

Politecnico di Milano
A.A. 2005 / 2006



Studio di affidabilità dei sistemi

Appello 11 Maggio, 2006

di

Fabio Arata 675536

Paolo Tagliaferri 675331

Indice generale

INDICE GENERALE	2
1.INTRODUZIONE	3
2.LE MONTAGNE RUSSE	5
2.1 IL MODELLO	5
2.2 ASSUNZIONI MODELLISTICHE	7
2.3 INCIDENTI STORICI E STATISTICHE	8
3. IL PROBLEMA DELL’AFFIDABILITÀ DEL SISTEMA	11
3.1 GLI ASPETTI CRITICI E POSSIBILI SOLUZIONI	12
3.1.1 VAGONI	13
3.1.2 STRUTTURA DI SOSTEGNO E TRACCIATO	16
3.1.3 CONTROLLORE DELL’IMPIANTO	20
3.2 MATRICE RPN	22
4. CONCLUSIONI E SVILUPPI FUTURI	24
A. APPENDICE	25

1.Introduzione

Un sistema è una collezione di elementi che vengono combinati per ottenere uno scopo non altrimenti raggiungibile con un singolo componente già disponibile in natura. Gli elementi che compongono il sistema possono essere di natura molto varia: esistono sezioni hardware, sezioni software, componenti d'interazione con l'uomo, svariate tecniche e tecnologie, politiche e procedure. L'insieme di tutti questi elementi caratterizza il sistema ed il suo comportamento.

L'affidabilità è una proprietà del sistema che entra in gioco quando uno o più componenti che lo caratterizzano presentano particolari caratteristiche di criticità relative al loro funzionamento: queste criticità, se non gestite, possono portare a guasti i quali a loro volta possono creare danni più o meno gravi alle cose e/o alle persone, oppure possono degradare in modo inaccettabile le prestazioni del sistema stesso. Un sistema viene quindi definito più o meno affidabile a seconda della tolleranza ai guasti che è in grado di esprimere, rispetto a precisi vincoli di condizioni e tempo.

L'affidabilità può essere definita a differenti livelli d'astrazione: lo scopo principale di questo documento è presentare la fase di specifica delle problematiche di affidabilità riguardo ad un sistema complesso di cui si andrà a modificare il modello iniziale (aggiungendo componenti, attuatori e sensoristica) in modo da rendere il sistema finale robusto e tollerante rispetto ai guasti critici che lo caratterizzano.

Questa sezione del presente documento rappresenta una breve introduzione sui principali concetti di affidabilità, evidenziando in particolar modo gli obiettivi che questa analisi si propone.

Nella seconda sezione verranno presentati il caso di studio vero e proprio e l'analisi dei componenti più importanti del sistema, considerando quindi gli aspetti di affidabilità relativi ai singoli elementi prima di dare uno sguardo d'insieme all'intero sistema. In questa sezione verranno anche presentati alcuni casi storici di incidenti legati al sistema studiato.

Nella terza sezione si discuterà dei possibili guasti che si possono verificare sull'impianto, delle modalità che li possono causare e dei danni che possono generare. Verrà anche studiato il

modo in cui questi malfunzionamenti possono essere evitati, attraverso l'aggiunta di sistemi di monitoraggio e controllo che rendono il sistema ragionevolmente affidabile.

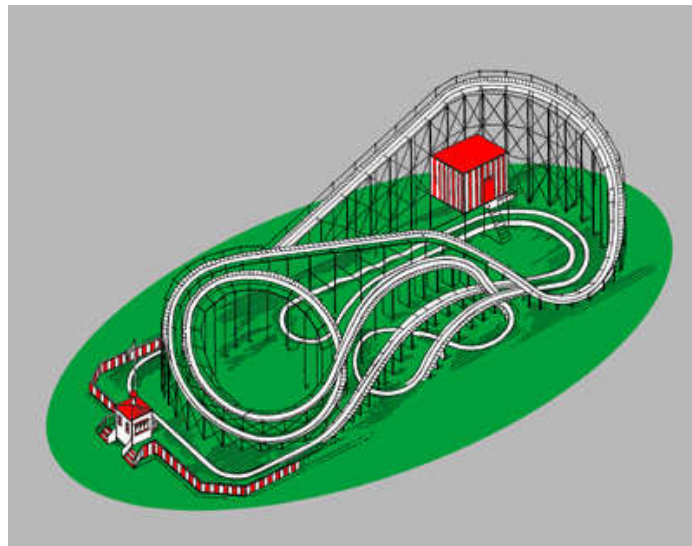
Infine nella quarta parte si tratteranno le conclusioni dello studio e si accenneranno le possibili direzioni di studio future. L'appendice conterrà le eventuali specifiche formali utilizzate nella discussione del sistema e la bibliografia.

Il lavoro sarà corredato da dati e informazioni relative alle tecnologie di impiego nel settore relativo al sistema studiato, e cercherà quindi di integrare l'aspetto modellistico con elementi che presentino riferimenti a situazioni reali ed impianti già esistenti.

2. Le montagne russe

Lo scopo di questo documento è l'analisi approfondita di un'attrazione molto conosciuta: le montagne russe. Nell'analisi si porrà particolare attenzione sulle problematiche di affidabilità e di sicurezza che contraddistinguono questo tipo di impianto. Per giungere a questo risultato, in questa sezione del documento si analizzeranno innanzitutto i componenti del sistema e i modelli fisici che li regolano, in modo da rendere chiaro il dominio del problema.

2.1 Il modello



Le montagne russe (*Roller Coaster* in inglese) sono attrazioni molto famose nei parchi di divertimento: la prima fu licenziata addirittura nel 1885. Essenzialmente, l'attrazione è un “*sistema ferroviario specifico*” che realizza un percorso chiuso con zone in salita ed in discesa, e spesso vere e proprie inversioni (come i giri della morte o gli avvitamenti). In realtà esistono anche percorsi “aperti” o “incompleti”, ma in questo documento ci focalizzeremo per semplicità sul sistema tradizionale.

