

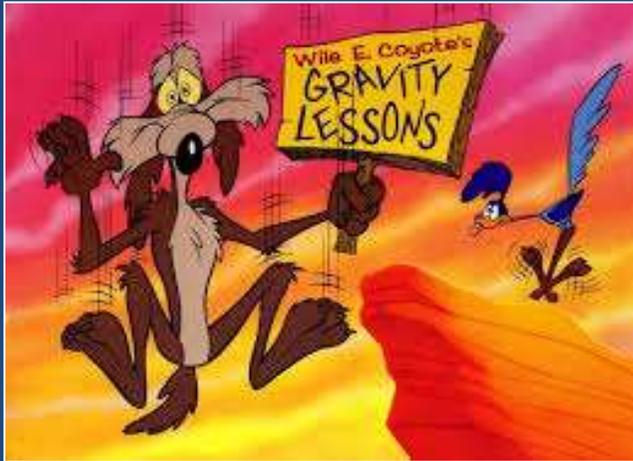
Corso di
Modelli per la Sicurezza

Michele Buonsanti
Dipartimento DICEAM email: michele.buonsanti@unirc.it

Lezione n° 2

Teorie sulle cause degli incidenti





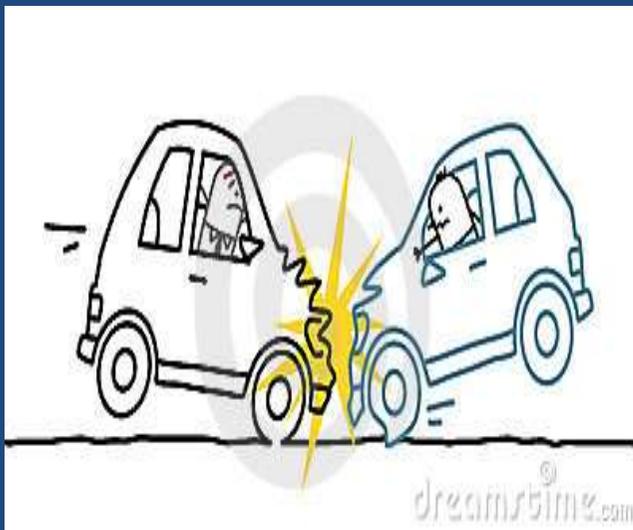
Cause
tecniche



Cause
organizzative



Cause
sociali



Cause
umane



Definizioni (M. Catino)

1-Incidente: un evento inatteso, non voluto, non desiderato e non desiderabile di azioni sociali razionali che ha conseguenze sulla vita e sulla integrità fisica e psichica di esseri umani e/o conseguenze economiche. Le conseguenze possono essere sia vicine sia distanti.

2-Incidente è una conseguenza che deriva dalla aggregazione o dalla composizione di azioni umane con interazioni del sistema fisico

3-Incidente è diverso da attentato o sabotaggio, il cui danno è volutamente cercato dagli autori. Non appartiene nemmeno al frutto di comportamenti irrazionali o privi di senso

Tipologie degli incidenti (M. Catino)

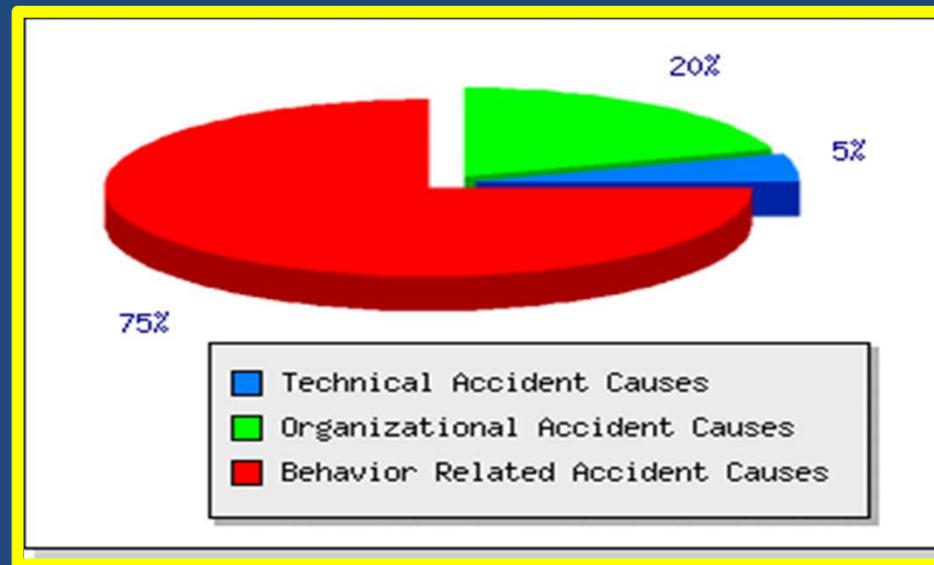
Incidenti alle persone: sono molto più numerosi e nel confronto sono certamente ad impatto minimo o trascurabile, rientrando nella normalità della vita comune.

Incidenti organizzativi: sono molto più rari ma molto spesso hanno impatto forte, a volte devastante, con conseguenze catastrofiche per la comunità. Accadono in organizzazioni complesse (industriali, infrastrutturali, telecomunicazioni). La loro frequenza è legata allo sviluppo tecnologico.

Incidenti e quasi incidenti: La differenza tra le due tipologie è nella intensità delle conseguenze rappresentando entrambi una criticità organizzativa. I primi sono evidenti per le conseguenze, i secondi, difficili da rilevare, in quanto legati alla cultura della sicurezza dell'organizzazione.

Perché accadono gli incidenti?

- Inizialmente la convinzione era per **cause tecniche**, dagli anni '80 è subentrato il fattore umano (80% - 90%)



- Gli incidenti **non accadono per violazioni di norme e/o procedure** tipiche dell'organizzazione ma, perché le stesse, quando in possibili mutati contesti, favoriscono la creazione di errori ed incidenti.

Teorie degli incidenti: **Motivazioni politiche**

(es.: British Petroleum, Vajont...)

- L'organizzazione, attuando una politica di risparmio sui costi della manutenzione e della sicurezza, porta ad una **diminuzione dell'affidabilità per tutto il sistema.**
- Il profitto per l'organizzazione considera **la sicurezza una esternalità e non una condizione necessaria per il corretto funzionamento del sistema.**
- **La sicurezza diventa variabile economica** esempio: se il costo assicurativo è inferiore al costo necessario per raggiungere un sufficiente livello di sicurezza, allora la scelta politica di convenienza affronta il problema per via assicurativa!!



