Modeling, Analyzing, and Mitigating Dissonance between Alerting Systems

Lixia Song and James K. Kuchar

Final Report
NASA NAG2-1425
February 2003

MIT International Center for Air Transportation
Department of Aeronautics & Astronautics
Massachusetts Institute of Technology
Cambridge, MA 02139   USA

MODELING, ANALYZING, AND MITIGATING DISSONANCE BETWEEN ALERTING SYSTEMS

LIXIA SONG AND JAMES K. KUCHAR

Abstract

Alerting systems are becoming pervasive in process operations, which may result in the potential for dissonance or conflict in information from different alerting systems that suggests different threat levels and/or actions to resolve hazards. Little is currently available to help in predicting or solving the dissonance problem. This thesis presents a methodology to model and analyze dissonance between alerting systems, providing both a theoretical foundation for understanding dissonance and a practical basis from which specific problems can be addressed.

A state-space representation of multiple alerting system operation is generalized that can be tailored across a variety of applications. Based on the representation, two major causes of dissonance are identified: logic differences and sensor error. Additionally, several possible types of dissonance are identified.

A mathematical analysis method is developed to identify the conditions for dissonance originating from logic differences. A probabilistic analysis methodology is developed to estimate the probability of dissonance originating from sensor error, and to compare the relative contribution to dissonance of sensor error against the contribution from logic differences. A hybrid model, which describes the dynamic behavior of the process with multiple alerting systems, is developed to identify dangerous dissonance space, from which the process can lead to disaster. Methodologies to avoid or mitigate dissonance are outlined.

Two examples are used to demonstrate the application of the methodology. First, a conceptual In-Trail Spacing example is presented. The methodology is applied to identify the conditions for possible dissonance, to identify relative contribution of logic difference and sensor error, and to identify dangerous dissonance space. Several proposed mitigation methods are demonstrated in this example. In the second example, the methodology is applied to address the dissonance problem between two air traffic alert and avoidance systems: the existing Traffic Alert and Collision Avoidance System (TCAS) vs. the proposed Airborne Conflict Management system (ACM). Conditions on ACM resolution maneuvers are identified to avoid dynamic dissonance between TCAS and ACM.

Also included in this report is an Appendix written by Lee Winder about recent and continuing work on alerting systems design. The application of Markov Decision Process (MDP) theory to complex alerting problems is discussed and illustrated with an abstract example system.

This document is based on the thesis of Lixia Song submitted to the Department of Aeronautics and Astronautics at the Massachusetts Institute of technology in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Estimation and Control.

MIT
ICAT

Modeling, Analyzing, and Mitigating Dissonance between Alerting Systems

Lixia Song and James K. Kuchar

Final Report
NASA NAG2-1425
February 2003

MIT International Center for Air Transportation
Department of Aeronautics & Astronautics
Massachusetts Institute of Technology
Cambridge, MA 02139   USA

Acknowledgements

This work was financially supported by the National Aeronautics and Space Administration under grant NAG2-1425. We would also like to thank Honeywell Lab in Minneapolis for their support and suggestions. The following professors deserve many thanks for their suggestions and contributions: R. John Hansman, Eric Feron, John Deyst, John-Paul Clarke, Kristina Lundqvist, and Dr. Lee Yang.

Table of Contents

List of Figures

List of Tables

Definitions

Alert Stage

A discrete categorization of the level of danger and urgency of the threat according to alerting system.

Dangerous Dissonance Space

A subset of dissonance space from which the process can lead to hazard space, equal to the union of all dangerous dissonance states.

Dangerous Dissonance State

A state within dissonance space from which the process can lead to hazard space.

Dissonance Space

A region in state space where perceived dissonance is present.

False Dissonance

Dissonance triggered by a measured state whose true state is outside dissonance space.

Hazard Alert Stage

A discrete categorization of the level of threat posed by a given hazard under observation by a alerting system.

Indicated Dissonance

A mismatch of information (different alert stages or different resolution commands) between alerting systems.

Missed Dissonance

Dissonance not triggered by a measured state whose true state is inside dissonance space.

Perceived Dissonance:

A situation in which information from two or more alerting systems have content and representations that suggest different timing of alerts and actions to resolve a hazard.

Resolution Command

The type of resolution action to be performed and the magnitude of that maneuver given by alerting system based on the alert stage and other information on the situation.

System Alert Stage

The resultant level of threat posed by all the hazards under observation by a alerting system, equal to the maximum of all individual hazard alert stages.

Acronyms

ACM	Airborne Conflict Management
AILS	Airborne Information for Lateral Spacing parallel approach
ASRS	Aviation Safety and Reporting System
ATC	Air Traffic Controller
CTAS	Center TRACON Automation System
EGPWS	Enhanced Ground proximity Warning System
GPWS	Ground Proximity Warning System
ILS	Instrument Landing System
RA	Resolution Advisories of TCAS
RTCA	Radio Technical Committee on Aeronautics
TCAS	Traffic alert and Collision Avoidance System
TA	Traffic Advisories of TCAS
URET	User Request Evaluation Tool

1. Introduction

1.1 Problem Statement

Automated alerting systems are becoming increasingly pervasive in time-critical and/or safety-critical operations, with applications spanning aerospace vehicles, automobiles, chemical and power control stations, air traffic control, and medical monitoring systems. As these applications are pushed toward higher safety and capability, new alerting systems have been introduced to provide additional protection from hazards. Accordingly, there has generally been an evolutionary, incremental addition of alerting systems to these applications over time. Because it is costly to completely redesign and recertify automation, new alerting systems are typically independent enhancements that do not directly affect the operation of existing subsystems.

The addition of multiple alerting systems to an already complex operation carries several liabilities (Prichett, et al., 2002). First, there is an increase in the amount of information processing required by the human operator, who now must be trained and able to respond rapidly to more information. There is also a potential for simultaneous alerts from the different systems, possibly overloading or confusing the human. This is a classic human factors challenge found in many work environments (Momtahan, et al., 1993; Carrick, 1997). These alerts could also be conflicting in the sense that the information they provide suggests different actions be taken to resolve problems. Figure 1.1, for instance, shows an example conflict between alerting information: system A commands the operator to climb while system B commands a descent. The difference could be due to the use of different sensors or different alerting logic by alerting systems.

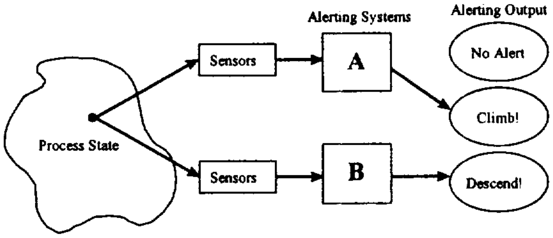


Figure 1.1 Schematic of an Alerting Conflict

In the late 1990s, Pritchett and Hansman explored the concepts of *consonance* and *dissonance* between an alerting system's decisions and a human operator's internal model of a threat situation (Pritchett & Hansman, 1997). Their work and observed incidents in the field have shown that a mismatch or dissonance between the human and automation could lead to undesirable behavior from the human including increased delay in taking action, failure to take action at all, or even implementing an action contrary to the automation's command. These human operator responses may lead the process to an accident, or at least an inefficient operation. In the long run, human operators may distrust the alerting system. One focus of the development of alerting systems should therefore be to ensure that the information that is conveyed, the timing of alerts, and the commands or guidance provided are as much in consonance with the human as possible. But, certainly there may be cases in which dissonance is unavoidable: for example when the human is completely unaware of a threat and does not feel there is a problem when in fact there is. In such cases, it is important to provide corroborating information with the alert so that the human rapidly understands the rationale behind the alerting decision and so comes into consonance with the automation as quickly as possible.

Dissonance is likely to be even more problematic when there are multiple automated systems that are not synchronized. The dissonance between a human command and automation may have a chance to be resolved through communication between the humans. For example, if a pilot receives dissonant commands between an air traffic controller and an on-board alerting system, the dissonance may be resolved through communication between the pilot and the air traffic controller. But if two on-board alerting systems give dissonant commands to the pilot, it is hard to get additional information from the alerting systems to resolve the dissonance. The development of new alerting systems should therefore consider possible dissonance with other alerting systems under development or that already exist. Otherwise, different systems might provide simultaneous but conflicting information which suggest different actions be taken to resolve problems.

1.2 Example Problems

Alerting systems on jet transport aircraft, for example, have become more prevalent and complex over the last several decades. In the era of "steamgauge" aircraft that relied on electromechanical instruments (before the 1980s), nearly all alerting functions on aircraft were used to monitor autoflight controls and internal components such as engines, hydraulics, or electrical systems. One comprehensive study found over 500 different alert displays and functions on the Boeing 747 flight deck (Veitengruber, et al., 1977). Another study also showed a history of exponential growth in the number of alerting functions on board aircraft, as shown in Table 1.1.

Table 1.1 Number of Warnings on Aircraft (Hawkins, 1987)

Airframer	A/c type	No. of Warnings		Airframer	A/c type	No. of Warnings
McDonnall Douglas	DC-8 (1959)	172		Boeing	B707 (1958)	188
	DC-10 (1971)	418			B747 (1970)	455

This trend was mitigated through the introduction of more advanced processing and electronic display technology in the 1980s. This technology allows for multifunction "glass cockpit" displays, reducing the number of separate lights and gauges, and enabling more comprehensive and integrative monitoring of systems, rather than requiring a separate display for each aircraft subsystem.

1.2.1 Dissonance between TCAS and Air Traffic Controller

Since the 1970s, aircraft alerting systems have been increasingly focused on external threats such as terrain, other air traffic, and weather. Several of these external-hazard systems are now being augmented by the addition of newer, more capable alerting systems. In the area of air traffic collision alerting, the Traffic Alert and Collision Avoidance System (TCAS), for example, was mandated for U.S. transport aircraft in 1993. TCAS uses range, range rate, altitude, and altitude rate between two aircraft via transponder messages. Based on this information, TCAS has two alerting functions: Traffic Advisories (TA), which direct the crew's attention to a potential threat, and

Resolution Advisories (RA), which provide vertical collision avoidance commands to the crew.

With the alerting system helping to monitor external threats, cases of dissonance between human and automation have been observed. The mid-air collision between a Russian passenger jet (TU154) and a DHL cargo jet (B757) that occurred on July 2nd, 2002 in Germany, which killed 71 people, exposed a dissonance problem between the TCAS and the air traffic controller. According to the German air accident investigation agency (German BFU Web, 2002), the pilot on the Russian passenger jet received conflicting information from TCAS and the air traffic controller (Figure 1.2).

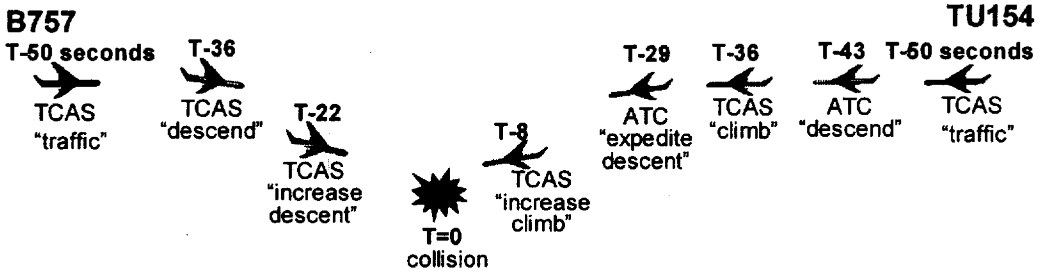


Figure 1.2 Mid-Air Collision on July 2nd in Germany

As we can see from Figure 1.2, the Russian passenger jet got a TCAS TA fifty seconds before the collision, then an Air Traffic Controller (ATC) "descend" command, a TCAS "climb" command, an ATC "expedite descent" command, and a TCAS "increase climb" command, ending in a collision.

Several near-misses have also happened because of the dissonant information provided to the pilot between TCAS and the air traffic controller. For example, on September 23rd, 1999 near Zurich, between aircraft CRX518 and BZH831, the air traffic controller issued CRX518 an instruction to climb, when CRX518 and BZH831 were approximately 10 nm apart on opposite courses (Swiss Aircraft Accident Investigation Bureau, 2001). At the same time, TCAS commanded CRX518 to descend and BZH831 to climb. Despite the measures taken, both by the air traffic controller and the pilot, a dangerous encounter occurred (3 nm horizontal and 700 feet vertical separation). Another near-miss happened On February 26th, 1999 near Lambourne, UK between a Boeing 737 (B737) and a Gulfstream IV (GIV) (UK AAIB Web, 1999). The B737 was turning outbound when the pilot reported that he had TCAS traffic descending. The controller responded by giving an avoiding action descent, but at that time the pilot of the B737 was executing a TCAS climb maneuver. If there were no left turn avoiding maneuver taken by the GIV, the B737 would have passed just behind the GIV. In fact with the maneuvers carried out by each aircraft, the GIV passed by the B737 at a range of 1.3 nm with a 400 feet vertical separation.

1.2.2 Dissonance during Parallel Approach

Recently, additional collision alerting systems have been under development to enhance safety and capability for closely-spaced approaches to parallel runways (Waller & Scanlon, 1996; Kuchar & Carpenter, 1997). Specialized systems are required for parallel approach capability since TCAS was not developed with this type of operation in mind and would require major modifications to work in that environment. Thus, there could soon be two separate traffic collision-warning systems (TCAS plus an alerting system for parallel approaches). Figure 1.3 shows a possible dissonant situation between TCAS and the possible alerting system for closely-spaced runway approaches, such as the Airborne Information for Lateral Spacing parallel approach (AILS) (Waller & Scanlon, 1996).

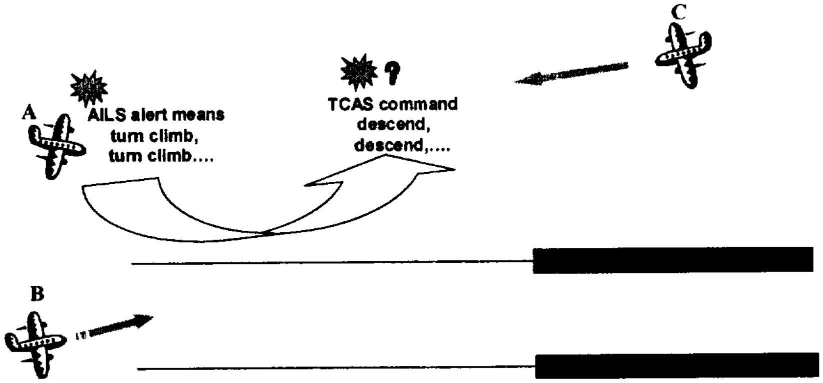


Figure 1.3 Dissonance between AILS and TCAS

Consider the scenario shown in Figure 1.3. Two aircraft, A and B, are executing parallel approaches when the AILS alerts aircraft A and commands a turning-climb, because aircraft B is judged as blundering based on the alerting thresholds of AILS. While aircraft A is taking the evading maneuver (turn-climb), TCAS on aircraft A commands a descent because of aircraft C (elsewhere in the traffic pattern). The confused pilot may not be able to avoid aircraft B or aircraft C.

One means of trying to ensure compatibility of a parallel approach alerting system with TCAS is to modify air traffic control procedures to reduce the likelihood of a simultaneous TCAS alert and parallel traffic alert. That is, giving restrictions to other departure and arrival aircraft when two aircraft are parallel approaching, so that if a blunder happens, the evading trajectory of the other approaching aircraft will not trigger TCAS alerts. However, without knowing when and where the dissonance could happen, it is difficult to implement the proper operational procedure changes. Also changing operational procedures may largely reduce the efficiency of the airspace around the airport.

1.2.3 Dissonance between GPWS and EGPWS

The Ground Proximity Warning System (GPWS) is another alerting system for the external threats. GPWS was mandated on U.S. transport aircraft in the mid-1970s. GPWS uses measurements of the height of the aircraft above terrain to predict whether there is a threat of an accident, and is susceptible to occasional false alarms or late alerts. In 1999, the Enhanced Ground Proximity Warning System (EGPWS) was introduced to provide earlier and more accurate warnings of terrain threats. EGPWS uses an on-board terrain database and includes a graphical display of the terrain field around the aircraft. EGPWS improved several GPWS alert modes, which resulted in about four times fewer false alarms, and improved GPWS operation under temperature variation through replacing barometric altitude with geometric altitude in GPWS envelope modulation tables. Due to cost and certification issues, GPWS has been retained on aircraft and EGPWS has been added as a separate, independent system that does not change the operation of GPWS. The result is that there are now two separate systems, each monitoring terrain threats and each with different alert threshold criteria and displays. It is then possible to have dissonant information provided to a pilot from EGPWS and GPWS for the same terrain situation. For example, EGPWS could command a pilot to climb but GPWS does not rate the terrain as a threat.

This dissonance may be prevented through training. The human operators can be trained to understand that EGPWS and GPWS use different decision-making logic, and that alerts from the two systems may not occur in concert. But pilots may still get confused if EGPWS does not rate the terrain as a threat while GPWS does, since EGPWS is designed to provide an earlier warning of terrain proximity than GPWS. For example, during an approach procedures, GPWS could give a glide slope alert without EGPWS alert, when the runway with an Instrument Landing System (ILS) with a good glide slope is in operation.

1.2.4 Dissonance between TCAS and GPWS

The following actual incident reported to the NASA Aviation Safety and Reporting System (ASRS) describes the problem of dissonance between two alerting systems for different threats (Ververs, et al., 1999).

> Upon departure from LaGuardia on runway 13, Whitestone climb, passing approximately 1000 ft agl, a TCASII traffic advisory (TA) 'traffic, traffic' sounded. At the time we were in instrument meteorological conditions. Immediately after that a resolution advisory (RA), 'reduce vertical speed,' came on with the TCASII target superimposed on our aircraft symbol. We began reducing our climb when an RA 'Descend, Descend' sounded with a vertical speed command of greater than 2000 fpm annunciated. The target was still directly on top of us with its relative altitude displayed. We immediately commenced our descent and exited the clouds at 900 ft agl at which time a GPWS warning came on saying 'too low, terrain.' By this time speed had built up to 280 knots. I then decided it was better to take a chance on hitting another airplane versus the sure thing of colliding with the ground, and directed the first officer to resume the climb and departure while I turned the transponder to TA only. At this time ATC gave us a new heading and altitude and I reported the TCASII RA maneuver. All this time either a TA, RA or GPWS warning had been going on and for a while 'descend, descend' and 'too low, terrain' were being broadcast simultaneously. The cockpit indeed was a cacophony of bells, whistles and flashing lights.

(*abbreviations were spelled out and nonessential text was added for readability*; ASRS ACCESSION NUMBER: 403254)

As described in the above incident, the crew of this flight received valid but opposing alerts from the TCAS and GPWS systems. In this time-critical, stressful situation, the pilots had to decide which alert would take precedence and the appropriate action to take. Each system was designed with its own goals and objectives. Since the systems are separate and independent they do not have a common framework to share intent.

To date, dissonance between TCAS and GPWS has been managed through prioritization. Terrain is given a higher priority than other air traffic, with the rationale that all else being equal, it is less likely that an aircraft would collide with another aircraft than it would hit terrain. Consequently, if TCAS and GPWS are both triggered, the TCAS alert is inhibited or only displayed passively (i.e., without separate attention-getting signals). Prioritization can run into trouble, however, if two alerts are both valid but the operator is only receiving or responding to one. As in the above example, chances to hit the other aircraft still exist when a pilot takes a maneuver according to GPWS.

1.2.5 Dissonance between TCAS and ACM

Systems similar to TCAS but using enhanced sensor information and different, more strategic alerting criteria are currently under development (Kelly, 1999). The Airborne Conflict Management (ACM) is an example. ACM uses an Automatic Dependent Surveillance-Broadcast (ADS-B) data link to enable longer look-ahead than is possible with TCAS. These systems could also result in multiple alerting systems monitoring traffic threats. The different surveillance methods used by TCAS and ACM may result in dissonance. Alerts from ACM should be harmonized with alerts from TCAS and vice-versa. The dissonance between TCAS and ACM is analyzed in more detail in chapter 8 as an example application of this thesis.

1.2.6 Dissonance Appears in Areas Other than Aerospace

Dissonance problems also appear in other areas where automated alerting systems are becoming increasingly pervasive, for example, automobiles, chemical and power control stations, and medical monitoring systems.

Multiple automobile alerting systems are being proposed and developed, with functions including obstacle avoidance, roadway departure and lane-change warnings, and intersection collision warning systems (Najm, et al., 2001). Different design logic of these systems may result in conflicting information for the driver.

In medical applications, increasingly sophisticated medical monitoring systems have been implemented which apply a rules engine to the information base in medical information systems (AMIA Panel Presentation, 2000). Many of these systems have been self-developed at individual institutions and different systems have been developed for different purposes based on different knowledge bases, which may result in dissonant alerts provided to caregivers.

1.3 Objective

To date, the management of potential dissonance between systems has occurred without a structured understanding of the specific issues involved. A potential dissonance situation is usually detected by chance during the individual system performance simulation or field test, and managed through prioritization or adding another filtering system to integrate alerts or procedure. This is not a complete and effective approach. Not all potential dissonance situations can be predicted through simulation or field tests; and without a structured understanding of the specific issues involved in dissonance, it cannot be mitigated effectively. To identify and eliminate all possible sources of confusion resulting from conflicting sensors, database, and algorithms, a system-specific analysis of the potential interactions among alerting systems should be undertaken, starting with early conceptual development and continuing through installation.

The identification of the potential for dissonance and the development of mitigation methods would be greatly facilitated through the application of a coherent, formal model that articulates the design issues. Such a model would have three benefits. First, it would aid in understanding the different types of dissonance that may occur. Second, the model would help in identifying when or where the different types of dissonance could occur in a given operation. Third, the model may be used to design and evaluate mitigation contingencies to prevent or preclude dissonance from occurring.

1.4 Overview of thesis

This thesis focuses on the interaction issues between multiple alerting systems, although a number of issues remain to be resolved regarding general alerting system design and evaluation (e.g., tradeoffs between nuisance alarms and safety). This thesis will not include issues that apply to single alerting systems.

This thesis presents a methodology for modeling and analyzing conflicts between multiple alerting systems. Although the thesis concentrates on applications of dissonance between alerting systems in aerospace, the methodology can easily be applied to other fields as well (ground transportation, medical, etc.). Because of its generalized development, the methodology can also be applied to interaction analysis between non-alerting decision aid functions (e.g., the Center TRACON Automation System (CTAS), User Request Evaluation Tool (URET) for controllers, etc.).

Chapter 2 presents a generic framework that facilitates articulating the specific information elements that are sensed, processed, and displayed by each alerting system, and the interactions between alerting systems. Based on this framework, different types of dissonance are presented. Major causes of dissonance are identified: logic differences and sensor error.

Two major causes of dissonance are analyzed in Chapters 3 and 4. In Chapter 3, a mathematical method is developed to help in identifying when or where the different types of dissonance could occur in a given operation when there are logic differences between two alerting systems. Chapter 4 develops a probabilistic method to analyze the contribution of sensor error to dissonance and compare it with the contribution of logic differences.

In Chapter 5, a hybrid model is developed to fully describe the dynamic behavior of the process incorporating multiple alerting systems, in which the continuous and discrete dynamics coexist and interact with each other. Dangerous dissonance space is identified using backward reachability analysis of the hybrid process. Then Chapter 6 suggests several methods to avoid or mitigate dissonance, especially the dangerous consequence of dissonance identified in Chapter 5.

The methodology is applied in two examples in Chapters 7 and 8. One is the conceptual In-Trail spacing example in Chapter 7, which demonstrates the modeling, analyzing, and mitigating methodologies for dissonance developed from Chapters 2 to 6. Then the methodology is applied to an actual air traffic separation problem in Chapter 8 to identify the conditions for dissonance and suggest ways to mitigate the dissonance.

Finally, Chapter 9 provides a summary and outlines the major contributions of the thesis.

2. Model of Dissonance
Between Multiple Alerting Systems

A significant body of research has focused on the design and use of automation, with the goal of determining how automation should be implemented to work harmoniously with the human operator (Endsley, 1995; Sheridan, 1992; Wickens, 1992; Sarter & Woods, 1995). Endsley, for example, presents arguments that the human's preconceptions and mental models have a direct effect on how automation improves or degrades Situation Awareness (SA) (Endsley, 1995). Automation, then, must be carefully designed and implemented to support the human. If not properly applied, automation can degrade SA by reducing the human's involvement in monitoring and control functions.

We move into the issues specifically related to dissonance between two or more alerting systems. The focus here, then, is on the automation, yet it is critical to remember that ultimately it is the human's understanding and interpretation of the automation's displays that affect whether dissonance has an impact.

2.1 General Alerting Systems Background

All alerting systems generally perform four functions, shown in Figure 2.1: monitoring, situation assessment, attention-getting, and problem resolution. First, on the left of Figure 2.1, information about the process under control and relevant hazard states must be monitored through a set of sensors. Each alerting system may use a different set of sensors, and thus may form a different estimate of what is truly occurring in the process and environment. Based on this observable information, the alerting system assesses and categorizes the situation into one of several threat levels according to the alerting thresholds shown in Figure 2.1. If the threat level is sufficiently high, the human operator is alerted to the problem. This attention-getting function can range from a simple aural or visual cue (e.g., a tone or illuminated light), to displays that indicate the cause for the alert (e.g., a textual or verbal readout such as "Generator Failure"), to displays that also indicate how to correct the problem. The attention-getting signal also provides an indication of the urgency of the problem. This urgency may be conveyed implicitly through the general type of hazard that is being encountered, or it may be more explicitly conveyed by the structure of the alarm signal. For example, a chime sound is often used for low-urgency alerts, whereas a buzzer or wailing alarm may be used in more threatening situations (Boucek, et al., 1981; Berson, et al., 1981).

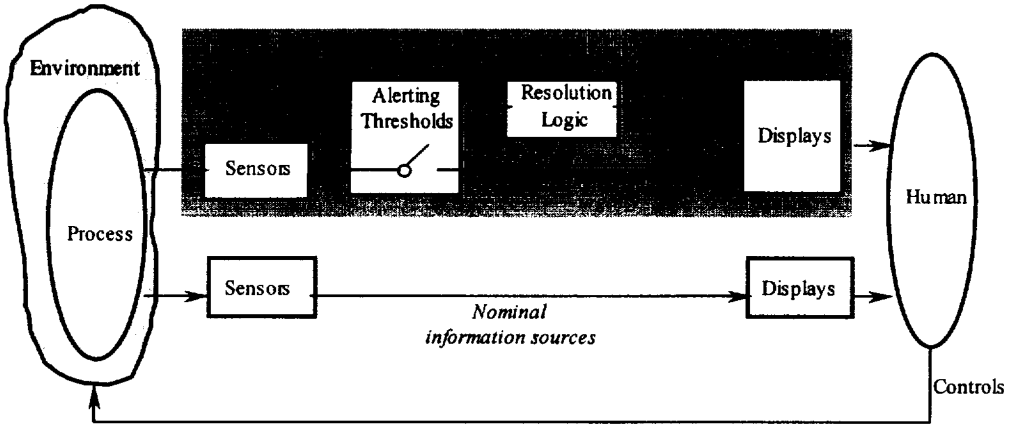


Figure 2.1 Generalized Alerting System Functions

If the alerting system assessed the situation as a threat, resolution commands or guidance may be given based on the resolution logic in Figure 2.1. Problem resolution may also be performed either explicitly or implicitly by the alerting system. In explicit systems, additional command or guidance information is presented to the operator. This may be a verbal message (e.g., "Climb!") and/or may include a visual display indicating the type of action to be taken and the aggressiveness with which that action should be taken. In more advanced systems, continuous guidance may be provided to aid in the resolution action. In implicit systems, the human operator may have a trained response to a particular alert stage, or may just decide at that time what action is most appropriate. Also shown in Figure 2.1 is the nominal information path by which the human operator obtains information about the controlled process and the environment. This information builds the human's internal model of the situation that may conflict with the conditions implied by alerting systems.

2.2 Generalized State-Space Representation of Multiple Alerting Systems

A generic state-space representation of the information flow of two alerting systems in a dynamic environment is shown in Figure 2.2. Additional alerting systems could be incorporated into this representation without loss of generality. To help illustrate the application of the representation to a specific alerting problem, TCAS is used as a case study.

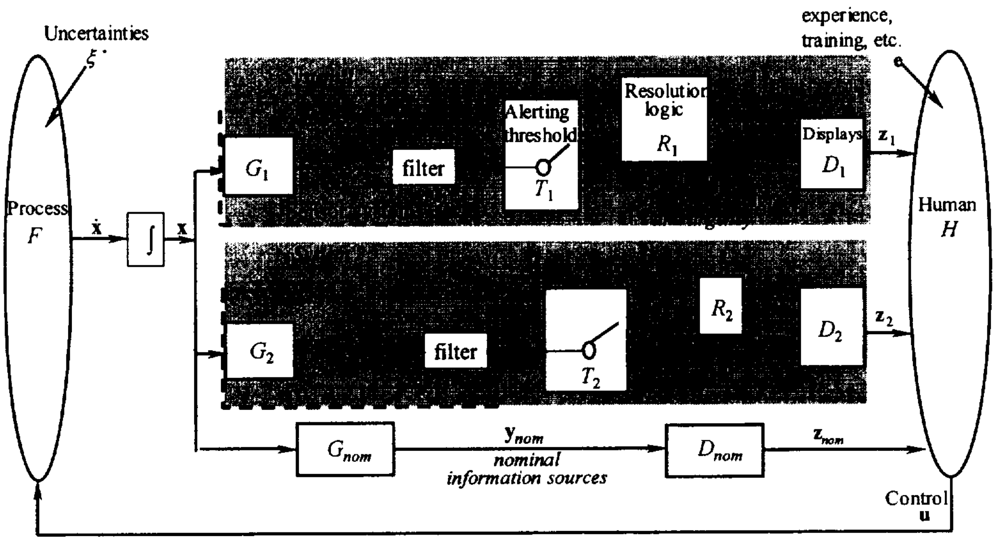


Figure 2.2 Generalized State-Space Representation of Multiple Alerting Systems

From a mathematical standpoint, we will denote **x** as the state vector representing the complete set of physical parameters that describe the dynamics of a hazard situation. In the case of TCAS, for example, **x** represents the three-dimensional position and velocity vectors of each aircraft involved.

On the left of Figure 2.2, the process' dynamics are determined from a generalized function, *F*, of the current state **x**, operator's inputs **u**, and modeling or process dynamics uncertainties, ξ:

$$\dot{\mathbf{x}} = F(\mathbf{x},\mathbf{u},\xi) \tag{2.1}$$

In general, the complete state vector **x** is not available to the alerting system logic, but is observed through a set of sensors. The resulting information that is observable to the alerting system is included in the vector **y**. The alerting systems use possibly different sets of observable states defined by different functions G_i operating on **x**. As shown in Figure 2.2, for the i^{th} alerting system,

$$\mathbf{y}_i = G_i(\mathbf{x}) \tag{2.2}$$

For TCAS, $\mathbf{y}$ is a vector including the range, range rate, relative altitude, and relative altitude rate between two aircraft. Uncertainties in the estimates are modeled through a noise input vector $\mathbf{n}$. We will denote $\hat{\mathbf{y}}$ as the measurement of vector $\mathbf{y}$ corrupted by noise $\mathbf{n}$. TCAS uses an alpha-beta tracker as an estimator to produce a filtered estimate of range and range rate (RTCA, 1983). A more complex nonlinear tracker is used to estimate altitude, and altitude rate. The alpha-beta tracker is a recursive estimator similar to a Kalman Filter but with constant filter gains of α and β.