L'altro elemento fondamentale delle montagne russe è rappresentato dai vagoni sui quali prendono posto i visitatori del parco: in genere essi sono raggruppati tra loro, collegati con vincoli quali sbarre e/o funi (nel sistema da noi considerato tratteremo piccoli convogli da due vagoni

collegati con una barra d'acciaio e cavi di sicurezza). I vagoni hanno capienze di vario tipo: nel nostro caso tratteremo vetture con capienza di quattro persone (quindi otto per convoglio). Generalmente la postura dei passeggeri è seduta, anche se esistono impianti ove i passeggeri rimangono in piedi all'interno di gabbie di contenimento, oppure sono alloggiati in vagoni rotanti su perni e così via. La nostra analisi considererà vagoni “standard” dove i visitatori restano in posizione seduta per tutta la durata del percorso.

Le carrozze non dispongono di un sistema di propulsione autonomo, ma percorrono i binari sfruttando la forza di gravità. Generalmente si ricorre ad una zona particolare del circuito subito dopo la partenza, detta **area di sollevamento**: essa consiste in una rampa (rettilinea o a spirale) dotata di cavi di trazione o di catene grazie ai quali le carrozze vengono trainate nel punto più elevato del circuito. Successivamente, il convoglio procederà lungo il percorso principale (**area di gravità**) sfruttando esclusivamente l'energia cinetica derivante dall'energia potenziale acquisita durante la salita. Contrariamente a quanto si crede, le carrozze non sono dotate di alcun tipo di impianto frenante autonomo: la riduzione della velocità viene conseguita sfruttando le leggi della fisica (ad esempio facendo percorrere al convoglio tratti in salita) oppure tramite particolari sezioni del percorso (in inglese *brake run*) specificatamente progettate per rallentare la carrozza ad una determinata velocità oppure per fermare totalmente il mezzo.

Queste zone particolari sono utilizzate lungo l'area di gravità ove sia necessario ridurre la velocità per evitare sollecitazioni troppo estreme su passeggeri e/o struttura di sostegno (ad esempio prima di una curva di raggio ridotto), quindi per evitare sia un'usura eccessiva, sia malessere nei passeggeri. In generale si progetta la struttura per dare una sensazione di alta velocità (imponendo accelerazioni marcate) mantenendo però un'andatura ridotta (nel nostro caso il carrello raggiungerà una velocità massima di 28 Km/h).

Oltre alle aree già citate, esiste l'**area di stazionamento** (che si trova al termine dell'area di gravità) : essa è la zona che permette ai visitatori di salire e scendere dai convogli e di effettuare la manutenzione dei treni. Per semplicità di studio la si può scomporre in varie sotto-aree:

- **Sosta4, Sosta3** sono le zone di ingresso direttamente adiacenti all'area di gravità: esse permettono di rallentare i vagoni, fino all'arresto totale se si hanno vagoni presenti nelle zone immediatamente successive;

- **Sosta2, Sosta1** realizzano aree di rallentamento in quanto i vagoni sono obbligati a fermarsi in queste zone per un breve periodo di tempo, venendo poi spinti automaticamente nell'area successiva. In questa zona è prevista una *piattaforma di trasferimento* per rimuovere/aggiungere veicoli (ad esempio per finalità di manutenzione);
- **Scarico** è l'area adibita alla discesa delle persone dai vagoni, le quali vengono poi indirizzate verso le zone di uscita dall'attrazione;
- **Carico** è l'area adibita alla salita delle persone sui vagoni per un nuovo giro, ove l'operatore umano si assicura che i passeggeri abbiano azionato correttamente i dispositivi di sicurezza;
- **Pronto** è la zona che precede l'inizio vero e proprio dell'attrazione, essa è utilizzata come passaggio dalla zona di carico alla zona di partenza, che avviene in modo automatico quando l'area successiva (*Partenza*) è libera;
- **Partenza** è la zona che immette all'area di sollevamento, che avviene in modo automatico. Per mantenere un ritmo di 1300 passeggeri/ora, i convogli devono lasciare la zona di partenza ogni 22 secondi. Questa frequenza può essere variata dall'operatore a seconda delle condizioni di affollamento dell'attrazione.

Sosta 4	Sosta 3	Sosta 2	Sosta 1	Scarico	Carico	Pronto	Partenza
----------------	----------------	----------------	----------------	----------------	---------------	---------------	-----------------

Per effettuare le manovre in modo automatico nelle varie sezioni sopra descritte, i vagoni vengono agganciati a catene circolari, simili a quella della zona di sollevamento, che permettono ai veicoli di spostarsi in tempi predefiniti, oppure vengono usati nastri di gomma che trascinano i vagoni. Si suppone che questo apparato sia collegato alla centrale informatica di controllo, che ha quindi in carico gli attuatori del sistema e riceve informazioni dalla sensoristica.

2.2 Assunzioni modellistiche

Al fine di specificare meglio il background del problema, sono state effettuate alcune assunzioni non specificate nel testo originale del caso di studio, ma che si ritengono importanti al fine di ottenere un'analisi sensata del problema.

Si suppone che l'operatore umano abbia a disposizione un pulsante atto a segnalare l'avvenuta messa in sicurezza di tutti i passeggeri sulle carrozze, in modo da segnalare al sistema informatico che è possibile instradare il treno nell'area 'Pronto'.

Si suppone inoltre che tutta la sensoristica presente sull'impianto e sui vagoni sia convogliata in una centrale informatica di controllo e supervisione, con un'apposita interfaccia per l'operatore: egli sarà quindi in grado sia di monitorare in ogni istante tutte le grandezze di interesse durante la corsa dei treni e di intervenire sull'impianto in caso di necessità. Inoltre il controllore si occuperà di attuare in modo autonomo tutte le azioni necessarie per il corretto funzionamento dell'attrazione quali freni e catene di trazione, intervenendo qualora venissero segnalate condizioni anomale.