Diga del Vajont Longarone (BL) 1963



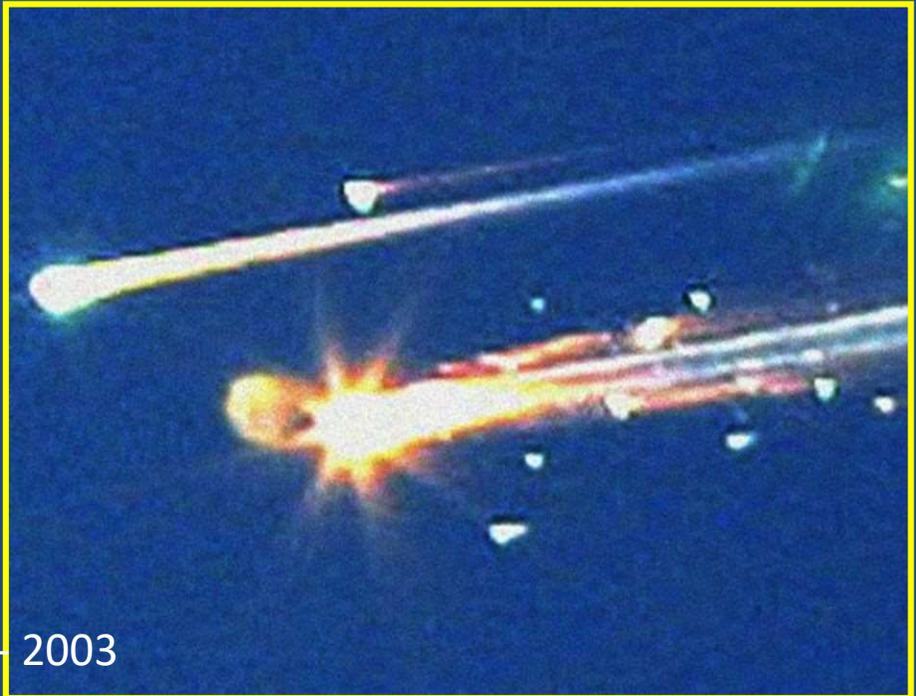
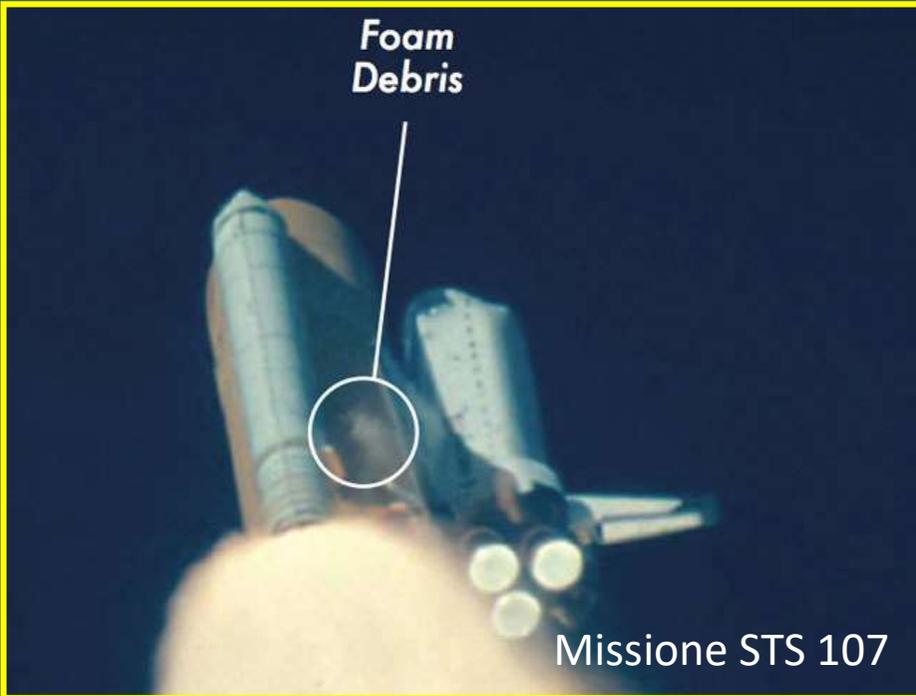
British Petroleum Golfo del Messico 2010

Teorie degli incidenti: **Modello ingegneristico**

- Origini: **ingegneria della affidabilità, ergonomia, tecniche di valutazione del rischio e dell'affidabilità umana.**
- Miglioramento della sicurezza indirizza ad ingegnerizzare l'affidabilità attraverso **metodi probabilistici.**

Il modello ingegneristico motiva le cause degli incidenti nel **biunivoco fallimento del rapporto tecnologia /fattore umano** basandosi su:

- Visione tecnocentrica delle organizzazioni e della sicurezza.**
- Considerare l'umano inaffidabile e portatore di insicurezza.**
- Errore derivante da negligenze dell'operatore.**
- Soluzioni come miglioramento tecnologico, sanzioni, rinforzo della normativa.**