Alert Stages

Using the information in $\hat{\mathbf{y}}$, each alerting system applies a set of threshold functions or other logic, *T* in Figure 2.2, to map the situation into an alert stage. The alert stage is represented by the vector **a**, and specifies the level of threat according to that alerting system:

$$\mathbf{a}_i = T_i(\hat{\mathbf{y}}_i) \tag{2.3}$$

The logic used by the alerting system to determine the appropriate alert stage and to provide guidance may vary from simple thresholds based on exceeding some fixed value to more complex algorithms involving a number of states. Many alerting systems work with two stages: non-hazardous and hazardous. More complex systems use a series of stages, each corresponding to a higher level of danger and urgency.

Alerting systems may categorize both the status of each individual hazard under observation, and also specify an overall threat level. TCAS does this, for example, by using different graphical icons depicting the threat posed by each nearby aircraft on a traffic display. Additional aural and visual displays are then used to indicate the overall threat level and whether any action is required. Thus, there may be two different types of alert stage, one for each individual hazard and one for the overall system. The *hazard alert stage* is defined as a discrete categorization of the level of threat posed by a given hazard under observation by a system. The *system alert stage* is the resultant overall level of threat posed by all the hazards under observation by that system. In TCAS, the system alert stage is equal to the maximum of all individual hazard alert stages. That is, the system as a whole takes the worst-case threat and uses its threat level. It could be desirable in other applications; however, to use a different method of translating hazard alert stages into system alert stages.

With TCAS, there are four *hazard alert stages*:

Stage 0 = No threat. The other aircraft is denoted by a hollow white diamond on the display.

Stage 1 = Proximate traffic. The other aircraft is shown as a filled white diamond on the display.

Stage 2 = Caution. The other aircraft is shown as a solid yellow circle.

Stage 3 = Warning. The other aircraft is shown as a solid red square.

There are three corresponding *system alert stages* for TCAS:

Stage 0 = No threat. No additional information is provided.

Stage 1 = Traffic Advisory (TA). A Master Caution light is illuminated in amber and an aural "Traffic, Traffic" alert is issued in the cockpit. Stage 1 is active if there is a caution hazard stage active but no active warning hazard stages.

Stage 2 = Resolution Advisory (RA). A Master Warning light is illuminated in red, an aural resolution command is issued (such as "Climb! Climb!") and the required climb angle or climb rate is shown on a cockpit display. Stage 2 is active if any hazard is in the warning stage.

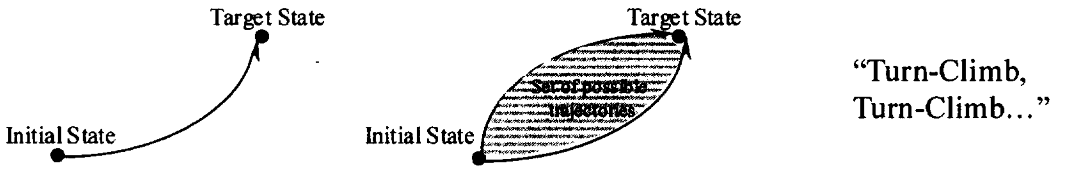
Resolution Commands

Based on the alert stage and on the other information on the situation, the alerting system may produce resolution information, **c** in Figure 2.2, according to the resolution logic *R* in Figure 2.2:

$$\mathbf{c}_i = R_i(\hat{\mathbf{y}}_i, \mathbf{a}_i) \tag{2.4}$$

The vector **c** includes the type of resolution action to be performed (e.g., turn or climb) and the magnitude of that maneuver. There are a variety of forms of resolution commands, depending on the complexity of the maneuver to be performed.

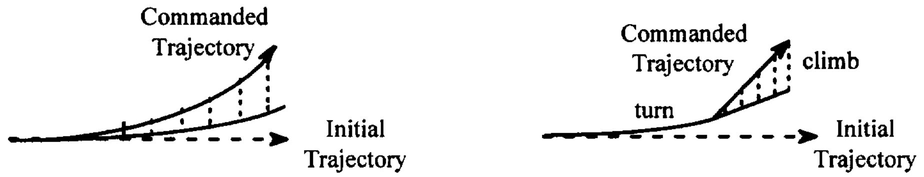
Figure 2.3 shows three different possible styles for the same general command in which a turning-climb maneuver is desired. Figure 2.3a represents a case in which a specific target state is conveyed along with a single, specific trajectory to follow to achieve that target state. In Figure 2.3b, a target state is specified, but the means to achieve that state is not. Finally, Figure 2.3c shows a verbal command; the target state is not given explicitly. Which command should be used in a given situation depends on the degree to which the automation can correctly model and predict the appropriate response. In poorly structured problems, with many uncertainties, the command without target or guidance may be the most reasonable as it allows the human to bring to bear his or her intuition and other information to solve the problem. In well-structured problems, however, a command with target and/or guidance may facilitate the human in implementing the most effective response.



(a) Target state with guidance (b) Target state without guidance (c) Guidance without target

Figure 2.3 Different Command Styles

Additionally, a complex command can be interpreted as either a simultaneous or sequential process. Figure 2.4 shows two different interpretations with "turn climb" as the example. Figure 2.4a describes a simultaneous turning-climb path, while Figure 2.4b shows a sequential case: first turn, then climb.



(a) Turn-climb simultaneously (b) Turn and climb sequentially

Figure 2.4 Command Sequencing

Given all the possible combinations of alert stages and command types, it is clear that there is a rich design space for alerting systems. As a consequence, it is possible (and even probable) that two different alerting systems will apply different alert stage or command definitions to a similar problem. This may lead to indicated dissonance as is discussed in a later section.

Complete Set of Transmitted Information

Referring back to Figure 2.2, **z** is the vector of complete information displayed to the human operator by the alerting system. In general, **z** includes signals designed to attract the operator's attention, the alert stage, and information to resolve the situation. The function D describes the display mapping from the state estimates available to the alerting system ($\hat{\mathbf{y}}$) to the information provided to the human operator (**z**) based on the alert stage (**a**) and resolution information (**c**):

$$\mathbf{z}_i = D_i(\hat{\mathbf{y}}_i, \mathbf{a}_i, \mathbf{c}_i) \qquad (2.4)$$

For TCAS, the information in **z** includes a traffic display in the cockpit, aural messages, lights, and any resolution command and guidance information.

In addition to the alerting systems, there may be other, nominal information sources that provide information to the operator. This information is included in the vector $\mathbf{y}_{nom}$, which is then modified by the nominal displays D_{nom} as shown on the bottom in Figure 2.2. Cockpit instruments, air traffic control communications, views through the windscreen, vestibular inputs, and aeronautical charts are examples of nominal information sources for a pilot. The operator is also affected by other factors such as the pilot's internal model of the situation, knowledge of the alerting system's role, prior training, fatigue, and previous experience. Past exposure to false alarms, for instance, has been observed to be a factor in delaying responses to alerts (DeCelles, 1992). This modifying information is included in the vector **e** in Figure 2.2. The function H on the right in Figure 2.2 then maps the observable states (via all the alerting systems and nominal information sources) to the control inputs **u**. That is,

$$\mathbf{u} = H(\mathbf{z}_{nom}, \mathbf{e}, \mathbf{z}_1, \mathbf{z}_2) \qquad (2.5)$$

Ultimately, it is how the inputs to the pilot (as contained in $\mathbf{z}_{nom}$, $\mathbf{z}_1$, $\mathbf{z}_2$, and **e**) are used to develop a control strategy that determines whether there is a perceived dissonance between the information elements being used. In this context, Pritchett and Hansman's work examined dissonance between $\mathbf{z}_1$ for a single alerting system and the nominal information provided to the human in $\mathbf{z}_{nom}$. Here, we focus on dissonance across the information provided by two different alerting systems, as contained in $\mathbf{z}_1$ and $\mathbf{z}_2$.

2.3 Multiple Alerting Systems Dissonance

Having introduced a general state-space representation for multiple alerting systems, it is now possible to more formally state the types of dissonance that may occur. Dissonance occurs when the alerting systems' states have information content and representations that explicitly suggest different timing of alerts and actions to resolve the hazard (Pritchett & Hansman, 1997). There are two main types of dissonance, indicated and perceived dissonance which we defined and discussed in the next two sections.

2.3.1 Indicated Dissonance

At a high level, all alerting systems can be thought of as mapping a set of estimated states of a controlled process into discrete alert stages and discrete or continuous hazard resolution commands. Indicated dissonance is a mismatch of information (different alert stages or different resolution commands) between alerting systems.

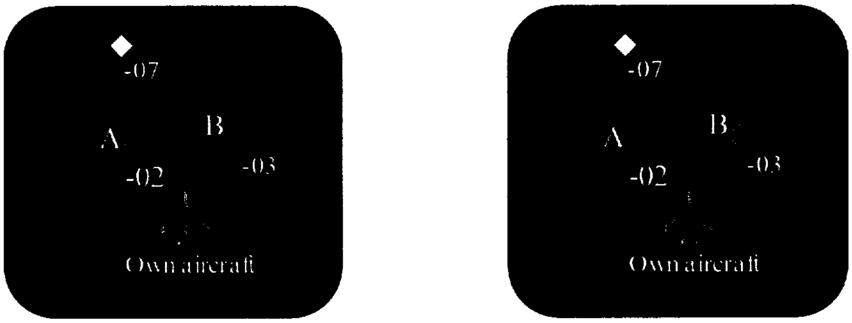
Table 2.1 provides a listing of different forms of indicated dissonance. Each row in Table 2.1 corresponds to a type of indicated dissonance with certain properties. The right side of the table provides an example situation with two alerting systems in which that category of indicated dissonance is present. For example, having one system command "climb" while a second system commanded "descend" would be a resolution polarity conflict. Each of these forms of indicated dissonance is discussed in more detail below.

Table 2.1 Alerting System Indicated Dissonance Types

		Example Dissonant Situation	
Indicated Dissonance Type		*System 1*	*System 2*
Alert Stage	system alert stage	no threat	warning
	hazard alert stage	aircraft A is a threat	aircraft B is a threat
Resolution	dimension	turn	climb
	polarity	climb	descend
	magnitude	turn 5°	turn 30°

As we stated in Figure 2.2, vector **z** includes the signals designed to attract the operator's attention, the alert stage, and the information to resolve the situation. So mathematically, when $\mathbf{z}_1 \neq \mathbf{z}_2$ at a given time for two alerting systems, indicated dissonance may exist. Breaking **z** into its components, first consider indicated alert stage dissonance. Differences in system alert stage can cause indicated dissonance (first row of Table 2.1). For example, EGPWS and GPWS are both alerting systems for terrain. EGPWS is designed to provide an earlier warning of terrain proximity than GPWS. So, usually the alert stage from EGPWS is at a higher level than that from GPWS. There is indicated dissonance since two systems are in different alert stages.

Another type of indicated dissonance can occur when there is a difference in the hazard alert stage for a given threat, even if the system alert stages are consistent (second row of Table 2.1). This could happen, for example, in a case with two traffic alerting systems monitoring two different aircraft A and B. If system 1 rates aircraft A as a low threat (circle) and aircraft B as a high threat (square) while system 2 does the opposite (Figure 2.5), then both systems may agree with the same high-threat system alert stage, but the underlying hazard alert stages for each threat are different. The operator then may distrust one or both systems since they are disagreeing on the cause for the system alert stage.



System 1

System 2

Figure 2.5 Indicated Dissonance Because of Different Hazard Alert Stages

Indicated dissonance can also occur due to the resolution information contained in **z**. Recalling Figures 2.3 and 2.4, the resolution information can be thought of as trajectories of varying levels of abstraction that are intended to direct the human operator to a safe target state. If two trajectories are in different dimensions, then there is indicated dissonance (e.g., a case where system 1 commands a change in altitude but system 2 commands a change in heading). If two commands are in the same dimension, then dissonance may still be indicated due to different polarities or magnitudes of the commands. If two systems are both commanding a change in altitude, but system 1 commands a climb and system 2 commands a descent, there is clearly indicated dissonance. Or, if system 1 commands a much stronger climb than system 2, there is indicated dissonance.

2.3.2 Perceived Dissonance

The mismatch of information between alerting systems may not be aware to be dissonant by the human operator. It really depends on the human to decide how difference between the information conveyed to the human ultimately translates into dissonance. We define perceived dissonance as a situation in which information from two or more alerting systems have content or representations that suggest different timing of alerts and actions to resolve a hazard.

The indicated dissonance may not perceived as dissonance if the human operator knows why dissonance is indicated. In the case of GPWS and EGPWS, if EGPWS alert without GPWS alert, that may not perceived as dissonance if the pilot understand the rationale behind the alerting decision. And if GPWS is at a higher alert stage than EGPWS, there may perceived as dissonance even if the pilot has been trained to understand the rationale behind the alerting decision, because the pilot may not understand why EGPWS does not rate the terrain as a threat while GPWS does.

Differences in system alert stage can be present without causing perceived dissonance if the two alerting systems have different roles. For example, EGPWS is designed to provide an warning of terrain and TCAS is designed for other traffic. There is no perceived dissonance if TCAS gives an alert while GPWS is silent, although there is indicated dissonance since two systems are in different alert stages. It could still have perceived dissonance if both TCAS and GPWS alert but TCAS commands to descend and GPWS commands to climb.

Given the wide variety of commands that can be issued as illustrated in Figures 2.3 and 2.4, there may be subtleties in the commands that affect whether certain differences are perceived to be dissonant or not. The general concept, however, is that the resolution trajectories implied by the command (whether implicit or explicit) should not be disjoint; otherwise, dissonance is likely to be perceived. That is, perceived command dissonance could occur if the intersection between the allowed action spaces of two alerting systems is empty. For example, in Figure 2.6 (a), system 1 commands a climb, which assumes that the pilot would follow a 0.25g pull-up to the commanded pitch attitude after a five second reaction time, so the allowed action space is the gray area in y-z space; system 2 commands a right turn, which implies that the pilot would take 5° bank angle to the commanded heading after a five second reaction time, thus the allowed action space of this command is the gray area in x-y space. The empty intersection of the two allowed action space means dissonance. Different human operators may have different interpretations of system commands, though. For example, the human operator may interpret the allowed action space of the climb or turn command as some subsets of x-y-z three-dimensional space (Figure 2.6 (b)). Then the intersection between the allowed action spaces of two alerting systems is not empty. Thus, the human operator may not think there is dissonance if one system commands a climb but the other commands a turn.

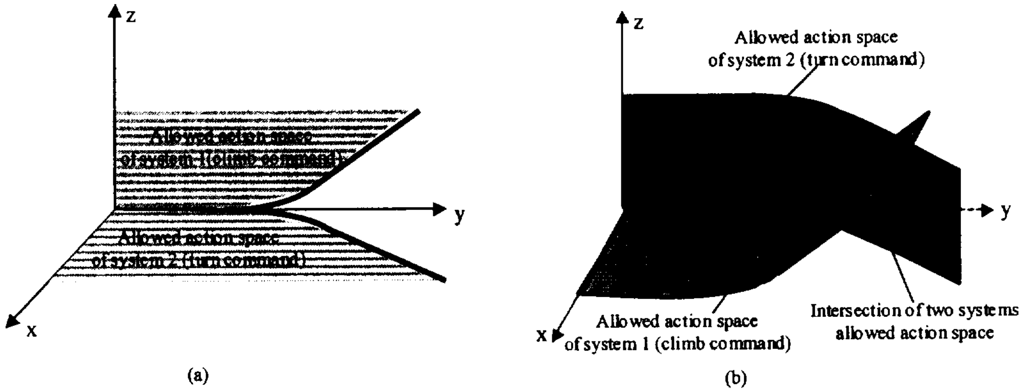

z
Allowed action space
of system 1 (climb command)
y
Allowed action space
of system 2 (turn command)
x
(a)
z
Allowed action space
of system 2 (turn command)
y
Allowed action space
of system 1 (climb command)
x
Intersection of two systems
allowed action space
(b)

Figure 2.6 Perceived Command Dissonance

In some cases, the indicated consonance may still be perceived as dissonance, with the human operator being affected by many other factors, for example, the dynamics of the process, the nominal information, the human mental model, etc. Consider two collision-alerting systems, where one system initially indicates no threat while the second system indicates a high degree of danger and a warning is issued (Figure 2.7). However, if the first system upgrades the alert stage to a caution while the second system downgrades the alert stage, also to a caution, perceived dissonance exists because of the effect of process dynamics. Even though the two systems now agree about the proper alert stage, there is no indicated dissonance, the human may be uncertain as to whether the situation is improving or getting worse due to the perceived dissonance.

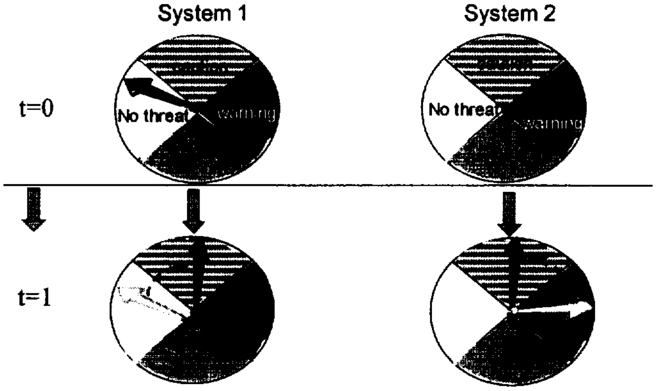


Figure 2.7 Example Perceived Dissonance Due to Process Dynamics (1)

Another example of perceived dissonance due to process dynamics is shown in Figure 2.8, where the process state is jumping between two alerting systems' alert spaces. As shown in Figure 2.8, the process state enters alert space of system 1, system 1 gives some commands to avoid hazard 1; just after the alert goes off, the process enters the alert space of system 2, which triggers system 2 alert and command to take opposite maneuver given by system 1; and the switch goes on and on. If the switches happen rapidly, dissonance may be perceived, and the operator may distrust both systems and try to get out of the oscillate situation with some other maneuvers.

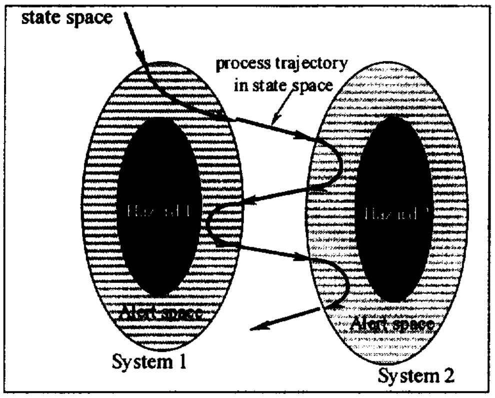


Figure 2.8 Example Perceived Dissonance Due to Process Dynamics (2)

One critical consideration of perceived dissonance due to process dynamics is that its impact may depend on how rapidly the changes in alert information occur. Recall the example above where one system initially indicated no threat and a second system indicated a high degree of danger. If both systems change to a moderate-caution level simultaneously, it is likely there would be a stronger perceived dissonance than if one system changed to caution followed by a significant delay before the second system also indicated caution.

2.3.3 Major Causes of Indicated Dissonance

To be able to deal with dissonance schematically, we need to identify when and where dissonance could happen, that is, the major causes and conditions for dissonance. Certainly, the perceived dissonance is the important one. However, most perceived dissonance are caused by indicated dissonance or somehow related to indicated dissonance. Thus, it's important to identify the causes of indicated dissonance. Based on the general state-space representation of multiple alerting systems, two major causes of indicated dissonance can be identified: logic differences and sensor error.

Alerting systems map a set of measured or estimated states of a controlled process into discrete alert stages and discrete or continuous hazard resolution commands. So, if there is indicated dissonance between alert stages or resolution commands (output $\mathbf{a}_i$ or $\mathbf{c}_i$) between two alerting systems, it could be because of (1) a difference in alerting thresholds or resolution logic (mapping T_i or R_i) or (2) a difference in measured states (input $\hat{\mathbf{y}}_i$) between the two alerting systems (Figure 2.9).

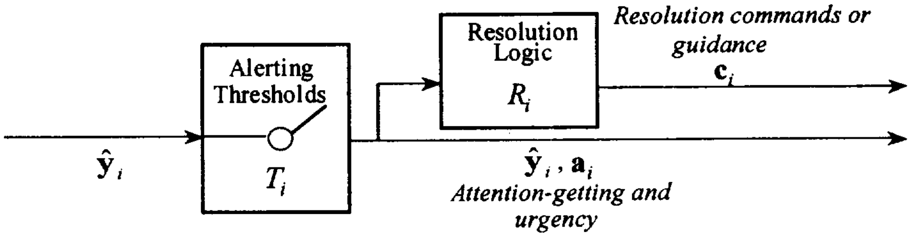

Resolution Logic
R_i
Resolution commands or guidance
$\mathbf{c}_i$
Alerting Thresholds
T_i
$\hat{\mathbf{y}}_i$
$\hat{\mathbf{y}}_i$, $\mathbf{a}_i$
Attention-getting and urgency

Figure 2.9 Mapping of Alerting System

Sensor systems, corrupted by noise $\mathbf{n}$, map the observable states $\mathbf{y}$ into the measured states $\hat{\mathbf{y}}$ (Figure 2.10). Thus, the difference between the measured states could be because of a difference in sensor error or a difference in the sensor coverage, that is, the types of observable states between the two alerting systems.

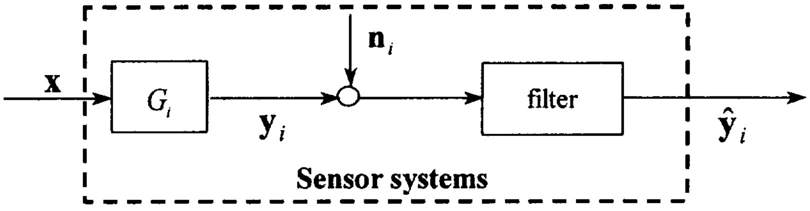


Figure 2.10 Mapping of Sensor

In next two chapters, mathematical methods are developed to identify the conditions for dissonance originating from two major factors: (1) the alerting thresholds or logic differences, and (2) sensor error. Since the different types of observable states will result in different alerting thresholds or logic, these two factors cover all possible causes of indicated dissonance.

It is also important to identify how the indicated dissonance would be perceived as dissonance by the human operator. In this thesis, we are not focusing on the human factor issues or the human operator's mental model to analyze other factors which will cause perceived dissonance. However, the methodology developed in the following chapters can be applied to mathematically represent the conditions for perceived dissonance, as long as some subsets of the state-space are examined to have perceived dissonance. Then the probabilistic method developed in Chapter 4 can be applied to analyze the contribution of sensor error to the perceived dissonance, the hybrid model developed in Chapter 5 can be applied to identify the dangerous consequence of perceived dissonance, and the methods outlined in Chapter 6 can be applied to avoid or mitigate perceived dissonance.

2.4 Summary

In this chapter, a state-space representation of multiple alerting systems was generalized, which facilitates articulating the specific information elements that are sensed, processed, and displayed by each alerting system, and the interactions between alerting systems. The representation was used to analyze different types of dissonance and identify the major causes of indicated dissonance.

Different types of indicated dissonance were identified, including how the indicated dissonance is connected to differences in alert stage or resolution command information. Major causes of indicated dissonance were identified to help in identifying conditions for dissonance in the following chapters.

Since the methodologies developed in the following chapters can be applied to both indicated and perceived dissonance, "dissonance" is used to indicate both indicated and perceived dissonance in the rest of the thesis.

3. Dissonance Originating from Logic Differences

The preceding chapter developed a generalized state-space representation of multiple alerting systems to classify different types of dissonance. An additional step is to formulate a means of identifying how these dissonances originate, that is, the conditions for dissonance. By exposing those situations that lead to dissonance, the system design can be modified, operations can be changed, or the operators can be trained to work around the dissonance.

As identified in Chapter 2, one of the major causes of dissonance is a logic difference between two systems. When two systems are designed to protect against different hazards or when different time scales are used by two systems for the same hazard, threshold functions T_i and resolution logic R_i as we defined in Chapter 2 are usually different in order to satisfy different objectives. Also, different systems may have different observable information. Thus, two systems may be in different alert stages or provide different resolution advisories for the same process state. In this chapter, we develop ways to identify the conditions in which the alert stages or resolution advisories produce dissonance.

3.1 Formal Description of Threshold Functions

To expose those conditions where dissonance may occur, we begin by examining the state space of the alerting system and observing when alerts are issued. The threshold functions for each alerting system, T_1 and T_2, map a given state of the process into a corresponding alert stage. These threshold functions are typically defined by a set of predicates (or inequality statements) based on certain parameter values. Each predicate evaluates to either true or false. One example predicate for collision alerting might be: "if the time to impact is less than p seconds, then use alert stage 1", where p is some parameter value. In general, there may be a set of such comparisons made between the states in y and a set of threshold parameters. To begin, we assume the alerting system uses the exact observable states, that is, no sensor error is considered.

Let the i^{th} alerting system have a number of such predicates where the j^{th} predicate is denoted f_{ij}. Each predicate represents a boundary that divides the state space into a subset. Inside the subset, the predicate is true; outside, the predicate is false. Combinations of these subsets then form the alert stage space within the universe of the state space, **U**. Each resulting subset is denoted A_{ik} for the k^{th} alert stage of system i (Figure 3.1). It is then possible to map out what states in the space of **y** lead to different alert stages. For example, in Figure 3.1, alerting system 1 has two alert stages. A_{11} represents the set of states in which system 1 is in alert stage 1 and A_{12} represnets alert stage 2. As shown, A_{11} is active when predicate f_{11} or f_{12} is true but f_{13} is false; and A_{12} is active when predicate f_{13} is true.

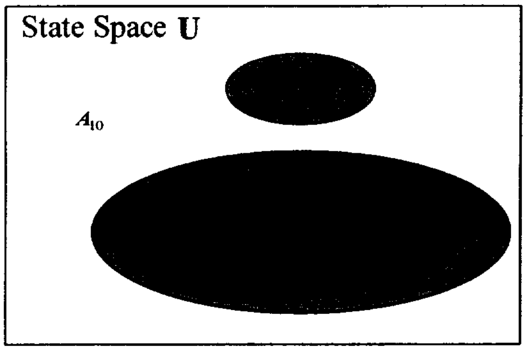


Figure 3.1 Example Predicates and Alert Stages

Thus, the threshold functions of an alerting system can be formally described by their corresponding predicates. For example, the threshold function of system 1 in Figure 3.1 can be formally described as,

$$\begin{cases} f_{11} : F_{11}(\mathbf{y}, \mathbf{p}_{11}) < 0 \\ f_{12} : F_{12}(\mathbf{y}, \mathbf{p}_{12}) < 0 \\ f_{13} : F_{13}(\mathbf{y}, \mathbf{p}_{13}) < 0 \\ A_{12} = f_{13} \\ A_{11} = \bar{f}_{13} \cap (f_{11} \cup f_{12}) \\ A_{10} = U - A_{11} - A_{12} \end{cases} \tag{3.1}$$

where the jth predicate f_{1j} is described as an inequality statement of the observable state y and a set of parameters $\mathbf{p}_{1j}$; and alert stages are the subsets of the whole state space described by the combinations of true or false of predicates. For example, when f_{13} is false and f_{11} or f_{12} is true, the given state **y** is in alert stage 1 of alerting system 1.

For some alerting systems, when system is in high alert stage, there may have different rules that decide different resolution command suggested to the human operator. These rules can also be represented as predicates, then the alert stage can be further separated into subsets. In each of these subsets, the alerting system would be in the same alert stage but with different commands. For example, when the system described in Figure 3.1 is in alert stage 2, if predicates f_{14} is true, then the system will command to climb, otherwise, it will command to descend. Then the subset A_{12} can be fatherly separated into two subsets A_{121} and A_{122} (Figure 3.2). In subset A_{121}, the system will command to climb, and in subset A_{122}, the system will command to descend.

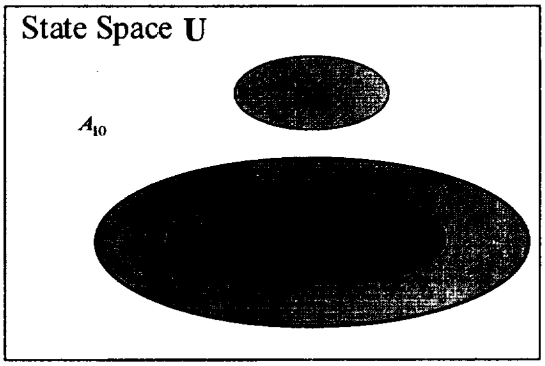


Figure 3.2 Example Subsets of Different Commands

The threshold function of system 1 in Figure 3.2 can be formally described as,

$$\begin{cases} f_{11} : F_{11}(\mathbf{y},\mathbf{p}_{11}) < 0 \\ f_{12} : F_{12}(\mathbf{y},\mathbf{p}_{12}) < 0 \\ f_{13} : F_{13}(\mathbf{y},\mathbf{p}_{13}) < 0 \\ f_{14} : F_{14}(\mathbf{y},\mathbf{p}_{14}) < 0 \\ A_{121} = f_{13} \cap f_{14} \\ A_{122} = f_{13} \cap \bar{f}_{14} \\ A_{11} = \bar{f}_{13} \cap (f_{11} \cup f_{12}) \\ A_{10} = U - A_{11} - A_{12} \end{cases} \tag{3.2}$$

3.2 Identification of Conditions to Dissonance

When the two systems operate simultaneously, the combinations of alert stages lead to behavior that may result in dissonance. The combinations of the alert stages of the two systems are given by the intersections of the A_{ik} sets. These intersection sets are denoted S_{mn} where m is the alert stage from system 1 and n is the alert stage from system 2:

$$S_{mn} = A_{1m} \cap A_{2n} \tag{3.3}$$

For example, if alerting system 2 can be represented in the same state space as system 1 (Figure 3.3), and the threshold function of alerting system 2 can be formally described as,

$$\begin{cases} f_{21} : F_{21}(\mathbf{y}, \mathbf{p}_{21}) < 0 \\ A_{21} = f_{21} \\ A_{20} = U - A_{21} \end{cases} \tag{3.4}$$

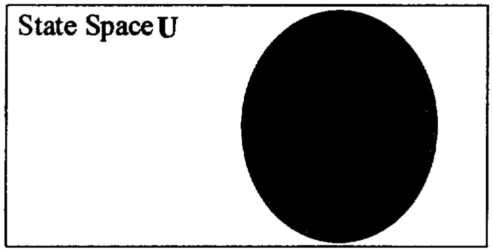


Figure 3.3 Predicates and Alert Stages of System 2

Then there are five combinations of the alert stages of the two alerting systems (Figure 3.4). S_{11}, for example, in Figure 3.4 represents the set of states where both systems are in alert stage 1.

