Integrazione di Usabilità e Sicurezza: l'Esempio del Controllo del Traffico Aereo

Fabio Paternò, Carmen Santoro	Vincenzo Sabbatino
CNUCE – C.N.R. Via S.Maria 36 56126 Pisa {F.Paterno, C.Santoro}@cnuce.cnr.it	Laboratorio per le Tecnologie dell'Informazione Alenia-Marconi Systems Via Tiburtina Km 12.400 00131 Roma svin@lti.alenia.it

Sommario

Le problematiche relative all'usabilità e la sicurezza sono spesso affrontate in modo separato, specialmente nello sviluppo di applicazioni interattive, critiche per la sicurezza. In queste applicazioni un errore umano può avere effetti catastrofici. Un esempio di tali applicazioni sono quelle per il Controllo del Traffico Aereo. In questo articolo si analizzano quali sono gli aspetti rilevanti per ottenere un metodo in grado di affrontare questa tematica e si discutono esperienze in corso per la sua applicazione ad un caso di studio, il controllo del traffico aereo in un aerodromo, anche se lo stesso approccio può essere applicato ad altri sistemi critici rispetto alla sicurezza.

1. Introduzione

La progettazione delle moderne interfacce utente è un processo che richiede un approccio multidisciplinare in grado di considerare tutti gli aspetti e le problematiche coinvolte: dalla conoscenza del dominio applicativo e delle funzionalità che il sistema deve supportare, alle attività che l'utente deve eseguire interagendo con il sistema, ai fattori umani e ai principi di psicologia cognitiva e di ergonomia, fino alle nozioni di ingegneria del software.

Uno dei benefici maggiormente rivendicati dall'introduzione di nuove tecnologie e di nuovi media nella progettazione delle interfacce utente è un potenziale aumento nell'efficienza dell'interazione tra uomo e macchina. Tale efficienza può essere ottenuta con l'introduzione di nuovi media e l'uso di rappresentazioni più vicine al modello concettuale dell'utente. Non a caso, uno dei concetti chiave connessi allo sviluppo di applicazioni interattive negli ultimi anni è perciò quello di *usabilità*, ossia la progettazione di interfacce utente che risultino il più possibile facili da usare. Tale aspetto ha un significato particolare quando si analizza il disegno di un sistema critico rispetto alla sicurezza dove ancora maggiore enfasi deve essere posta sul ruolo dell'operatore umano e sulla prevenzione di sue erronee interazioni con il sistema le cui conseguenze in ultima analisi possono minacciare la vita umana. In questi sistemi i due aspetti di usabilità e sicurezza devono essere accuratamente valutati in quanto un'interfaccia facile da usare non è necessariamente sicura, basti pensare al fatto che in un'applicazione critica per la sicurezza un errore umano può avere effetti gravi che non possono essere annullati in alcun modo e quindi strategie generalmente usate per aumentare l'usabilità (come incrementare l'uso di tecniche di interazione grafiche a manipolazione

diretta) non necessariamente risultano proficue dal punto di vista della sicurezza. Questo implica che il concetto di usabilità ha un significato diverso in questa classe di applicazioni rispetto ad altre.

L'idea di base per una integrazione tra i due aspetti sembra quella di rendere disponibili azioni che aumentano il controllo del sistema da parte dell'utente, e allo stesso tempo di rendere difficili o impossibili quelle pericolose per la sicurezza del sistema stesso. L'aspetto in comune tra i concetti di usabilità e sicurezza diviene proprio l'errore umano [4], poichè da una parte rappresenta per definizione un caso in cui l'utente è in difficoltà durante l'interazione con il sistema (e quindi potenziale oggetto di ulteriore studio per gli aspetti di usabilità) e dall'altra una situazione in cui la sicurezza dell'intero sistema può essere compromessa, poichè talvolta un errore può avere conseguenze molto pericolose.