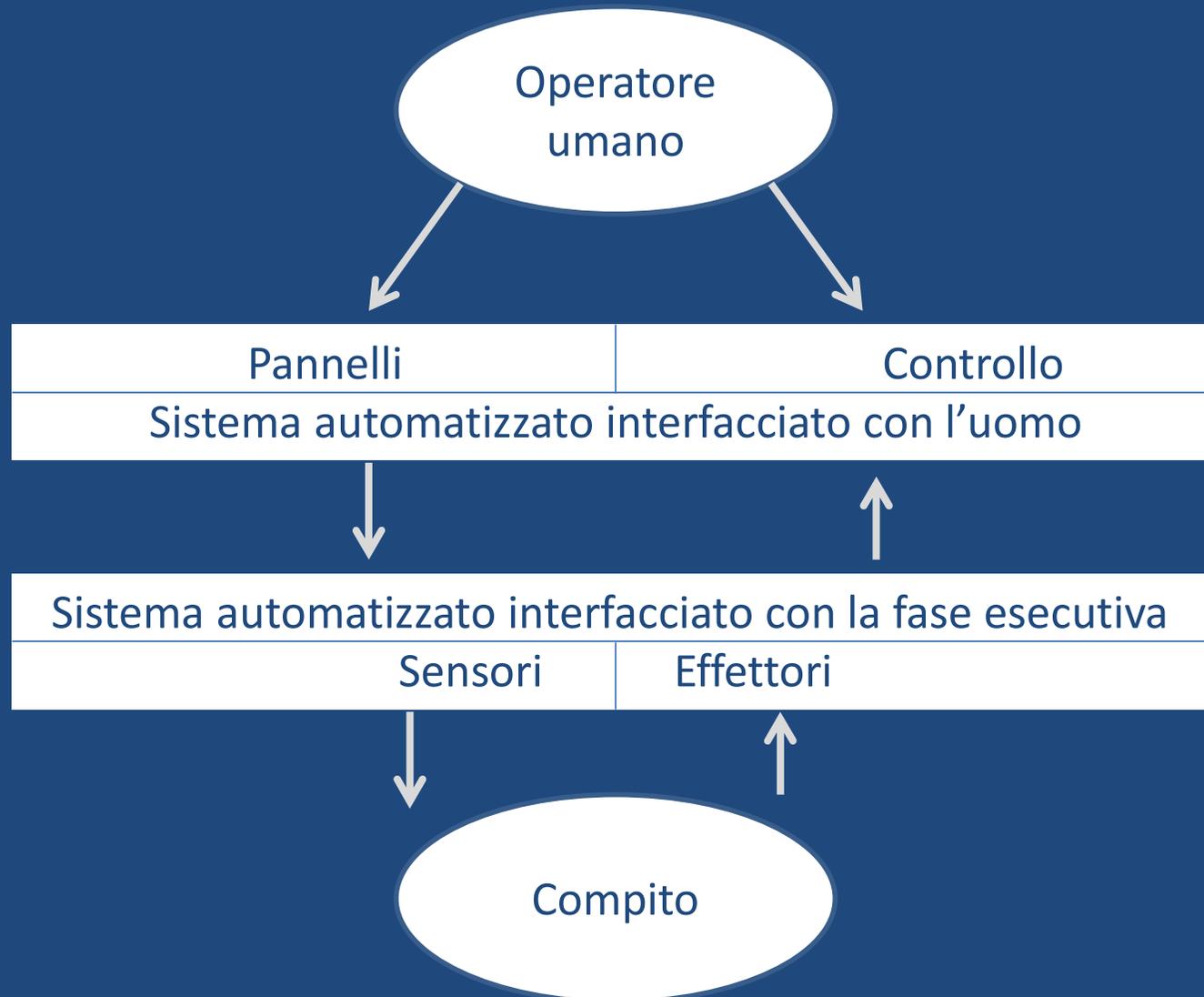


Shuttle Challenger 1986

Incidenze dello sviluppo tecnologico

- **Automazione dei sistemi:** azione di sistemi complessi incidenti sulle attività di trasformazione ed elaborazione delle informazioni dentro l'attività delle organizzazioni.
- **Interfaccia uomo-macchina:** evoluzione di tale rapporto e conseguente riduzione del ruolo materiale che l'uomo attua nel suo lavoro.
- **Aumento dei pericoli e delle difese:** La complessità rende più vulnerabili le organizzazioni e ciò comporta strategie di difesa più specifiche e incidenti per la riduzione del rischio.
- **Opacità dei sistemi:** Interfaccia M-M, tecnologia spinta, procedure complesse sono elementi che comportano poca trasparenza dei sistemi cioè, incertezza nel funzionamento.

Elementi base del controllo (Moray, 1986)



Modifica rapporto uomo-sistema

...il computer diventa l'attore principale, non l'essere umano. *Il computer prende le decisioni sul controllo e l'operatore, quando gli viene chiesto dalla macchina, può delegare o accettare il controllo.* Anche se l'uomo definisce gli obiettivi per la macchina, è quest'ultima a realizzarne il controllo (Moray, 1986)



Progettazione tecnocentrica e modifica interazione Man-Machine

Concezione progettuale

- Inaffidabilità dell'utente da parte del progettista
- Estrema complessità della macchina ai fini di una maggiore sicurezza dei risultati attesi.
- Le operazioni residue, non automatizzabili, sono lasciate all'operatore umano.

Riscontro

Difficoltà delle operazioni residue

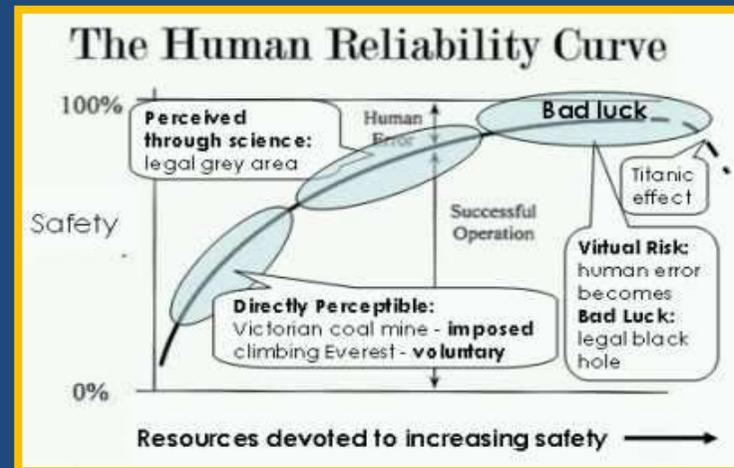
Difficoltà ad incanalare le operazioni residue in maniera sensata. Aumento della possibilità di errore.



Tecniche e metodologie per la sicurezza

(J. Reason, 1990)

VALUTAZIONE PROBABILISTICA DEL RISCHIO (PRA)



ANALISI PER L'AFFIDABILITA' UMANA (HRA)

Valutazione Probabilistica del Rischio (PRA)

(J. Reason, 1990)

Articolazione in modelli ad albero logico

- Albero dei problemi (come può verificarsi il problema ...)
- Albero dei danni (quali conseguenze ha il problema

Scopi: identificare le potenziali aree di rischio

- Identificazione dei rischi potenziali
- Identificazione delle conseguenze
- Quantificazione delle frequenze degli eventi
- Determinazione del rischio totale

Problemi: trascura problemi legati al fattore umano

Tecniche per l'analisi di Affidabilità Umana (HRA)

(J. Reason, 1990)

THERP: Tecnica per la predizione del tasso di H.E.

- Identificazione delle funzioni di sistema influenzabili da HF.
- Analisi delle operazioni umane connesse con le funzioni.
- Stima della probabilità di errore.
- Stima degli effetti dell'errore umano.