Sets S_{mn} can be examined to decide if there is perceived dissonance, the dissonance space is the subset in which dissonance would be perceived. Then, the conditions for dissonance are the conditions for those sets S_{mn}. In this example, since the subset A_{12} has been further separated into two subsets A_{121} and $A_{122,}$ we need to further examine which part of S_{21} would be perceived as dissonance. Assume that system 2 will command to descend when it is in alert stage 1, then the part of S_{21} (S_{211}) in which system

1 command to climb and system 2 command to descend is the dissonance space. Then the condition for this dissonance space is

$$S_{211} = A_{121} \cap A_{21} = f_{13} \cap f_{14} \cap f_{21} \qquad (3.5)$$

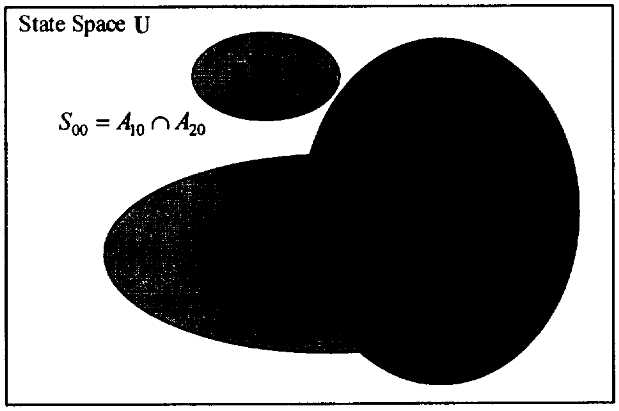


Figure 3.4 Example Combinations of Alert Stages

It is worth mentioning that the observable states are usually different for different alerting systems. Thus, the threshold functions for different alerting systems are usually described in different state spaces. To be able to identify the conditions for dissonance, we need to map the threshold functions of the different alerting systems into the same state space. For the example talked above, if the original threshold functions of alerting system 2 are described in state space $\mathbf{y}'$, that is, the predicate f_{21} is originally described as

$$F'_{21}(\mathbf{y}', \mathbf{p}'_{21}) < 0 \qquad (3.5)$$

it needs to be mapped into

$$F_{21}(\mathbf{y}, \mathbf{p}_{21}) < 0 \qquad (3.6)$$

which is in the same state space as alerting system 1, through state space transformation. And if two state spaces are orthogonal, then the union of state spaces are needed to identify the conditions for dissonance. For example, if the threshold functions of alerting system 1 are described in state space $\mathbf{y}_1$ while system 2 in state space $\mathbf{y}_2$, and $\mathbf{y}_1$ and $\mathbf{y}_2$ are orthogonal, then the formal descriptions of both systems' threshold functions are needed to be presented in state space $\mathbf{y} = \mathbf{y}_1 + \mathbf{y}_2$.

3.3 Dissonance Analysis Due to Process Dynamics

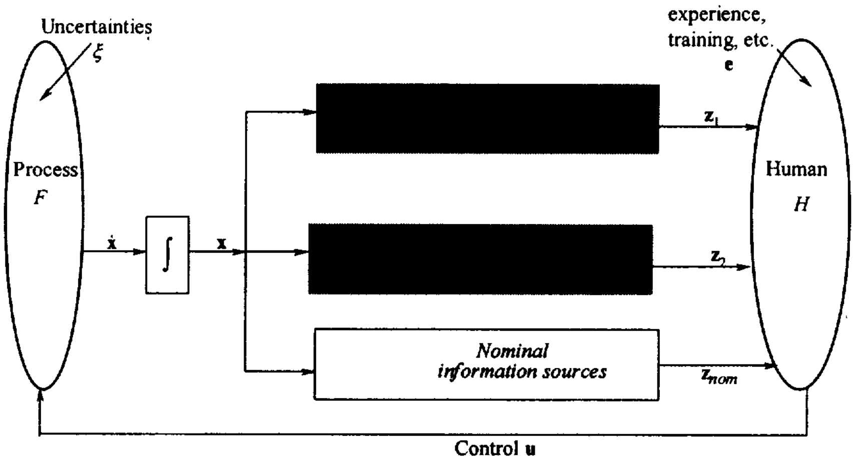


Figure 3.5 Closed Loop for System Dynamics

The state space map described above can also be used to examine time-varying behavior leading to perceived dissonance. By injecting the system dynamics from the functions F (where $\dot{\mathbf{x}} = F(\mathbf{x},\mathbf{u},\xi)$) and H (where $\mathbf{u} = H(\mathbf{z}_{nom},\mathbf{e},\mathbf{z}_1,\mathbf{z}_2)$) (Figure 3.5), complete state trajectories can be developed in the state space. Then, the progression of the process state from one alerting region to another can be predicted. This can highlight dissonance that may perceived when one system upgrades the alert stage while a second system downgrades it (e.g., transitions from S_{10} to S_{01}).

Figure 3.6 shows a example trajectory in the state space shown in Figure 3.4 with two alerting systems.

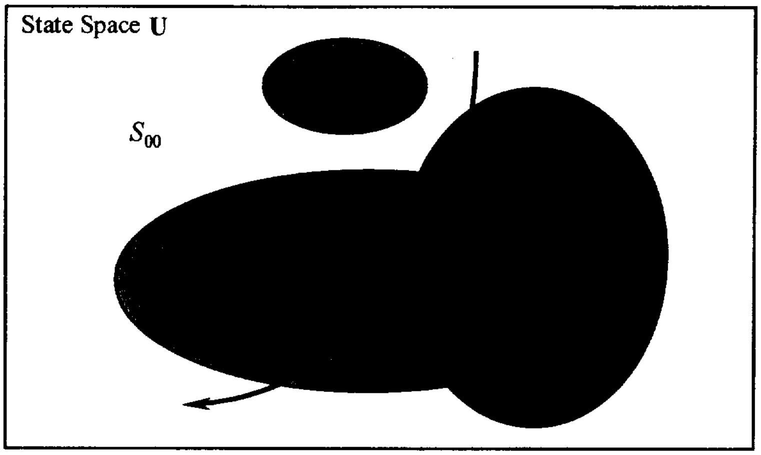


Figure 3.6 Example Analysis of Dissonance Due to Process Dynamics

As we can see from Figure 3.6, following the trajectory shown, the process will first trigger a system 2 alert, then a system 1 alert, and as the process leaves the alert space of system 2, system 1 is further upgrading its alert stage. The different trends of alert information from two systems may be perceived as dissonance due to process dynamics.

When examining perceived dissonance due to process dynamics, it is important to also consider the timescales over which the alerting systems transition from one alert stage or resolution command to another. Whether dissonance would be perceived when two systems' alert information change in opposite directions depends on how rapidly this change occurs relative to the timescales of the system dynamics and the human's cognition. It is unlikely that two systems would change alert stages in opposition at precisely the same moment. Rather, there would probably be some time lag between these changes. A short lag may result in perceived dissonance, while a longer lag may not result in any dissonance. Further work in this area of human factors is needed to determine how rapidly systems must change for dissonance to be perceived.

The trajectory shown in Figure 3.6 assumes that the human operator does not respond to the alerting systems alerts, thus, there is no discrete change in the continuous dynamics of the process. In Chapter 5, the interaction between the continuous dynamics and the discrete state changes will be formally modeled. Then, the dangerous dissonance space can be identified, and the dangerous consequences of dissonance can be eliminated.

3.4 Summary

In this chapter, we presented a mathematical analysis method to identify the conditions for dissonance originating from logic differences, through formally describing the threshold functions of alerting systems.

Perceived dissonance due to process dynamics can also be analyzed by introducing the trajectory of the process into the state space representation of the threshold functions.

4. Dissonance Originating from Sensor Error

When two alerting systems use different sensors to monitor the process, even if they have the same alerting threshold function or resolution logic, they may be in different alert stages due to sensor error. In this chapter, an analysis of how sensor error affects dissonance is provided. A probabilistic analysis methodology has been developed to compare the contribution of sensor error to dissonance against the contribution of logic differences. In this thesis, we focused on the sensor error, but not measurement update rate issues, though one extension to the method is provided for cases where sensors have different discrete update rates.

4.1 Analysis of Dissonance Originating from Sensor Error

Given a true state that is outside the dissonance space defined by a logic difference, the measurement of that state given by two systems could still trigger dissonance with some probability because of measurement error.

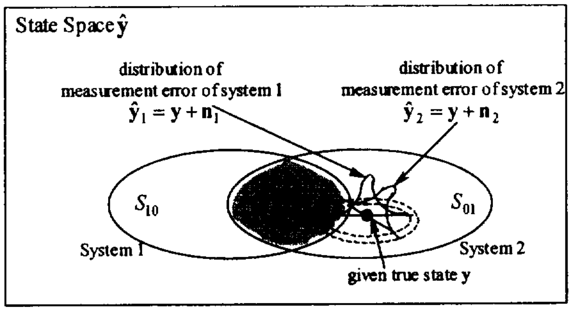

State Space $\hat{\mathbf{y}}$
distribution of measurement error of system 1
$\hat{\mathbf{y}}_1 = \mathbf{y} + \mathbf{n}_1$
distribution of measurement error of system 2
$\hat{\mathbf{y}}_2 = \mathbf{y} + \mathbf{n}_2$
S_{10}
S_{01}
System 1
System 2
given true state y

Figure 4.1 The Measurement of a True State

For example, in Figure 4.1, suppose the dissonance space is S_{11}, where both alerting systems alert but present dissonant resolution advisories. The given true state **y** is in space S_{01}, which is outside the dissonance space S_{11}. With sensor error, the measurement obtained by system 1 may still trigger an alert placing $\hat{\mathbf{y}}_1$ inside its alert threshold boundary, and the measurement obtained by system 2 may trigger an alert if $\hat{\mathbf{y}}_2$ is inside its alert threshold boundary. Thus, a true state outside dissonance space may still trigger dissonance.

4.1.1 Probability of Dissonance Given a True State

Given a true state y, because of the measurement noise of each system $\mathbf{n}_i$, the measured state is given by $\hat{\mathbf{y}}_i = \mathbf{y} + \mathbf{n}_i$. Given the probability density function (PDF) of the measurement noise of each alerting system $\mathbf{f}_{\mathbf{n}_i}(\mathbf{n}_i)$, the PDF $\mathbf{f}_{\hat{\mathbf{y}}_i|\mathbf{y}}(\hat{\mathbf{y}}_i \mid \mathbf{y})$, describing the measured state, is given as

$$\mathbf{f}_{\hat{\mathbf{y}}_i|\mathbf{y}}(\hat{\mathbf{y}}_i \mid \mathbf{y}) = \int_{-\infty}^{+\infty} \mathbf{f}_{\mathbf{y}}(\mathbf{y})\mathbf{f}_{\mathbf{n}_i}(\hat{\mathbf{y}}_i - \mathbf{y})d\hat{\mathbf{y}}_i = \mathbf{f}_{\mathbf{n}_i}(\hat{\mathbf{y}}_i - \mathbf{y}) \tag{4.1}$$

Then the probability of system 1 alert for the given true state in the example described above can be given as (Figure 4.2)

$$P_{11} = P(System1Alert \mid \mathbf{y}) = \int_A^B \mathbf{f}_{\hat{\mathbf{y}}_1|\mathbf{y}}(\hat{\mathbf{y}}_1 \mid \mathbf{y})d\hat{\mathbf{y}}_1 \tag{4.2}$$

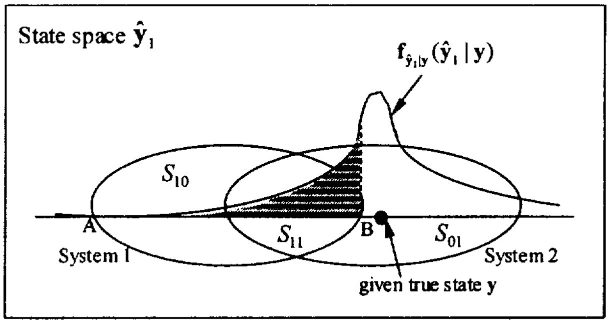

State space $\hat{\mathbf{y}}_1$
$\mathbf{f}_{\hat{\mathbf{y}}_1|\mathbf{y}}(\hat{\mathbf{y}}_1 \mid \mathbf{y})$
S_{10}
A
B
S_{11}
S_{01}
System 1
System 2
given true state y

Figure 4.2 Probability of System 1 Alert

And the probability of system 2 alert is (Figure 4.3)

$$P_{21} = P(System2Alert \mid \mathbf{y}) = \int_C^D \mathbf{f}_{\hat{\mathbf{y}}_2|\mathbf{y}}(\hat{\mathbf{y}}_2 \mid \mathbf{y})d\hat{\mathbf{y}}_2 \tag{4.3}$$

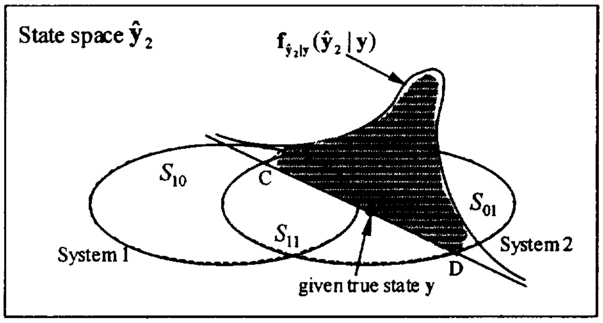

State space $\hat{\mathbf{y}}_2$
$\mathbf{f}_{\hat{\mathbf{y}}_2|\mathbf{y}}(\hat{\mathbf{y}}_2 \mid \mathbf{y})$
S_{10}
C
S_{01}
S_{11}
System 1
System 2
D
given true state y

Figure 4.3 Probability of System 2 Alert

Then if the measurements from two systems are independent, then the probability of dissonance is

$$P(D \mid \mathbf{y}) = P(S_{11} \mid \mathbf{y}) = P_{11} \times P_{21} \tag{4.5}$$

If the measurements from two systems are correlated, we can run a Monte Carlo Simulation to obtain the ratio of the measured state being in dissonance space, which is the probability of dissonance for the given true state. Also note that equations (4.2) and (4.3) could be extended to multidimensional PDFs.

4.1.2 False Dissonance and Missed Dissonance

With the measurement noise, it is possible that the measured state triggers dissonance although the true state is not in the dissonance space (false dissonance); or the measured state may not trigger dissonance even though the true state is in dissonance space (missed dissonance). Given a true state and the PDF $\mathbf{f}_{\hat{\mathbf{y}}_i \mid \mathbf{y}}(\hat{\mathbf{y}}_i \mid \mathbf{y})$ for both systems, we can obtain the probability of false dissonance and missed dissonance.

For the same example shown in Figure 4.1, given a true state which is outside the dissonance space S_{11}, false dissonance occurs if each measured state triggers each system alert. That is, the probability of false dissonance is

$$P(FalseDissonance \mid \mathbf{y}) = P(S_{11} \mid \mathbf{y}) = P_{11} \times P_{21} \tag{4.6}$$

which is the same as equation (4.5).

Given a true state y which is inside the dissonance space S_{11}, missed dissonance occurs when one or both of the two alerting systems misses detecting the hazard. That is, the probability of missed dissonance is

$$\begin{aligned} P(MissedDissonance \mid \mathbf{y}) &= P(S_{10} \mid \mathbf{y}) + P(S_{01} \mid \mathbf{y}) + P(S_{00} \mid \mathbf{y}) \\ &= P_{10} \times P_{21} + P_{11} \times P_{20} + P_{10} \times P_{20} \end{aligned} \tag{4.7}$$

Where P_{10} is the probability with no system 1 alert. That is (Figure 4.4)

$$P_{10} = P(System1NoAlert \mid \mathbf{y}) = \int_{-\infty}^{A} \mathbf{f}_{\hat{\mathbf{y}}_1 \mid \mathbf{y}}(\hat{\mathbf{y}}_1 \mid \mathbf{y}) d\hat{\mathbf{y}}_1 + \int_{B}^{\infty} \mathbf{f}_{\hat{\mathbf{y}}_1 \mid \mathbf{y}}(\hat{\mathbf{y}}_1 \mid \mathbf{y}) d\hat{\mathbf{y}}_1 \tag{4.8}$$

And P_{20} is the probability with no system 2 alert. That is (Figure 4.5)

$$P_{20} = P(System2NoAlert \mid \mathbf{y}) = \int_{-\infty}^{C} \mathbf{f}_{\hat{\mathbf{y}}_2|\mathbf{y}}(\hat{\mathbf{y}}_2 \mid \mathbf{y})d\hat{\mathbf{y}}_2 + \int_{D}^{\infty} \mathbf{f}_{\hat{\mathbf{y}}_2|\mathbf{y}}(\hat{\mathbf{y}}_2 \mid \mathbf{y})d\hat{\mathbf{y}}_2 \qquad (4.9)$$

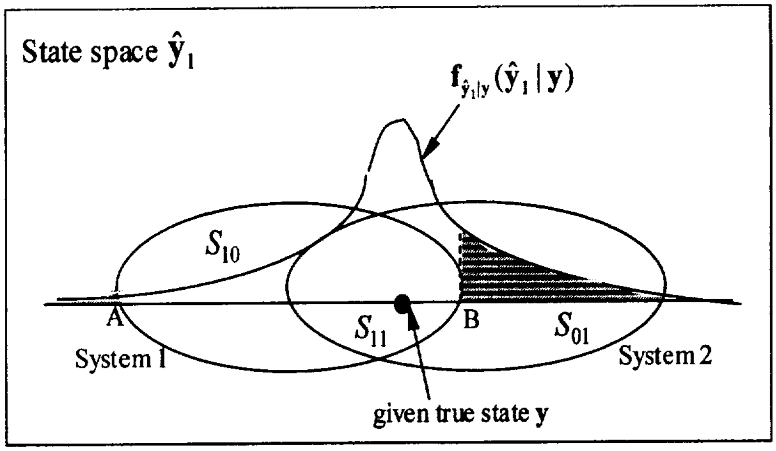

State space $\hat{\mathbf{y}}_1$
$\mathbf{f}_{\hat{\mathbf{y}}_1|\mathbf{y}}(\hat{\mathbf{y}}_1 \mid \mathbf{y})$
S_{10}
A
S_{11}
B
S_{01}
System 1
System 2
given true state y

Figure 4.4 Probability of System 1 No Alert

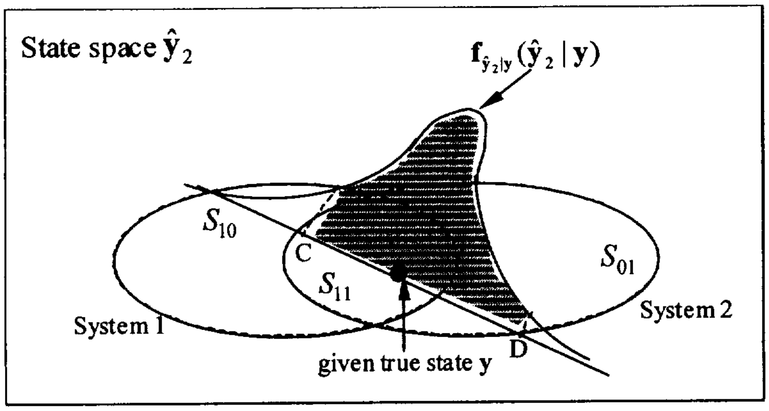

State space $\hat{\mathbf{y}}_2$
$\mathbf{f}_{\hat{\mathbf{y}}_2|\mathbf{y}}(\hat{\mathbf{y}}_2 \mid \mathbf{y})$
S_{10}
C
S_{11}
S_{01}
System 1
System 2
given true state y
D

Figure 4.5 Probability of System 2 No Alert

4.1.3 Redistribution of Threshold Functions Considering Sensor Error

From another aspect view of sensor error, we can translate the sensor error into a redistribution of the threshold functions of each alerting system. Then, a similar method to that developed in Chapter 3 for logic difference can be applied to identify the conditions for dissonance originating from sensor error.

Since the threshold function is a function of $\hat{\mathbf{y}}$, the threshold functions are themselves functions of random variables. That is,

$$\mathbf{a} = T(\hat{\mathbf{y}}) = T(\mathbf{y} + \mathbf{n}) \qquad (4.10)$$

The distributions of threshold functions for each alerting system can be determined through algebraic operations on random variables.

For example, in Figure 4.6, the solid line is the original threshold boundary. That is, if the measured state $\hat{y}$ is inside the boundary, the system will give an alert. Given the sensor error distribution, the threshold boundary in terms of y are the dashed lines, between which the measured state will trigger system alert with some probability. The alerting space has been enlarged to the outer dashed line because of the false alarms introduced by sensor error. And those states inside the original threshold function have some probability of missed detection.

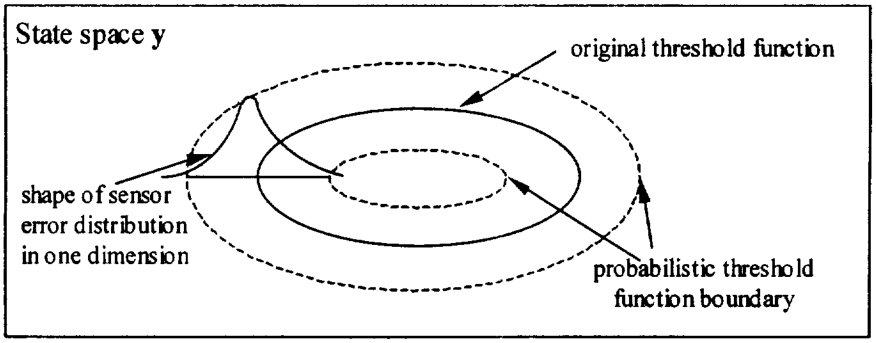

State space y
original threshold function
shape of sensor error distribution in one dimension
probabilistic threshold function boundary

Figure 4.6 Translate Sensor Error to Threshold Boundary Change

Now, using the same example as in Figure 4.1 with S_{11} as dissonance space, we can consider the threshold change after introducing the sensor error and analyze the redistribution of dissonance space (Figure 4.7).

In Figure 4.7, dissonance space is now probabilistic. For example, point C in Figure 4.7 is outside the original dissonance space, but it could trigger dissonance with some probability because of sensor error, which is false dissonance. Similarly, point A will trigger system dissonance with some probability. The dark space between inner dashed lines is smaller compared to the original dissonance space because of missed dissonance. For example, point B in Figure 4.7 is inside the original dissonance space, but it may not trigger dissonance because of sensor error, which is missed dissonance.

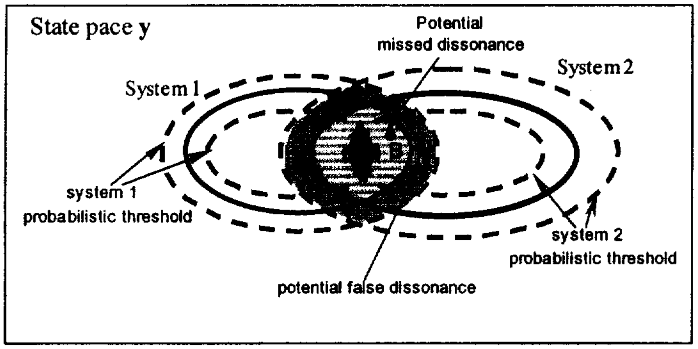

State pace y
Potential missed dissonance
System 1
System 2
system 1 probabilistic threshold
system 2 probabilistic threshold
potential false dissonance

Figure 4.7 Dissonance Space Change with Sensor Errors

Given a requirement of the probability for dissonance, the new alert stage boundaries can be determined, and then the same analysis method we used for dissonance due to logic differences can be used to identify the conditions leading to dissonance with some probability.

4.2 Example Analysis of the Contribution of Sensor Error

For a real alerting system, sensor error always exists at some level. Given a restriction that there should be no dissonance with some probability, we can modify the system design to avoid dissonance by identifying the conditions for dissonance with some probability. Since dissonance occurs from two different parts, logic difference and sensor error, we want to identify the contribution of each part. This can be used to help the designer to decide the best way to mitigate dissonance (such as, using a more accurate sensor, or modifying the design of the alerting logic). Knowing the probability of dissonance for each true state in the design space would help the designer to reshape the threshold functions for each alerting system.

In this section, we will give some example analysis of the probability of dissonance, identify the contribution of sensor error to dissonance for a set of uncertain trajectories, and compare it with the contribution of logic difference. At this point, it is assumed that each alerting system is affected independently by noise.

Let P_{1m} denote the probability that system 1 is in alert stage m, P_{2n} the probability that system 2 is in alert stage n, and D be the event of dissonance. For a given true state $\mathbf{y}$, if the dissonance space is S_{mn}, and if the measurements from two systems are independent, then the probability of dissonance for the given true state y is

$$P(D \mid \mathbf{y}) = P_{1m} \times P_{2n} \tag{4.11}$$

That is, equation (4.11) is the probability when system 1 is in alert stage m and system 2 is in alert stage n for the given true state. Probabilities P_{1m} and P_{2n} can be obtained analytically as we described in section 4.1.1 or through simulation. If the measurements of two systems are correlated, the probability of dissonance for the given true state can be obtained by counting the fraction of measured states in dissonance space during the simulation.

If an entire trajectory is expected to be followed, the designer may want to know the cumulative probability of dissonance occurring at some point along the trajectory. This will help the designer or the operator to modify the procedures to mitigate dissonance.

Consider a given true trajectory T. We define the cumulative probability of dissonance up to time t along the trajectory as

$$P_c(D \mid T(t)) = 1 - \prod_{t=0}^{t}(1 - P(D \mid \mathbf{y}(t))) \tag{4.12}$$

where $\prod_{t=0}^{t}(1 - P(D \mid \mathbf{y}(t)))$ is the probability of no dissonance up to time t. And as time goes to infinity, we have the cumulative probability of dissonance over the entire trajectory T,

$$P_\infty(D \mid T) = \lim_{t \to \infty} P_c(D \mid T(t)) \tag{4.13}$$

This value helps the designer or operator to know the trend of the probability of dissonance along the trajectory.

It is worth mentioning that we assumed that two systems have the same measurement update rate in equation (4.12). Thus, two systems are measuring the same true state $\mathbf{y}(t)$ at time t. If two systems have different measurement update rates (τ_1 for system 1 and τ_2 for system 2), the true state that system 1 measures would be different from the true state that system 2 measures at time t (Figure 4.8). In Figure 4.8, $y(t)$ is the true states as time changes, $y_1(t)$ is the state that system 1 measures as time changes, and $y_2(t)$ is the state that system 2 measures as time changes.

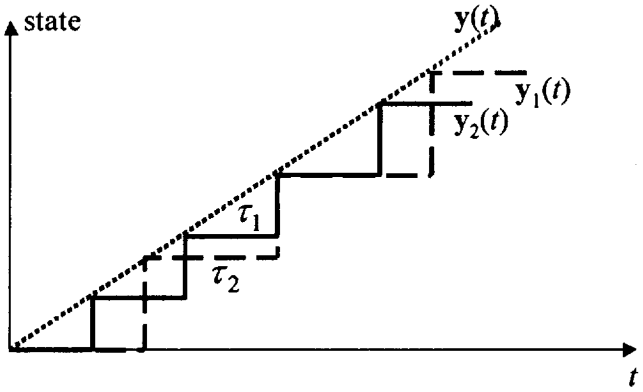


Figure 4.8 Considering Different Measurement Update Rate

Assuming S_{mn} is the dissonance space, then the probability of dissonance at time t would be given by

$$P(D \mid t) = P_{1m}(y_1(t)) \times P_{2n}(y_2(t)) \tag{4.14}$$

That is, it is equal to the probability of system 1 being in alert stage m given $y_1(t)$ times the probability of system 2 being in alert stage n given $y_2(t)$, assuming the measurement of two systems are independent. If the measurements of two systems are correlated, the probability of dissonance at time t can be obtained by counting the fraction of measured states causing dissonance during the simulation. Then the cumulative probability of dissonance up to time t along the trajectory is given by

$$P_c(D \mid T(t)) = 1 - \prod_{t=0}^{t} (1 - P(D \mid t)) \tag{4.15}$$

In most cases, we don't know exactly which trajectory will be followed. Based on experience or after running simulations, we may be able to determine the probability distribution of a set of r different uncertain trajectories $P(T_i)$. From this, we can get an overall cumulative probability of dissonance for a set of uncertain trajectories:

$$P_\infty(D) = \sum_{i=1}^{r} P_\infty(D \mid T_i) \times P(T_i) \tag{4.16}$$

This value helps the designer or operator to know what the chance is of getting a dissonance situation in the future, given a starting point.

After defining the probability of dissonance, we can analyze the effect of sensor accuracy on the probability of dissonance.

Consider a set of possible trajectories without any noise. We use P' to denote probabilities in ideal conditions without any noise. This set of trajectories can be separated into two subsets. Subset A includes those trajectories in which there are states in the dissonance space, that is, $P'_\infty(D \mid T_i) = 1$. Subset B includes those trajectories in which there is no state in dissonance space, that is, $P'_\infty(D \mid T_i) = 0$. So, due to logic difference alone, the overall cumulative probability of dissonance for a set of uncertain trajectories is

$$P'_\infty(D) = \sum_{i=1}^{r} P'_\infty(D \mid T_i) \times P(T_i) \tag{4.17}$$

From this, the contribution of sensor error to dissonance $P_\infty(D)$ can be compared to the contribution of logic difference to dissonance $P'_\infty(D)$.

Considering sensor accuracy, we can define the probability of false dissonance as the probability of dissonance triggered by those trajectories in subset B, on which there is no true state in the dissonance space contributed by logic difference. That is,

$$P_{FD} = \sum_{T_i \in B} P(T_i) \times P_\infty(D \mid T_i) \tag{4.18}$$

And the probability of missed dissonance is defined as the probability of dissonance missed by those trajectories in subset A, on which there are true states in the dissonance space contributed by logic difference, that is,

$$P_{MD} = \sum_{T_i \in A} P(T_i) \times P_\infty(\overline{D} \mid T_i) = \sum_{T_i \in A} P(T_i) \times (1 - P_\infty(D \mid T_i)) \tag{4.19}$$

where $\overline{D}$ means no dissonance. So, the total probability of dissonance with sensor error would be

$$P_\infty(D) = P'_\infty(D) + P_{FD} - P_{MD} = \sum_i P(T_i) \times P_\infty(D \mid T_i) \qquad (4.20)$$

Usually, sensor error would increase the overall probability of dissonance. However, when $P_{FD} < P_{MD}$, $P_\infty(D) < P'_\infty(D)$, and sensor error may actually provide some benefit, decreasing the overall probability of dissonance. This may not be a good thing though. Decreased overall cumulative probability of dissonance means a larger probability of missed dissonance, which also means that one of the alerting systems may have missed detection of the hazard. The hazard may not be able to be avoided because of this missed detection.

This analysis method will be demonstrated in Chapter 7 for the In-Trail separation example to compare the contribution of sensor error to dissonance with the contribution of logic differences. The ways to mitigate dissonance through modifying alerting system threshold functions will be described in Chapter 6 and demonstrated in Chapter 7 for the In-Trail separation example.

4.3 Summary

In this chapter, a method is provided to identify the conditions for dissonance originating from sensor error, which is similar to the method in Chapter 3 for the dissonance originating from logic differences, by translating the sensor error into the threshold function redistribution.

A probabilistic analysis method is developed to compare the contribution of sensor error to dissonance with the contribution of logic differences. Concepts of False Dissonance and Missed Dissonance are defined to explain the contribution of sensor error to dissonance.

5. Hybrid System Analysis of Consequences of Dissonance

Human operators may increase delay in taking action, fail to take any action at all, or implement action contrary to automation command when they are exposed to dissonance. This unpredictable response to dissonance may cause the process to become unsafe, even though each alerting system alone has been designed to avoid hazards. This type of dissonance should be avoided or mitigated.