Da questo punto di vista, la progettazione di interfacce utente per il sistema del Controllo di Traffico Aereo rappresenta un esempio emblematico di applicazioni in cui analizzare le possibilità di integrazione tra i due aspetti di usabilità e sicurezza. Infatti, pur considerando il sistema corrente sostanzialmente sicuro, il suo crescente sviluppo (attuale e previsto) sta evidenziando l'urgenza di produrre una nuova generazione di interfacce utente che rendano il lavoro del controllore più semplice e più efficiente, consentendogli allo stesso tempo di monitorare la situazione, di prevenire eventuali problemi, di trovare soluzioni a conflitti, suggerendogli eventualmente delle possibili soluzioni.

2. Il Controllo del Traffico Aereo: il Sistema Corrente

Il Controllo del Traffico Aereo è un'importante area di applicazione in cui molti problemi sono ancora lontani dall'essere risolti. Il numero e la durata dei ritardi, (specialmente durante le ore di punta o in condizioni metereologiche avverse) mostrano che il sistema del controllo del traffico aereo non sempre è in grado di far fronte alle richieste dei passeggeri; alcuni incidenti sono avvenuti a causa degli effetti indesiderati generati dall'interazione dei controllori con il sistema e con i piloti o per la mancanza di efficienza del sistema stesso; infine il numero crescente di vettori presenti nelle aerovie e la conseguente maggiore frequenza nelle comunicazioni tra controllore e piloti hanno iniziato a sottolineare le limitazioni dei canali VHF attualmente utilizzati a questo scopo, in quanto essi diventano ben presto saturi durante livelli eccessivi di traffico.

Tali esigenze hanno evidenziato da una parte la necessità di introdurre nuove tecnologie e strumenti più sofisticati per la gestione del traffico aereo per aumentare l'efficienza con cui i controllori eseguono la loro attività e di conseguenza l'efficienza (e la sicurezza) globale del sistema stesso; dall'altra, hanno sottolineato la necessità di un'analisi ancora più accurata dell'interazione uomo-macchina e dei fattori umani associati, in quanto l'introduzone di nuovi media in questo sistema può modificare il modo in cui il controllore esegue la sua attività.

Il compito fondamentale dei controllori è quello di garantire sicurezza e regolarità al flusso del traffico aereo: *sicurezza* significa che deve essere rispettata la separazione minima tra gli aerei, *regolarità* significa che i voli devono seguire il più possibile i piani di volo iniziali. Attualmente i controllori svolgono gran parte del loro lavoro avvalendosi in minima parte di strumenti interattivi. Infatti, dal punto di vista degli strumenti e dei tools, essi utilizzano principalmente:

- Le "flight strips", strisce di carta generate automaticamente dal sistema che contengono informazioni sui voli (ad esempio il tipo di aereo, la rotta prevista, etc.) e sulle quali essi annotano le evoluzioni del traffico nel settore,

- Le comunicazioni vocali (via radio, via telefono e direttamente) per comunicare rispettivamente con i piloti, con i colleghi di altri settori e dello stesso settore,

- Altri strumenti (ad esempio il radar, che consente loro di monitorare la situazione corrente del traffico, specialmente quando non è possibile averne una visione ad "occhio nudo" come avviene per i controllori del traffico aereo "en-route", ossia dei voli che viaggiano a velocità di crociera)

Il tipo di strumenti utilizzati costituisce allo stesso tempo la forza e la debolezza del sistema in quanto ha un impatto diretto sulle attività stessa del controllore: infatti essi da una parte garantiscono un elevato grado di sicurezza derivante dal livello di conoscenza e "confidenza" che i controllori hanno acquisito nell'uso di questi strumenti rimasti praticamente immutati nel tempo; dall'altra costituiscono proprio l'aspetto su cui sono necessari i maggiori sforzi per un aumento della performance del sistema, in funzione dell'attuale e soprattutto del previsto sviluppo di questo settore nei prossimi anni.