2.3 Incidenti storici e statistiche

Verranno ora brevemente introdotti alcuni casi storici che mostrano la gravità dei problemi di affidabilità per l'applicazione considerata:

- 25 Luglio 1973: una donna di 45 anni perde la vita cadendo dalla cima di un ottovolante a Salisbury Beach, Massachusetts (USA).
- 25 Marzo 1980 : un ragazzino di 13 anni perde la vita e numerose persone vengono ferite in un parco a tema a Santa Clara, California (USA). Il bambino, cercando di salire sul vagone dell'attrazione, viene colpito da un'altro vagone in arrivo nell'area di stazionamento
- 9 Luglio 1980: un uomo di 26 anni muore in un parco di divertimenti del Missouri (USA). L'operatore, pensando che il treno sia vuoto, lo invia verso un'area di manutenzione dove l'uomo a bordo sbatte la testa contro una trave rasente al percorso.
- 10 Settembre 1983: un ragazzino di 13 anni muore colpendo un ostacolo con la testa durante il percorso a Doswell, Virginia (USA).
- 7 Luglio 1984: una donna perde la vita durante una corsa su un ottovolante a Eureka, Missouri (USA). Durante la corsa viene sbalzata fuori dal treno e precipita ad una distanza di 6 metri.
- 28 Luglio 1984: un ragazzino di 9 anni precipita per 10 metri dopo un looping a Minot, North Dakota (USA). E' stato appurato che l'operatore non aveva inserito correttamente il dispositivo di sicurezza.

- 2 Giugno 1985: un operatore di 56 anni viene travolto da un treno durante i lavori di manutenzione a Baton Rouge, Louisiana (USA)
- 30 Marzo 1996: un operatore di 25 anni viene travolto e ucciso da un treno di 6 tonnellate a Valencia, California (USA). L'uomo stava attraversando i binari nell'area di stazionamento in un area priva di segnalazioni.
- 20 Aprile 1997: un ragazzo di 14 anni muore e 5 persone risultano ferite in un incidente che ha coinvolto due vagoni dell'ottovolante a Tulsa, Oklahoma (USA). Durante la fase di salita, si rompe il meccanismo che blocca il vagone alla catena di traino. Il vagone precipita all'indietro lungo la rampa e colpisce un altro treno che si stava avvicinando all'area di sollevamento. L'incidente è stato causato dal fallimento del dispositivo di bloccaggio (non ridondante) del vagone durante la salita. (all'indirizzo [3] è disponibile un rapporto tecnico esaustivo dell'incidente)

Molti tragici avvenimenti in questa lista sono stati omessi per brevità, in quanto si è cercato di rappresentare la più vasta casistica di errori ed omissioni che hanno portato ad incidenti fatali. In ogni caso, da un'analisi preliminare, si identificano già i principali fattori di disastro che causano incidenti, e cioè:

1. La **scarsa efficacia dei dispositivi di sicurezza** dei vagoni (cinture di sicurezza e sbarre di contenimento), che in molti casi non hanno impedito ai passeggeri di cadere oppure di assumere posture non corrette.
2. La **mancanza di un sistema di segnalazione chiaro ed efficiente** che permetta al personale di manutenzione di intervenire sull'impianto solamente in condizioni di sicurezza
3. In un caso, la mancata **ridondanza dei sistemi di sicurezza** e bloccaggio dei vagoni ha avuto conseguenze disastrose.

Senza quindi entrare nello specifico, già da una prima analisi superficiale della storia degli incidenti avvenuti su questo tipo di attrazione permette di evidenziare una classe di problematiche che andrà sicuramente valutata con maggior attenzione rispetto alle altre.

Concludendo la panoramica, si può fare riferimento ad alcuni dati statistici disponibili al pubblico riguardante gli incidenti che avvengono sugli ottovolanti:

1. Uno studio del **CPSC** (*Consumer Product Safety Commission*) ha rilevato che nel 2001 negli USA sono stati necessari 134 ricoveri in ospedale tra tutti i visitatori dei parchi di divertimento, e di questi in media 2 all'anno sono dovuti alle montagne russe.
2. Uno studio commissionato dal parco di divertimenti Six Flags ha rilevato che circa 319 milioni di persone hanno avuto accesso ad un parco di divertimenti nel 2001. Lo studio ha concluso che un visitatore ha una probabilità di uno su 10^9 di rimanere ferito in modo fatale, e la percentuale di incidenti dovuti alle attrazioni è molto basso. Inoltre molto spesso i parchi di divertimenti pagano assicurazioni maggiori per giostre come il Carosello piuttosto che per un otovolante, ad indicare la grande attenzione alla sicurezza che si investe in questo tipo di attrazioni.

Dopo aver avuto una panoramica del problema oggetto dello studio, nella prossima sezione si tratteranno in dettaglio le cause di guasto e le strategie per aumentare l'affidabilità dell'impianto.

3. Il problema dell'affidabilità del sistema



Lo scopo di questa sezione è quello di fornire un'analisi dettagliata del sistema descritto in precedenza per evidenziare le problematiche di sicurezza e di affidabilità, facendo particolare riferimento all'identificazione dei possibili guasti in cui può incorrere il sistema.

A questo proposito, il modello utilizzato è quello **FMEA** (*Failure Models and Effects Analysis*): nello specifico si prenderanno in considerazione tutti i componenti principali dell'attrazione e, per ognuno di essi, sarà svolta una ricerca dei possibili guasti che possono verificarsi e quindi delle possibili soluzioni ai suddetti inconvenienti.

Questo tipo di analisi, pur essendo di tipo prevalentemente informale, permette di identificare rapidamente gli aspetti sopracitati e di applicarli in modo *tout-court* al design dell'attrazione in modo efficace. Inoltre è possibile operare una classificazione degli aspetti identificati per fornire un indice di rischio (*RPN, Risk Priority Number*) di ogni aspetto considerato, facendo riferimento ad una valutazione qualitativa di vari aspetti relativi ad un generico guasto (severità, frequenza e capacità di rilevazione).