Modifying the design of logic to eliminate all of dissonance space may decrease overall system efficiency and capability. Meanwhile, unsafe consequences of dissonance should be avoided. Thus, the regions of dangerous dissonance space, in which the human operator's unpredictable response will cause the process to become unsafe, need to be identified. Then the process can still stay safe by modifying the design of logic to eliminate regions of dangerous dissonance space, or through modifying the process' operation to avoid regions of dangerous dissonance space.

A process with logical alerting systems can be considered as a hybrid system, since the process dynamics are continuously changing and the state of alerting systems are discretely changing. Thus continuous and discrete dynamics coexist and interact with each other in the process with multiple alerting systems. In this chapter, a hybrid model is developed to accurately describe the dynamic behavior of the process incorporating multiple alerting systems. Using the hybrid model, dangerous dissonance space is identified through backward reachability analysis. Then, the mitigation method to avoid dangerous dissonance space through modifying control strategy is described in Chapter 6.

5.1 Dangerous Dissonance Space

To be able to focus on the unsafe consequences because of dissonance only, we assume here that each alerting system is individually well designed. That is, if the human operator would commit to each alerting system's command, even with small uncertainties of the operating environment and disturbance of the human operator's response, each alerting system alone should have been designed to efficiently avoid the monitored hazard. An example alerting space and the monitored hazard space are presented in the state space in Figure 5.1. As shown in this figure, when the continuous state hits the boundary of alert space, the alerting system will command the human operator to take some maneuver. The trajectory followed as commanded with small disturbance would be able to avoid the hazard space.

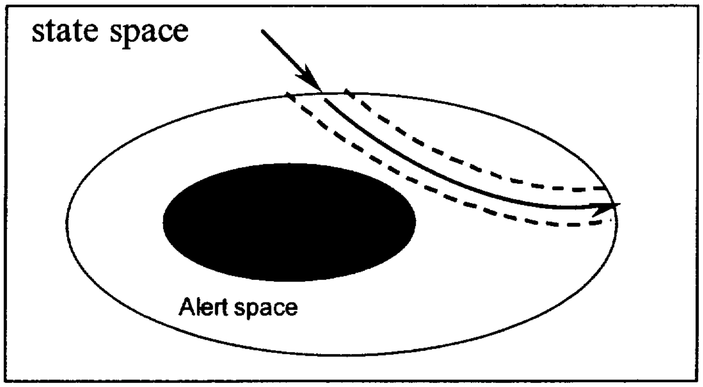


Figure 5.1 State Space Representation of Alerting System for Hazard

With multiple alerting systems in the same process, it's possible to have dissonance, and the human operator may lead the process to a hazard because of dissonance. The dissonance space can be identified with the method developed in Chapter 3 and 4. Figure 5.2 shows an example of process with two alerting systems, and the dissonance space is the space where both systems alert but with dissonance resolution advisories. As shown in Figure 5.2, the human operator's possible response to dissonance could lead the process to a hazard. In Figure 5.2, the human operator follows the first alerting system command after the continuous state hits the first alerting system alert space boundary (at point A). But before the process gets out of the first alerting system alert space, the continuous state hits the second alerting system alert space boundary (at point B), where the second alerting system commands the operator to take some maneuver that is dissonant with the first alerting system command. Different operators may follow different trajectories in such a confusing situation, and some of them may lead the process to hazard space. We define a *dangerous dissonance state* as a state in dissonance space from which hazard space can be reached with a possible human operator's response to dissonance. So, state B in Figure 5.2 is a *dangerous dissonance* *state*. We want to identify those dangerous dissonance states in dissonance space so that the unsafe consequences of dissonance can be avoided.

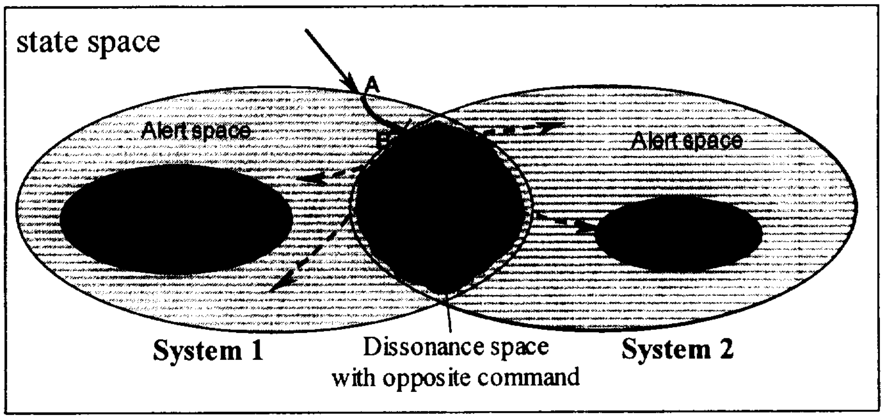


Figure 5.2 Uncertain Operator's Responses in Dissonance Space

As shown in Figure 5.3, dangerous dissonance space is a subset of the dissonance space. Although the rest of the dissonance space is not dangerous, in the long-term view, the human operator may still distrust the system. So, the system designer should at least eliminate the dangerous dissonance space and if possible, all dissonance space.

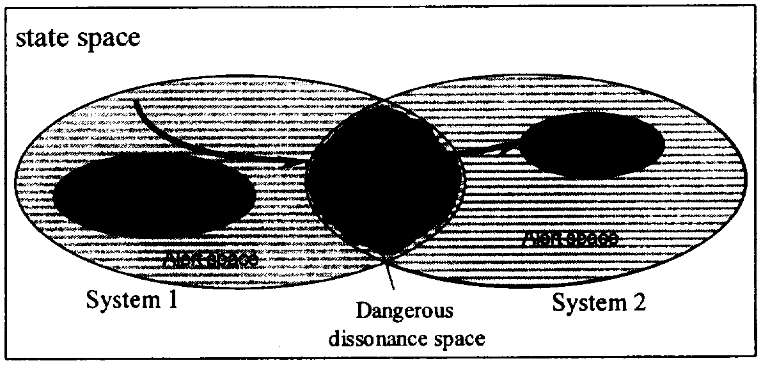


Figure 5.3 Dangerous Dissonance Space

One way to identify the dangerous dissonance space is to predict the human operators behavior given a specific dissonance situation. The set of possible trajectories following dissonance can be the worst case of trajectory prediction or can be restricted by the physical performance of the process. Then we can work forward to check if the human's response could lead the process to any hazard. With such a forward reachability analysis (Figure 5.4), we need to exhaustively check infinite states (which is impractical) in dissonance space with all possible human operator responses numerically to determine the dangerous dissonance states.

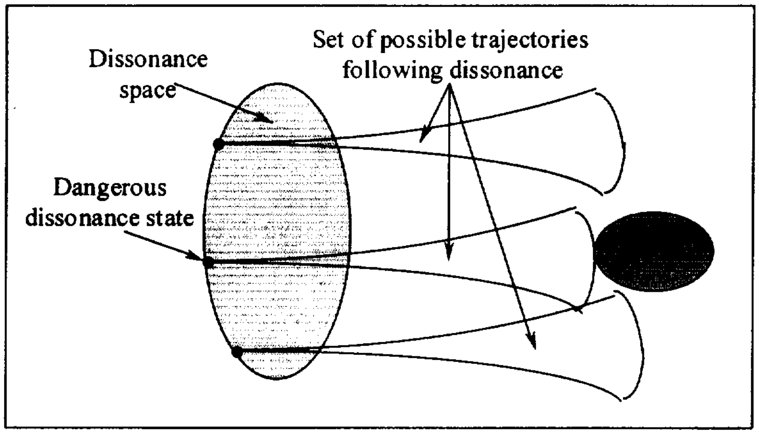

Dissonance space
Set of possible trajectories following dissonance
Dangerous dissonance state

Figure 5.4 Forward Reachability Analysis

The other way to identify the dangerous dissonance space is to use backward reachability analysis (Figure 5.5). Given the hazard space and the set of possible future trajectories following dissonance, the dangerous dissonance space can be analytically identified with backward reachability analysis. Backward reachability analysis can also be used to identify the subset of human actions that could lead the process to the hazard space.

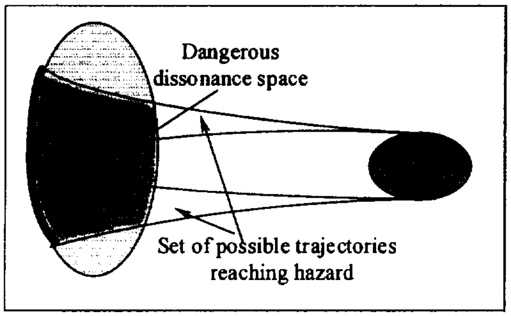

Dangerous dissonance space
Set of possible trajectories reaching hazard

Figure 5.5 Backward Reachability Analysis

Although it is impractical to predict the exact human operator's behavior in front of specific dissonance, and it is hard to generalize a human's behavior for all dissonance situations, we may be able to find a probabilistic distribution of human operator responses through running an experiment or simulation. Or we can just assume that the set of future trajectories following dissonance is uniformly distributed and restricted by the physical performance of the process.

In the following section, we will develop a model to accurately describe the dynamic behavior of the process incorporating multiple alerting systems. Using the hybrid model, dangerous dissonance space can be identified mathematically.

5.2 Hybrid Model for the Process Incorporating Multiple Alerting Systems

5.2.1 Introduction to Hybrid Systems

A **Hybrid System** is an interacting collection of dynamical systems, each evolving on continuous state spaces, and subject to continuous and discrete controls, and some other discrete phenomena (Branicky, et al., 1994). Hybrid models have been used to describe complex systems to fully take into consideration the relations and interactions of the continuous and discrete parts of the system. Examples of such systems include robotics, chemical process control systems, manufacturing, automated highway systems, air traffic management systems, integrated circuit design, and multi-media (Special issue on hybrid systems, 1998, 1999, 2000).

The underlying mathematical theory behind hybrid systems combines models, stability, and reachability analyses to prove safety and performance properties for complex interactions. Formal analysis of hybrid systems is concerned with verifying whether the hybrid system satisfies desired specifications. These specifications could be safety specifications where it is important to guarantee that the state of the system avoid certain unsafe regions. The specifications could also be reachability specifications, where the problem is whether, under the dynamics of the hybrid system, a given set of states can be reached from a given set of initial conditions. Techniques have been developed for synthesizing controllers that satisfy safety specifications and establishing whether the set of reachable states is contained in a certain set (Lynch, et al., 1996; Lygeros, et al., 1999; Tomlin, et al., 2000; Koutsoukos, et al., 2000; Asarin, et al., 2000).

5.2.2 Hybrid Phenomenon of the Process Incorporating Multiple Alerting Systems

The process incorporating logical decision support subsystems can be considered as a hybrid system, since the continuous and discrete dynamics coexist and interact with each other in the process. In (Branicky, et al., 1994) a unified hybrid systems model is introduced, which captures many discrete phenomena arising in hybrid systems. These phenomena include autonomous switching, which is the phenomenon where the vector field defining the continuous dynamics changes discontinuously when the continuous state hits certain boundaries, and controlled switching when the vector field changes abruptly in response to a control command.

The hybrid phenomenon appearing in a process incorporating alerting systems is a combination of autonomous and controlled switching. The switching of the vector field governing the continuous dynamics is activated when the continuous state hits boundaries defined by the threshold functions of the alerting systems. Ultimately, the vector field switches in response to the human operator's discrete control strategy for the process based on alerting system advisories. A method is needed to model this autonomously activated but controlled switching phenomenon.

5.2.3 Hybrid Model with Transition Functions

To be able to model the hybrid phenomenon described above, transition functions are introduced to model human operator responses to alerting system commands. The transition functions are activated when the continuous state hits a boundary satisfying alerting system threshold functions. Human operators are assumed to follow the alerting system commands with some uncertainties in each alerting system's alert space individually, and these uncertainties can be included in a small set of disturbances on the set of trajectories determined by the alerting system's command. The transition function in each alerting system's alert space acts as a random processor, randomly choosing one trajectory from the set of trajectories determined by the alerting system command. Since we assumed each alerting system has been well designed to avoid hazard space, the switched vector field governing the continuous dynamics will not reach the hazards. In the dissonance space, since human operator responses are more uncertain, we assume that the possible set of trajectories in dissonance space are probabilistically distributed and bounded by the worst case or the physical performance of the process. That is, the switched vectored field is not determined but belongs to a probabilistic distributed set

(Figure 5.6). The transition function in dissonance space acts as a random processor, choosing one trajectory from the probabilistic distributed set of trajectories.

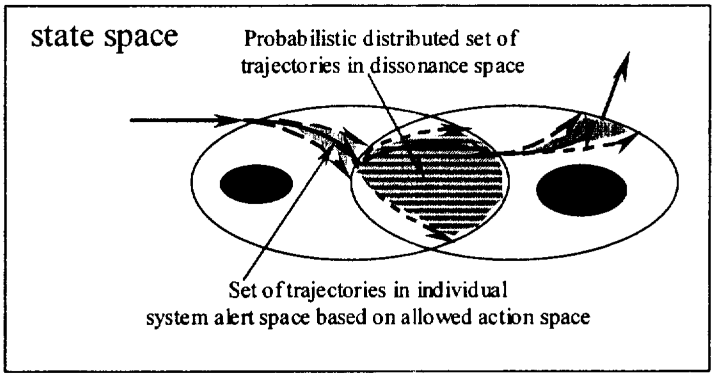

state space
Probabilistic distributed set of trajectories in dissonance space
Set of trajectories in individual system alert space based on allowed action space

Figure 5.6 Transition Functions in Dissonance Space

Mathematically, given the i^{th} alerting system, at any time t, we can separate the whole state space $\mathbf{U}$ into several subsets A_{ik} based on the system alert stages of the i^{th} alerting system,

$$\mathbf{U} = \bigcup_{k} A_{ik} \tag{5.1}$$

Where each A_{ik} is a connected, open set of $\mathbf{R}^n$. $\mathbf{R}^n$ is the continuous state space of the process. A_{ik} is the k^{th} system alert stage space of the i^{th} alerting system, as defined in chapter 2.

For the i^{th} alerting system, the continuous dynamics in each discrete state space A_{ik} is given by a set of vector fields $\mathbf{F}_{ik} : A_{ik} \to \mathbf{R}^n$, which is based on the allowed action space of the i^{th} alerting system, governed by the differential equation

$$\dot{\mathbf{x}}(t) = \mathbf{f}_{ik}(\mathbf{x}(t), \mathbf{u}(t), \mathbf{d}(t), t) \in \mathbf{F}_{ik} \tag{5.2}$$

where $\mathbf{u}(t)$ is the continuous control applied to the process at time t while the alerting system is in alert stage k, and $\mathbf{d}(t)$ is the disturbance at time t.

Given two alerting systems i and j, as we introduced in Chapter 2, the intersections of their alert stages are denoted by the sets S_{mn} where m is the alert stage from system i and n is the alert stage from system j. The whole state space then can be separated into subsets S_{mn}, that is,

$$\mathbf{U} = \bigcup_{m,n} S_{mn} = \bigcup_{m,n} (A_{im} \cap A_{jn}) \tag{5.3}$$

If S_{mn} is not a dissonance space, then the continuous dynamics of the process is governed by

$$\mathbf{F}_{mn} = \mathbf{F}_{im} \cap \mathbf{F}_{jn} \tag{5.4}$$

which is defined by the intersection of the two alerting systems' allowed action space. But if S_{mn} is a dissonance space, the intersection of two alerting systems' allowed action space may be empty. That is, $\mathbf{F}_{mn} = \mathbf{F}_{im} \cap \mathbf{F}_{jn} = \phi$. In this case, $\mathbf{F}_{mn}$ is not well defined in the dissonance space. Exposed to this situation, the confused human operator might take any action, and the continuous dynamics would be given by a set $\mathbf{F}$ of differential operators. $\mathbf{F}$ could be uniformly distributed and bounded by the physical performance of the process, or could be a probabilistic distributed set and bounded by the worst case describing the human operator's response in dissonance space. This set could be determined through running an experiment or simulation. The transition functions in space S_{mn} act as a random processor, which randomly chooses a governing differential operator from the set $\mathbf{F}_{mn}$ if S_{mn} is not a dissonance space or $\mathbf{F}$ if S_{mn} is a dissonance space.

For example, given two alerting systems A and B with threshold functions shown in state space as the physical space in Figure 5.7, both have two alert stages 0 and 1. There are four subsets in the whole state space: $S_{00} = A_{\mathrm{A0}} \cap A_{\mathrm{B0}}$, $S_{01} = A_{\mathrm{A0}} \cap A_{\mathrm{B1}}$, $S_{10} = A_{\mathrm{A1}} \cap A_{\mathrm{B0}}$, and $S_{11} = A_{\mathrm{A1}} \cap A_{\mathrm{B1}}$. When system A is in alert stage 1, system A commands a right turn within the set of required heading changes; and in alert stage 0, there is no restriction for the action space. When system B is in alert stage 1, system B commands a left turn within the set of required heading changes; and no action restriction in alert stage 0. So, when the continuous state hits the boundary of subset $S_{10} = A_{\mathrm{A1}} \cap A_{\mathrm{B0}}$, the transition function is activated which randomly chooses a governing differential equation within the intersection set of allowed action spaces of two alerting systems $\mathbf{F}_{10} = \mathbf{F}_{A1} \cap \mathbf{F}_{B0} = \mathbf{F}_{A1}$. This would be some form of right turn. When the continuous state hits the boundary of subset $S_{11} = A_{A1} \cap A_{B1}$, the activated transition function randomly chooses a governing differential equation within set $\mathbf{F}$, which is bounded by the mechanical performance of the process (e.g., the maximum turn the process could have). When the continuous state hits the boundary of subset $S_{01} = A_{A0} \cap A_{B1}$, the activated transition function randomly chooses a governing differential equation within set $\mathbf{F}_{01} = \mathbf{F}_{A0} \cap \mathbf{F}_{B1} = \mathbf{F}_{B1}$, which would be a left turn. It is assumed here that the effect of dissonance on the operator's choice of control does not continue into the non-dissonance region S_{01}.

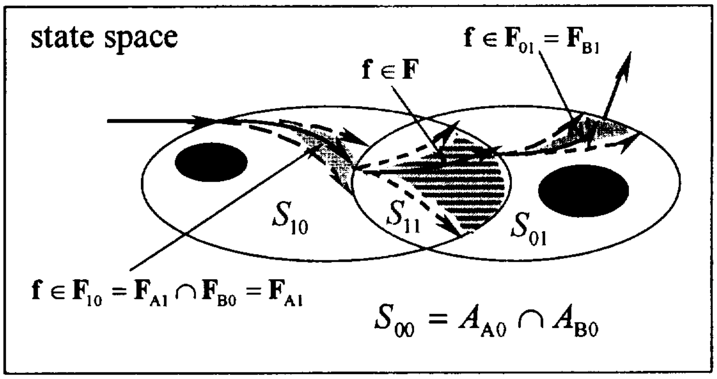

state space
$\mathbf{f} \in \mathbf{F}_{01} = \mathbf{F}_{B1}$
$\mathbf{f} \in \mathbf{F}$
S_{10}
S_{11}
S_{01}
$\mathbf{f} \in \mathbf{F}_{10} = \mathbf{F}_{A1} \cap \mathbf{F}_{B0} = \mathbf{F}_{A1}$
$S_{00} = A_{A0} \cap A_{B0}$

Figure 5.7: Example Transition Function

Now we can define the hybrid model of the process incorporating multiple alerting systems. The model consists of a state space

$$\mathbf{U} = \bigcup_{q \in Q} \mathbf{U}_q, \quad Q \equiv \{1,...,N\} \tag{5.5}$$

Where each $\mathbf{U}_q$ is a connected, open set of $\mathbf{R}^n$. $\mathbf{R}^n$ is the continuous state space of the hybrid process, and $Q \equiv \{1,...,N\}$ is the set of discrete states. A state of the process is a pair $(q, \mathbf{x}) \in Q \times \mathbf{U}$. $\mathbf{B}$ is the boundary associated with each discrete state, meaning that the state $(q, \mathbf{x})$ may flow within q only if $\mathbf{x} \notin \mathbf{B}$, and when $\mathbf{x} \in \mathbf{B}$, transition function $\mathbf{T}$ is activated, a discrete transition is forced, and the continuous dynamics within the following discrete state q' is decided by the transition function. In each discrete state q, the continuous state $\mathbf{x} \in S_{mn}$. The continuous dynamics are given by vector fields

$\mathbf{f} : \mathbf{U}_q \rightarrow \mathbf{R}^n$ as decided by transition functions. The model also includes $\mathbf{H}_i$, the hazard space monitored by the *i*th alerting system. The state of the process $(q, \mathbf{x})$ is required to stay outside the hazard space $\mathbf{H}_i$.

Since the human operator's response has some time delay, we use Δ_q to represent the transition delay. The dynamics of the hybrid process can now be described as follows. There is a sequence of *pre-switch times* $\{\tau_i\}$ and another sequence of *post-switch times* $\{\Gamma_i\}$ satisfying $0 = \Gamma_0 \le \tau_1 < \Gamma_1 < \tau_2 < \Gamma_2 < \cdots \le \infty$, such that on each interval $[\Gamma_{j-1}, \tau_j)$ with a non-empty interior, $\mathbf{x}(\cdot)$ evolves according to the differential equations $\dot{\mathbf{x}}(t) = \mathbf{f}$ decided by transition function $\mathbf{T}$ in some U_i. At the next pre-switch time (say, τ_j), $\mathbf{x}(\cdot)$ hits the boundary $\mathbf{B}$, and the vector field switches according to transition functions at time $\Gamma_j = \tau_j + \Delta_i$.

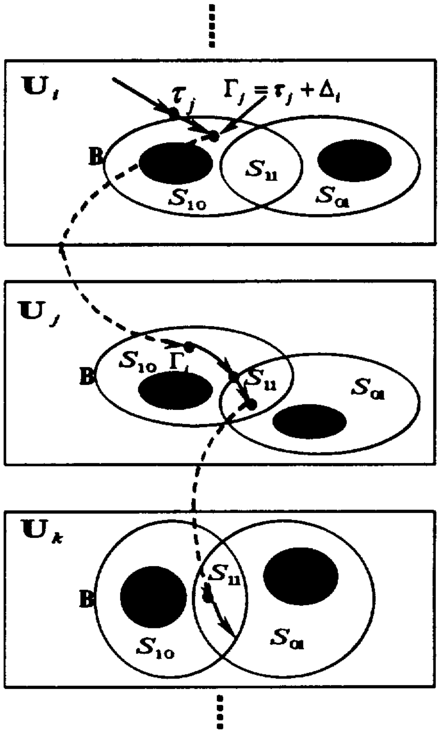


Figure 5.8: Example Dynamics of the Hybrid Model

Part of the dynamics of the example we introduced above (in Figure 5.7) is shown in Figure 5.8. The state $(q_i, \mathbf{x})$ flows within q_i before τ_j; at time τ_j, the state hits the boundary of S_{10}, and the activated transition function chooses a governing differential equation from $\mathbf{F}_{10} = \mathbf{F}_{A1}$ within time delay Δ_i. During the time delay Δ_i, the state $(q_i, \mathbf{x})$ still flows within q_i governed by differential equation $\dot{\mathbf{x}}(t) = \mathbf{f} \in \mathbf{F}_{00}$ as before τ_j. At time $\Gamma_j = \tau_j + \Delta_i$, the process is in discrete state q_j, on interval $[\Gamma_j, \tau_k)$, and $\mathbf{x}(\cdot)$ evolves according to the differential equations $\dot{\mathbf{x}}(t) = \mathbf{f}$ decided by transition function $\mathbf{T}$ in $\mathbf{U}_j$; and the process dynamics continue.

5.3 Identification of Dangerous Dissonance Space

As mentioned above, some subset of the trajectories following dissonance may encounter hazards, although each alerting system has been designed to be able to avoid the monitored hazard individually. Using backward reachability analysis of the hybrid model we developed above, we can identify those dangerous dissonance spaces in which the human operator's possible response could lead the process to some hazards. Here, we assume the hazard spaces are metric spaces, and the set of functions $\mathbf{F}_{mn}$ and $\mathbf{F}$ are all monotonic, then from the boundary of the hazard spaces, the boundary of the dangerous dissonance space can be identified through backward reachability analysis.

Continuing the example given in the last section, the process to identify dangerous dissonance space can be described with Figure 5.9. First consider those continuous dynamics hitting the boundary of the dissonance space S_{11} from S_{10}. That is, the continuous state first hits the boundary of S_{10}; following $\mathbf{f}_{10} \in \mathbf{F}_{10}$, the continuous state then hits the boundary of the dissonance space S_{11}. Following the set of possible differential operators $\mathbf{F}$ in dissonance space, some of these trajectories hit the hazard spaces. For the hazard space $\mathbf{H}_B$ monitored by alerting system B (Figure 5.9 (a)), with $\mathbf{H}_B$ as the initial conditions, the states between A and B can be identified by solving the set of differential equations $-\dot{\mathbf{x}}(t) = \mathbf{F}_{01}(\mathbf{x}(-t), \mathbf{u}(-t), \mathbf{d}(t), -t)$ at time Γ_q. Any state between A and B could then encounter $\mathbf{H}_B$. Also, with the hazard space $\mathbf{H}_A$ monitored by alerting system A as the initial conditions, the states between C and D can be identified by solving the set of differential equations $-\dot{\mathbf{x}}(t) = \mathbf{F}_{10}(\mathbf{x}(-t), \mathbf{u}(-t), \mathbf{d}(t), -t)$ at time Γ_q. Now, those dangerous dissonance states between J and K (Figure 5.9 (b)) in dissonance space can be identified by solving the set of differential equations $-\dot{\mathbf{x}}(t) = \mathbf{F}(\mathbf{x}(-t), \mathbf{u}(-t), \mathbf{d}(t), -t)$ at time Γ_{q-1}, with those states between A and B, and C and D as initial conditions. The dangerous dissonance space on the dissonance space boundary (between X and Y) can then be identified with one more backward step, solving the set of differential equations $-\dot{\mathbf{x}}(t) = \mathbf{F}_{10}(\mathbf{x}(-t), \mathbf{u}(-t), \mathbf{d}(t), -t)$ at time τ_{q-1} with the states between J and K as initial conditions (Figure 5.9 (c)). The dangerous dissonance space is then that dissonant space that could be reached from the dangerous dissonance states between X and Y.

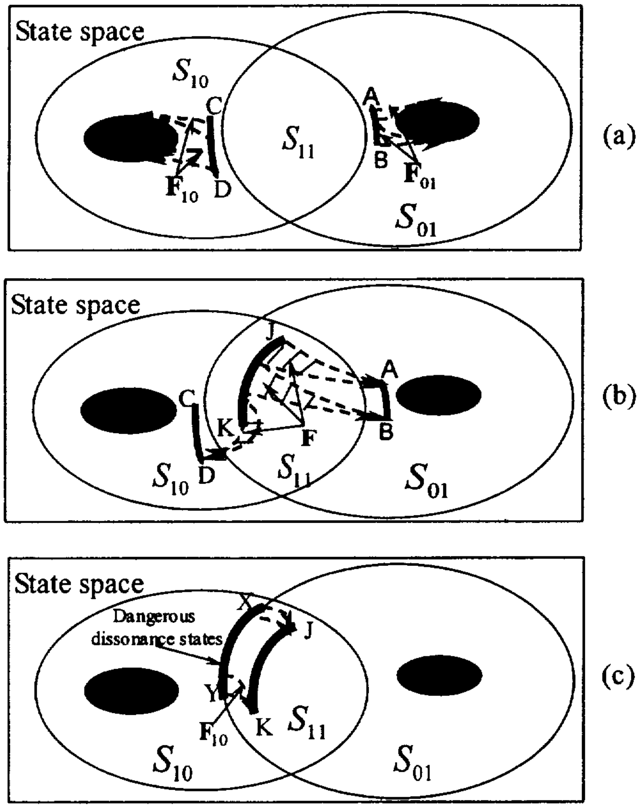


Figure 5.9: Identification of Dangerous Dissonance Space

After identifying dangerous dissonance space, the dangerous effect of dissonance now can be avoided through modifying one or both alerting system designs to eliminate the dangerous dissonance space. Due to restrictions on each system's performance requirements, if the alerting system design cannot be modified to eliminate the dangerous dissonance space, we need to identify what control procedures could be used to avoid the dangerous effects of dissonance. That is, we need to identify what is the subset of the differential operators in set **F** in dissonance space following which the hazard spaces could still be avoided. Or, we could determine what is the proper alerting system command that could avoid entering the dangerous dissonance space. These mitigation methods are presented in Chapter 6.

5.3 Summary

This chapter developed a hybrid model to describe the interactions between the discrete state of alerting systems and the continuous dynamics of the process incorporating multiple alerting systems. The concept of a transition function has been introduced to model the human operator's response to alerting system alerts individually and to the dissonant commands in dissonance space.

Because of the unpredictable response of a human operator to dissonance, the process could be led to hazards. That is, there would be a dangerous effect of dissonance. The concept of a dangerous dissonance state has been defined. The method has been developed to identify the dangerous dissonance space that includes all dangerous dissonance states in dissonance space.

As the dangerous dissonance space is being identified, the unsafe consequences of dissonance can be avoided by changing the logic design of the alerting systems to eliminate the dangerous dissonance space, or by restricting alerting system commands to avoid entering the dangerous dissonance space once in alert space, or by restricting the human operator's discrete control to avoid the hazard spaces once in dangerous dissonance space. These options are presented in Chapter 6 in more detail.

A similar method as used for dangerous effects of dissonance can also be used to avoid other negative effects of dissonance. For instance, inefficient dissonance space can be identified in which the human operator's response could cause the operation to become inefficient. Also restrictions could be given on the human operator's response (chosen from differential operators governing continuous dynamics) in inefficient dissonance space to guarantee that the process stays inside the efficient operating space.

Or the alerting system resolution advisories could be restricted in alert space to prevent the process from entering the inefficient dissonance space.

6. Avoiding and/or Mitigating Dissonance

As we stated in Chapter 5, when exposed to dissonance, the confused human operator may lead the process to an accident or suffer inefficient/unnecessary operation. The human operator may distrust the alerting system after several dissonant situations happened. So, dissonance should be avoided or mitigated, or at least, the dangerous consequences of dissonance should be avoided.

In this chapter, we suggest several ways to avoid or mitigate dissonance. Each way has its advantages and disadvantages. Mitigation methods should be chosen based on the specific performance requirement of the alerting system designs. Also, different mitigation methods may be required for different dissonance situations or under different circumstances for the same alerting systems.

6.1 Prioritization

To date, dissonance between automation has been largely managed through prioritization. Each alerting system can be prioritized, and if more than one alerting system is triggered, the lower priority alerts may be inhibited or only displayed passively (i.e., without separate attention-getting signals). Several complex prioritization schemes have been investigated for the various alerting systems on board an aircraft (Boucek, et al., 1981; Berson, et al., 1981).

The Ground Proximity Warning System (GPWS), for example, uses measurements of the height of the aircraft above terrain to predict whether there is a threat of collision with terrain. Traffic Alert and Collision Avoidance System (TCAS) warns the pilots to an immediate collision with other aircraft and provides escape commands and guidance. TCAS and GPWS, while alerting pilots of conditions outside the aircraft, are separate systems and are aimed at different specific conditions. When both TCAS and GPWS detect a hazard (other aircraft and terrain), only a GPWS alert will be presented to the pilot, since terrain is given a higher priority than other air traffic, with the rationale that all else being equal, it is less likely that an aircraft would collide with another aircraft than it would hit terrain.