Strumenti:

- Albero dei danni (albero di probabilità)

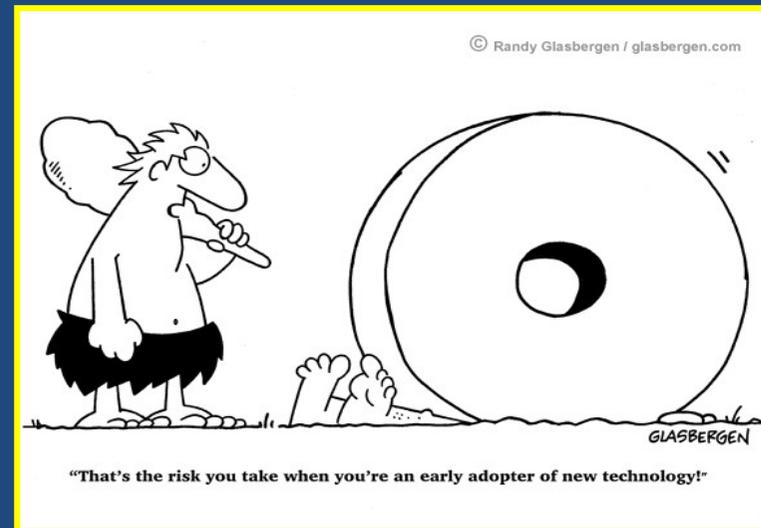
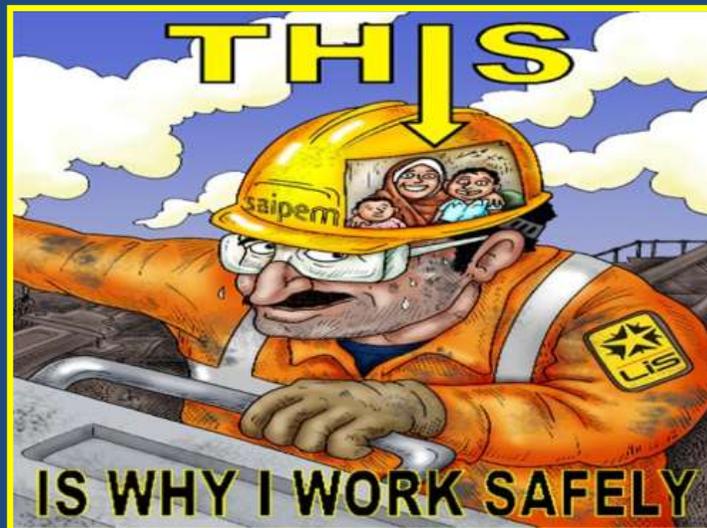
Strumenti metodologici per la sicurezza (Reason1997)

| Strumento | Ambito | Livello applicativo | Reattivo / proattivo |
|------------------------|----------------------------------|-----------------------|-----------------------|
| Tripod-Delta | Produzione trasporto petrolifero | Fattori organizzativi | Proattivo |
| Review | Ferrovie | Fattori organizzativi | Proattivo |
| MESH | Aeronautico | Manutenzione | Proattivo |
| Human Error assessment | Operazioni rischiose | Fattori organizzativi | Proattivo |
| IDM | Operazioni rischiose | Fattori organizzativi | Proattivo Reattivo |

Strumenti metodologici per la sicurezza

Strumenti proattivi:

Metodologie e strumenti volti a prevenire gli incidenti e utilizzati per migliorare la sicurezza a priori.



Strumenti reattivi: utilizzati dopo gli incidenti per analizzarne le cause e sviluppare le azioni correttive

ERRORE ORGANIZZATIVO: TEORIA

La teoria dell'errore organizzativo afferma che nelle organizzazioni tanto più è ampio il numero di criticità organizzative, di difetti di progettazione e mancanza di controllo, tanto più è probabile che un'azione-decisione umana errata attivi un incidente

Gli incidenti sono l'effetto non voluto di processi di aggregazione ed interazione di azioni e decisioni individuali con fattori organizzativi critici.

Livelli di failures in TEO: individuale, organizzativo e livello inter-organizzativo

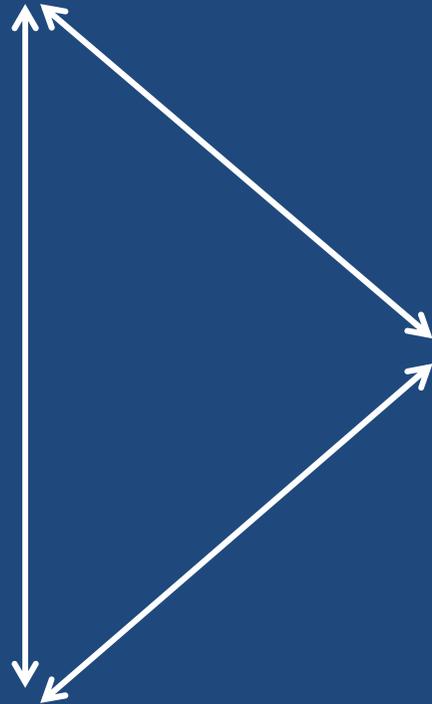
*MITIGATE
CONSEQUENCES
OF ERROR*

TRAP ERROR

AVOID ERROR

ERRORI ORGANIZZATIVI

Livello inter-organizzativo

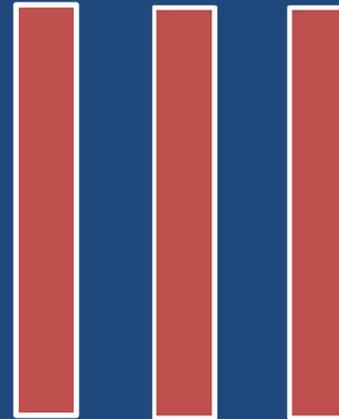


Livello organizzativo

Livello
individuale



Difese



Modello per diversi livelli di
failures (Catino)

Failures individuali

- Sono gli errori umani (*slips, lapse, mistake*), delle *violazioni* e delle *decisioni erranee* da parte degli operatori.
- Relazioni tra gli operatori, aspettative, stimoli ambigui.
- L'attore è vincolato da capacità cognitive limitate e da informazioni incomplete.
- Problemi di attenzione, memoria, comprensione, e di comunicazione caratterizzano le decisioni



Incidente ferroviaria a Santiago de Compostela 24 luglio 2013



Failures organizzative

- Sono le failures basate sulla interazione **uomo-macchina**, sul team e sul lavoro cooperativo, sui processi di comunicazione e di coordinamento operativo.
- Questi fattori sono relativi a dimensioni le cui origini possono essere **lontane dall'incidente sia nel tempo che nello spazio**.
- E' il livello della **comprensione dei processi organizzativi**, dei sistemi di attività, delle strategie e della specifica cultura della organizzazione.
- **Livello critico**: management locale, il sistema locale di coordinamento la formazione, le debolezze del sistema, le decisioni.