Inoltre questa analisi è iterabile a vari livelli d'astrazione: è possibile quindi specificare ulteriormente l'indagine e studiare nel dettaglio gli aspetti particolarmente critici, per suddividere

un particolare problema in tanti sotto-problemi più gestibili, andando infine a identificare soluzioni “a grana più fine” che permettono di raggiungere gradi più elevati di affidabilità.

3.1 Gli aspetti critici e possibili soluzioni

Lo scopo dell'impianto considerato nel presente documento è quello di far divertire le persone che vi salgono a bordo. Perché questo avvenga, è necessario che le fasi di carico e scarico, così come la corsa vera e propria, avvengano in condizioni di totale sicurezza e di comfort per gli utenti. Questo ci permette di identificare subito due particolari prospettive di interesse per il nostro sistema:

- **Hard Safety:** l'aspetto principale da considerare è la sicurezza e l'incolumità delle persone a bordo dei treni. L'infrastruttura, così come i meccanismi di controllo, devono essere tali da rendere quanto più improbabili possibile eventuali danni a persone e/o cose, sia a bordo dei treni, sia nelle immediate vicinanze dell'impianto. Bisogna tenere conto che un'infrazione a questo principio potrebbe avere gravissime conseguenze (ferimento / morte di una o più persone, nonché rilevanti danni economici e di immagine per il parco divertimenti), per cui è fondamentale garantire che l'impianto esprima comportamenti accettabili (da questo punto di vista) sia in condizioni operative di normalità, sia in condizioni anormali (nel limite del possibile);
- **Comfort:** il goal principale dell'attrazione è quello di garantire il divertimento degli utenti che percorrono le montagne russe. Per questa ragione è indispensabile che le specifiche di affidabilità tengano conto non solo dell'incolumità delle persone e della stabilità delle strutture, ma anche del fatto che le corse si svolgano nel modo il più regolare possibile senza malfunzionamenti che, pur non essendo di per sé pericolosi, potrebbero “rovinare il divertimento” degli utenti (ad esempio se una sezione frenante operasse più energicamente del dovuto, il treno potrebbe rallentare eccessivamente e la corsa potrebbe risultare “noiosa” per i viaggiatori)

I due obiettivi sopra enunciati rappresentano dei *goal* che ci permettono di classificare la *performance* dell'impianto. Al fine di raggiungere gli obiettivi sopra enunciati, si rende necessario quindi esplicitare le problematiche che possono prevenirne il conseguimento. Questo è possibile

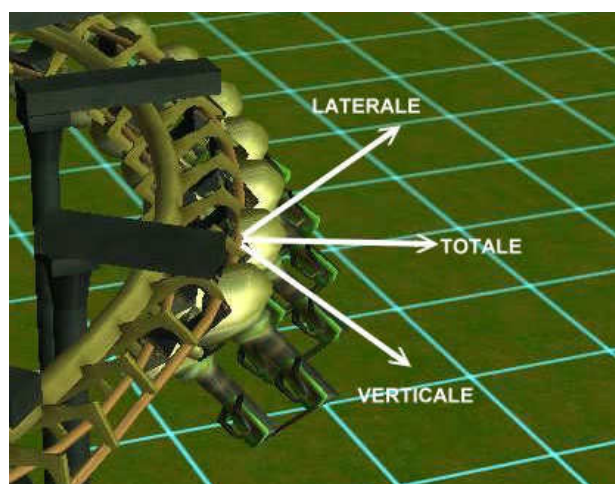
effettuando un'analisi del sistema e dei suoi componenti, per individuarne le criticità e proporre soluzioni atte a prevenire i guasti e a rendere l'esperienza quanto più piacevole possibile per gli utenti. Si considerano quindi nel dettaglio tutti i componenti dell'impianto.

3.1.1 Vagoni

I vagoni sono il componente a diretto contatto degli utenti dell'attrazione, ed ospitano al loro interno i dispositivi di sicurezza che i viaggiatori devono utilizzare durante la loro corsa. Le parti principali sono:

- la struttura esterna che da forma al veicolo;
- i quattro sedili interni alla struttura dove i passeggeri si possono accomodare per fare il giro sull'attrazione;
- le ruote che permettono alla vettura di spostarsi sui binari;
- le cinture di sicurezza per mantenere la persona saldamente ancorata al veicolo durante la corsa;
- il paraurti lungo il perimetro della carrozza;
- la barra d'acciaio che si collega all'altro vagone per formare un treno
- i cavi di sicurezza, ridondanti per assicurare il collegamento tra i vagoni in caso di cedimento della barra.

Il veicolo è soggetto a sollecitazioni meccaniche di notevole intensità: in un ottovolante infatti ogni vagone è sottoposto ad accelerazioni orizzontali, verticali e laterali (lungo quindi tutti e tre gli assi cartesiani in un piano tridimensionale), e spesso si verificano transizioni molto brusche



da uno stato di moto ad un altro: questo è fonte di notevole stress per tutti i dispositivi e le strutture.

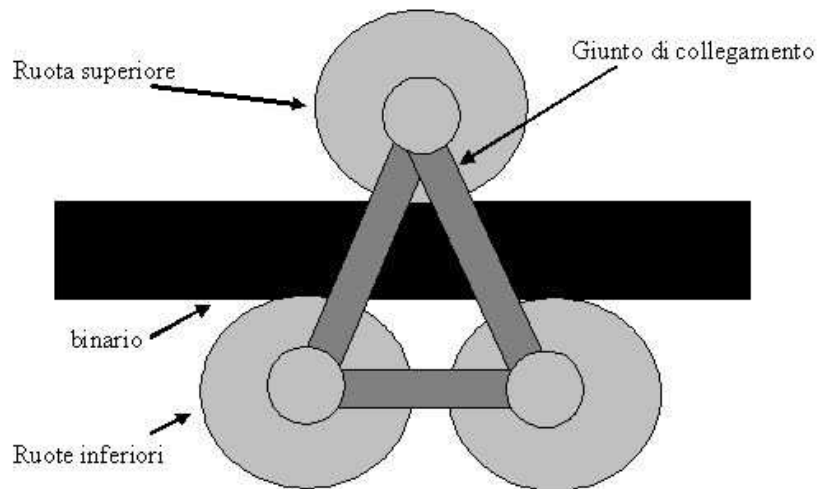
3.1.1.1 Guasti del vagone

I vagoni possono essere soggetti a vari tipi di guasto, che possiamo classificare secondo un criterio di severità:

