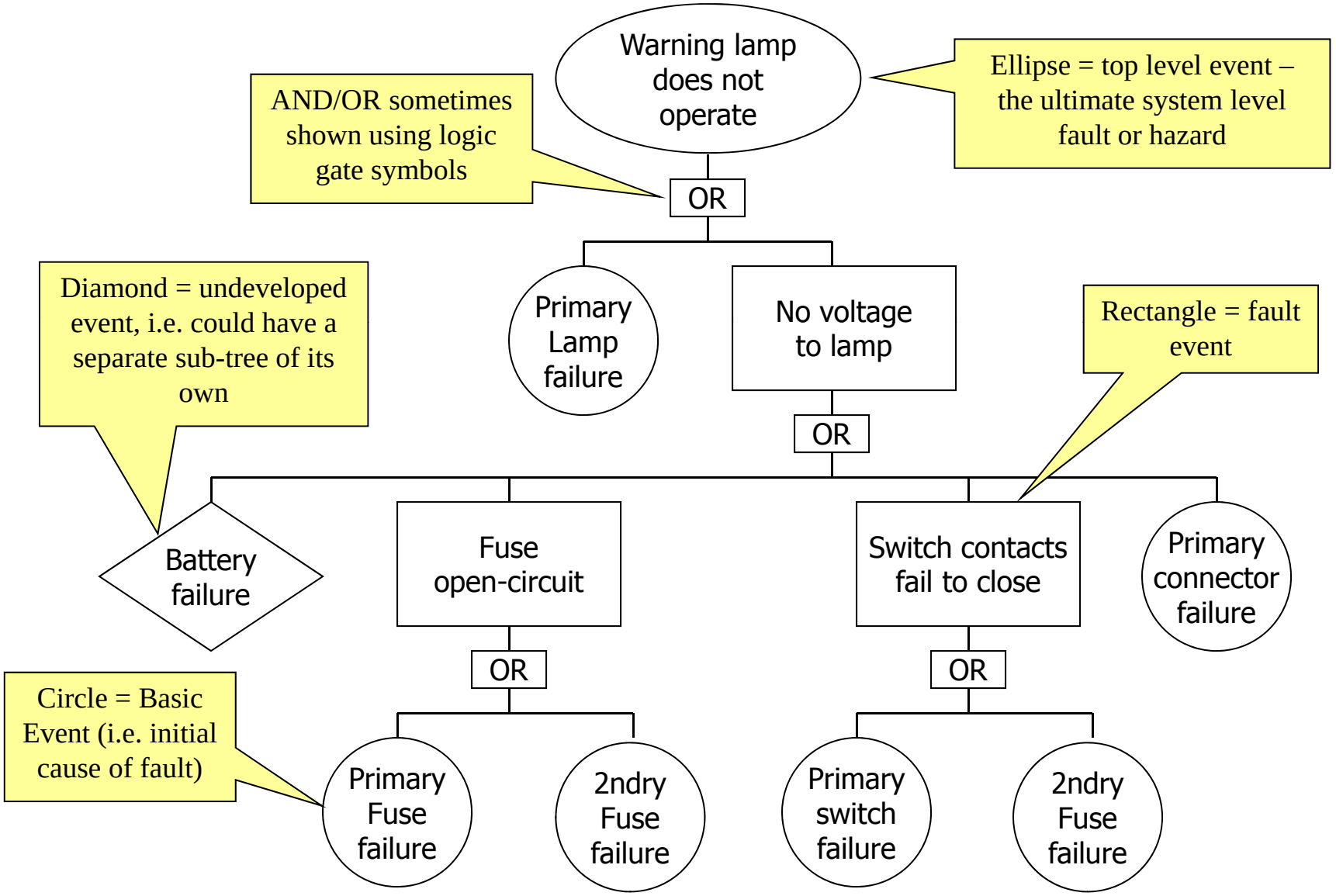


Ex: analiza pentru un circuit

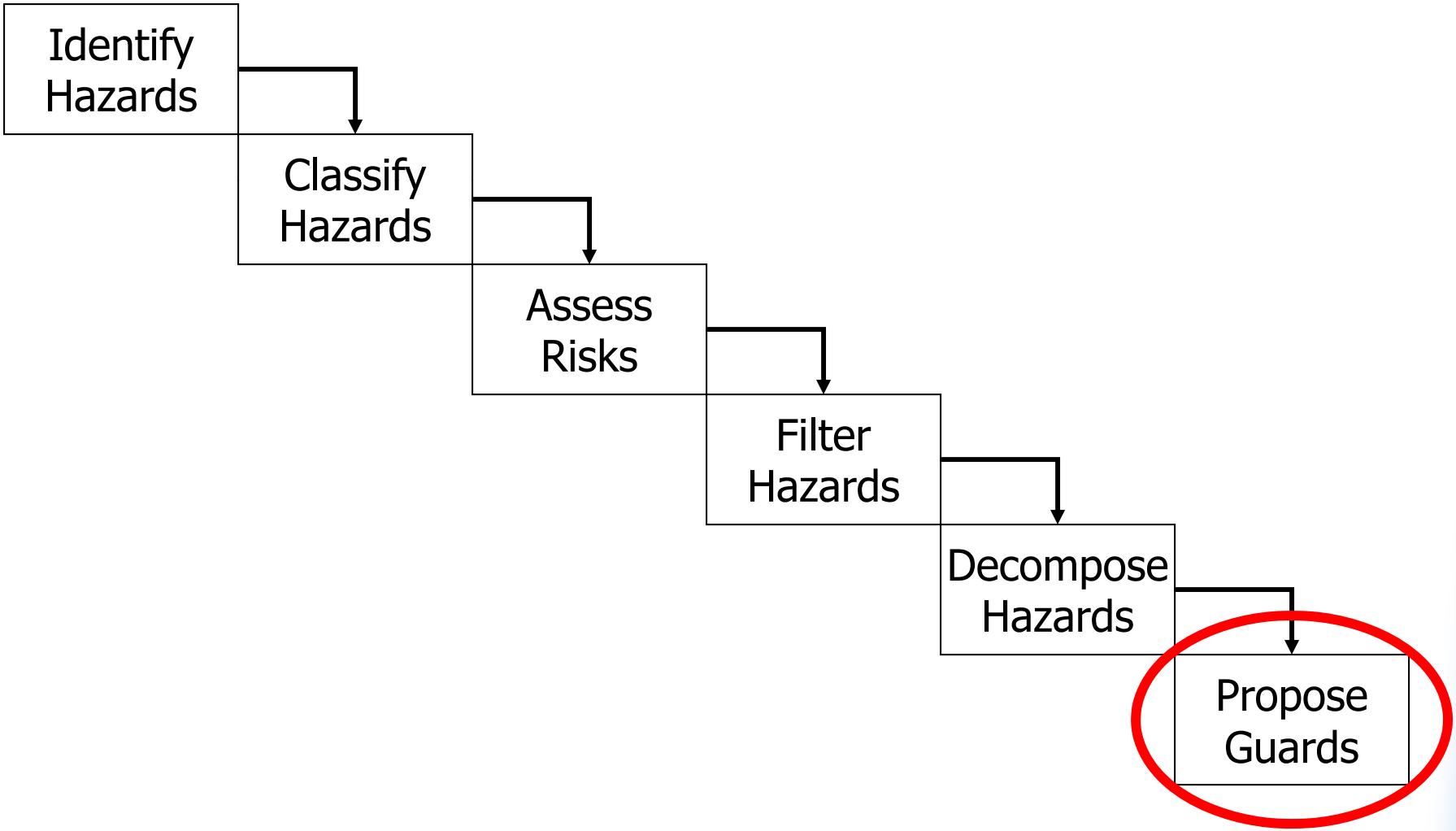


Sistem de avertizare pt. nivelul de fluid

Arbore de defecte



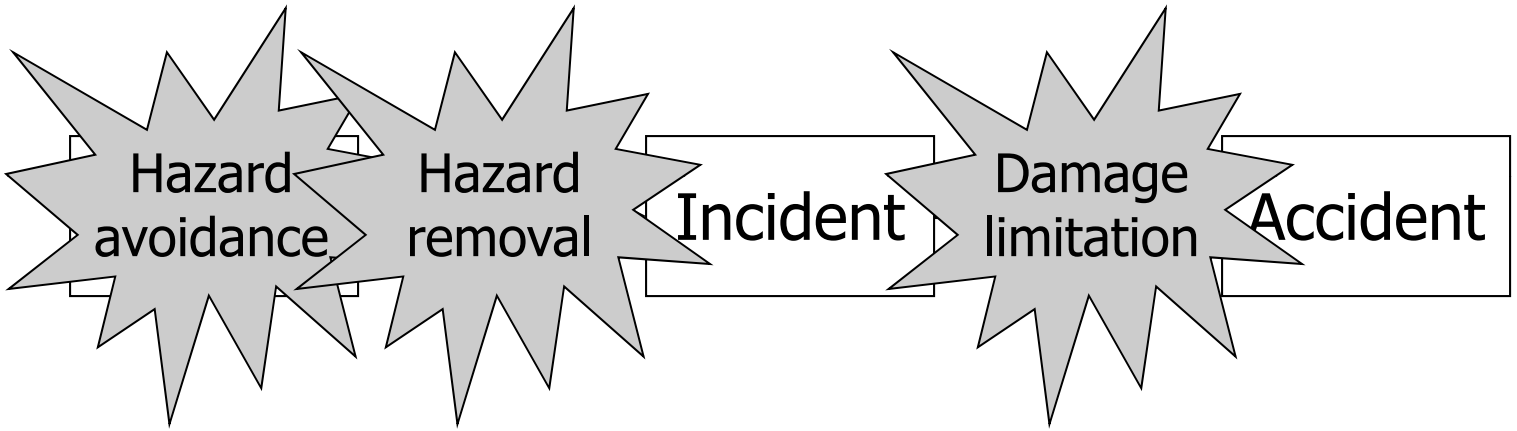
Procesul de analiză a hazardelor



Propoziția Gardă

- Previne cauze ale hazardelor:
  - Interlock-uri
  - Gărzi fizice
  - Software de control
  - Practici și proceduri de lucru
- Blochează consecința incidentelor
- În contradicție cu limitarea defectelor…

Limitarea defectelor



Abordări pt. limitare

- Aserțiuni și verificări de stare
- Gestiunea excepțiilor
- Stări de siguranță (sisteme fail-safe)
- Flexibilitate umană
- Raportarea incidentelor
- Proceduri de urgență (ex., exerciții de evacuare în caz de urgență)

Stări de oprire

- Fail-controlled: defecțiune elegantă