6 agosto 2005
incidente di Capo Gallo
(PA)
Velivolo ATR72 *Tuninter*
Flight BARI - DJERBA



Failures inter-organizzative

- Ogni organizzazione agisce *embedded* in un contesto formato da altre organizzazioni.
- Ogni organizzazione è un **nodo** nella rete del campo (organizzativo e giuridico) composto da tutte le organizzazioni con norme e regole
- Il focus è sulla **rete organizzativa**, connessioni, differenziazioni ed integrazioni tra le varie componenti.
- Tanto maggiori sono le **criticità** tanto più è probabile che un fallimento individuale diventi un incidente



Sicurezza e logica tecno-centrica

- Il modello ingegneristico della sicurezza enfatizza la potenzialità tecnologica a discapito del ruolo che il comportamento umano ha dentro il sistema.
- Affidamento a tecnologica e tecniche di valutazione del rischio per migliorare l'affidabilità e la sicurezza del sistema.

Tabella di Norman, 1998

| Persone | Macchine |
|----------------|---------------|
| Vaghe | Precise |
| Disorganizzate | Ordinate |
| Distratte | Non distratte |
| Illogiche | Logiche |

Teoria organizzativa degli incidenti

Conoscenza ed errore discendono dalle stessi fonti psichiche; solo il risultato permette di distinguerli. L'errore riconosciuto con chiarezza è, come correttivo, altrettanto utile cognitivamente della conoscenza positiva. (Ernest Mach, da Conoscenza ed errore)

Un incidente nelle organizzazioni può essere spiegato secondo:

- la teoria dell'errore umano
- la teoria dell'errore organizzativo



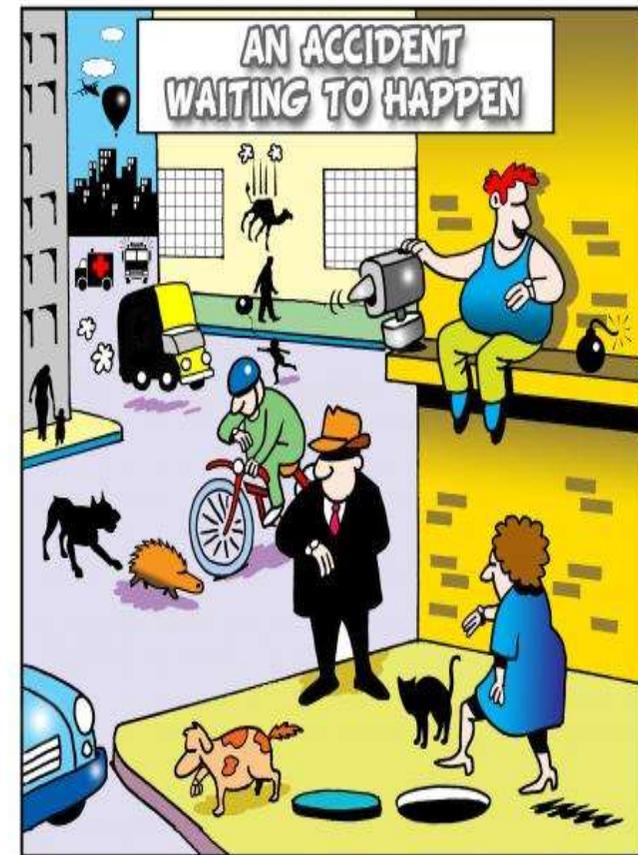
Teoria organizzativa degli incidenti

- L'incidente deriva dalla aggregazione o composizione di azioni umane con comportamenti del sistema fisico. Gli incidenti organizzativi hanno cause multiple e possono avere risultati disastrosi per le persone e per l'ambiente.
- Non c'è differenza tra incidente e quasi incidente (near miss) se il fatto presenta caratteristiche morfologiche simili.
- La differenza tra incidente e mancato incidente sta nella magnitudo delle conseguenze
- Temi comuni, negli ambiti sociotecnici, quali generatori di incidente sono le criticità latenti.

Condizioni critiche latenti

Le c.c.l. contribuiscono al breakdown delle difese dei sistemi. Le c.c.l. sono collegate ai processi organizzativi di base:

- Progettazione
- Manutenzione
- Comunicazione
- Organizzazione del lavoro
- Selezione del personale
- Formazione
- Addestramento
- Cultura della sicurezza nel sistema
- Supervisione e controllo
- Leadership e management