In (Ververs, et al., 1999), alert prioritization was proposed to consider both the critical nature of the condition to maintaining a safe mission and the time until the condition is encountered. Each alert is prioritized into one of three categories using the dimensions identified in Figure 6.1 (Ververs, et al., 1999). The lines in the diagram are purely conceptual.

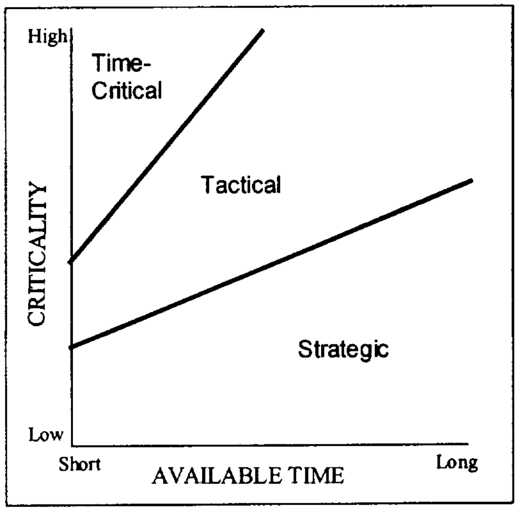


Figure 6.1 Alert Prioritization (Ververs, 1999)

As described in (Ververs, et al. 1999) for Figure 6.1, time-critical alerts are assumed to be highly critical, and need immediate attention of the flight crew, thus are put in highest priority. Time-critical alerts are defined to concern problems that lie within a 60-second time window. When a time-critical situation arises, the crew is presented with a correlated aural/visual alert that is designed to quickly direct their attention to the nature and location of the threat and also to command the pilot on what actions to take to evade the threat.

Tactical alerts, which are concerned with problems that may affect the mission within 10 minutes (Ververs, et al., 1999), are assumed to have less urgency than time-critical alerts, but still require the pilot's attention to the situation, and have a high probability of requiring pilot response in the near future. A repeating non-verbal aural alert is used to inform the crew that there is a tactical situation. In addition to the aural alert, corresponding visual information is provided to the crew that describes the nature of the alert in more detail.

Strategic alerts address problems that are at least 10 minutes away and those that are probabilistic, such as, a weather cell that is near the destination that is moving away from the airport or pilot reports of windshear. While this strategic information is important to the overall situation awareness of the crew for planning and informed decisions, the notification system for strategic information must be designed such that the crew does not have their current tasks interrupted, or be overloaded with new information. Therefore, subtle yet informative aural and visual alerts are needed to allow the crew to decide whether or not they will address the situation then, or at a later time, depending on their current workload.

The other way prioritization comes into play is to resolve a conflict within the threat levels themselves. We need to consider the criticality of the hazard within the levels. The most problematic hazard is considered to be the most critical one. For example, the effects of turbulence may be less critical than wind shear, so the alert for wind shear is put in higher priority than the alert for turbulence. Another example is that if two time-critical alerts get triggered - TCAS and GPWS, which one has higher priority? There is a prioritization assigned to each type of alert with time-critical alerts. In general, GPWS has a higher priority than TCAS with the reason that it is less likely that an aircraft would collide with another aircraft than it would hit terrain. Similarly, TCAS placed at a higher priority than convective weather. Within the other levels (tactical and strategic), the alerts are prioritized by the time they come into the queue with the most recent given the highest priority.

Prioritization can run into trouble, however, if two alerts are both valid but the operator is only receiving or responding to one. When TCAS and GPWS alerts are both valid, the probability of collision with other aircraft still exists when the pilot is taking a maneuver according to the GPWS command. Also, it would be difficult to "undo" an earlier alert if the higher-priority system acts later. For example, if GPWS gives a command to climb when the pilot is already taking a descent maneuver according to a previous TCAS alert, it may be hard for the pilot to mentally cancel the descent maneuver that is being taken. This may ultimately cause an accident. Finally, the prioritization schemes can be quite complex. Consider the fact that the number of warning displays increased from 188 on the Boeing 707 to over 450 on the Boeing 747 (Hawkins, 1987).

Still, prioritization can help reduce sensory and cognitive overload of the human during a time of high stress.

Prioritization is somewhat like modifying one of alerting system's designs to avoid dissonance (Figure 6.2), since one of the alerting systems is inhibited so that only one alert is effective in the dissonance space. But prioritization is not actually changing the internal alerting system threshold functions, as presented in the next section.

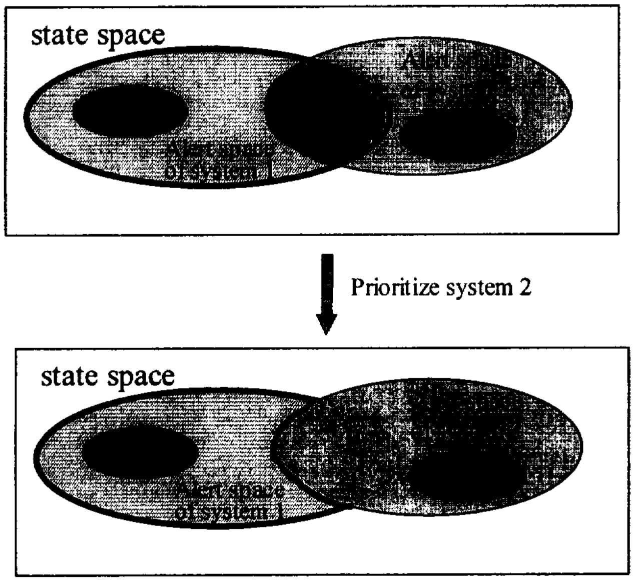


Figure 6.2 State-Space Representation of Prioritization (System 2 Placed at Higher Priority Than System 1)

6.2 Modify System Design

It may be necessary to modify the design of the alerting logic or algorithm in the new (or existing) alerting system to reduce the potential for dissonance as much as possible, especially those regions of dangerous dissonance space identified in Chapter 5.

If the threshold functions of alerting systems can be expressed explicitly in state space, given the conditions for dissonance space the threshold functions could be reshaped to eliminate the dissonance space or at least the dangerous dissonance space. But the reshaping of threshold functions may affect the satisfaction of other performance requirements.

For example, in Figure 6.3 (a), system 1 was designed to monitor some kind of hazard, which is presented as hazard space inside alert space of system 1 in state space representation, and system 2 was designed to avoid other kinds of hazard. There is dissonance space with the original alerting systems' threshold functions, where both systems alert but provide dissonant resolution advisories. If we change the threshold function of system 1 to eliminate dissonance space, the safety requirement of system 1 may not be able to be satisfied (Figure 6.3 (b)). That is, the original designed evading maneuver in new alert space of system 1 may not be able to avoid the monitored hazard, as the example shown in Figure 6.3 (b). If we change the threshold function of system 2 to eliminate the dissonance space, the safety requirement of system 2 may not be able to be satisfied (Figure 6.3 (c)).

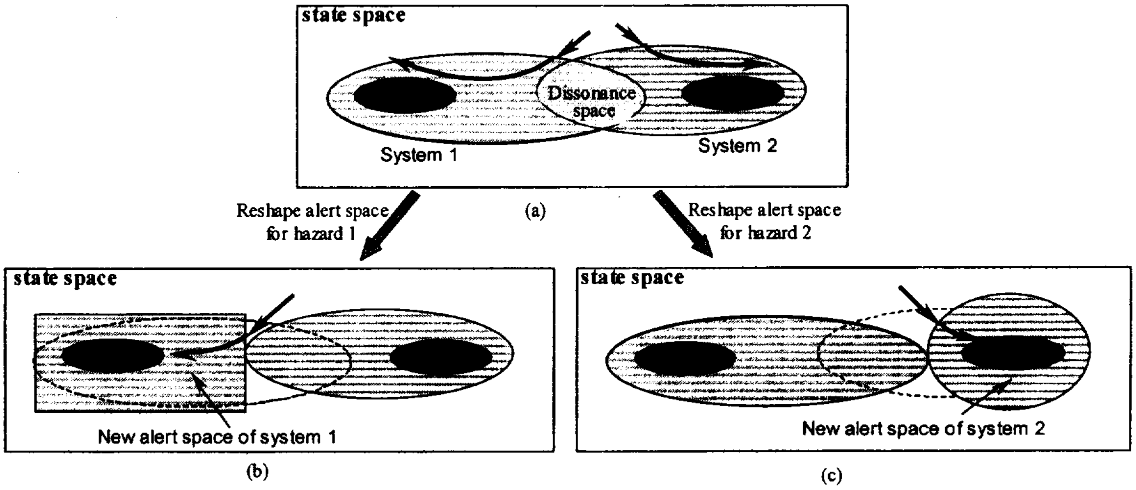

state space
Dissonance space
System 1
System 2
Reshape alert space for hazard 1
(a)
Reshape alert space for hazard 2
state space
New alert space of system 1
(b)
state space
New alert space of system 2
(c)

Figure 6.3 Reshape Threshold Functions to Eliminate Dissonance Space

Designing an alerting system to compromise with other alerting systems can be considered a multi-objective optimization problem. The multi-objective optimization problem is to find the optimum that maximizes or minimizes a multitude of objectives subject to a number of constraints and bounds.

$$\min_{\mathbf{x}\in\mathbf{R}^n} \mathbf{G}(\mathbf{x}) = [g_1(\mathbf{x}),\ldots,g_i(\mathbf{x}),\ldots,g_m(\mathbf{x})]^T \tag{6.1}$$

Subject to

$$h_i(\mathbf{x}) = 0 \quad i = 1,\ldots,q \tag{6.2}$$

$$r_j(\mathbf{x}) \le 0 \quad j = 1,...,p \tag{6.3}$$

$$x_k^l \le x_k \le x_k^u \quad k = 1,...,n \tag{6.4}$$

Where the components of the objective function vector, $\mathbf{G}(\mathbf{x}) = [g_1(\mathbf{x}),...,g_i(\mathbf{x}),...,g_m(\mathbf{x})]^T$, are usually incommensurate and in conflict with one another with respect to their minimum points. For the example shown in Figure 6.3, the objective function vector could have three components: $g_1(\mathbf{x})$, minimizing the probability of dissonance, $g_2(\mathbf{x})$, minimizing the probability of missed detection of hazard 1, and $g_3(\mathbf{x})$, minimizing the probability of missed detection of hazard 2. These three components are in conflict with one another as shown in Figure 6.3. The design vector, $\mathbf{x} = [x_1,...,x_k,...,x_n]^T$, consists of all design variables in the problem may be bounded in Equation (6.4). The collection of equality constraints, $\mathbf{H}(\mathbf{x}) = [h_1(\mathbf{x}),...,h_i(\mathbf{x}),...,h_q(\mathbf{x})]^T$, is an equality constraint vector, and similarly the inequality constrain vector, $\mathbf{R}(\mathbf{x}) = [r_1(\mathbf{x}),...,r_j(\mathbf{x}),...,r_p(\mathbf{x})]^T$. For the example shown in Figure 6.3, the safety requirement for both systems can be expressed as equality and/or inequality constraints of some design variables (for instance, range and range rate between two vehicles).

Given the condition for dangerous dissonance space, mitigating dangerous dissonance space can be introduced as a component of the objective function vector in multi-objective problem. That is, one objective is to minimize the size of the dangerous dissonance space or the probability of dangerous consequences of dissonance. It also can be introduced as components of equality and/or inequality constraint vectors.

Since the components of the objective function vector are competing in general, there is generally no unique solution to this problem. The purpose of this problem is to search for a best compromise solution to ensure objectives are close to their corresponding preference points as much as possible. For the example shown in Figure 6.3, the safety and elimination of dissonance space may compete against each other, but we can search for the best solution to ensure these objectives are close to their corresgponding preference points.

6.3 Modify Operational Procedures to Avoid Dissonance

As long as the conditions for dissonance between alerting systems have been identified, it may be possible to modify the operation of the process so that dissonance is unlikely to occur. One means of trying to ensure compatibility of a parallel approach alerting system with TCAS, for example, is to modify air traffic control procedures to decrease the likelihood of a simultaneous TCAS alert and parallel traffic alert. That is, giving restrictions to other departing and arriving aircraft when two aircraft are parallel approaching, so that if a blunder happens, the evading trajectory won't trigger TCAS alerts. The identified conditions for dissonance can be used as restrictions to other departing and arriving aircraft.

A request to pilots to reduce their vertical speed as the aircraft nears a target altitude, for example, is one operational change that has already been made to help reduce the likelihood of dissonance between TCAS false alarms and air traffic controllers. For example, in Figure 6.4, aircraft A is descending to some target altitude above the aircraft B. The high descent rate of aircraft A may trigger a TCAS alert and command aircraft B to climb, which is a false alarm and may cause collision after aircraft B climbs and aircraft A levels off. This is an observed common source of dissonance between air traffic controllers and TCAS. The solution that has been put in place is to train pilots to reduce vertical speed when approaching their assigned altitude.

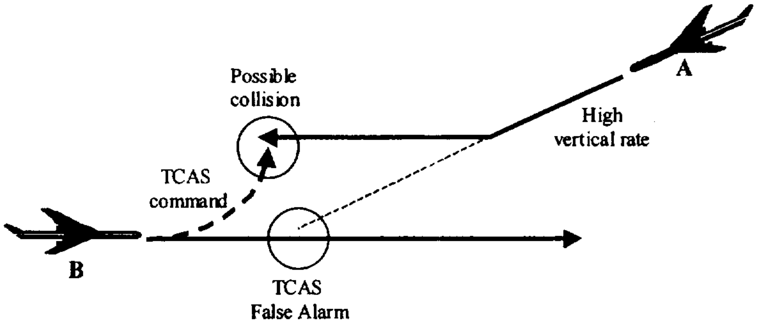


Figure 6.4 Reduce Vertical Speed to Avoid Dissonance

6.4 Modify Control Strategy

After identifying dangerous dissonance space using the hybrid model developed in Chapter 5, the dangerous effect of dissonance can be avoided by modifying the control strategy of the process. That is, we can identify the subset of the differential operators of set $\mathbf{F}$ in dissonance space, following which the hazard spaces can be avoided; or the proper alerting system command that could avoid entering the dangerous dissonance space.

With the dangerous dissonance states as initial conditions, and the states between A and B, and C and D (Figure 6.5) as the target states, the subset $\mathbf{F}_D$ of the differential operators set $\mathbf{F}$ in dissonance space can be identified, following which the hazard space can not be avoided. Then the subset $\mathbf{F}-\mathbf{F}_D$ includes differential operators in dangerous dissonance space that will avoid the hazard spaces. Thus, if the dangerous dissonance space can not be eliminated in the alerting system design, then human operators can be given certain operating command in dangerous dissonance space such that the continuous dynamics would be given by the differential operators in set $\mathbf{F}-\mathbf{F}_D$.

Figure 6.5 shows an example of restricted trajectories in dangerous dissonance space to avoid the hazards. Given a dangerous dissonance state P, part of the original restricted set of trajectories intersects the states between A and B, which will lead the process to the hazard space. After identifying the dangerous subset $\mathbf{F}_D$ of the original differential operators set $\mathbf{F}$ in dissonance space, the trajectories governed by those differential operators in subset $\mathbf{F}-\mathbf{F}_D$ (e.g., turn right at least 30 degrees or turn left at least 25 degrees) would be able to avoid both hazards monitored by both alerting systems.

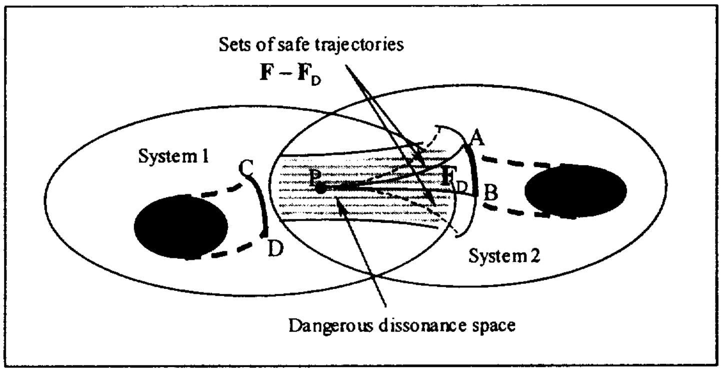

Sets of safe trajectories
$\mathbf{F}-\mathbf{F}_D$
System 1
C
D
P
$\mathbf{F}_D$
A
B
System 2
Dangerous dissonance space

Figure 6.5 Restricted Trajectories in Dangerous Dissonance Space to Avoid Hazards

Another way to avoid the dangerous effect of dissonance is to modify the alerting system command (the allowed action space) such that the continuous dynamics in alert space of each alerting system would not hit dangerous dissonance space. With the alert space boundary of each alerting system as initial conditions, and the dangerous dissonance states as target states, the subset of differential operators in alert space $\mathbf{F}_{mn\mathrm{D}}$ can be identified, following which the continuous dynamics would hit the dangerous dissonance space. Then the continuous dynamics given by any differential operator in set $\mathbf{F}_{mn} - \mathbf{F}_{mn\mathrm{D}}$ can avoid the dangerous dissonance space, and thus the dangerous effect of dissonance space.

Figure 6.6 shows an example of modified evading trajectories. Given an alert state P in alert space of system 1, the original set of evading trajectories according to the alerting system's resolution advisories (e.g., turn left at least 10 degrees) is entering the dangerous dissonance space. After modifying the resolution advisories (e.g., turn left at least 30 degrees), the corresponding evading trajectories governed by any differential operator in set $\mathbf{F}_{mn} - \mathbf{F}_{mn\mathrm{D}}$ would be able to avoid both hazards monitored by both alerting systems since it is not entering the dangerous dissonance space.

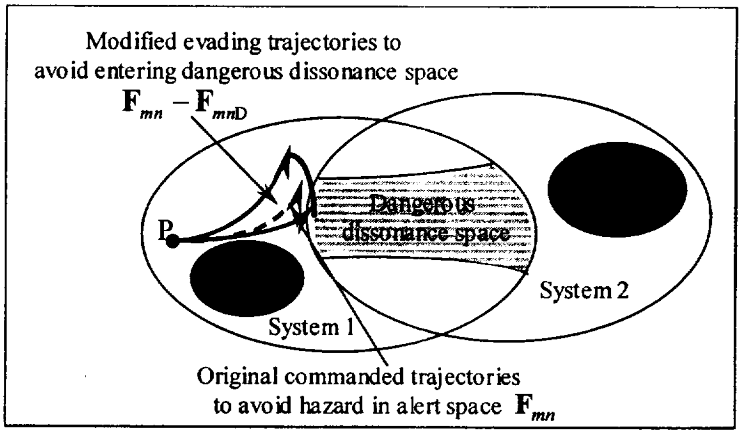

Modified evading trajectories to avoid entering dangerous dissonance space
$\mathbf{F}_{mn} - \mathbf{F}_{mn\mathrm{D}}$
P
Dangerous dissonance space
System 2
System 1
Original commanded trajectories to avoid hazard in alert space $\mathbf{F}_{mn}$

Figure 6.6 Modify Evading Trajectories to Avoid Unsafe Effect of Dissonance

6.5 Modify Procedures Under Dissonance

A final way to mitigate dissonance between alerting systems is through procedures for responding to dissonance. The human operators can be trained to know exactly how the alerting systems work. Then if any dissonance happens, they know why it happened and how to deal with it. Pilots are trained, for example, that EGPWS and GPWS use different decision-making logic, and that alerts from the two systems may not occur in concert.

Dissonance may still be perceived if the logic or sensor error differences result in situations different from the trained situation. Continuing EGPWS and GPWS as the example, EGPWS is designed to provide an earlier warning of terrain proximity than GPWS. Should this happen, there is no perceived dissonance for the trained pilots. But if the opposite occurred, there may be perceived dissonance because the pilot may not understand why EGPWS does not rate the terrain as a threat while GPWS does.

In more severe cases, however, training may fall short. For instance, two accidents of Boeing B757 aircraft in 1996 (the first near Puerto Plata, Dominican Republic, and the second near Lima, Peru) involved simultaneous, dissonant alerts in the cockpit. Both accidents were caused by clogged air data systems that resulted in alerts that the aircraft was flying too fast (from one system) and too slow (from a second, independent system). This led to significant confusion in the cockpit as to which alert to believe, and ultimately led to the accidents.

The control strategy may not have to be modified in system design as we described in section 6.4 as long as the safe set of maneuvers is identified. The human operator could be trained to take a safe maneuver in dangerous dissonance space (for example, turning at least 30 degrees) such that the continuous dynamics would be given by the differential operators in set $\mathbf{F}-\mathbf{F}_D$, which can avoid hazards although the process has been in dangerous dissonance space.

6.6 Summary

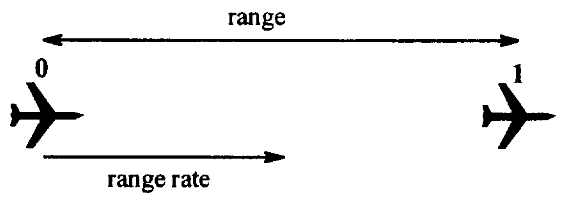
In this chapter, several methods to avoid or mitigate dissonance were suggested from different points of view. Each of these methods has its own advantages and disadvantages. The mitigation method should be chosen depending on the characteristics of different alerting systems and different kinds of dissonance situations. There is no absolute best solution for all dissonance situations. To actually select mitigation method requires more information on the frequencies of the dissonance, the effects of dissonance on human operators, and the cost of each mitigation method, etc.

Each of these mitigation methods incurs some costs as far as overall system performance is concerned. For example, prioritization and inhibition essentially hide part of the available information from the operator. This reduces the benefit of having the additional alerting system components, since their information is not transmitted to the operator. Reducing the likelihood of dissonance by modifying the process' operation (e.g., increasing separation between vehicles to reduce alert probability) may decrease overall system capability. Finally, modifying the design of the logic is complex, costly, and may have other negative impacts on system performance. To minimize these negative effects, mitigation strategies should only be employed where necessary. That is one reason why we need to identify the dangerous dissonance space from Chapter 5. Methods should be chosen to mitigate those negative effects of dissonance with the least overall cost to system performance.

7. Example Application: In-Trail Spacing

In this chapter, we use a conceptual In-Trail separation example to demonstrate the framework of dissonance modeling and analysis we developed in previous chapters. We are then interested to identify when and where dissonance could occur through formally describing the threshold functions of the alerting systems involved; identify the dissonance originating from the sensor errors and compare it with the contribution of logic differences; identify the dangerous dissonance space by establishing a hybrid model of the process; and apply the methods outlined in Chapter 6 to avoid or mitigate dissonance.

Consider a simplified one-dimensional problem in which the in-trail separation of two vehicles is monitored by two independent alerting systems placed in the trailing vehicle. As a baseline, assume that system 1 is set up to issue an alert if the two vehicles get too far apart. An alert from system 1 would command the trailing operator to accelerate to reduce the separation between vehicles, to satisfy a requirement of spacing. System 2 is set up to alert if the vehicles are projected to be too close within some amount of time, or if the vehicles are very close together and not diverging fast enough. An alert from system 2 would command the trailing operator to decelerate and increase separation, to satisfy a safety requirement (Figure 7.1). The leading vehicle (vehicle 1) follows some path open-loop, while the trailing vehicle (vehicle 0) may receive alerts to speed up or slow down to maintain spacing.



System 1: Command aircraft 0 to accelerate if range > threshold

System 2: Command aircraft 0 to decelerate if time to impact < threshold

Figure 7.1 In-Trail Example

It is a conceptual example since the dynamics of the process and the threshold functions of two alerting systems are much simpler than a real system. However, through this example, we can demonstrate all the dissonance issues presented in the previous chapters and apply the modeling and analysis tools we developed to analyze and mitigate the dissonance.

Although it is a conceptual example, there are real applications in the air traffic control area. Increased demand for air travel translates into a need to accommodate more aircraft in the terminal airspace. Separation between aircraft pairs must be small enough to be efficient while remaining sufficiently large to be safe. Researchers have investigated the feasibility of performing in-trail spacing by pilots, and pilots suggested technology enhancements such as display of other aircraft airspeed or automated speed-up/slow-down cues (Pritchett & Yankosky, 2000).

7.1 Dissonance Originating from Logic Differences

In this example, the positions and velocities of the two vehicles make up the complete state space:

$$\mathbf{x} = [x_0, x_1, \mathrm{v}_0, \mathrm{v}_1]^{\mathrm{T}} \tag{7.1}$$

where $[x_0, \mathrm{v}_0]^{\mathrm{T}}$ is the state of the trailing (own) aircraft, and $[x_1, \mathrm{v}_1]^{\mathrm{T}}$ is the state of the front (other) aircraft.

System 1 measures only the range between the vehicles, while system 2 uses both the range and range rate. So,

$$\mathbf{y}_1 = [r] = [x_1 - x_0] = G_1\mathbf{x}$$

$$\mathbf{y}_2 = [r,\ \dot{r}]^{\mathrm{T}} = [x_1 - x_0,\ \mathrm{v}_1 - \mathrm{v}_0]^{\mathrm{T}} = G_2\mathbf{x} \tag{7.2}$$

This example has a simple, binary alert stage for each system: 0 or 1. System 1 alerts ($\mathbf{a}_1 = 1$) when the range between vehicles is greater than a threshold distance R_1. In the notation we have developed, predicates (or inequalities) denoted f_{ij} are defined to divide the state space into subsets. When the state is inside the subset, the predicate is true; when outside, the predicate is false. Combinations of these subsets then form the alert stage space within the universe of the state space, **U**. Each resulting subset is denoted A_{ik} for the k^{th} alert stage of system i. So, for system 1, an alert occurs when the state is in region A_{11}. The threshold function is then formally defined as:

$$T_1 = \begin{cases} f_{11} : r > R_1 \\ A_{11} = f_{11} \\ A_{10} = \mathbf{U} - A_{11} \end{cases} \tag{7.3}$$

According to equation (7.3), an alert is issued (state is in A_{11}) when condition f_{11} is true; this is equivalent to $r > R_1$. Otherwise, the state is in region A_{10}, which indicates that system 1 is in alert stage 0.

System 2 alerts ($\mathbf{a}_2 = 1$) when the vehicles are converging and projected to be less than a range R_2 apart within τ seconds, or if they are close together and diverging but at a slow rate ($r\dot{r} < H$, where H is some constant). So, four predicates are needed to separate the alert space A_{21} from the universal state space U,

$$f_{21} : \dot{r} < 0 \tag{7.4}$$

$$f_{22} : \frac{r - R_2}{-\dot{r}} < \tau \tag{7.5}$$

$$f_{21} : r\dot{r} < H \tag{7.6}$$

$$f_{24} : r < R_2 \tag{7.7}$$

This is similar to the logic used by TCAS (RTCA, 1983). Thus, for system 2, the threshold function is formally defined as:

$$T_2 = \begin{cases} f_{21} : \dot{r} < 0 \\ f_{22} : \dfrac{r - R_2}{-\dot{r}} < \tau \\ f_{23} : r\dot{r} < H \\ f_{24} : r < R_2 \\ A_{21} = (f_{21} \cap f_{22}) \cup (f_{23} \cap f_{24}) \\ A_{20} = \mathbf{U} - A_{21} \end{cases} \tag{7.8}$$

Figure 7.2 shows the two alerting systems' alert spaces in the two-dimensional y space of r and $\dot{r}$. A "+" has been added to the active alert stage in the diagram for system 1 to emphasize that an alert from that system commands the trailing operator to increase speed. A "0" implies that no command or guidance information is displayed by the alerting system. A "–" is used to show where a command to reduce speed would be given by system 2.

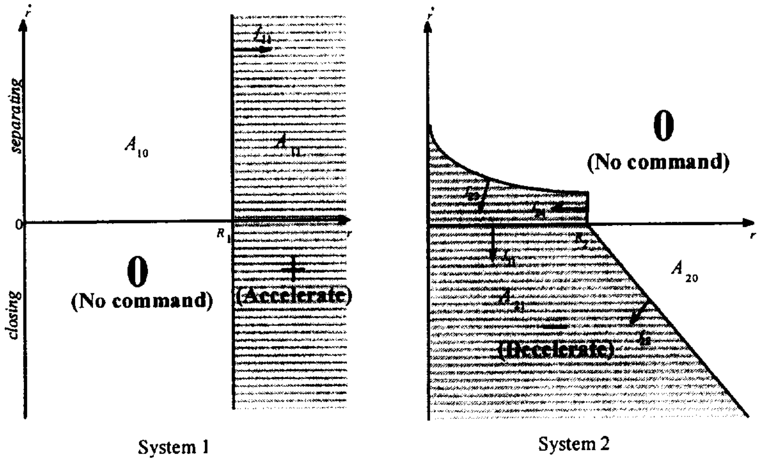


Figure 7.2: Example In-Trail Separation Alert Stage Mapping

7.1.1 Possible Perceived Dissonance

Having set up the basic alert stage regions in state space, we can analyze the two systems together as shown in Figure 7.3. We assume that the range threshold for efficient operation would be larger than the range threshold for the safety requirement, that is, $R_1 > R_2$. When the two systems are combined, the intersections of their alert stages are denoted by the sets S_{mn} where m is the alert stage from system 1 and n is the alert stage from system 2:

$$S_{mn} = A_{1m} \cap A_{2n} \tag{7.9}$$

There are four possible combinations of alert spaces between the two systems: $S_{00} = A_{10} \cap A_{20}$, $S_{01} = A_{10} \cap A_{21}$, $S_{10} = A_{11} \cap A_{20}$, and $S_{11} = A_{11} \cap A_{21}$. To help identify potential dissonance, the "+", "–", or "0" notations from Figure 7.2 have been carried through in Figure 7.3. The notation, "+0", for example, indicates that system 1 commands an acceleration while system 2 does not display any command information.

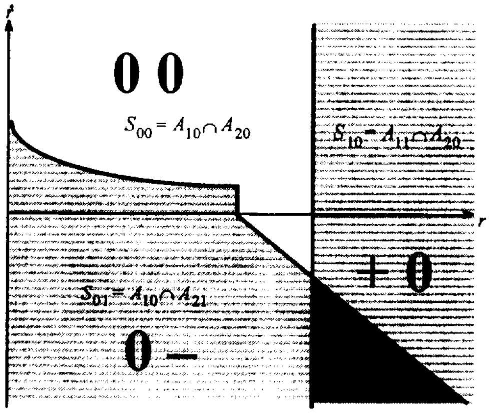

$\dot{r}$
0 0
$S_{00} = A_{10} \cap A_{20}$
$S_{10} = A_{11} \cap A_{20}$
r
+ 0
$S_{01} = A_{10} \cap A_{21}$
0 –

Figure 7.3: Combined In-Trail Alert Stages

To better visualize the potential perceived dissonance, consider Figure 7.4, which shows the one-dimensional space of potential acceleration actions by the trailing vehicle for each alerting condition. Assume there is some limit on the potential acceleration of the vehicle, $a_{\max}$. If System 1 is not alerting, then the operator is conceivably allowed to apply any acceleration he or she may desire within that acceleration limit. Thus, stage A_{10} can be thought of mapping to the action space [$-a_{\max}$ $a_{\max}$]. If System 1 does alert, then the operator should accelerate the trailing vehicle above $a_{\min}$. This corresponds to the action space [$a_{\min}$ $a_{\max}$]. Similar mappings can be made for System 2. System 2 has the same action space as System 1 if there is no alert. However, an alert from System 2 commands the trailing vehicle to decelerate with the magnitude of the deceleration above $a_{\min}$, corresponding to action space [$-a_{\max}$ $-a_{\min}$].