- **Rottura del paraurti esterno del veicolo:** il paraurti esterno ha la funzione di ammortizzare le collisioni con altri vagoni in attesa nell'area di stazionamento, ed eventualmente di assorbire eventuali urti non previsti durante la corsa. L'eventuale rottura per usura del paraurti non comporta grossi rischi per i passeggeri a bordo, in quanto in condizioni normali le collisioni avvengono solamente a bassa velocità nell'area di stazionamento, mentre è assolutamente imperativo impedire in generale le collisioni lungo il percorso adottando altri accorgimenti (ad esempio, suddividendo il percorso in *block run*). Tuttavia l'assenza del dispositivo di ammortizzamento potrebbe portare a danni allo chassis del veicolo, ed eventualmente ad un'usura maggiore per il veicolo nel suo insieme. L'unica soluzione possibile per evitare questo tipo di guasto è una manutenzione regolare che preveda la sostituzione dell'apparato in caso di danno.
- **Rottura dei dispositivi di sicurezza e contenimento:** come già è stato fatto notare in precedenza, il mancato intervento dei dispositivi di sicurezza presenti sul vagone sono una delle cause principali di danni alle persone in caso di incidenti. Si possono distinguere due cause principali legate a questo mancato intervento: in primo luogo spesso essi non sono progettati in modo tale da impedire alla persona di modificare la propria postura durante la corsa del treno, permettendo quindi di assumere posizioni pericolose che pregiudicano la sicurezza dell'attrazione. In secondo luogo in molti casi non è agevole per l'operatore la verifica della messa in sicurezza dei passeggeri prima della partenza dei vagoni, e questo è un grave rischio soprattutto quando i passeggeri sono di giovane età oppure diversamente abili, per cui non sono in grado di rendersi conto del rischio che possono correre utilizzando l'attrazione senza le dovute precauzioni. Le soluzioni per ovviare a questi problemi sono tante e

si differenziano a seconda del dispositivo di sicurezza impiegato: vi sono infatti cinture di sicurezza e barre meccaniche di contenimento. In entrambi i casi si possono integrare dei sensori nei meccanismi di aggancio e/o di blocco, in modo tale da emettere avvisi acustici e/o visivi qualora il dispositivo non risultasse correttamente inserito prima della partenza del treno. In questo modo si potrebbe impedire la partenza del treno anche tramite il controllo elettronico senza operatore, evitando che il convoglio lasci la zona di carico e raggiunga quella di pronto. Inoltre sarebbe utile implementare dei dispositivi di bloccaggio “a discesa” (sia per quanto riguarda le cinture che le gabbie di contenimento): in questo modo l'operatore potrebbe accorgersi molto più facilmente di eventuali malfunzionamenti e/o omissioni con una semplice occhiata, notando immediatamente i dispositivi non correttamente posizionati

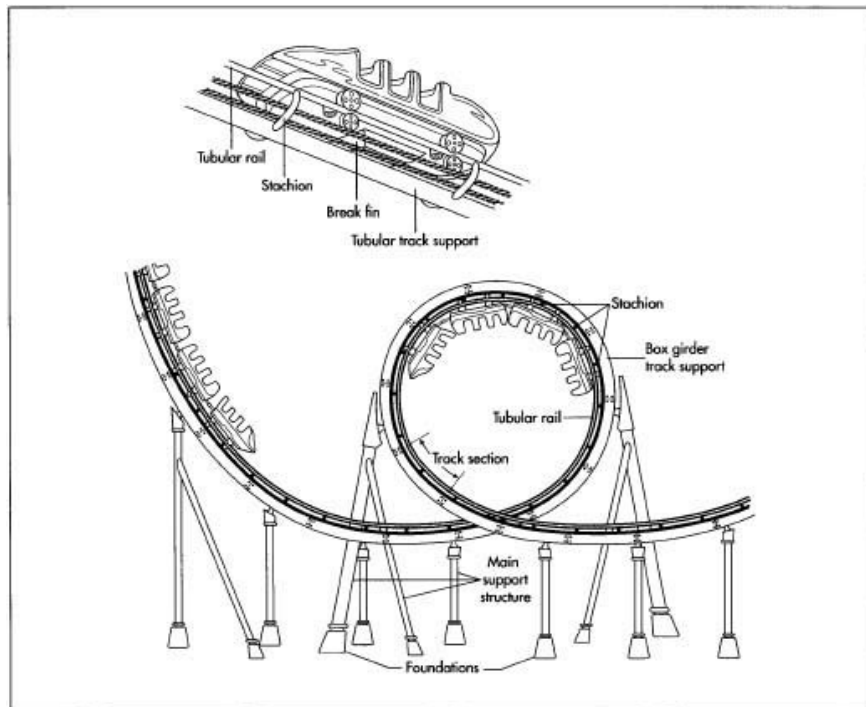
- **Uscita del vagone dai binari:** un grave rischio è dovuto all'eventuale deragliamento di uno o più vagoni dal percorso. Escludendo le cause legate al cedimento dei supporti strutturali del tracciato (di cui si tratterà in seguito), questo potrebbe essere causato da un cattivo bilanciamento del carico a bordo o da un'eccessiva velocità del vagone, oppure dal cedimento di un componente del vagone (come le ruote). I danni causati da questo guasto sono probabilmente i più gravi immaginabili, con grandi rischi non solo per i passeggeri ma anche per le persone e le cose in prossimità del luogo di impatto. La soluzione principale a questo problema prevede un testing accurato dello svolgimento della corsa tramite vagoni speciali dotati di sensoristica adeguata a rilevare le anomalie e le sezioni “eccessivamente spinte” del tracciato: questi test andranno condotti in tutte le possibili condizioni di carico ammissibile del vagone, mantenendo il più ampio margine di sicurezza possibile. Inoltre sarebbe molto utile dotare ogni vagone di un set di sensori *wireless* (magari ridotto rispetto al vagone di test di cui si è parlato sopra) in grado di rilevare tensioni eccessive, vibrazioni impreviste e/o temperature al di fuori della norma operativa, permettendo quindi di prevedere una possibile rottura di un componente (in aggiunta quindi alla normale manutenzione dei veicoli). Un'altra possibile soluzione è quella di dotare il vagone di una o più ruote speciali sotto i binari, collegate con il veicolo, come nella figura sottostante. In questo caso si permette di ancorare saldamente il vagone al binario, evitando uscite di sede durante la corsa.