Non a caso in questa classe di applicazioni (così come avviene in tutte le applicazioni critiche rispetto alla sicurezza) l'introduzione di nuove tecnologie rappresenta al tempo stesso una sfida ed una potenziale minaccia: una sfida per la varietà di aspetti che devono essere considerati e le loro implicazioni sul disegno complessivo del sistema, una minaccia in quanto il loro impatto (specialmente in termini di usabilità e sicurezza) non è sempre noto e, nel peggiore dei casi, può mettere in pericolo la vita umana: da qui la (comprensibile) difficoltà con cui viene accolta qualsiasi modifica in tali sistemi. La conseguenza diretta di questo problema è evidenziata proprio dalle carenze presenti nel sistema corrente: un traffico aereo sempre più congestionato e l'efficienza dell'intero sistema affidata sostanzialmente alla capacità (soggettiva) dei controllori di prevenire e/o risolvere conflitti nel sistema. Tale capacità, fortemente legata al livello di esperienza del singolo controllore, se può essere sufficiente ad assicurare buoni standard di sicurezza nel caso di normali condizioni di traffico, si è già rivelata inaccettabile nel caso di intensi flussi di traffico, richiedendo soluzioni a lungo termine che forniscano al controllore un supporto automatico che lo agevoli nello svolgimento delle sue attività.

3. Incidenti

In tutti i sistemi critici rispetto alla sicurezza, qualsiasi incidente (useremo questo termine per riferirci ad entrambe le accezioni di "incidente" ed "accidente" così come sono definite in [2]) non avviene mai per il singolo errore dell'operatore umano o per il fallimento di un singolo componente, in quanto tali sistemi sono progettati per essere robusti rispetto ai fallimenti del sistema e in genere non consentono di portare il sistema in uno stato di "non-sicurezza" con una singola operazione. Molto più spesso invece gli incidenti avvengono per il verificarsi di cause molteplici e concomitanti, in maggiore o minor misura dipendenti tra loro e in condizioni ambientali non previste o differenti da quelle ipotizzate.

Ad esempio, le procedure correnti relative al controllo degli aerei, dei veicoli di terra e del personale all'interno dell'area dell'aerodromo sono basate principalmente sul principio del "see and be seen" per mantenere le separazioni tra gli aerei e/o i veicoli all'interno dell'aerodromo. Tuttavia, si sta verificando un numero sempre crescente di incidenti durante i movimenti a terra, incluse le incursioni sulle piste. I fattori che contribuiscono includono il progressivo aumento del traffico, la complessità del layout dell'aerodromo ed il numero sempre crescente di operazioni che hanno luogo in condizioni di bassa visibilità. Di seguito riportiamo due esempi emblematici di incidenti aerei, entrambi accaduti a terra.

- L'incidente di Tenerife può considerarsi il piu grave mai accaduto nella storia dell'aviazione che abbia coinvolto aerei al suolo. L'evento si è verificato a Los Rodeos Airport di Tenerife (isole Canarie) il 27 Marzo 1977 e ha coinvolto due Boing 747 in una collisione a terra. La conseguenza di tale collisione è stata la morte di 583 persone. Diverse sono le circostanze

che hanno condotto a questa tragedia: luci di centro pista inoperative, incroci scarsamente segnalati, nebbia, equipaggio stanco, un aeroporto non familiare ai piloti, documentazione non chiara dell'aeroporto, confusione nella comunicazione in entrambe le cabine di pilotaggio e nella torre. Il KLM 747, dopo essersi portato alla fine della pista ha iniziato la procedura di decollo. La procedura è iniziata in seguito ad una autorizzazione che la torre di controllo ha emesso dopo un ambiguo scambio radio. Tuttavia Il PAN-AM 747 appena atterrato ha mancato l'uscita dalla pista e stava continuando il movimento in cerca della successiva uscita. L'aeroporto era in quel momento immerso nella nebbia rendendo difficile la reciproca vista dei due aerei.

- Nel dicembre del 1990, nell'aeroporto di Detroit Metropolitan, un B727 e un DC9 si sono scontrati in conseguenza di una differenza tra la rotta autorizzata e quella realmente presa dal DC9. Il DC9 è entrato all'intersezione di una runway ed è stato colpito dal B727 in decollo. L'incidente, avvenuto in condizioni complesse e di bassa visibilità, ha causato la morte di 9 persone.