With this notation, then, it is possible to observe perceived dissonance situations. For example, S_{11} is a perceived dissonance region because the intersection of the two systems' action spaces { [$a_{\min}$ $a_{\max}$] and [$-a_{\max}$ $-a_{\min}$]} is empty. That is, the two systems are issuing contradictory resolution commands (one to accelerate, the other to decelerate). The condition for this perceived dissonance space is,

$$S_{11} = f_{11} \cap f_{21} \cap f_{22} = \{(r,\dot{r}) \mid \dot{r} < 0, r > R_2, \frac{r - R_2}{-\dot{r}} < \tau\} \qquad (7.10)$$

Regions S_{01} and S_{10} would probably not be perceived as dissonance, because the intersection of their action spaces is not empty. Although there is a disagreement in alert stages in S_{01} and S_{10}, the two systems have different roles and so would not be expected to operate simultaneously. So, "+0" or "0–" conditions would likely be acceptable.

The "+ –" dissonance in region S_{11} could be quite problematic. This corresponds to a case in which the vehicles are rather far apart but closing rapidly. The operator receives one alert to accelerate (from system 1) while system 2 is simultaneously commanding the operator to decelerate. Depending on the relative strengths with which these commands are issued, the operator may be uncertain as to the correct action to take.

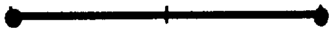
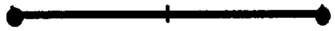
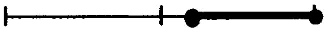
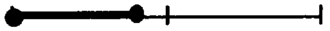
	System 1	System 2
No Alert	*acceptable acceleration range*  $-a_{max}$ 0 a_{max} A_{10}	*acceptable acceleration range*  $-a_{max}$ 0 a_{max} A_{20}
Alert	*acceptable acceleration range*  $-a_{max}$ 0 a_{min} a_{max} A_{11}	*acceptable acceleration range*  $-a_{max}$ $-a_{min}$ 0 a_{max} A_{21}

Figure 7.4 Action Spaces for Alerting Situations

7.1.2 Dynamic Analysis

The analysis above for dissonance does not completely describe the interactions between the two systems. It is also necessary to examine the process dynamics to see how dissonance may evolve over time.

Here, we assume two aircraft are flying on the same straight line, so the thrust T_0 is the only control input. To simplify the case study, we assume that the front aircraft does not change its velocity, and the trailing aircraft changes velocity constantly according to each system's alert space. A Point-Mass equation of motion is adequate to analyze dissonance in this case.

Thus, the dynamics of the whole process for this one-dimensional case can be described as

$$\dot{x}_0 = v_0$$

$$\dot{x}_1 = v_1$$

$$\dot{v}_0 = T_0 / m_0 \tag{7.11}$$

$$\dot{v}_1 = 0$$

where m_0 is the mass of the trailing aircraft.

For this example, we can get **x**(t) by integration, that is,

$$x_0(t) = x_0(0) + v_0(0)t + \frac{1}{2}a_0 t^2$$

$$x_1(t) = x_1(0) + v_1(0)t + \frac{1}{2}a_1 t^2 \tag{7.12}$$

$$v_0(t) = v_0(0) + a_0 t$$

$$v_1(t) = v_1(0) + a_1 t$$

With $a_0 = T_0 / m_0$, $a_1 = 0$, and the initial state $[x_0(0), v_0(0)]^T$ for the trailing aircraft and $[x_1(0), v_1(0)]^T$ for the front aircraft.

In observable state space $(r, \dot{r})$, the trajectory of the process is given by

$$r(t) = r_0 + \dot{r}_0 t + \frac{1}{2}(a_1 - a_0)t^2 \tag{7.13}$$

$$\dot{r}(t) = \dot{r}_0 + (a_1 - a_0)t \tag{7.14}$$

Where $r_0 = x_1(0) - x_0(0)$ and $\dot{r}_0 = v_1(0) - v_0(0)$. Now, we can analyze the dissonance situation on $(r, \dot{r})$ state space by examining the trajectories as time changes.

In this case, there is a specific physical coupling between the range and range-rate states, meaning that only certain trajectories are possible. Specifically, it is impossible to enter region S_{11} from the left; by definition, the negative range rate indicates that the range must be decreasing. So, the only way in which dynamic dissonance can occur is for the range to be decreasing at a large rate while in region S_{10}. In a specific problem, the possible trajectories in the S_{mn} diagram can be examined to determine whether it is possible to have the large range and closure-rates needed to enter region S_{11}.

As an example dynamic analysis, Figure 7.5 overlays several potential state trajectories on the state space diagram. Assume that the process dynamics are such that the relative speed between vehicles can be increased or decreased by an acceleration of no more than a certain amount. Starting at the state denoted **A** in Figure 7.5, for example, the future state trajectory must lie somewhere between the parabolic curves shown.

Consider now starting at state **B**. Here, the vehicles are diverging and the state has just entered region S_{10}. The trailing operator receives an alert from system 1 to speed up and decrease spacing. If the vehicle is accelerated at its limit, the state will follow the trajectory shown, just crossing past region S_{11} through point **C**. If a lower magnitude of acceleration were used, the trajectory would lie to the right of that shown and could therefore enter region S_{11}.

The transition from region S_{10} to S_{01} that occurs at point **C** may initially appear to be a case of dissonance. As Figure 7.6 shows, however, when transitioning from S_{10} to S_{01}, there is a similar trend in the action spaces from each system suggesting a deceleration. This implies that such a transition may not be perceived as dissonant since the operator will have a consistent change in the acceleration level to apply.

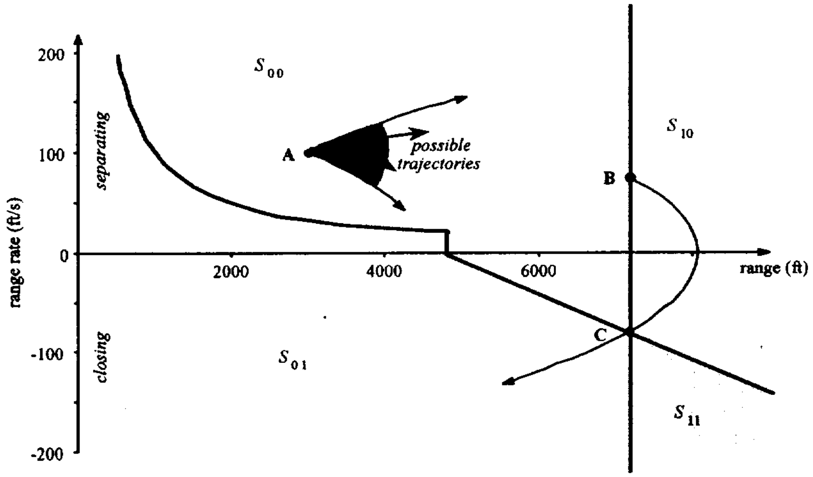


Figure 7.5 Dynamical Trajectory Analysis

Similar dynamic analyses could be performed under different conditions and assumptions. The general approach, however, is one in which potential paths through the different alerting regions can be explored. This identifies what conditions may lead to perceived dissonance. Additional effort can then be focused on those conditions to determine how likely they are, the impact of the dissonance, and to develop countermeasures to reduce the effect of the dissonance on operator performance.

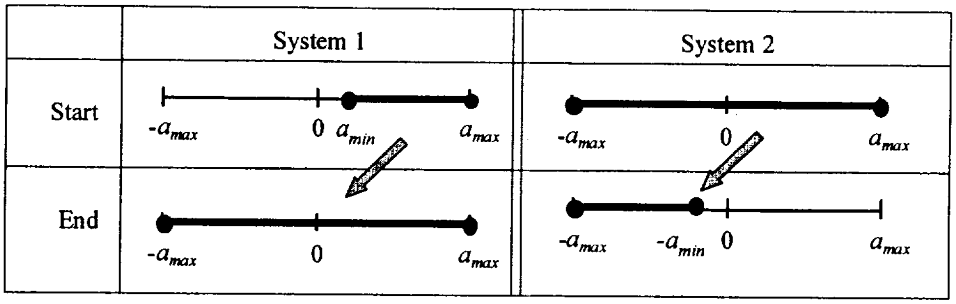


Figure 7.6 Dynamic Changes in Alerting Actions From S_{10} to S_{01}

7.2 Dissonance Originating from Sensor Error

In the dissonance analysis of the previous section, we did not consider any measurement error of the observable states, range and range rate. For a real alerting system, sensor error always exists at some level. When two alerting systems use different sensors to monitor the process, even if they have the same alerting threshold function or resolution logic, they may be in different alert stages due to sensor error.

Considering the measurement error of measured states for both systems in this In-Trail example, we are interested to identify the dissonance originating from sensor error, and compare it with the dissonance originating from logic differences.

7.2.1 Threshold Function Distribution with the Measurement Error

Continuing the previous In-Trail example, system 1 measures only the range between the vehicles, while system 2 uses both the range and range rate. Suppose the measurement noises are normally distributed with zero mean and standard deviation $\sigma_{n_{r1}}$ for system 1 and $\sigma_{n_{r2}}$, $\sigma_{n_{\dot{r}2}}$ for system 2.

To examine the effect of error magnitude on dissonance, we use a generalized sensor error model, with a single parameter to represent system-wide sensor accuracy (Figure 7.7). That is, we assume

$$\sigma_{n_{r1}}^{2} = \sigma_{n_{r2}}^{2} = K^{2} \qquad (7.15)$$

and

$$\sigma_{n_{\dot{r}_2}}{}^2 = (K/100)^2 \tag{7.16}$$

Thus, a single parameter K is used to represent system-wide accuracy.

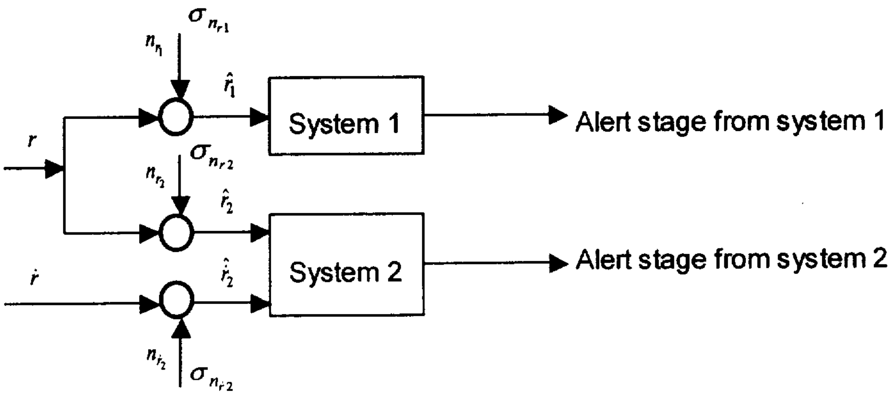


Figure 7.7 Example Sensor Error Model

For system 1, the threshold function is $r = R_1$. So, for a given normally distributed noise of the measurement with standard deviation $\sigma_{n_{r1}}$, we can recast the problem into one in which $\hat{r}_1$ is normally distributed with mean $m_{\hat{r}_1} = R_1$ and standard deviation $\sigma_{\hat{r}_1} = \sigma_{n_{r1}}$.

For system 2, consider the function $\frac{r - R_2}{-\dot{r}} = \tau$, that is, $r + \dot{r}\tau = R_2$. Let $s = r + \dot{r}\tau$, then if $\mathbf{y} = [r \quad \dot{r}]^T$,

$$s = [1 \quad \tau]\begin{bmatrix} r \\ \dot{r} \end{bmatrix} = \mathbf{Ay} \tag{7.17}$$

s is a linear function of range and range rate. So the mean of *s* can be expressed as

$$m_s = \mathbf{Am}_\mathbf{y} = [1 \quad \tau]\begin{bmatrix} m_{\hat{r}_2} \\ m_{\hat{\dot{r}}_2} \end{bmatrix} = m_{\hat{r}_2} + m_{\hat{\dot{r}}_2}\tau \tag{7.18}$$

Where $m_{\hat{r}_2}$ and $m_{\hat{\dot{r}}_2}$ are equal to the measurement given by system 2, $\hat{r}_2$ and $\hat{\dot{r}}_2$. We assume that range and range rate are not correlated, so the covariance of *s* can be obtained from the following operation,

$$\sigma_s^{\,2} = \begin{bmatrix} 1 & \tau \end{bmatrix} \begin{bmatrix} \sigma_{\hat{r}_2}^{\,2} & 0 \\ 0 & \sigma_{\hat{\dot{r}}_2}^{\,2} \end{bmatrix} \begin{bmatrix} 1 \\ \tau \end{bmatrix} = \sigma_{\hat{r}_2}^{\,2} + \sigma_{\hat{\dot{r}}_2}^{\,2} \tau^2 \qquad (7.19)$$

where $\sigma_{\hat{r}_2} = \sigma_{n_{r2}}$, and $\sigma_{\hat{\dot{r}}_2} = \sigma_{n_{\dot{r}2}}$. Thus, we can obtain the redistribution the alert stage boundaries in negative range rate state space (Figure 7.8).

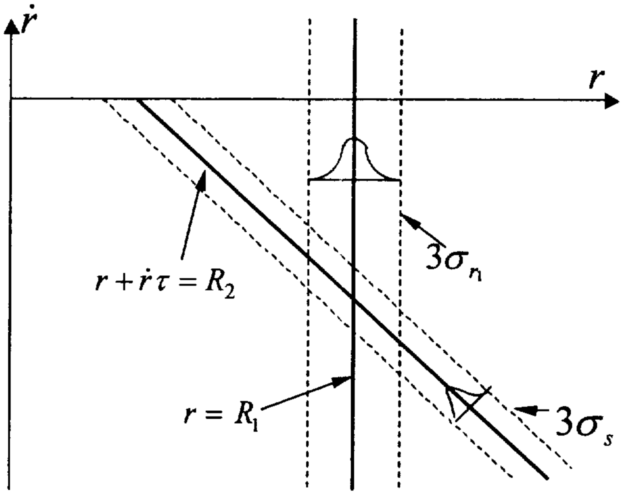


Figure 7.8 Threshold Boundary Change Due to Sensor Error

7.2.2 Contribution of Sensor Error to Dissonance

As explained in Section 7.1, S_{11} is a perceived dissonant region, where the two systems are issuing contradictory resolution commands (one to accelerate, the other to decelerate). Here, we want to identify the contribution of sensor error to this conflict resolution command dissonance, and compare it with the contribution of logic differences.

For this example, we examine three different cases. First, for a given true state, we identify the probability of that the measurement of the true state will result in dissonance, and how the probability of dissonance changes as the measurement accuracy (K) changes. Second, for a given complete true state trajectory, we identify the cumulative probability of dissonance along the given trajectory. Finally, if the trajectory is uncertain for a given initial state, we identify the overall cumulative probability of dissonance for a set of possible trajectories, and how the sensor accuracy affect the probability of dissonance.

Given a true state $(r, \dot{r})$, the probability of the true state causing a system 1 alert is:

$$P_{11}(r) = \int_{R_1}^{\infty} \frac{1}{\sqrt{2\pi\sigma_{\hat{r}_1}^2}} \exp\{-\frac{1}{2\sigma_{\hat{r}_1}^2}(\xi - r)^2\} d\xi \tag{7.20}$$

And the probability of the true state causing system 2 alert is:

$$P_{21}(r, \dot{r}) = \int_{-\infty}^{R_2} \frac{1}{\sqrt{2\pi\sigma_s^2}} \exp\{-\frac{1}{2\sigma_s^2}(\xi - r - \dot{r}\tau)^2\} d\xi \tag{7.21}$$

And since the measurements from two systems are independent, the probability of dissonance would be $P_{S_{11}} = P_{11} \times P_{21}$.

Thus, for a given true state, the probability of dissonance

$$P(D \mid \mathrm{y}) = P_{11} \times P_{21} \tag{7.22}$$

where P_{11} and P_{21} are as stated above.

If the range and range rate estimate errors are correlated with some correlation coefficient e ($0 \le e \le 1$), then

$$\sigma_s{}^2 = \begin{bmatrix} 1 & \tau \end{bmatrix} \begin{bmatrix} \sigma_{\hat{r}_2}{}^2 & e\sigma_{\hat{r}_2}\sigma_{\hat{\dot{r}}_2} \\ e\sigma_{\hat{r}_2}\sigma_{\hat{\dot{r}}_2} & \sigma_{\hat{\dot{r}}_2}{}^2 \end{bmatrix} \begin{bmatrix} 1 \\ \tau \end{bmatrix} = \sigma_{\hat{r}_2}{}^2 + \sigma_{\hat{\dot{r}}_2}{}^2\tau^2 + 2e\tau\sigma_{\hat{r}_2}\sigma_{\hat{\dot{r}}_2} \tag{7.23}$$

we can still obtain the probability of dissonance through (7.22).

If we do not know the correlation coefficient or if system 1 is correlated with system 2, given a true state, we can run a Monte Carlo Simulation to obtain the ratio of the measured state being in dissonance space, which is the probability of dissonance for the true state.

In this example, the alerting system threshold parameters are given in Table 7.1, which is similar to TCAS TA threshold parameter values set assuming two aircraft are at an altitude of 20,000 ft (RTCA 1983)

Table 7.1

Alerting System Threshold Parameters

	System 1	System 2
Threshold function	$r = R_1$	$r + \dot{r}\tau = R_2$
Parameters	$R_1 = 7050ft$	$R_2 = 4650ft$, $\tau = 25s$

Thus, for example, the true state $\mathbf{y} = [r \quad \dot{r}]^T = [7100ft \quad -97ft/s]^T$ is in space S_{10} (Figure 7.9). That is, system 1 will give an alert but system 2 will not alert. But with the sensor error, when K=30ft, the probability of dissonance for this given true state is 0.2. Figure 7.9 also shows the probability of dissonance contours when K=30ft.

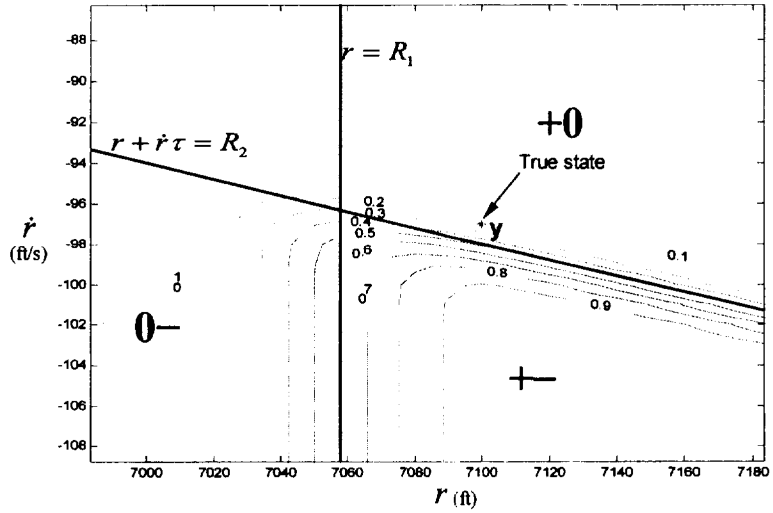


Figure 7.9 Probability of Dissonance for a True State (K=30ft)

Now, when the sensor accuracy becomes worse, that is, as the value of K increases, the probability of dissonance for the given true state increases. For our example, $\mathbf{y} = [7100ft \quad -97ft/s]^T$, when K=100ft, the probability of dissonance for this true state is increased to 0.28 (Figure 7.10). The probability of dissonance contours also change.

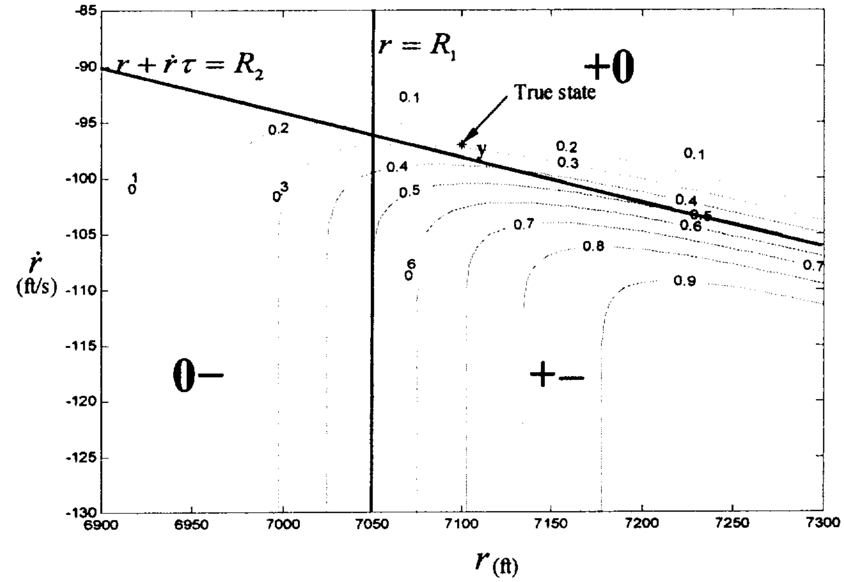


Figure 7.10 Probability of Dissonance for a True State (K=100ft)

Figure 7.11 shows how the probability of dissonance for this given true state changes with a change in sensor accuracy.

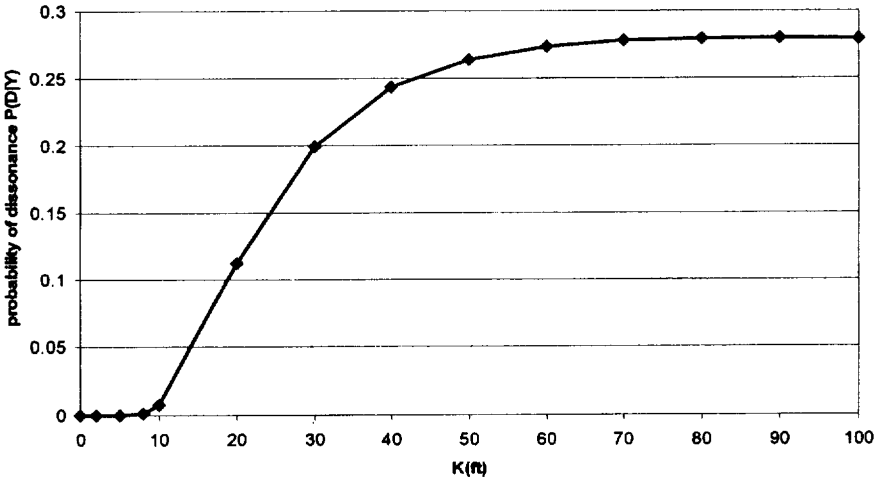


Figure 7.11 Effect of Sensor Accuracy on Probability of Dissonance for a True State

Probability of dissonance contours give system designer a complete picture of probability of dissonance around the dissonance space, which helps the system designer to decide new alert thresholds or control procedures to avoid or mitigate dissonance.

If the relative costs of each alerting system's false alarms ($C_i(FA)$), missed detections ($C_i(MD)$), and the relative cost of dissonance between two systems (C_D) can be quantified, then a multiple alerting cost function, **J**, can be defined that weights these costs by the probability of each undesirable outcome,

$$\mathbf{J} = P(D)C_D + \sum_{i=0,1} P_i(FA)C_i(FA) + P_i(MD)C_i(MD) \tag{7.24}$$

Thus, the optimal alerting threshold can be set to minimize the cost of alerting.

As K goes to infinity, that is, the variance of the estimate error is very large, no matter where the true state is, the probability of the measured state being in dissonance space S_{11} would be 0.25, since the whole state space has been separated into four approximately equal-area subsets S_{00}, S_{10}, S_{01}, and S_{11}. Thus, as K goes to infinity, the curve in Figure 7.11 should go to approximately 0.25.

Now, we want to check the effect of senor accuracy on the probability of dissonance for a given complete true state trajectory. In this example, the given true state trajectory starts from the initial state $\mathbf{y}_0 = [7500ft \quad -90ft/s]^T$, with the acceleration $a = a_1 - a_0 = 0 - (-1.22ft/s^2) = 1.22ft/s^2$ (the own aircraft decelerates and the front aircraft does not change its speed), and two systems have the same measurement update rate 0.25s. The true state trajectory is shown moving from right to left in Figure 7.12, where the probability of dissonance contours are based on K=30ft.

The cumulative probability of dissonance up to time *t* along the given trajectory is given by

$$P_c(D \mid T(t)) = 1 - \prod_{t=0}^{t} (1 - P(D \mid \mathbf{y}(t))) \tag{7.25}$$

As time goes to infinity, the cumulative probability of dissonance over the entire trajectory is given by

$$P_\infty(D \mid T) = \lim_{t \to \infty} P_c(D \mid T(t)) \tag{7.26}$$

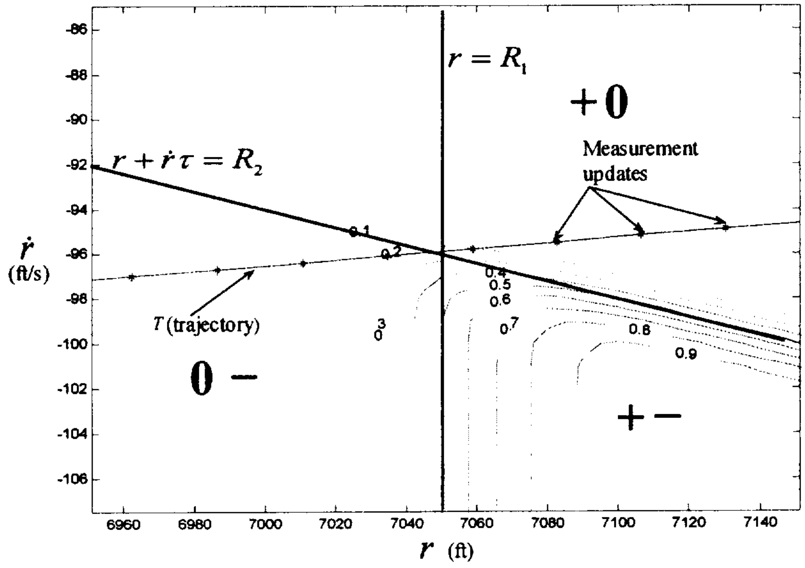


Figure 7.12 True state Trajectory with Measurement Update Rate 0.25s

Here, we assumed that the measurement error at each time is uncorrelated. The following diagram (Figure 7.13) shows the probability of dissonance along the example trajectory with K=30ft.

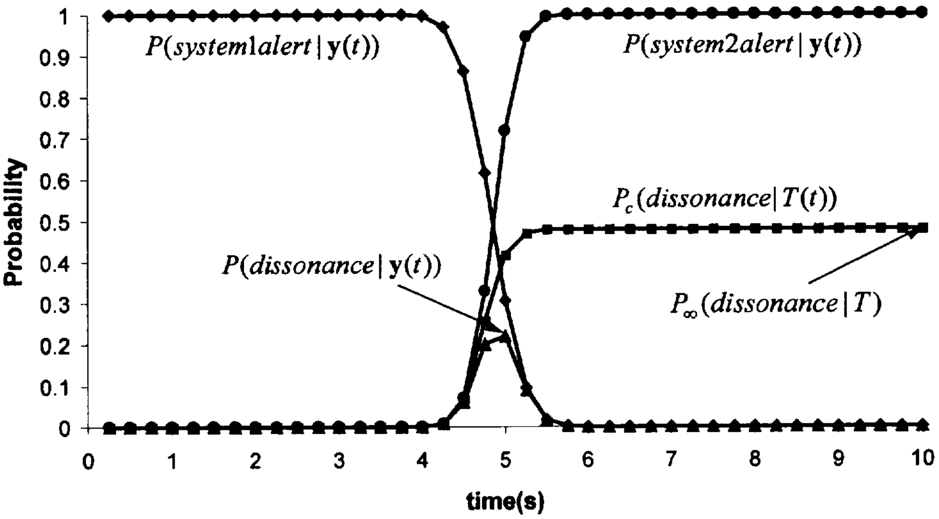


Figure 7.13 Probability of Dissonance along Example Trajectory

As we can see from Figure 7.12, after four seconds from the initial state, the given trajectory approaches the alerting systems' threshold boundary. The alert of system 1 is turned off as the trajectory is leaving alert space A_{11} to space A_{10}, so the probability of system 1 alert given the measured state is decreasing from 1 to 0. Meanwhile, the alert of system 2 is turning on, the trajectory is leaving space A_{20} to alert space A_{21}, so the probability of system 2 alert given the measured state is increasing from 0 to 1. Thus, the probability of dissonance increases when the trajectory approaches the intersection point of four subsets and decreases when the trajectory leaves the intersection point. Since the given true trajectory almost crosses the intersection point of subsets (Figure 7.12), the overall opportunity to trigger dissonance for this trajectory should be close to 0.5, that is why $P_{\infty}(D\,|\,T)$ is close to 0.5.

Different trajectories will result in different shapes of curves in Figure 7.13. Even for the same trajectory, if we choose a different initial start time, the measured state would be different, which makes the probability of dissonance at each time different; and if the update rate of measurements increases, the cumulative probability of dissonance would change at each time since more measured states would be added. But the trend of the curves would stay same.

Now, suppose the process starts from the same initial point as above, but we don't know which trajectory will actually be followed. We assume one of three trajectories with $a = a_1 - a_0 = 1.02 ft/s^2$, $a = a_1 - a_0 = 1.22 ft/s^2$, or $a = a_1 - a_0 = 1.42 ft/s^2$ (Figure 7.14) must be followed. Each trajectory has the same opportunity to be chosen, that is, $P(T_i) = 1/3$.

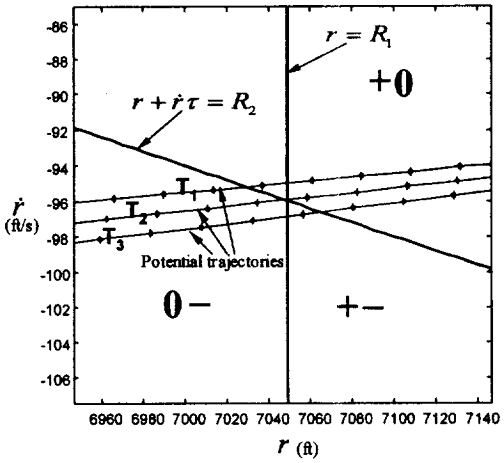


Figure 7.14 Set of Uncertain True State Trajectories without Sensor Error

As we can see from Figure 7.14, if there is no sensor error, only T_3 would cross the dissonance space, that is, $P'_\infty(D \mid T_1) = 0$, $P'_\infty(D \mid T_2) = 0$, and $P'_\infty(D \mid T_3) = 1$.

But if we consider sensor accuracy, the measurement of each state on the trajectories T_1 and T_2, which do not cross the dissonance space, would have the probability to be in the dissonance space. Thus, the cumulative probability of dissonance along these trajectories would no longer be zero. Figure 7.15 shows the case with K=30ft, $P_\infty(D \mid T_1) = 0.27$ and $P_\infty(D \mid T_2) = 0.48$. It's also possible to have the measurement of the states on the trajectory T_3 be outside the dissonance space, so the cumulative probability of dissonance along this trajectory would also change. In this example, when K=30ft, $P_\infty(D \mid T_3) = 0.68$.