Anche questo apparato necessiterà di continua manutenzione e di un eventuale monitoraggio elettronico, in quanto l'usura cui sono sottoposte le ruote è di notevole intensità e solo un'accurata e regolare ispezione può permettere di mantenere alti livelli di affidabilità.

3.1.2 Struttura di sostegno e tracciato

La struttura di sostegno di un impianto di montagne russe può essere realizzata in vari modi, ed è diversa a seconda del tipo di attrazione considerata. In generale, si distingue tra roller coaster in acciaio e in legno. I primi sono quelli più diffusi, perchè il materiale utilizzato (tubolari in acciaio e gomme rivestite in poliuretano) permette di creare tracciati più spinti e avvincenti, in grado di sopportare sforzi molto grandi. Le strutture in legno al contrario non permettono le cosiddette “*inversioni*” (come i giri della morte) o curve particolarmente inclinate. Essi sono costituiti da supporti in legno con binari in acciaio.



Esistono anche altri tipi di montagne russe non tradizionali molto diffuse: tra di esse ricordiamo ad esempio quelle invertite (con le carrozze vincolate ai binari nella parte superiore), quelle sospese (con carrozze “flottanti” ancorate superiormente al tracciato) o quelle “*pipeline*” (con i binari laterali alla carrozza). Tuttavia non si tratteranno in questo documento in quanto l'analisi è incentrata sulle attrazioni di tipo tradizionale.

3.1.2.1 Guasti dei sostegni e del tracciato

Anche in questo caso si adotterà una classificazione dei problemi a seconda dei rischi che possono causare:

- **Mancato allineamento dei vagoni:** può verificarsi un allineamento imperfetto dei vagoni nelle zone in cui essi transitano (nell'area di stazionamento), dovuto all'inerzia impressa ai corpi dagli attuatori per svolgere in automatico le operazioni richieste e anche all'inerzia degli attuatori stessi che difficilmente saranno in grado di ottenere un'elevata precisione nel posizionamento del mezzo. Si ritiene che questo guasto sia poco significativo in quanto ben difficilmente può essere fonte di danni per gli altri mezzi e per le persone: per ovviare al problema si ritiene che sia sufficiente allargare le zone, e in particolare quelle di carico e scarico, per poter così

agevolare la salita e discesa delle persone dai vagoni mettendo a disposizione più spazio per muoversi.

- **Cedimenti strutturali dei sostegni e del percorso:** a causa degli sforzi meccanici cui la struttura è sottoposta è possibile che si verifichino dei cedimenti strutturali che pregiudichino la sicurezza dell'impianto. Questo tipo di guasto è abbastanza critico, perché può portare a danni molto gravi per cose e/o persone (sia ai viaggiatori sulle carrozze, sia agli eventuali utenti in attesa e/o al personale, nonché a tutti coloro che si trovino in prossimità delle strutture in cedimento). Gli unici modi per prevenire questo tipo di problemi sono la manutenzione periodica delle strutture ed il monitoraggio continuo delle forze e delle sollecitazioni cui la struttura è sottoposta mentre è operativa. Questo può essere effettuato aggiungendo sensori collegati al controllore che inviano periodicamente misure relative a grandezze fisiche d'interesse (tensioni e vibrazioni in primis), con i quali è possibile ottenere una mappatura dello stato dell'impianto. Questi componenti potrebbero essere integrati con il “vagone di test” già citato in precedenza.
- **Malfunzionamento della piattaforma di manutenzione:** un ulteriore problema può essere identificato nel funzionamento delle piattaforme di trasferimento in quanto un non perfetto riallineamento con i binari dell'attrazione in seguito all'utilizzo della piattaforma potrebbe causare la fuoriuscita dalla sede ferroviaria dei vagoni in transito. Questo è un rischio grave, in quanto può causare danni ingenti ai viaggiatori e a coloro che si trovano nelle vicinanze. Per evitare che questo accada si possono inserire dei sensori che controllino che la piattaforma di trasferimento venga riposizionata, dopo l'utilizzo, nel modo corretto (ovvero perfettamente allineata con i binari dell'attrazione). Questi sensori saranno collegati al terminale di controllo il quale non permetterà l'avanzamento dei vagoni in coda in modo automatico finché non riceverà un segnale di perfetto allineamento dell'apparato.
- **Rottura del blocco della catena di traino:** nell'area di sollevamento i vagoni vengono bloccati da un meccanismo e trainati dalla catena verso l'inizio dell'area di

gravità. La rottura del meccanismo potrebbe innescare un disastro di gravi proporzioni (come quello riportato nella sezione precedente – 1997). Si crede quindi che l'aggiunta di ridondanza su questo meccanismo possa fornire ulteriore affidabilità al sistema.