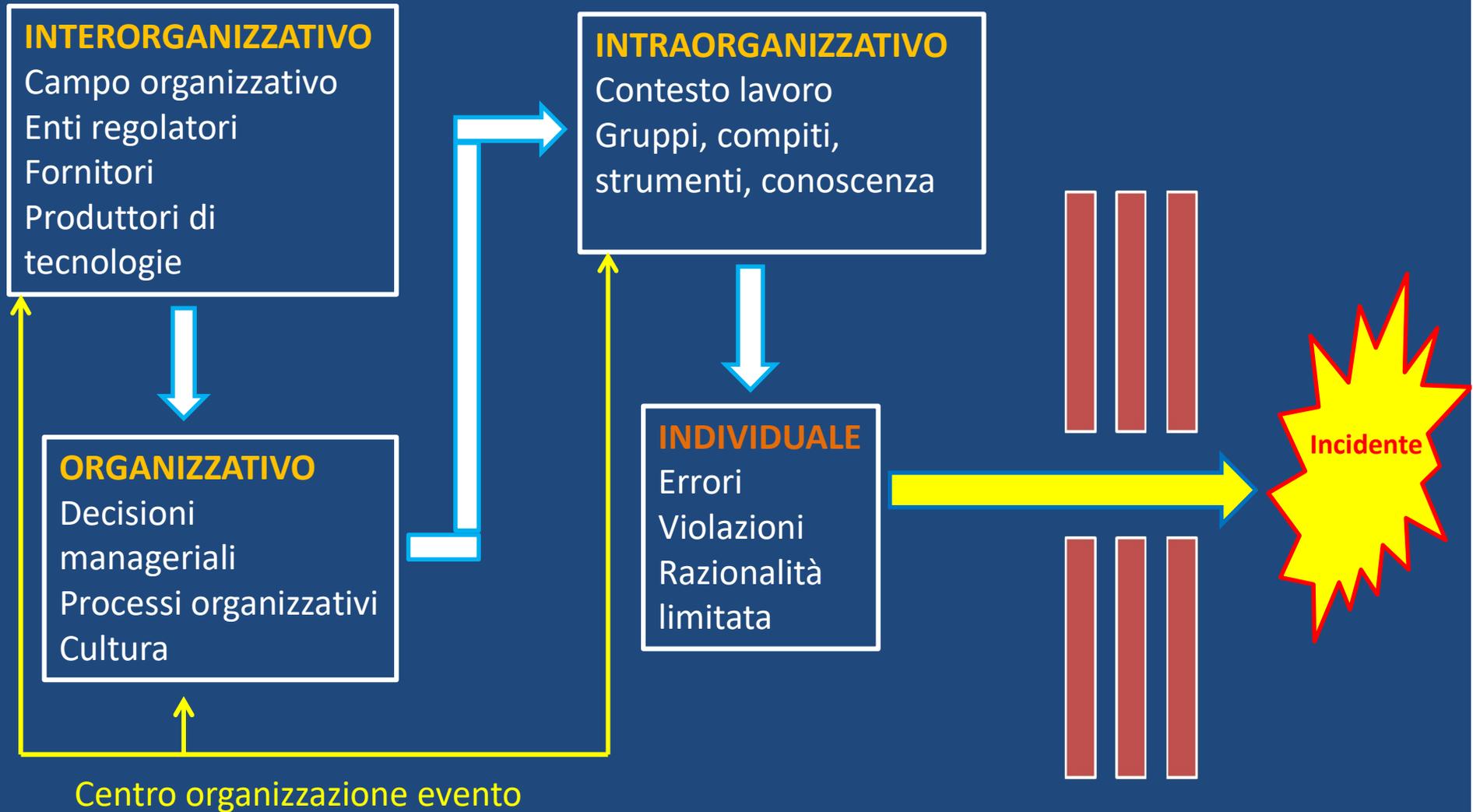
La teoria dell'errore organizzativo

Con il termine **errore organizzativo** si identifica una situazione che predispone all'errore indipendentemente dalla persona, che realizza uno specifico compito, che commette una violazione, un errore o prende una decisione sbagliata.

In questa ottica gli incidenti sono generati da errori umani ma, sono resi possibili da un **insieme di criticità** a diversi livelli del tessuto organizzativo

E' una prospettiva **probabilistica** e non deterministica: una situazione di errore aumenta la **probabilità** che un errore umano attivi l'incidente

La teoria dell'errore organizzativo: livelli (Catino)



Failures individuali: gli errori umani

Definizione di ERRORE: "Tutte quelle occasioni in cui una sequenza mentale programmata di un'attività fisica o mentale fallisce il raggiungimento del risultato voluto, e quando questo fallimento non può essere attribuito a interventi occasionali esterni (J. Reason)

Cause di un ERRORE

- 1-Azione che non vanno come devono andare.*
- 2-Azioni che non vengono fatte nel modo giusto.*

Classificazione dell'ERRORE

- 1- Slips = Sviste*
- 2- Lapses = Dimenticanze*
- 3- Mistakes = Errore*
- 4- Violations = Violazioni*

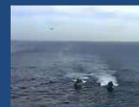
MISTAKES = Azioni intenzionali che non vanno come vorremmo (Errori)

Riguardano l'interpretazione della situazione (percezione) e la scelta della linea di azione opportuna

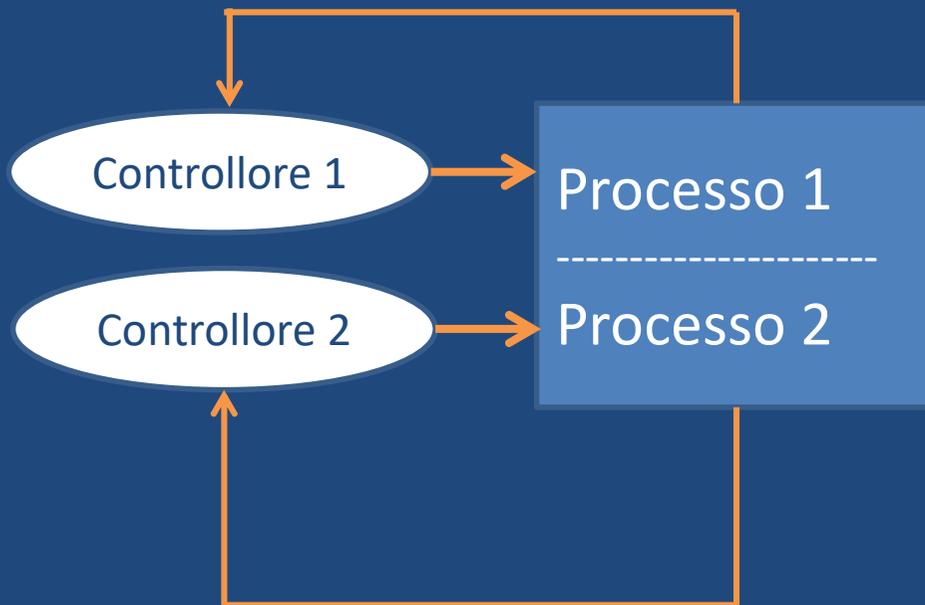
Azione è fatta bene, ci ricordiamo tutto, ma ciò che stiamo facendo non è appropriato per il tipo di situazione

Case study, simulatori, briefing sono strumenti che aiutano a migliorare la percezione vera della situazione

Esempi: Linate, Tenerife



Failures del contesto intra-organizzativo



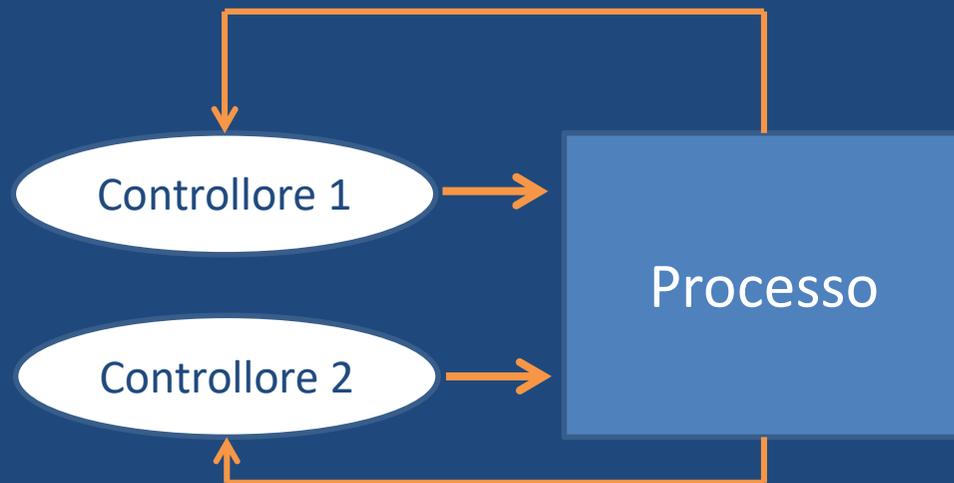
**Problematiche
di
Coordinamento**
(Leveson)

Controllo sovrapposto

Aree di confine

Riscontro di maggior incidenti:

- Nelle aree di confine per responsabilità non definite.
- Controllo sovrapposto per eccesso di ridondanza.