4. Lo studio di un caso

Per quanto riguarda la gestione del traffico aereo nell'immediata vicinanza dell'aereoporto e all'interno dell'aerodromo si possono individuare sostanzialmente due figure di controllori che lavorano fianco a fianco all'interno della torre di controllo e che comunicano (in momenti differenti) con i piloti utilizzando la radio (ciascuno con una frequenza diversa) ed hanno accesso a informazioni provenienti dalle flight strips, da una visione ad "occhio nudo" dell'aerodomo ed eventualmente dal radar. Analizziamo di seguito le attivita' dei due controllori:

- il *controllore di terra* (o "Ground" controller) si preoccupa di gestire i movimenti del traffico a terra, ossia (per gli aerei in partenza) di instradare gli aerei dal gate di partenza fino al punto immediatamente prima dell'inizio della "runway" (pista di decollo), e (per quelli in arrivo) di rilevarli dalla fine della pista di atterraggio e instradarli fino al gate di arrivo, comunicando loro il cammino da seguire (per semplicità analizzeremo nel seguito solo il caso degli aerei in partenza). Per far questo il controllore di terra, in funzione del gate di partenza e della runway assegnata, (entrambe le informazioni sono riportate sulle flight strips), deve costruirsi mentalmente la mappa della situazione corrente del traffico e di conseguenza decidere quando e a chi fornire le autorizzazioni per percorrere le cosiddette "taxiway" (che permettono i movimenti tra le varie zone dell'aeroporto e le piste di atterraggio/decollo), attraversare eventuali incroci con altri raccordi o piste, ed arrivare all'inizio della pista di decollo, minimizzando ovviamente la possibilità di conflitti. Quando il pilota sta per arrivare vicino alla "holding position" (ossia l'inizio della pista di decollo), il pilota contatta il controllore di terra segnalandogli la sua posizione corrente, e a quel punto il controllore di terra gli trasmette la frequenza su cui si dovrà sintonizzare per comunicare con il controllore di torre, in quanto a questo punto il controllo dell'aereo passa di fatto all'altro controllore.

- il *controllore di torre* (o "Tower" controller), si preoccupa di mantenere le separazioni tra i vari aerei, e quindi di allocare l'accesso alla runway e stabilire i tempi di partenza. Egli riceve le strip dal suo collega di terra e, quando riceve dal pilota la richiesta di autorizzazione al decollo egli deve, in funzione del tipo di aereo che è appena partito, di quello che ha appena fatto la richiesta e della sua prevista direzione di decollo, e infine del tipo di aereo che lo dovrebbe seguire subito dopo, calcolare come coprire le separazioni per assicurare che non si verifichino conflitti tra gli aerei che decollano. Anche queste informazioni (tipo degli aerei e rispettivi "cammini di decollo" o SID, ossia rotte prestabilite seguite dagli aerei immediatamente dopo la partenza) sono riportate sulle flight strips. Il

controllore deve predisporre la sequenza di partenza in modo tale da ottimizzare il più possibile l'uso delle piste e dei cammini di decollo, mantenendo allo stesso tempo le separazioni tra aerei "consecutivi", necessarie per annullare gli effetti dei cosidetti "wake vortex", ossia i vortici d'aria provocati dagli aerei in fase di decollo (tali separazioni vengono calcolate *mentalmente* dai controllori).

Ad esempio, possono sorgere dei problemi quando aerei più leggeri ma più lenti sono tra aerei più veloci e più pesanti: ad esempio, un aereo "leggero" che segue uno "pesante" richiede una separazione maggiore e quindi provoca un ritardo maggiore sulla pista rispetto ad un aereo "pesante" che segue un altro aereo "pesante". Inoltre, quando un (lento) aereo turbopropulsore è seguito da un (veloce) jet *sulla stessa SID*, uno spazio sufficiente dovrebbe essere mantenuto tra i due aerei per far si che il secondo non raggiunga il primo: il tempo di attesa viene solitamente riempito dal controllore facendo partire un altro aereo che necessita di una SID differente.

In generale si può notare come in condizione di bassa visibilità (per esempio, per nebbia) l'aeroporto diventa un punto cruciale che spesso limita fortemente la regolarità dei voli. Così per mantenere lo stesso livello di sicurezza i controllori aumentano le distanze tra gli aerei (o chiudono l'aeroporto) a scapito della capacità aeroportuale e quindi della domanda di traffico. Nuovi strumenti, come strumenti di pianificazione o radar più sofisticati, possono permettere ai controllori di operare anche in condizioni non ottimali di visibilità mantenendo lo stesso livello di sicurezza e una sufficiente capacità aeroportuale.