- **Guasti ai brake run:** come già detto, sulle montagne russe i vagoni non sono provvisti di dispositivi di frenata autonomi. Essi sono infatti implementati in apposite sezioni del percorso (*brake run*), che hanno il compito di frenare o bloccare completamente un treno in transito. Le maggiori tipologie sono i *trim brakes* (in grado di rallentare i treni) e i *block brakes* (utilizzati per implementare le sezioni del percorso accessibili ad un treno per volta – *block run* – e comprendenti dispositivi di riavvio del treno una volta che è stato fermato – *drive tires*). Le tecnologie utilizzate negli impianti frenanti sono di vario genere: esistono i freni a pattino (che rallentano il treno tramite frizione meccanica con la base delle carrozze, poco usati negli impianti recenti), i freni ad alette (molto utilizzati, che comprendono una scanalatura comprimibile controllata elettronicamente nella quale passa un'aletta solidale alla carrozza, realizzando una sorta di “freno a disco”) e i più moderni freni magnetici che non sfruttando l'attrito non sono soggetti a variazioni del punto di lavoro (ad esempio in caso di maltempo) e permettono frenate molto più confortevoli e sicure per i passeggeri. I guasti possibili sono tanti: oltre alla rottura fisica dei dispositivi, potrebbero verificarsi problemi di controllo legati ai dispositivi elettronici che comandano gli attuatori (sia per problemi software, sia per malfunzionamenti dell'hardware). Il rischio collegato a questo tipo di incidente è molto elevato, perchè potrebbe portare a incidenti gravi quali scontro tra treni, deragliamento delle carrozze oppure uno stress eccessivo delle strutture meccaniche dovuto alla grande velocità, per non parlare di quello cui verrebbero sottoposti i passeggeri. Per aumentare l'affidabilità occorre sicuramente sottoporre tutti gli impianti ad una manutenzione molto accurata, soprattutto per quanto riguarda le parti meccaniche, ed eventualmente introducendo ridondanze essendo questo un sistema molto critico. Gli errori di controllo rientrano nella casistica dei problemi relativi al controllore, per cui verranno trattati nella sezione successiva. Tuttavia, per avere un grado di sicurezza ancora più elevato, si potrebbe realizzare l'impianto partendo dal presupposto che ogni corsa deve poter continuare in condizioni di sicurezza anche

nel caso che tutti gli impianti frenanti del circuito vadano fuori uso, nel senso che si deve garantire che il treno non deragli anche transitando nelle sezioni del circuito ad una velocità molto superiore di quella operativa e a pieno carico.

3.1.3 Controllore dell'impianto

Nei *roller coaster* moderni gran parte degli impianti sono soggetti all'azione svolta dal controllore elettronico, che ha un gran numero di funzioni: oltre al controllo vero e proprio degli attuatori, esso è il principale attore per quanto riguarda la gestione della sicurezza e dell'affidabilità in quanto svolge una funzione di supervisione dell'impianto in modo che esso funzioni sempre all'interno dei limiti di operatività previsti dal sistema. Il controllore è inoltre in grado di arrestare in sicurezza il sistema qualora si rilevi una condizione anomala.

Negli impianti moderni il controllore non è singolo, ma è generalmente replicato in tre elementi (PCU) funzionanti in parallelo. Quando viene rilevata un'anomalia, anche da un solo PCU, l'impianto viene arrestato immediatamente in condizioni di sicurezza. E' compito dell'operatore poi il riavvio dell'impianto dopo aver determinato la causa del problema oppure semplicemente dopo aver appurato che era un falso allarme.

- **Scontro tra vagoni (violazione del block run):** questo guasto, pur coinvolgendo i vagoni, può essere causato da vari motivi che coinvolgono direttamente il controllore. Il percorso infatti è generalmente suddiviso in sezioni (*block run*), ed è regola generale che un solo treno deve trovarsi all'interno di un *block run* in ogni istante di tempo. Uno scontro tra vagoni (se si escludono quindi gli urti di lieve entità che possono avvenire nella zona di stazionamento) è quindi possibile solamente se viene meno l'imposizione di questo invariante nel sistema da parte del controllore. Il guasto può avere molteplici cause: si può avere un malfunzionamento del sensore che determina la presenza di un treno all'interno di una sezione: questo problema può essere risolto replicando i sensori in più punti dato il loro basso costo. In questo modo si potrebbero anche realizzare un meccanismo di voting per evitare rilevazioni errate. Un'altra possibile causa è dovuta al danneggiamento dei cavi di collegamento della sensoristica: per evitare questo inconveniente si può utilizzare

una segnalazione elettrica a “zero vivo” per rilevare immediatamente i danni sulle linee (che possono essere segnalati sul pannello dell'operatore), oppure adottare una topologia wireless autoconfigurante (se compatibile con i disturbi elettromagnetici presenti sull'impianto) con una rete ad-hoc di sensori e una o più *basestations* per il raccoglimento dei dati. Il guasto potrebbe essere causato anche da un malfunzionamento del controllore, si tratterà questo aspetto nel punto seguente.

- **Malfunzionamento generico del controllore:** come ogni calcolatore digitale, anche il controllore è suscettibile di guasti di vario genere che possono pregiudicare la validità dei risultati o interrompere il flusso dei dati. I rischi derivanti da questo problema sono molteplici, e si può andare da un semplice deterioramento del funzionamento del sistema fino alla possibilità di disastri di ampie proporzioni, per cui la criticità del problema è molto alta. Le cause che possono generare questo malfunzionamento sono di vari tipi. Ad esempio, potrebbe verificarsi il blocco (*freeze*) di uno o più processori. Questo problema si può risolvere con l'ausilio di apposite strutture *watchdog* in grado di rilevare il blocco delle macchine e di forzare il riavvio delle stesse. In ogni caso la replicazione delle PCU dovrebbe comunque garantire che almeno un risultato corretto venga sempre inviato dove necessario, escludendo casi di blocco totale e contemporaneo di tutte le macchine (che possono essere statisticamente ridotti al minimo aumentando il numero di PCU in parallelo). Secondariamente, potrebbero verificarsi errori di calcolo durante l'esecuzione del codice: questo fattore potrebbe avere conseguenze ininfluenti in certi casi (ad esempio, se un attuatore è pilotato da un valore numerico assoluto – non differenziale e ricalcolato ad ogni ciclo - un errore di calcolo verrà automaticamente sovrascritto al ciclo successivo), mentre potrebbe avere conseguenze fatali in altri casi (ad esempio, un errore su un valore booleano come il bloccaggio del vagone alla catena di traino potrebbe causare un disastro). Questo evidenzia il fatto che esisteranno sezioni di codice su cui non si vuole correre alcun rischio e che quindi potranno essere oggetto di misure di affidabilità a grana ancora più fine. Ad esempio, si potrebbero utilizzare delle firme intra e inter blocco per intercettare dei branch errati nel flusso di istruzioni, oppure si potrebbe replicare una routine critica implementandola con linguaggi e metodi differenti su ogni PCU.