Failures del contesto intra-organizzativo

Contesto generale & contesto
individuale

- Interazioni uomo macchina
- Team e lavoro cooperativo
- Processi di comunicazione
- Coordinamento operativo

Controllo

- Controllo sovrapposto
- Aree di confine

Failures del contesto organizzativo



LIVELLO ORGANIZZATIVO

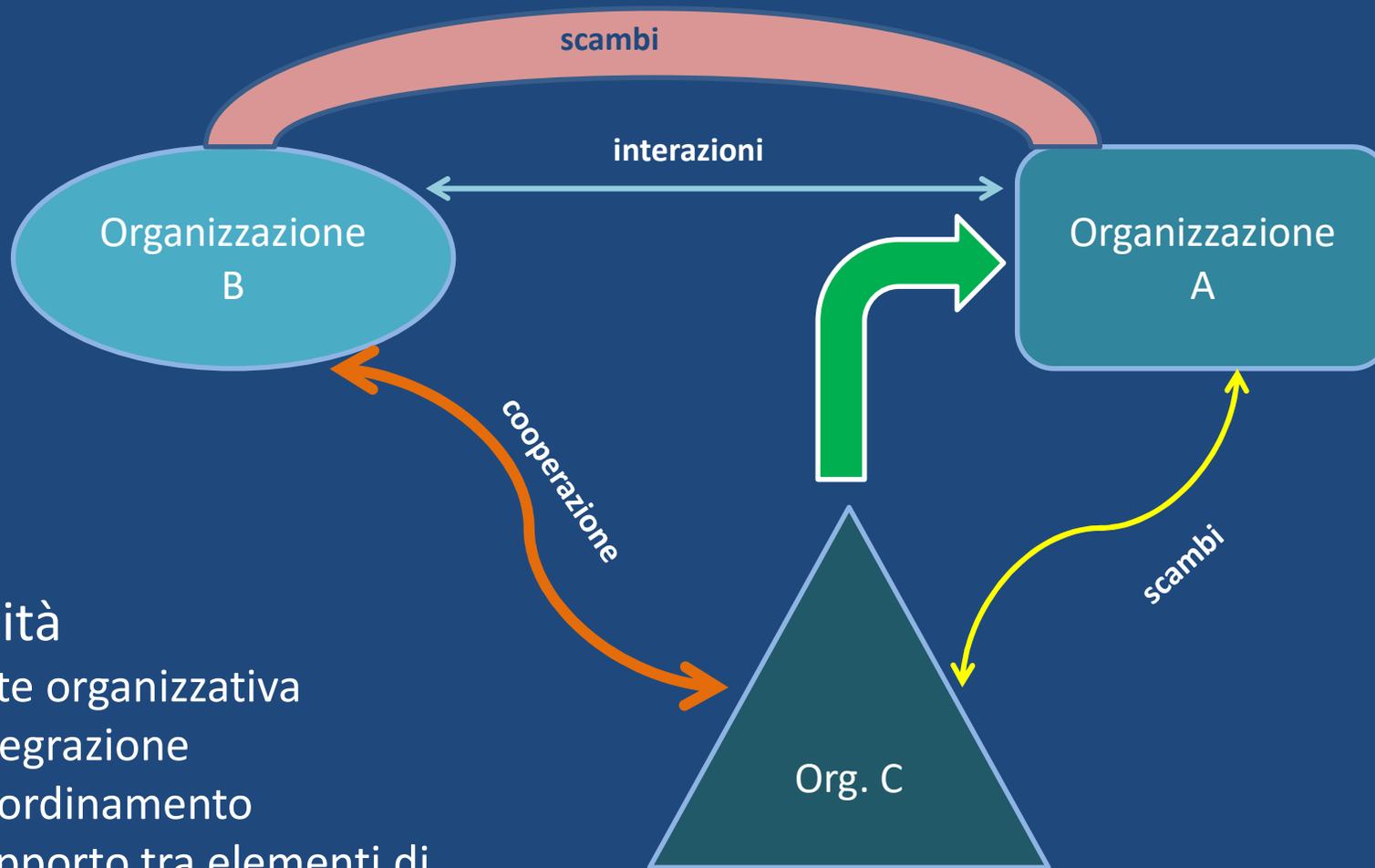
Comprensione

- Dei processi organizzativi
- Dei sistemi di attività
- Delle strategie
- Della specifica cultura dell'organizzazione

Criticità

- Management locale
- Allocazione di responsabilità
- Divisione del lavoro
- Coordinamento-controllo
- Formazione
- Decisioni management
- Condizioni equivoche

Failures del contesto inter-organizzativo



Criticità

- Rete organizzativa
- Integrazione
- Coordinamento
- Rapporto tra elementi di diverse organizzazioni

Es. Linate

SINTESI

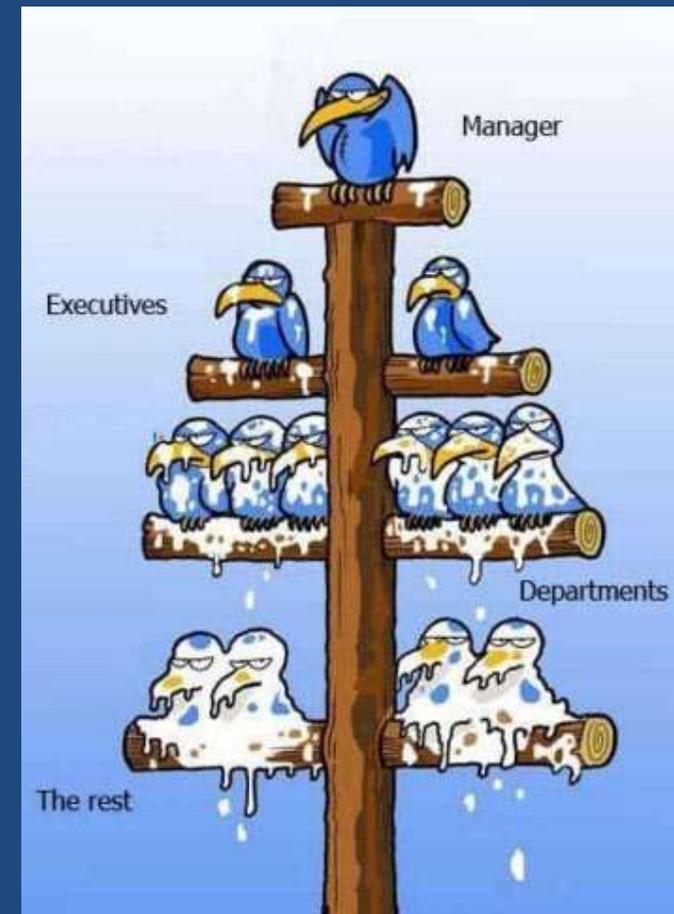
- Errori organizzativi sono situazioni predisposte all'errore indipendentemente dalle persone che commettono errori o violazioni o prendono decisioni sbagliate
- Gli incidenti organizzativi sono costruiti generalmente da 4 livelli di failures, ovvero: individuale, intra-organizzativo, organizzativo, inter-organizzativo.
- Tanto maggiore sono le criticità intra/inter/organizzativo tanto più è probabile che una failure attivi un incidente. Dalle aree di criticità devono partire le soluzioni rimedio
- L'errore umano è soltanto la parte finale della genesi e della dinamica incidentale.
- Mutamenti al solo livello individuale non modificano le condizioni di rischio