5. Metodo e Risultati

Il processo metodologico proposto parte da un primo modello dei task che fa riferimento alla situazione esistente e descrive come le attività vengono eseguite tra i vari tipi di utenti, tra gli utenti ed il sistema, tra gli utenti e l'ambiente circostante. Dopo vi è una prima proposta di un modello dei task rivisto per poter utilizzare nuovi dispositivi (nel nostro caso l'uso di strumentazione automatica per il supporto delle decisioni e di comunicazioni dati oltre che via microfono).

L'introduzione di nuovi dispositivi di comunicazione in questo tipo di applicazioni ha solitamente tre tipi di effetti:

- cambiamento dell'allocazione dei task tra controllori e macchina (spesso alcuni compiti che venivano fatti manualmente diventano automatici);
- cambiamento di task tra utenti dei vari ruoli coinvolti;
- cambiamento degli oggetti manipolati per eseguire i compiti (vedi ad esempi la possibilità di introdurre strip elettroniche),
- cambiamento delle rappresentazioni fornite dagli oggetti coinvolti nell'applicazione considerata.

Alla prima proposta di nuovo modello per eseguire i task viene applicato un approccio di tipo HAZOP-like [1] per analizzare le possibili conseguenze prodotte sia da erronee interazioni dell'utente con il sistema sia (nel caso di sistemi cooperativi [3]) dell'utente con altri utenti, ottenendo così un "nuovo" modello dei task. In questo tipo di approccio si identificano i task più significativi e si cerca di capire cosa può succedere se vi sono deviazioni inaspettate durante la loro esecuzione (ad esempio se si trasmette un dato sbagliato, o se si trasmette un dato nel momento sbagliato o se non si trasmette affatto un dato che invece è rilevante).

In questo senso uno studio di tipo HAZOP-like rappresenta un vero e proprio punto di collegamento tra la "storia" del sistema (ad esempio si annotano le ragioni di decisioni prese durante lo studio, o si evidenziano particolari meccanismi di protezione che sono già presenti nel sistema) e il "futuro" sviluppo del sistema, ossia ulteriori miglioramenti da introdurre durante le fasi successive del progetto del sistema.

Questa analisi viene fatta non solo in termini di sicurezza ma anche in termini di usabilità e consente di generare un modello dei task "migliorato" da cui si ottiene il primo prototipo di interfaccia utente. Test empirici su tale prototipo eseguiti da una classe rappresentativa di utenti consentono di introdurre ulteriori miglioramenti e di ottenere l'interfaccia utente "finale".

Il modello dei task ottenuto è "migliorato" sotto molteplici punti di vista: ad esempio perchè vengono considerati aspetti che erano stati trascurati nel modello iniziale e/o perchè vengono modificati aspetti che erano stati già considerati. In tutti i casi si ottiene un modello più affidabile del precedente in quanto è stato analizzato in modo sistematico come il sistema affronta possibili situazioni di azzardo.

6. Conclusioni

In questo articolo abbiamo introdotto alcune delle problematiche affrontate nell’ambito del progetto europeo Esprit LTR MEFISTO (http://giove.cnuce.cnr.it/mefisto.html) che mira a sviluppare metodi per la progettazione di applicazioni interattive critiche per la sicurezza integrando aspetti di usabilità e sicurezza.

7. Riferimenti

[1] Burns, D.J. and Pitblado, R.M., A Modified HAZOP Methodology For Safety Critical System Assessment. Directions in Proc. of the Safety-Critical Systems Symposium, Bristol, 1993, Springer-Verlag.

[2] Leveson, N.G., System Safety and Computers, Addison-Wesley Publishing Company, 1995.

[3] Paternò, F., Santoro, C., Tahmassebi, S., Formal Models for Cooperative Tasks: Concepts and an Application for En-Route Air Traffic Control. In Proc. DSV-IS '98, Abingdon, U.K., June 1998.

[4] Reason J., Human Error, Cambridge University Press, UK, 1990.