- Mancanza di energia elettrica:** tutto l'impianto ovviamente fa affidamento sulla presenza dell'energia elettrica, che può venire a mancare. In questo caso è possibile risolvere il problema in due modi: in primis, è necessario integrare nel sistema dispositivi in grado di reagire in maniera robusta alla mancanza di corrente: ad esempio si può fare in modo che la catena di traino si blocchi meccanicamente in caso di mancanza di energia, mantenendo bloccati anche i fermi dei vagoni in modo che non precipitino all'indietro. Inoltre si può progettare il percorso in modo tale che, in caso di assenza di energia ai dispositivi frenanti, il treno sia comunque in grado di percorrere a pieno carico e senza incidenti l'intero percorso (anche se in modo “movimentato”). Secondariamente (anche se la soluzione è abbastanza dispendiosa e poco applicabile) si potrebbero fornire generatori alternativi di back-up che garantiscano l'alimentazione, per un ragionevole lasso di tempo, ai componenti essenziali del sistema (freni, dispositivi di sicurezza, controllori elettronici).

3.2 Matrice RPN

Dopo aver enunciato tutti i principali guasti, possiamo riportare in una matrice un indice qualitativo che viene assegnato ad ogni guasto relativamente agli attributi di *severity*, *frequency*, e *detection* in modo da guidare la fase successiva di implementazione mantenendo le priorità sugli aspetti più importanti. Grazie ai valori assegnati si è in grado di calcolare il **Risk Priority Number**, ovvero il fattore che indica dove bisogna porre l'attenzione. I valori di Severity, Frequency e Detection sono stati attribuiti su una scala da 1 a 5, mentre RPN è calcolato come $(S * F * D)$

	<i>Severity</i>	<i>Frequency</i>	<i>Detection</i>	<u>RPN</u>
Rottura del paraurti esterno del veicolo	1	2	1	2
Rottura dei dispositivi di sicurezza e contenimento	5	2	3	30
Uscita del vagone dai binari	5	1	1	5
Mancato allineamento dei vagoni	1	3	1	3

	<i>Severity</i>	<i>Frequency</i>	<i>Detection</i>	<i>RPN</i>
Cedimenti strutturali dei sostegni e del percorso	5	1	1	5
Malfunzionamento della piattaforma di manutenzione	4	2	3	24
Rottura del blocco della catena di traino	5	2	4	40
Guasti ai brake run	5	3	2	30
Scontro tra vagoni (violazione del block run)	5	1	3	15
Malfunzionamento generico del controllore	4	4	3	48
Mancanza di energia elettrica	3	4	1	12

Grazie all'analisi tabellare, siamo in grado di rilevare quali sono i malfunzionamenti su cui occorrerà porre maggiore attenzione: come prevedibile, il malfunzionamento generico del processore è il fattore di maggior rischio, in quanto potrebbe coinvolgere numerosi sottosistemi in cascata ad esso. Seguono immediatamente tutti i dispositivi di sicurezza principali, dal cui corretto funzionamento dipende l'incolumità dei passeggeri. Altri fattori, come l'allineamento nella zona di carico e i guasti al paraurti risultano essere meno importanti.

In definitiva quindi, dopo aver vagliato attentamente ogni componente del sistema e aver ricercato tutte le possibili cause di guasto, possiamo intervenire sulle specifiche originali (guidati dalle indicazioni fornite dai valori RPN trovati durante l'analisi) e introdurre i componenti proposti nei punti precedenti per aumentare l'affidabilità dell'impianto.

4. Conclusioni e sviluppi futuri

Concludendo, in questo studio si è analizzato un sistema complesso mettendo in primo piano le problematiche di affidabilità che caratterizzano una specifica sicura di un impianto. Data la particolare natura del problema, sono state affrontate tematiche di sicurezza relative a vari campi dell'ingegneria (meccanica, informatica ed elettronica) a vari livelli di dettaglio, in modo da fornire uno scorcio quanto più ampio e interdisciplinare possibile sulle problematiche inerenti questo tipo di applicazione.

Per brevità, non sono stati trattati tutti i problemi particolari legati alle particolari implementazioni di otovolante che sono ormai diffusissime, essendo i parchi di divertimento alla ricerca di continue novità per soddisfare i propri visitatori. Ad esempio esistono otovolanti i cui convogli vengono “sparati” lungo un percorso singolo di andata e ritorno (circuiti aperti), e queste strutture hanno caratteristiche tali da richiedere una definizione specializzata delle problematiche in essi presenti.

Inoltre non si è trattato in modo particolareggiato dei problemi legati all'affidabilità dell'esecuzione del codice, specialmente per quanto riguarda le possibili soluzioni ed il loro impatto sulle performance del sistema. D'altra parte, il controllo richiesto e le dinamiche ad esso collegate non contengono problematiche di tipo real-time di grande rilievo, quanto più una correttezza logica dei valori di controllo e attuazione nonché delle sequenze corrette di operazioni da svolgere, ragion per cui le performance computazionali del sistema non sono essenziali ai fini del problema.

Si ritiene comunque che quanto trovato possa essere un'ottima base di partenza per sviluppare un impianto affidabile.



“Yuppiiieeee!! Siamo ancora vivi!”

A. Appendice

Fonti:

- [1] – Wikipedia (<http://www.wikipedia.org>)
- [2] – Ride Accidents (<http://www.rideaccidents.com/>)
- [3] - <http://www.rideaccidents.com/bells3.txt>