Prevenire ed apprendere dagli incidenti

...in numerosi casi di incidente è evidente come le organizzazioni coinvolte hanno dimostrato una incapacità ad apprendere da segnali deboli, da evidenze negative sulle condizioni di sicurezza o da fattori critici. (Catino)

Intelligenza organizzativa di un sistema:

Capacità di una organizzazione di ottenere ed elaborare informazioni chiare, complete nonché affidabili e tali da consentire una consapevolezza degli eventi.



Miopie organizzative (Baldissera, 1998)

I sistemi complessi non sono reattivi rispetto a segnali inusuali trascurando le informazioni a causa di:

- Informazioni sconosciute prima dell'evento.
- Informazione percepite non correttamente.
- Informazioni non assemblate correttamente.
- Informazioni impossibili da classificare.
- Deficit di informazioni legati alla struttura organizzativa
- Informazioni su segnali deboli o *near miss* non sono raccolte e/o elaborate.
- La *blame culture* ostacola la segnalazione dei reporting di errori ed anomalie.

Case Study



Stazione di Viareggio 29 giugno 2009
Deragliamento treno merci 50325
Trecate-Gricignano

Descrizione dell'evento

A seguito del deragliamento, l'urto con un elemento metallico dell'infrastruttura ferroviario provocava fuoriuscita di gas GPL da uno dei carri cisterna innescando in tal modo, un incendio di vastissime proporzioni che ha interessato la stazione di Viareggio per parecchie centinaia di metri nonché, le aree circostanti.





Convoglio Merci 50325
-Locomotiva E656.175
-14 carri cisterna a carrelli



Descrizione tecnica del convoglio e fasi salienti

- Il treno, composto da 14 carri cisterna, era trainato dalla Locomotiva E.655.175.
- Il primo carro era immatricolato presso la compagnia ferroviaria polacca PKP costruito nel 2004, revisionato il 2 marzo 2009 da una società di Bozzolo (MN), la Cima Riparazioni.
- Gli altri 13 carri erano immatricolati presso le ferrovie tedesche Deutsche Bahn.
- I carri con il gas sono stati instradati del raccordo interno della raffineria SARPOM a San Martino di Trecate (NO) alla rete ferroviaria convenzionale da FS Logistica, che prima avrebbe compiuto le operazioni di verifica della sicurezza dei 14 carri per formare il convoglio alla Stazione di Novara.
- Le cisterne del convoglio, tra cui quella da dove è fuoriuscito il gas che ha innescato l'incendio, appartengono alla multinazionale americana GATX e poi date in locazione a FS Logistica che ha utilizzato i carri per i servizi.

Analisi degli eventi

Alle 23:48 del 29 giugno 2009, il convoglio deraglia per cause probabilmente legate al **cedimento del carrello del primo carro cisterna**, che trascina fuori dai binari altri quattro carri. Solo dal primo carro, la cui cisterna viene perforata da un elemento dell'infrastruttura, fuoriesce il gas GPL che al contatto con l'ossigeno ha sviluppato l'incendio.

Il deragliamento si è verificato in corrispondenza del sovrappasso pedonale che scavalca il fascio binari sud della stazione ferroviaria di Viareggio, collegando via Burlamacchi con via Ponchielli. Il gas sembra essersi propagato in direzione di quest'ultima via, nella cui area si registra infatti il maggior numero di vittime, feriti e di edifici crollati o danneggiati.



Probabili cause

- La perizia disposta dal giudice per le indagini preliminari ha individuato la causa dell'incidente nel cedimento "a fatica" dell'assile del primo carrello del primo carro cisterna.
- Ha altresì accertato che la "cricca", la cui propagazione ha determinato la frattura dell'assile, era già presente quando il pezzo di ricambio fu spedito dall'officina tedesca Jugenthal di Hannover all'officina italiana Cima Riparazioni di Bozzolo, che provvede alla sua installazione sul carro, circa tre mesi prima dell'incidente.
- Ha accertato infine che lo squarcio della cisterna fu provocato dall'impatto contro un elemento fisso dell'infrastruttura (la punta di una controrotaia dello scambio "piegata a zampa di lepre").

Probabili cause

- Le prime indagini si sono concentrate su una «sala montata» (il complesso composto dall'asse e delle ruote) del carro.
- L'asse è risultato tranciato nella parte che sporge dalla ruota - detta "fusello" - poco prima della "boccola", la quale consente all'asse stesso e alle ruote di girare. La sezione di rottura ha evidenziato una «cricca estesa», che ha portato la sezione esistente a ridursi notevolmente fino al totale cedimento».



- La probabile causa dell'incidente è attribuibile al cedimento strutturale di un'asse del carrello del primo carro-cisterna deragliato.
- La foto sembra confermare che l'incidente sia stato provocato dalla rottura dell'asse per fatica dato che la sezione fratturata mostra la classica superficie "marezzata" per il 90% della sua superficie. Questa modalità di rottura è tipica degli assili ferroviari e per prevenirla sono previste stringenti procedure cicliche di controllo, che nel caso di specie non sarebbero state rispettate.

Questions to investigate

Analisi tra le organizzazioni presenti, loro struttura interna, interazioni, decisioni, responsabilità controllo.....

Incidente organizzativo o fatto causale?