- Fail-uncontrolled: defecțiune scandaloasă
- Fail-stop: oprire fără output
- Fail-silent: continuare a operării, fără output
- Fail-safe: oprire și trecere într-o stare de siguranță
- Fail-operational: încă există o parte din funcționalitate operabilă

Componentele umane

- Ce efect au oamenii asupra unui sistem
  - Injectare de nesiguranță sau ne-predictibilitate?
  - Injectare de flexibilitate și reziliență?
  - …Probabil un pic din ambele
- Trebuie luat în calcul avantajele provenite din includerea componentelor umane…
- … raportat la limitările umane
- Avioanele moderne încă au nevoie și de un pilot!
- (se deschid tot felul de probleme legate de trust)

Vina

- Toate defecțiune au la bază oameni:
  - Dezvoltatori
  - Administratori
  - Operatori
- Operatorii în particular sunt buni “țapi ispășitori” dacă lucrurile nu merg precum ar trebui
  - Mai ales dacă au și decedat!
- Adesea erorile de “operatori” au la bază UI-ul

FMECA (sau doar FMEA)

- **Failure Mode** – o modalitate ca ceva să se defecteze
- Cause – ce a condus la defecțiune
- **Effect** – consecința defecțiunii
- Severity – seriozitatea efectelor
- Occurrence – prob. de apariție a cauzei
- **Criticality** - severity x occurrence
- Current control – existența unei gărzi asupra cauzei
- Detection – prob. de succes a controlului
- Risk priority - criticality x detection

Exercițiu de grup

Identificați cât mai multe hazarde potențiale ale unui zbor efectuat într-un Airbus A320. Se vor considera toate probleme socio-tehnice ce pot apărea. Se vor folosi următoarele mecanisme de identificare:

- Brainstorming
- Comparație între precedență și cazuri de test
- Analiza HazOp