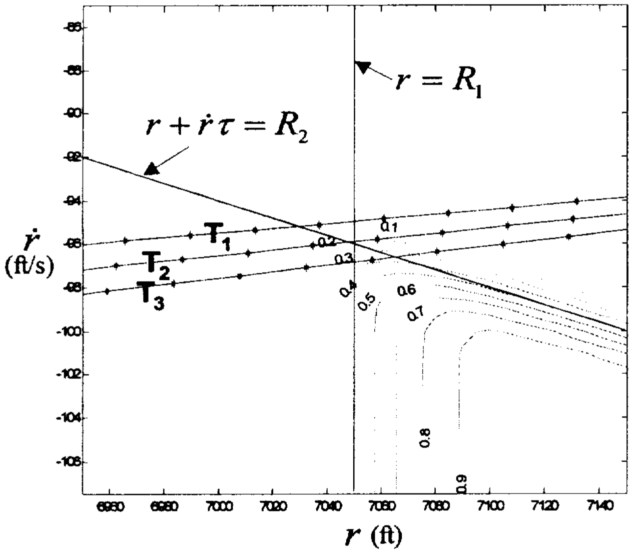


Figure 7.15 Set of Uncertain True State Trajectories with K=30ft

As the sensor accuracy changes (the value of K changes), we can see how the cumulative probability of dissonance along each trajectory changes (Figure 7.16). Figure 7.16 shows that when K increases, the cumulative probability of dissonance for those trajectories not crossing the dissonance space (T_1 and T_2) increases. For the trajectory crossing the dissonance space (T_3), the cumulative probability of dissonance decreases first and then increases. This can be explained from the definition of the cumulative probability of dissonance over the entire trajectory. Since

$$P_\infty(D\,|\,T) = \lim_{t\to\infty} P_c(D\,|\,T(t)) \qquad (7.27)$$

and

$$P_c(D\,|\,T(t)) = 1 - \prod_{t=0}^{t}(1 - P(D\,|\,\mathbf{y}(t))) \qquad (7.28)$$

if $P(D\,|\,\mathbf{y}(t))$ is constant and $0 < P(D\,|\,\mathbf{y}(t)) \le 1$ for each true state $\mathbf{y}(t)$, then when t goes to infinity, $\prod_{t=0}^{t}(1 - P(D\,|\,\mathbf{y}(t)))$ must go to zero, which will make $P_\infty(D\,|\,T)$ go to one. As we explained in Figure 7.11, when K goes to infinity, $P(D\,|\,\mathbf{y}(t))$ goes to 0.25 (a constant between 0 and 1) for any given true state y(t), so the cumulative probability of dissonance $P_\infty(D\,|\,T)$ over any entire trajectory T goes to one when K goes to infinity. As we mentioned for Figure 7.13, the cumulative probability of dissonance for each given K value would be different if the measurement update rate were different, but the trends of the curves in Figure 7.16 would be similar.

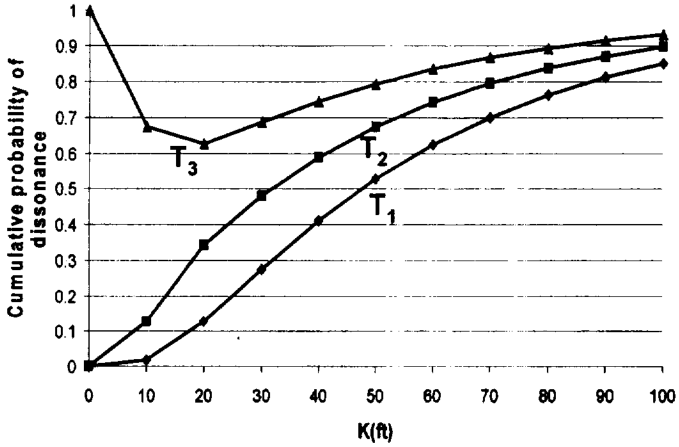


Figure 7.16 Overall effect of Standard Deviation on $P_\infty(D\,|\,T_i)$

Now, for this set of uncertain trajectories, given $P(T_i) = 1/3$, we can get the overall cumulative probability of dissonance and the effect of sensor accuracy on it (Figure 7.17).

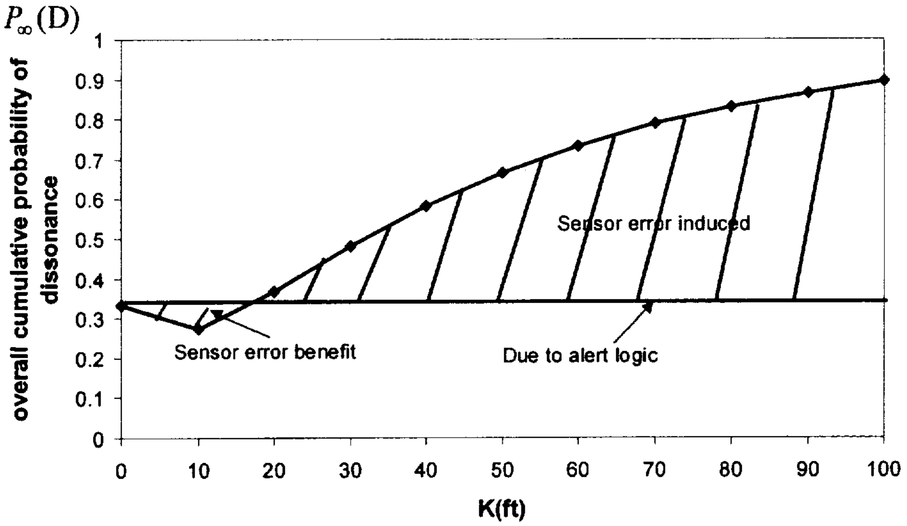


Figure 7.17 contribution of Sensor Error to Dissonance

Recall that we assumed that each trajectory is equally likely to be chosen, and we considered three trajectories, and only one of them crosses the dissonance space. When there is no sensor error, K=0, $P'_\infty(D) = 0.33$, which is shown as a horizontal reference line in Figure 7.17. The contribution of logic difference to the overall cumulative probability of dissonance is therefore 1/3. As we can see from Figure 7.17, for most values of K, sensor error induces dissonance, and the larger the values of K, the more the dissonance is induced. But for some value of K (less than approximately 17ft), the overall cumulative probability of dissonance decreases compared to the base line (the case without the sensor error).

As we defined in chapter four, the probability of False Dissonance and Missed Dissonance in this example are

$$P_{FD} = \frac{1}{3}P_\infty(D \mid T_1) + \frac{1}{3}P_\infty(D \mid T_2) \qquad (7.29)$$

and

$$P_{MD} = \frac{1}{3}(1 - P_\infty(D \mid T_3)) \qquad (7.30)$$

When K=10ft, the probability of False Dissonance is less than the probability of Missed dissonance (Figure 7.18), which explains the apparent sensor error benefit on Figure 7.17.

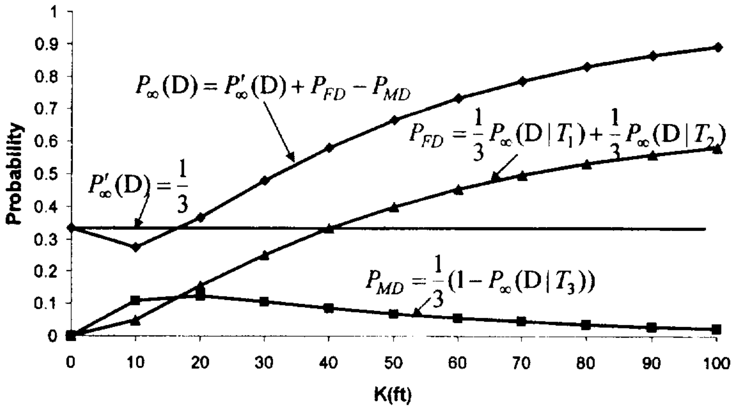


Figure 7.18 Sensor error Benefit of Dissonance

Although for some value of K (less than approximately 17ft in this example), the overall cumulative probability of dissonance decreases compared to the baseline (the case without the sensor error), it may not be a good thing. As we can see from Figure 7.18, decreased overall cumulative probability of dissonance means the increased probability of missed dissonance, which also means that one of the alerting systems may have a missed detection of the hazard. The hazard may then not be able to be avoided because of this missed detection.

7.3 Consequences of Dissonance

The dangerous dissonance space is identified for the In-Trail example in this section, which is part of the dissonance space S_{11} with opposite commands.

7.3.1 Hybrid Model of the Process

In this example, we will not consider any uncertainty. We assume that the human operator would respond to the alerting system command without any delay on each alert space boundary. That is, $\Delta_q = 0$ for each $q \in Q \equiv \{1,...,N\}$.

Given alerting system 1 in this example, the whole state space $\mathbf{U}$ can be separated into two subsets A_{10} and A_{11} (Figure 7.2), that is, $\mathbf{U} = A_{10} \cup A_{11}$ and $A_{10} \cap A_{11} = \phi$. In state space A_{10}, the continuous dynamics of the process are given by the vector field $\mathbf{F}_{10} : A_{10} \rightarrow \mathbf{R}^2$. As we explained in Section 7.1, in state space A_{10}, the operator is conceivably allowed to apply any acceleration he or she may desire within that acceleration limit. To simplify the study case, we assume the operator would not change the velocity if there were no alerting system command. So, in state space A_{10}, the process dynamics is governed by the differential equation (7.11) with $T_0 = 0$, both aircraft move with constant velocities. That is, the trajectory is given by equations (7.13) and (7.14) with $a = a_1 - a_0 = 0$. In state space A_{11}, the continuous dynamics of the process is given by vector field $\mathbf{F}_{11}$. The alerting system commands the pilot of the trailing aircraft to accelerate with $a_0 \geq a_{\min}$, and the trajectory is given by equations (7.13) and (7.14) with $a = a_1 - a_0 \in [-a_{\max} \quad -a_{\min}]$ (the trailing aircraft accelerates and the front aircraft does not change speed).

Similar to alerting system 1, the whole state space $\mathbf{U}$ can be separated into two subsets A_{20} and A_{21} given alerting system 2. In state space A_{20}, the vector field is $\mathbf{F}_{20}$, we assume the trajectory is given by equations (7.13) and (7.14) with $a = a_1 - a_0 = 0$. In state space A_{21}, the vector field is $\mathbf{F}_{21}$. Alerting system 2 commands the pilot of the trailing aircraft to decelerate with $a_0 \leq -a_{\min}$, the trajectory is given by equations (7.13) and (7.14) with $a = a_1 - a_0 \in [a_{\min} \quad a_{\max}]$ (the trailing aircraft decelerates and the front aircraft remains at the initial speed).

With two alerting systems working together, the whole state space $\mathbf{U}$ can be separated into four subsets $S_{00} = A_{10} \cap A_{20}$, $S_{01} = A_{10} \cap A_{21}$, $S_{10} = A_{11} \cap A_{20}$, and $S_{11} = A_{11} \cap A_{21}$. The governing vector field and acceptable acceleration range on each subset is listed in Table 7.2.

Table 7.2

Governing Vector Field and Possible Acceleration on Four Subsets

Subset	Governing vector field	Possible acceleration
$\mathbf{x} \in S_{00}$	$\mathbf{f} \in \mathbf{F}_{00}$	$a = 0$
$\mathbf{x} \in S_{10}$	$\mathbf{f} \in \mathbf{F}_{10}$	$a \in [-a_{\max} \quad -a_{\min}]$
$\mathbf{x} \in S_{01}$	$\mathbf{f} \in \mathbf{F}_{01}$	$a \in [a_{\min} \quad a_{\max}]$
$\mathbf{x} \in S_{11}$	$\mathbf{f} \in \mathbf{F}_{11}$	$a \in [-a_{\max} \quad a_{\max}]$

When $\mathbf{x} \in S_{11}$, as we analyzed in Section 7.1.1, there is dissonance since the two systems are issuing contradictory resolution commands (one to accelerate, the other to decelerate), and the vector field is not well defined. We assume the aircraft would apply any acceleration or deceleration within the performance limits in this dissonance space. That is, the trajectory is given by equations (7.13) and (7.14) with $a = a_1 - a_0 \in [-a_{\max} \quad a_{\max}]$.

In this example, alerting system 1 is monitoring the efficient operation of the process, so the larger the range between two aircraft, the more inefficient the operation of the process. Alerting system 2 is monitoring the hazard space, where two aircraft will crash when $r = 0$. Since the part with negative range rate and $r = 0$ is not reachable, we define the hazard space of this example as

$$\mathbf{H}_2 = \{(r, \dot{r}) \mid r = 0, \dot{r} < 0\} \tag{7.31}$$

And we assumed that the designed threshold functions and required least deceleration $-a_{\min}$ of alerting system 2 could avoid the hazard space. The dissonance space is given by equation (7.10).

Thus, the hybrid model of this process consists of a state space $\mathbf{U} = \bigcup_{q \in Q} \mathbf{U}_q$, where $q \in Q \equiv \{1, \ldots, N\}$. Q could be an infinite set if two aircraft will not crash and the process dynamics carry on. The state $(q, \mathbf{x})$ of the process may flow within q only if the continuous state is within any of the following sets, $S_{00} = A_{10} \cap A_{20}$, $S_{01} = A_{10} \cap A_{21}$, $S_{10} = A_{11} \cap A_{20}$, and $S_{11} = A_{11} \cap A_{21}$. The dynamics of the process within each subset do not change unless the state reaches the boundaries of these subsets. That is, the acceleration a does not change within each subset once it is chosen.

Figure 7.19 shows an example of the dynamics of the process. When the continuous state hits the boundary of S_{10}, a discrete transition is forced; the continuous dynamics within S_{10} in the following discrete state q' is decided by the transition function, which functions as a random processor to choose an acceleration a from $[-a_{\max} \quad -a_{\min}]$ based on some assumed probabilistic distribution function of a. Thus, the trajectory is given by equations (7.13) and (7.14) with $a \in [-a_{\max} \quad -a_{\min}]$, and a does not change within S_{10} once it is chosen. When the continuous state hits the boundary of S_{11}, the activated transition function chooses an acceleration a from $[-a_{\max} \quad a_{\max}]$; the trajectory is given by equations (7.13) and (7.14) with $a \in [-a_{\max} \quad a_{\max}]$. When the continuous state hits the boundary of S_{01}, the activated transition function chooses an acceleration a from $[a_{\min} \quad a_{\max}]$; the trajectory is given by equations (7.13) and (7.14) with $a \in [a_{\min} \quad a_{\max}]$. Finally, when the continuous state hits the boundary of S_{00}, the activated transition function sets the acceleration a to be zero; the trajectory is given by equations (7.13) and (7.14) with $a = 0$.

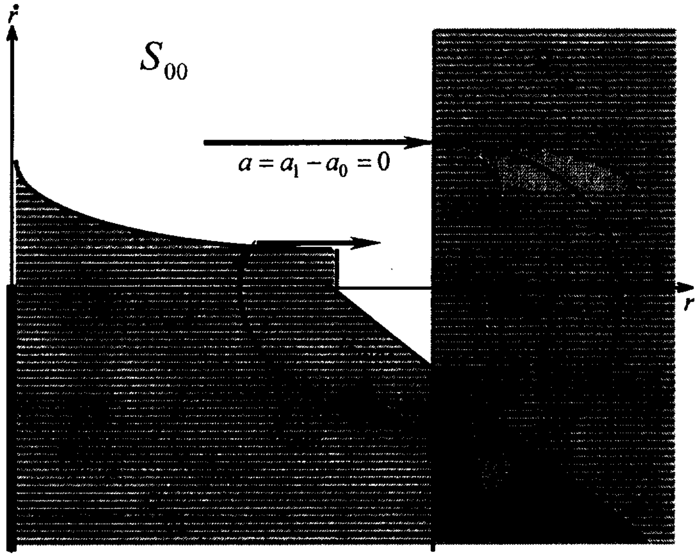


Figure 7.19 Dynamics of the In-Trail Process

Figure 7.20 shows three example dynamics of this In-Trail process with threshold parameters of two alerting systems given in Table 7.3. The trajectory with a solid line in Figure 7.20 shows a case (case 1) where the aircraft crashes. Case 1 starts with initial state (4000ft, 150ft/s), the transition function chooses $a = -1.52 ft/s^2$ within $[-a_{\max} \quad -a_{\min}] = [-3.0 \quad -1.5] ft/s^2$ when the continuous state hits the boundary of S_{10}; when the continuous state hits the boundary of S_{11}, the transition function chooses $a = -1.82 ft/s^2$; and when entering S_{01}, although the transition function chooses

$a = 1.52 ft/s^2 \in [a_{\min} \quad a_{\max}] = [1.5 \quad 3.0] ft/s^2$, it's too late to avoid the hazard space, and the two aircraft crash. Case 2 (dashed trajectory in Figure 7.20) starts with the same initial state as in case 1, but the transition function chooses $a = -1.82 ft/s^2$ when the continuous state hits the boundary of S_{10}; when the continuous state hits the boundary of S_{11}, the transition function chooses $a = 0$ (i.e., the pilot does nothing when he or she gets confused); and when entering S_{01}, the transition function chooses $a = 1.82 ft/s^2$, which leads the process out of the space S_{01}, and settle in space S_{00} with $a = 0$. Case 3 (dotted trajectory in Figure 7.20) starts with a different initial state (4000ft, 80ft/s), which makes the whole trajectory stay outside the dissonance space S_{11}. In this case, the transition function chooses $a = -1.52 ft/s^2$ in S_{10}, $a = 1.52 ft/s^2$ in S_{10}, and $a = 0$ otherwise.

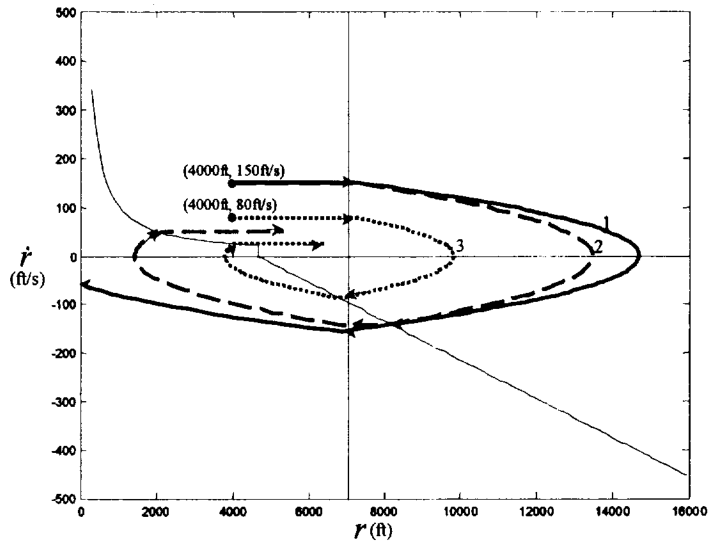


Figure 7.20 Example Process Dynamics

Table 7.3

Threshold Parameters for the Example Process Dynamics

	System 1	System 2
Threshold function	$r = R_1$	$r + \dot{r}\tau = R_2$ $r\dot{r} = H$
Parameters	$R_1 = 7050 ft$	$R_2 = 4650 ft$, $\tau = 25 s$ $H = 102631 ft^2 / s$

7.3.2 Identification of the Dangerous Dissonance Space

Given the hazard space $\mathbf{H}_2 = \{(r,\dot{r}) \mid r = 0 \,\&\, \dot{r} < 0\}$ monitored by alerting system 2, we can use the backward reachability analysis to identify the dangerous dissonance space in the dissonance space S_{11}.

As we can see from Figure 7.21, if the trajectory with $a = a_{\min}$ can reach the hazard space $\mathbf{H}_2 = \{(r,\dot{r}) \mid r = 0 \,\&\, \dot{r} < 0\}$, then there must be trajectories with some $a \in [a_{\min} \quad a_{\max}]$ that could also reach the hazard space. So, in state space S_{01}, using equations (7.13) and (7.14) with $a = a_{\min}$ and destination state $r(t) = 0$ and $\dot{r}(t) = 0$

$$0 = r_{\mathrm{A}} + \dot{r}_{\mathrm{A}} t + \frac{1}{2} a_{\min} t^2 \qquad (7.32)$$

$$0 = \dot{r}_{\mathrm{A}} + a_{\min} t \qquad (7.33)$$

We can identify point A (Figure 7.21) on the boundary of alerting system 1 $\{(r,\dot{r}) \mid r = R_1\}$. Solving equations (7.31) and (7.32) with $r_{\mathrm{A}} = R_1$, we can get $\dot{r}_{\mathrm{A}} = -\sqrt{2a_{\min} R_1}$. From any point below A on the boundary of alerting system 1 $\{(r,\dot{r}) \mid r = R_1, \dot{r} \le -\sqrt{2a_{\min} R_1}\}$, it is possible to reach the hazard space following the trajectory given by equations (7.13) and (7.14) with $a \in [a_{\min} \quad a_{\max}]$ in state space S_{01}.

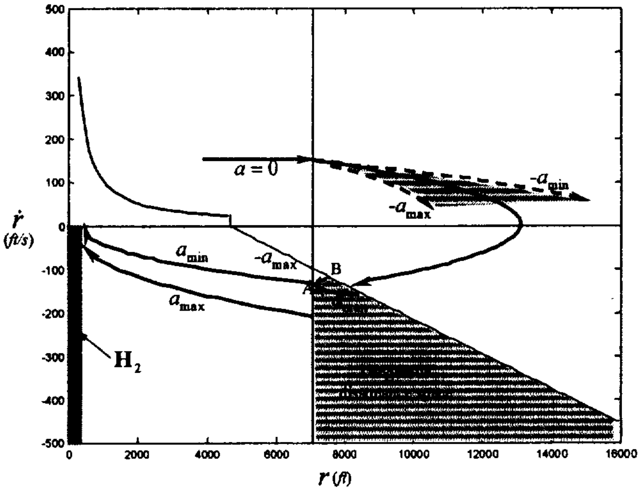


Figure 7.21 Dangerous Dissonance Space

Now, with points $\{(r,\dot{r}) \mid r = R_1, \dot{r} \le -\sqrt{2a_{\min}R_1}\}$ as the target states, with system dynamics given by equations (7.13) and (7.14) with $a \in [-a_{\max} \quad a_{\max}]$, we want to identify those initial states on the boundary of alerting system 2 $\{(r,\dot{r}) \mid \frac{r-R_2}{-\dot{r}} = \tau\}$. As we can see from Figure 7.21, we only need to identify point B, since if the trajectory with $a = -a_{\max}$ can reach point A from point B, then any state below B on $\{(r,\dot{r}) \mid \frac{r-R_2}{-\dot{r}} = \tau\}$ could reach points $\{(r,\dot{r}) \mid r = R_1, \dot{r} \le -\sqrt{2a_{\min}R_1}\}$ following the trajectories given by equations (7.13) and (7.14) with some $a \in [-a_{\max} \quad a_{\max}]$.

In state space S_{11}, solving equations (7.13) and (7.14) with $a = -a_{\max}$ and destination state $r(t) = R_1$ and $\dot{r}(t) = -\sqrt{2a_{\min}R_1}$ (state A)

$$R_1 = r_{\mathrm{B}} + \dot{r}_{\mathrm{B}}t - \frac{1}{2}a_{\max}t^2 \tag{7.34}$$

$$-\sqrt{2a_{\min}R_1} = \dot{r}_{\mathrm{B}} - a_{\max}t \tag{7.35}$$

and an additional condition

$$\frac{r_{\mathrm{B}} - R_2}{-\dot{r}_{\mathrm{B}}} = \tau \tag{7.36}$$

We can identify point B with

$$\dot{r}_{\mathrm{B}} = a_{\max}\tau - \sqrt{2(a_{\min} + a_{\max})R_1 - 2a_{\max}R_2 + a_{\max}{}^2\tau^2} \tag{7.37}$$

and equation (7.35). So the dangerous dissonance space boundary is the set

$$\{(r,\dot{r}) \mid \frac{r-R_2}{-\dot{r}} = \tau \;\&\; \dot{r} \le a_{\max}\tau - \sqrt{2(a_{\min} + a_{\max})R_1 - 2a_{\max}R_2 + a_{\max}{}^2\tau^2}\} \tag{7.38}$$

As shown in Figure 7.22, the dangerous dissonance space is the space below the curve AB in the dissonance space S_{11}. Entering S_{11} above the curve will be safe as long as $a \in [-a_{\max} \quad a_{\max}]$.

7.4 Ways to Mitigate Dissonance

In this section, several ways to mitigate dissonance (especially, the dangerous dissonance) are presented based on the trade off between efficiency and the risk of hazard.

7.4.1 Prioritization

In this example, System 1 has been designed to monitor the efficient operation of the process, while System 2 is for a collision hazard. Since a hazard alert is highly critical, it needs immediate attention of the flight crew, so it could be logical to put System 2 in higher priority. That is, we can prioritize System 2 with a higher priority than system 1 (or inhibit system 1) whenever both systems would otherwise be triggered. Thus, the process can only go from S_{10} to S_{01}, which is not likely to be dissonant because of the similar trend in the action spaces of each system (recall Figure 7.6). This prioritization is shown in Figure 7.22 as a change in the threshold function of alerting system 1.

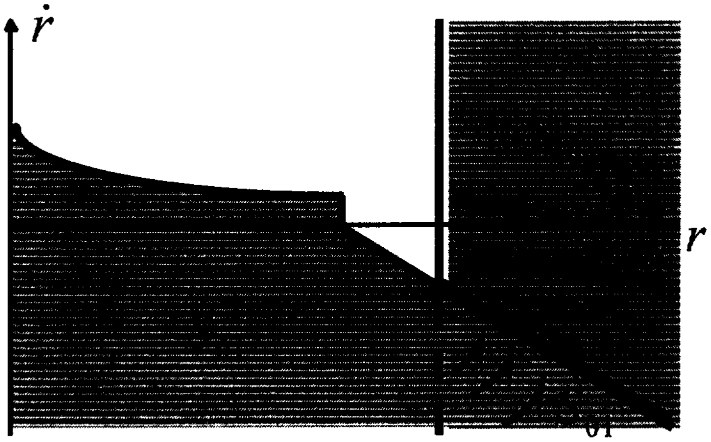


Figure 7.22 Avoid Dissonance through Prioritizing System 2

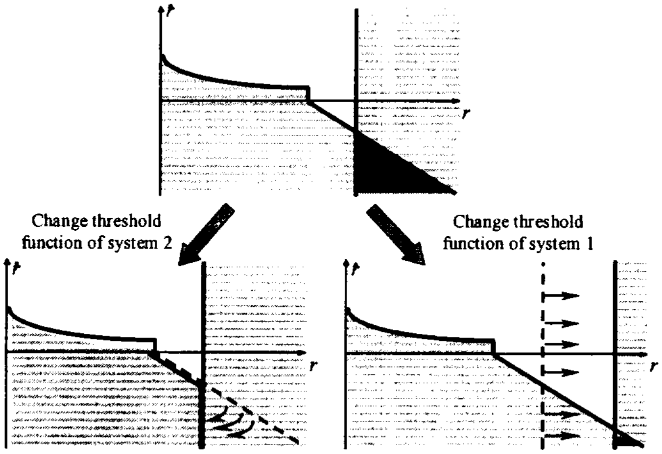
7.4.2 Modify System Design

The potential for dissonance could be reduced by modifying one or both systems' decision thresholds to reduce the size of S_{11}.

As shown in Figure 7.23, we can modify the threshold function $\frac{r - R_2}{-\dot{r}} = \tau$ to

$$\begin{cases} \dfrac{r - R_2}{-\dot{r}} = \tau & when \quad R_2 \le r < R_1 \\ r = R_1 & when \quad r \ge R_1 \end{cases} \tag{7.39}$$

which eliminates the dissonance space. But it may not be a proper way. With the new threshold function, when the closure rate is large, the alert from system 2 may be too late for the pilot to avoid the hazard.



$\dot{r}$
r
Change threshold function of system 2
Change threshold function of system 1
$\dot{r}$
r
$\dot{r}$
r

Figure 7.23 Modify System Design to Reduce the Potential for Dissonance

We assume the range between two aircraft is the only observable information to system 1, so the only way to change the threshold function of system 1 is to change R_1. As we can see from Figure 7.23, increasing R_1 can reduce the size of dissonance space, but that may not satisfy the efficient operation requirement, as aircraft may operate too far apart from one another.

To be able to optimize both system designs to minimize the dissonance space and maximize operation efficiency with restriction for the safety requirement, we need to solve a specific multi-objective optimization problem, depending on which parameters can be changed and the definition of the efficient operation. Also, the safety requirement will be related to the choice of resolution maneuvers.

For example, assume that efficient operation is measured by the distance between two aircraft, and, in any case, the distance between two aircraft is not allowed to be bigger than some value $R_{\max}$. Also assume that the safety requirement is that the two aircraft will not crash if the trailing aircraft decelerates with $a_0 = -a_{\max}$ when the range rate between two aircraft reaches some maximum value $-\dot{r}_{\max}$. Given the minimum safe separation between two aircraft R_2, we want to optimize R_1 and τ to minimize the dissonance space to satisfy the efficient operation and safety requirement. Thus, the multi-objective optimization problem has been simplified as a single objective optimization problem with the performance requirements of safety and efficient operation as constraints.

To satisfy the efficient operation requirement, we need to identify the constraint related to efficient operation. Suppose the highest possible closure rate between two aircraft is given as $\dot{r}_{\max}$. With state $(R_{\max},0)$ as the target state, solving the equations (7.13) and (7.14) with $a = -a_{\min}$ and initial state $(R_1, \dot{r}_{\max})$,

$$R_{\max} = R_1 + \dot{r}_{\max}t - \frac{1}{2}a_{\min}t^2 \tag{7.40}$$

$$0 = \dot{r}_{\max} - a_{\min}t \tag{7.41}$$

the constraints satisfying efficient operation can be given as

$$R_1 \leq R_{\max} - \frac{\dot{r}_{\max}{}^2}{2a_{\min}} \tag{7.42}$$

To satisfy the safety requirement, starting from the point with highest closure rate $-\dot{r}_{\max}$ on $\frac{r - R_2}{-\dot{r}} = \tau$ $(R_2 + \dot{r}_{\max}\tau, -\dot{r}_{\max})$, the trajectory given by the equations (7.13) and (7.14) with $a = a_{\max}$ should not be able to reach the target state (0,0). That is, solving

$$0 = R_2 + \dot{r}_{\max}\tau - \dot{r}_{\max}t + \frac{1}{2}a_{\max}t^2 \tag{7.43}$$

$$0 = -\dot{r}_{\max} + a_{\max}t \tag{7.44}$$

we get $\tau = \frac{\dot{r}_{\max}{}^2 - 2R_2 a_{\max}}{2a_{\max}\dot{r}_{\max}}$. So, the constraint satisfying safety can be given as

$$\tau \geq \frac{\dot{r}_{\max}^{2} - 2R_2 a_{\max}}{2a_{\max}\dot{r}_{\max}} \tag{7.45}$$

Given the maximum range rate (250ft/s) the process could have, the area of the dissonance space is shown in Figure 7.24.

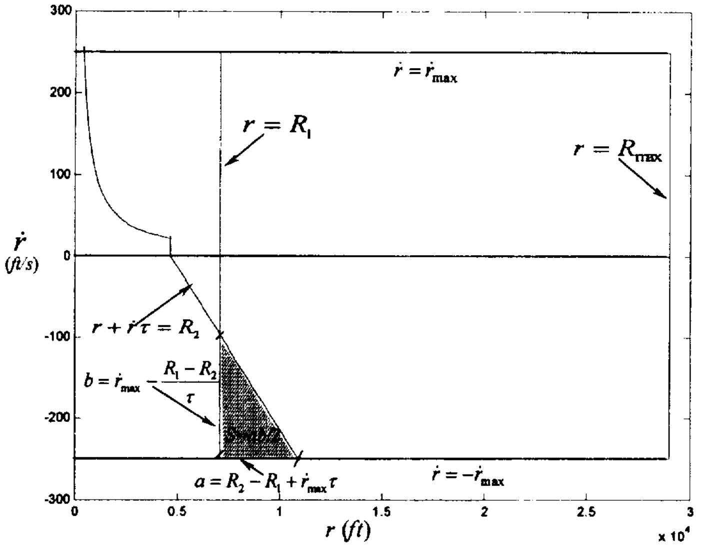


Figure 7.24 The Area of Dissonance Space

This simplified single objective optimization problem can be stated as follows,

$$\min_{R_1,\tau} f(R_1,\tau) = S = \frac{1}{2}\left(\frac{R_2 - R_1}{\sqrt{\tau}} + \dot{r}_{\max}\sqrt{\tau}\right)^2 \tag{7.46}$$

Subject to

$$R_1 \leq R_{\max} - \frac{\dot{r}_{\max}^{2}}{2a_{\min}} \tag{7.42}$$

$$\tau \geq \frac{\dot{r}_{\max}^{2} - 2R_2 a_{\max}}{2a_{\max}\dot{r}_{\max}} \tag{7.45}$$

The first-order necessary conditions, in addition to the constraints, are,

$$-\frac{1}{\sqrt{\tau}}\left(\frac{R_2 - R_1}{\sqrt{\tau}} + \dot{r}_{\max}\sqrt{\tau}\right) + \mu_1 = 0 \tag{7.47}$$

$$(\frac{R_2-R_1}{\sqrt{\tau}}+\dot{r}_{\max}\sqrt{\tau})[\frac{1}{2}\dot{r}_{\max}\tau^{\frac{-1}{2}}-\frac{1}{2}(R_2-R_1)\tau^{\frac{-3}{2}}]-\mu_2=0 \tag{7.48}$$

$$\mu_1 \geq 0 \tag{7.49}$$

$$\mu_2 \geq 0 \tag{7.50}$$

$$\mu_1(R_1-R_{\max}+\frac{\dot{r}_{\max}^{\ \ 2}}{2a_{\min}})=0 \tag{7.51}$$

$$\mu_2(\frac{\dot{r}_{\max}^{\ \ 2}-2R_2a_{\max}}{2a_{\max}\dot{r}_{\max}}-\tau)=0 \tag{7.52}$$

Intuitively, larger R_1 and smaller τ may result in smaller $f(R_1,\tau)$. Thus, assuming both constraints are inactive ($\mu_1=0$ & $\mu_2=0$), the problem has the solution

$\tau=\frac{\dot{r}_{\max}^{\ \ 2}-2R_2a_{\max}}{2a_{\max}\dot{r}_{\max}}$, $R_1=R_{\max}-\frac{\dot{r}_{\max}^{\ \ 2}}{2a_{\min}}$. Since $\mu_1=\mu_2=0$, we conclude that this solution satisfies the first-order necessary conditions.

Figure 7.25 compares the threshold functions using optimal parameters R_1 and τ (solid lines) to the original designed threshold functions (dashed lines), given $R_2=4650ft$, $a_{\max}=3.0ft/s^2$, $a_{\min}$=1.5 ft/s^2, $R_{\max}=29000ft$, and $\dot{r}_{\max}=250ft/s$.

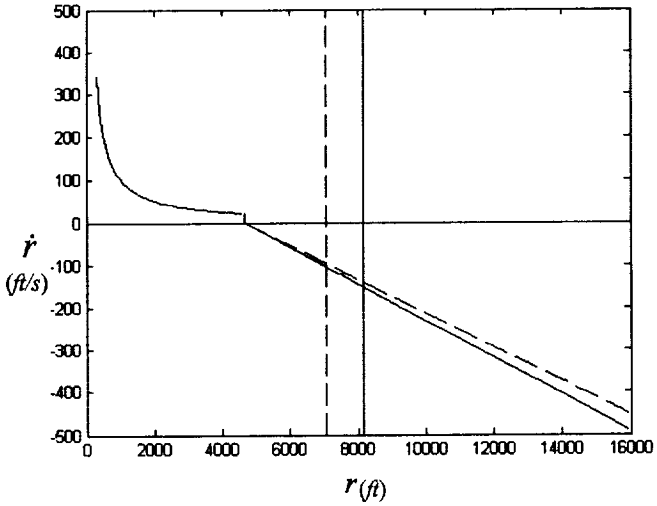


Figure 7.25 Optimal Threshold Functions

Table 7.4 shows the value of the original thresholds and the optimal thresholds.

Table 7.4

The Optimal Thresholds

	original	optimal
R_1	7050 ft	8167 ft
τ	25 s	23 s

We also want to check the safety benefit of the optimal threshold function. Assuming that the initial range rate is uniformly distributed between 0 and $\dot{r}_{\max} = 250 ft/s$, we want to compare the ratio of initial range rate that could lead the process to the dangerous dissonance space between the original designed threshold functions and the optimal ones. With point B (upper point of the dangerous dissonance space boundary) in Figure 7.21 as the target state, equation (7.13) and (7.14) can be used to identified the initial range rate on $r = R_1$, with which the process could reach point B with $a = a_{\max} = 3.0 ft/s^2$. That is, solving

$$r_B = R_1 + \dot{r}_0 t - \frac{1}{2} a_{\max} t^2 \tag{7.53}$$

$$\dot{r}_B = \dot{r}_0 - a_{\max} t \tag{7.54}$$

we can get

$$\dot{r}_0 = \sqrt{\dot{r}_B^2 + 2a_{\max}(r_B - R_1)} \tag{7.55}$$

where

$$r_B = R_2 - a_{\max}\tau^2 - \tau\sqrt{2a_{\min}R_1 - 2a_{\max}R_2 + a_{\max}{}^2\tau^2} \tag{7.56}$$

$$\dot{r}_B = a_{\max}\tau - \sqrt{2a_{\min}R_1 - 2a_{\max}R_2 + a_{\max}{}^2\tau^2} \tag{7.57}$$

Thus, with the original design of threshold functions ($R_1 = 7050ft, \tau = 25s$), $r_B = 7848ft$, $\dot{r}_B = -128ft/s$, then $\dot{r}_0 = 145ft/s$. That is, with any initial range rate bigger than $145ft/s$ (42% of the possible initial states), the process could reach the dangerous dissonance space with the original design of threshold functions. But with the optimal design ($R_1 = 8167ft, \tau = 23s$), $r_B = 8232ft$, $\dot{r}_B = -155ft/s$, then $\dot{r}_0 = 156ft/s$. That is, unless the initial range rate is bigger than $156ft/s$ (37% of the possible initial states), the process would not reach the dangerous dissonance space with the optimal design of threshold functions. Since the aircraft could crash when entering the dangerous dissonance space, we could say the safety is improved by 5% (from a risk of 42% to 37%) with the optimal design of threshold functions.

If both range and range rate are observable for system 1, then the system design can be modified more flexibly. For example, we can change the shape of the threshold function of system 1 to eliminate the dissonance space and command the aircraft 0 to accelerate according to the range rate between two aircraft (Figure 7.26). When the range rate is positive (the front aircraft is moving faster than the rare aircraft), the larger the range rate, the larger the acceleration that the system 1 should command. Thus if the threshold function of system 1 can reflect this relation (the curve in the positive range rate region shown in Figure 7.26), then the system 1 can be designed to have a unique acceleration command. Also shown in Figure 7.26, the threshold function in the negative range rate region of system 1 is designed to have a gap with the threshold function of system 2, which can avoid the possible dynamic dissonance caused by command changing from accelerating to decelerating in very short time period.

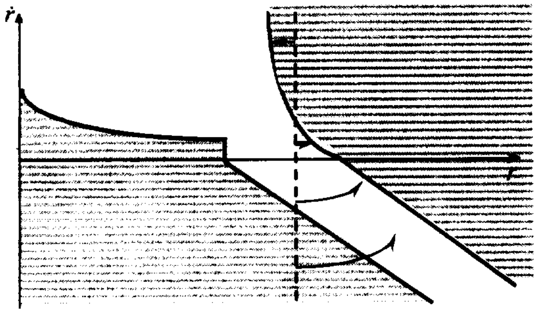


Figure 7.26 Change the Shape of Threshold Function to Avoid Dissonance

7.4.3 Modify Control Strategy

As we can see from section 7.4.2, the whole dissonance space is hard to eliminate through modifying system design alone, to satisfy safety and efficient operation requirements at the same time. To avoid the unsafe consequences of dissonance, we can modify the required control of the trailing aircraft in the alert space of system 1 to prevent the two vehicles from entering the dangerous dissonance space in $S_{11;}$ or we can identify the required control of the trailing aircraft in dangerous dissonance space to prevent the hazard (collision of two aircraft).

Given an initial condition, we can identify the acceleration requirement for the trailing aircraft in the alert space of system 1 to avoid entering the dangerous dissonance space in $S_{11.}$ With point B in Figure 7.21 as the target state, equations (7.13) and (7.14) can be used to identify the relation between initial range rate on $r = R_1$ and the required acceleration of trailing aircraft in alert space of system 1 to prevent the two vehicles from entering the dangerous dissonance space in $S_{11.}$ That is, solving

$$R_2 - a_{\max}\tau^2 - \tau\sqrt{2a_{\min}R_1 - 2a_{\max}R_2 + a_{\max}{}^2\tau^2} = R_1 + \dot{r}_0 t - \frac{1}{2}at^2 \qquad (7.58)$$

$$a_{\max}\tau - \sqrt{2a_{\min}R_1 - 2a_{\max}R_2 + a_{\max}{}^2\tau^2} = \dot{r}_0 - at \qquad (7.59)$$

we can get the relationship between a and $\dot{r}_0$

$$a = \frac{\dot{r}_0^2 - \dot{r}_B^2}{2(r_B - R_1)} \qquad (7.60)$$

where

$$r_B = R_2 - a_{\max}\tau^2 - \tau\sqrt{2a_{\min}R_1 - 2a_{\max}R_2 + a_{\max}{}^2\tau^2} \qquad (7.61)$$

$$\dot{r}_B = a_{\max}\tau - \sqrt{2a_{\min}R_1 - 2a_{\max}R_2 + a_{\max}{}^2\tau^2} \qquad (7.62)$$

That is, given an initial state $(R_1, \dot{r}_0)$, to prevent the two vehicles from entering the dangerous dissonance space in $S_{11,}$ the acceleration of the trailing aircraft a_0 in state space S_{10} must be larger than $\dfrac{\dot{r}_B^2 - \dot{r}_0^2}{2(r_B - R_1)}$ since $a = a_1 - a_0 = -a_0$. But when $\dot{r}_0 > \dot{r}_B$, $\dfrac{\dot{r}_B^2 - \dot{r}_0^2}{2(r_B - R_1)}$ is negative. That is, if the initial range rate is bigger than $\dot{r}_B$, it is impossible (with $a \in [-a_{\max} \quad a_{\max}]$) to prevent the two vehicles from entering the dangerous dissonance space in S_{11}. Thus, the initial condition must be restricted to avoid entering the dangerous dissonance space. Also, as we identified in Section 7.4.2, with any initial range rate $\dot{r}_0 < \sqrt{\dot{r}_B^2 + 2a_{\max}(r_B - R_1)}$ on $r = R_1$, it is not possible (with $a \in [-a_{\max} \quad a_{\max}]$) to enter the dangerous dissonance space, so the process is safe.

Figure 7.27 shows the required acceleration in S_{10} given the initial range rate between $\sqrt{\dot{r}_B^2 + 2a_{\max}(r_B - R_1)}$ and $\dot{r}_B$ on $r = R_1$ to avoid entering the dangerous dissonance space.

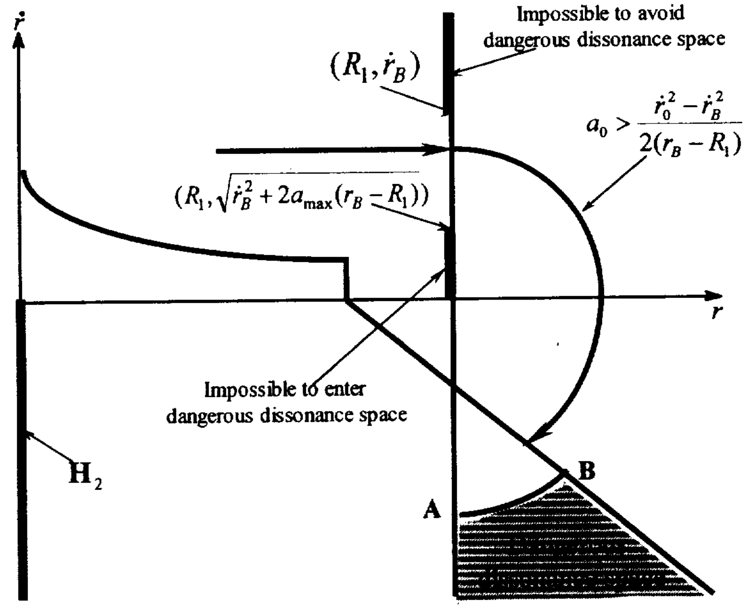

$\dot{r}$
Impossible to avoid dangerous dissonance space
$(R_1, \dot{r}_B)$
$a_0 > \dfrac{\dot{r}_0^2 - \dot{r}_B^2}{2(r_B - R_1)}$
$(R_1, \sqrt{\dot{r}_B^2 + 2a_{\max}(r_B - R_1)})$
r
Impossible to enter dangerous dissonance space
H_2
A
B

Figure 7.27 Required Acceleration to Avoid Entering Dangerous Dissonance Space

Once in dangerous dissonance space, we can restrict the deceleration of the trailing aircraft to avoid the hazard. Since we assumed that the required deceleration command $-a_{\min}$ and the threshold function $\frac{r - R_2}{-\dot{r}} = \tau$ of alerting system 2 has been designed to be able to avoid the hazard, then the hazard should be able to be avoided as long as the trailing aircraft decelerates with $a_0 \leq -a_{\min}$ once in dangerous dissonance space.

7.4.4 Modify Operational Procedures

From the beginning of this example, we assumed that the acceleration of the process a is constant in each subset S_{mn} as long as it has been chosen. To avoid dissonance, we can change the operational procedure. That is, we can command the trailing aircraft to accelerate until some range rate $\dot{r}^*$ in S_{10}, and then keep that range rate to avoid entering the dissonance space. This procedure is shown in Figure 7.28.

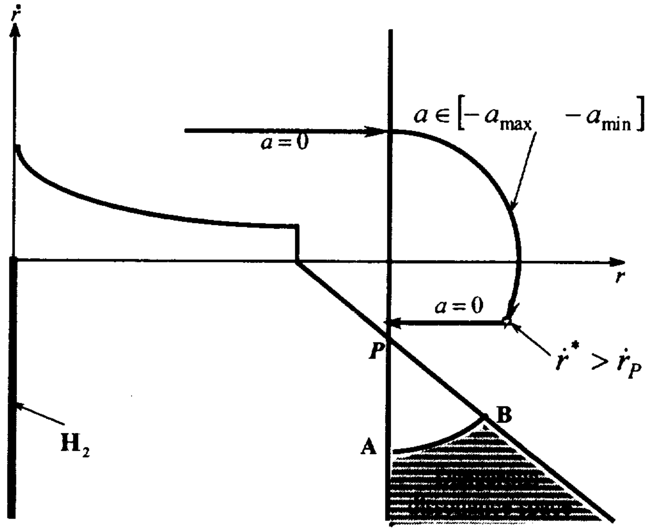


Figure 7.28 Change Operational Procedure to Avoid Dissonance

As we can see from Figure 7.28, as long as the range rate $\dot{r}^*$ is larger than the range rate of the intersection point P of two alerting systems boundaries, which is $\frac{R_2 - R_1}{\tau}$ (negative), the process would always be able to avoid entering the dissonance space.

7.4.5 Training

Without inhibiting the alert of system 1, we can train the pilot to always follow the maneuver according to command of system 2 once in dissonance space. This would make sense to the pilot since the pilot would understand that the alert for safety is more critical than an alert for efficiency.

The trailing pilot can be trained to take the maneuver we identified in Section 7.4.3 in S_{10} to prevent the two vehicles from entering the dangerous dissonance space, or once in dangerous dissonance space to avoid the hazard.

7.5 Summary

This chapter has demonstrated the framework of dissonance modeling and analysis we developed in previous chapters using a conceptual In-Trail example.

Through formally describing the alerting systems logic, the conditions for the possible perceived dissonance have been identified mathematically and graphically. The dissonance space with conflict resolution command was identified to be problematic and has been analyzed.

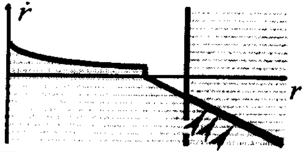
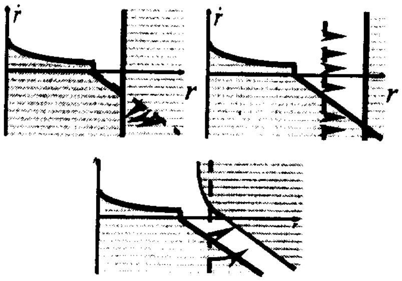
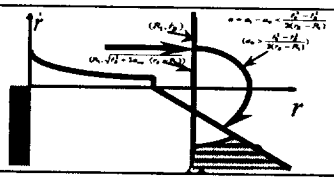
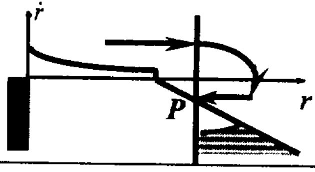
With a simple sensor error model, several example analyses have been performed: the probability of dissonance for a given true state, the cumulative probability of dissonance over the given trajectory, and the overall cumulative probability of dissonance for a set of uncertain trajectories. The changes of these probabilities as the sensor error distribution change were also analyzed. Finally, the contribution of sensor error to dissonance was identified.

A hybrid model was built to analyze the hybrid phenomenon of the process in this example. The dangerous dissonance space was identified through backward reachability analysis.

Mitigation methods suggested in chapter 6 were demonstrated in this example to prevent the dissonance or reduce the effect of dissonance based on the trade off between efficiency and the risk of hazard. The following table (Table 7.5) gives a summary of all these methods, including the advantages and disadvantages for each of them.

Table 7.5

Comparison of Mitigation Methods

Mitigation method	Related diagram	Advantages	Disadvantages
Prioritization		Simple and easy to be implemented	The operation may not Satisfy efficiency requirement in some area
Modify system design		Avoid dissonance from the root	Hard to find optimal solution for most multi-objective optimization problem
Modify control strategy		Guarantee to be safe and efficient operation	Required maneuver may be hard to implement
Modify operational procedure		Guarantee to be safe and efficient operation	Lose some operation space
Training		No additional requirement for system design	May fall short in high stress case

8. Example Application: Air Traffic Separation

One area where dissonance is becoming an identified issue involves airborne alerting systems for traffic management safety. Several different traffic alerting system concepts are in use or under development, and they must be carefully matched to prevent dissonance. Time-critical collision alerting is the function of an Airborne Collision Avoidance System (ACAS), and more strategic maintenance of separation between aircraft is the function of a different Airborne Separation Assurance System (ASAS). Each type of system has distinct requirements due to different timescales, consequences, and information quality with which to base decisions. Combining ASAS and ACAS components within a single aircraft and between different aircraft will be a challenging problem to overcome to ensure that these systems convey consistent information to decision-makers.

One form of ACAS already in operation is the Traffic Alert and Collision Avoidance System (TCAS), which has been mandated on U. S. transport aircraft since the early 1990s (RTCA, 1983). TCAS uses range, range rate, altitude, and altitude rate between two aircraft via transponder messages. The quality of this information limits the ability to make accurate collision predictions beyond approximately 45 seconds. Based on this information, TCAS has two alerting functions: Traffic Advisories (TA), which direct the crew's attention to a potential threat, and Resolution Advisories (RA), which provide vertical collision avoidance commands to the crew. As mentioned earlier, climb/descend dissonance has already been noted between TCAS and air traffic controller instructions in actual operations. Dissonance between two different automation systems may exacerbate this type of human factors dilemma.

Recently, an ASAS concept termed Airborne Conflict Management (ACM) is being developed, and initial concepts and specifications have been drafted by an RTCA subcommittee (Kelly, 1999; RTCA, 2000). ACM uses an Automatic Dependent Surveillance-Broadcast (ADS-B) data link to enable longer look-ahead than is possible with TCAS. ADS-B periodically broadcasts aircraft information such as identification, horizontal position, velocity, altitude, and the next trajectory change point. This information may enable accurate prediction of traffic conflicts on timescales on the order of minutes. In the initial concept, ACM includes three alert levels built around two separation zones called the Protected Airspace Zone (PAZ), and a smaller Collision Avoidance Zone (CAZ). A Low Level Alert is issued well before the violation of the PAZ with the intent to allow the crew time to resolve the conflict efficiently. If implemented and used properly, Low Level Alerts should be the only alerts issued from ACM. However, if the conflict remains unresolved, a PAZ Alert will be issued. A maneuvering response should then be initiated with a minimum of delay. If the conflict is still not resolved, a CAZ Alert is ultimately issued when immediate action is required to avoid a near-miss.

Several issues relate to the interoperability between TCAS and ACM. One set of issues relates to cases where TCAS and ACM are both installed on the same aircraft. TCAS measures relative range and bearing, while ACM receives the broadcast state vector and intent. The different surveillance sources may result in two targets that need to be merged or fused on displays (Abeloos, 2000). The different surveillance methods used by TCAS and ACM may also produce different threat projections between the same targets. While ACM PAZ alerts will protect a much larger minimum separation than TCAS, the enhanced accuracy of ADS-B may allow ACM to determine that no threat exists while TCAS still predicts a threat (in some geometries). As such, TCAS may issue alerts when ACM sees no conflict at all. This may cause a problem if pilots have become accustomed to receiving ACM alerts prior to TCAS alerts. An additional source of concern would be transitioning from a lateral maneuver, which might be preferable during the resolution of a PAZ alert, to a vertical maneuver commanded by TCAS. The ability of pilots to make this transition or the degree to which they may continue the lateral maneuver needs to be studied. Finally, it would be preferable to not experience TCAS alerts at all if an ACM advisory is being followed. It is unlikely, however, due to certification requirements, that TCAS thresholds could be modified to reduce this type of dissonance. So, adjustments may need to be made to ACM instead.

A second group of issues relates to cases where TCAS is installed on one aircraft but ACM is installed on another. In this case, both aircraft can detect each other, but the two systems may issue different resolution advisories at different times. A problem exists if these resolutions are not coordinated or compatible.

Finally, a third group of issues revolves around the integration of both ACM and TCAS with yet other automated traffic alerting systems. Examples include existing or proposed ground-based conflict detection and resolution systems or specialized collision alerting systems for closely-spaced parallel approach (Isaacson, 1997; Brudnicki, 1997; Samanant, 2000). Ensuring that these systems all operate harmoniously is going to be an increasingly challenging problem given these systems' complexity.

In this chapter, we apply the framework of dissonance developed in previous chapters to model and analyze the possible dissonance between TCAS and ACM, including perceived dissonance due to process dynamics. We are then interested to mathematically identify the conditions for dissonance between the two systems, and suggest methods to avoid or mitigate the dissonance.

8.1 Identification of Conditions for Dissonance

8.1.1 Aircraft Encounter Kinematics

To simplify the case study, the analysis of TCAS and ACM is limited here to only horizontal-plane motion where the two aircraft are coaltitude and converging. Similar analysis could be done for three dimensional cases.

Several kinematics parameters are required for the mathematical description of TCAS and ACM later. Figure 8.1 shows two aircraft (0 and 1) in the horizontal plane using Cartesian coordinates oriented along and perpendicular to aircraft 0's velocity vector. This choice of frame is arbitrary but simplifies the kinematics equations somewhat. The aircraft are a distance x and y apart in this frame, and have velocity vectors $\mathbf{v}_0 = [v_{0x}, v_{0y}]^T$ with $v_{0y}=0$ and $\mathbf{v}_1 = [v_{1x}, v_{1y}]^T$. The relative position of the aircraft can also be expressed in terms of their range r and bearing χ:

$$r = \sqrt{x^2 + y^2} \tag{8.1}$$

$$\chi = \tan^{-1}(y / x) \tag{8.2}$$

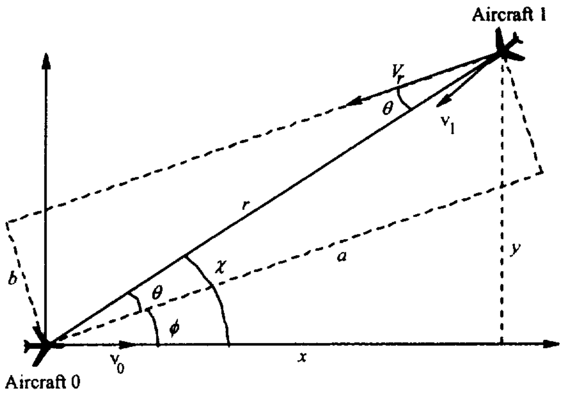


Figure 8.1 Horizontal Plane Kinematics

The relative velocity between aircraft is

$$V_r = \sqrt{(v_{1x} - v_{0x})^2 + v_{1y}{}^2} \tag{8.3}$$

which can be expressed in terms of the range rate

$$\dot{r} = -V_r \cos\theta \tag{8.4}$$

where

$$\theta = \chi - \phi \tag{8.5}$$

and

$$\phi = \tan^{-1}\left(\frac{v_{1y}}{v_{1x} - v_{0x}}\right) \tag{8.6}$$

Finally, the distance until the closest point of approach, *a*, and the miss distance, *b*, are given by:

$$a = r\cos\theta \tag{8.7}$$

$$b = r\sin\theta \tag{8.8}$$

8.1.2 Formal Description of TCAS and ACM

In the case of TCAS and ACM, the complete state vector **x** represents the three-dimensional position and velocity vectors of each aircraft involved. As mentioned above, we will focus on the horizontal plane motion of two aircraft, though the examples can be extended to three dimensions.

Consider a situation in which both ACM and TCAS are implemented on aircraft 0 in Figure 8.1. The complete state vector is not available to the alerting system logic, but is observed through a set of sensors. The resulting information that is observable to each alerting system is included in the vector **y**. For TCAS (system 1), **y** is a vector including the range and range rate between two aircraft (again, considering the horizontal plane only):

$$\begin{aligned} \mathbf{y}_1 &= [r, \dot{r}]^T \\ &= \left[\sqrt{x^2+y^2}, -V_r \cos\theta\right]^T \\ &= G_1(\mathbf{x}) \end{aligned} \qquad (8.9)$$

In contrast, ACM (system 2) uses the basic state vector components:

$$\mathbf{y}_2 = [x, y, \mathrm{v}_{0x}, \mathrm{v}_{1x}, \mathrm{v}_{1y}]^T = G_2(\mathbf{x}) \qquad (8.10)$$

So, ACM is able to observe the complete kinematics relationship in Figure 8.1. TCAS only has access to range and range rate, which significantly limits the degree to which it can predict the evolution of the encounter between aircraft.

TCAS has three system alert stages:

Stage 0 = No threat. Traffic is shown on a map display using a white diamond symbol that also indicates its altitude and whether it is climbing or descending. No additional information is provided. $\mathbf{a}_1 = 0$.

Stage 1 = Traffic Advisory (TA). A Master Caution light is illuminated in amber, the traffic icon changes to a yellow circle on the traffic display, and an aural "Traffic, Traffic" alert is issued in the cockpit. $\mathbf{a}_1 = 1$.

Stage 2 = Resolution Advisory (RA). A Master Warning light is illuminated in red, the traffic icon changes to a red square on the traffic display, and an aural resolution command is issued (such as "Climb! Climb!") and the required climb angle or climb rate is shown on a cockpit display. $\mathbf{a}_1 = 2$.

We will focus on the higher two ACM alert stages: the PAZ alert ($\mathbf{a}_2 = 1$), and the CAZ alert ($\mathbf{a}_2 = 2$). It should be remembered, however, that the TCAS alert stages carry different meanings than the ACM stages. For example, $\mathbf{a}_1 = 2$ means that an RA is issued from TCAS, while $\mathbf{a}_2 = 2$ means that a CAZ alert is issued from ACM. The actions the pilot should take in each case may be significantly different. The symbolic notation, though, provides a means for articulating the different alert stages within each system.

The vector **z** combines all the information that is displayed to the human operator by the alerting system. For TCAS and ACM, the information in **z** includes a traffic display in the cockpit, aural messages, lights, and any resolution command and guidance information.

The converging, horizontal-plane TCAS thresholds are based on four parameters: *DMOD*, *DMODTA*, τ, and τ_{TA}. At its core, the RA threshold can be defined as (RTCA, 1983):

$$r < (DMOD - \tau\dot{r}) \Leftrightarrow \text{RA Alert} \qquad (8.11)$$

if an RA is not issued, a TA occurs when the following is satisfied:

$$r^2 < DMODTA^2 - r\dot{r}\tau_{TA} \Leftrightarrow \text{TA Alert} \qquad (8.12)$$

Even though TCAS operates with only r and $\dot{r}$ as states, its thresholds can be rewritten in terms of the more general state parameters from figure 8.1. From Equation 8.12, the TA threshold then lies in state space according to the following equation:

$$a^2 + b^2 < DMODTA^2 + V_r\tau_{TA}a \qquad (8.13)$$

Or equivalently,

$$(a - \frac{V_r\tau_{TA}}{2})^2 + b^2 < DMODTA^2 + (\frac{V_r\tau_{TA}}{2})^2 \qquad (8.14)$$

So, aligned in a new (a, b) Cartesian coordinate frame in figure 8.1 (along and perpendicular to the relative velocity vector), the TA threshold is a circle centered on $(\frac{V_r\tau_{TA}}{2}, 0)$ with radius $\sqrt{DMODTA^2 + (\frac{V_r\tau_{TA}}{2})^2}$.

In a similar manner and coordinate system, the criterion for an RA (Equation 8.11) can be rewritten as:

$$(a-\frac{V_r\tau}{2})^2+b^2 < DMOD\sqrt{a^2+b^2}+(\frac{V_r\tau}{2})^2 \qquad (8.15)$$

The alert stage sets for TCAS are then formally defined by the threshold function T_1 using predicates:

$$T_1 = \begin{cases} f_{11} :(a-\frac{V_r\tau_{TA}}{2})^2+b^2 < DMODTA^2+(\frac{V_r\tau_{TA}}{2})^2 \\ f_{12} :(a-\frac{V_r\tau}{2})^2+b^2 < DMOD\sqrt{a^2+b^2}+(\frac{V_r\tau}{2})^2 \\ A_{10}=\bar{f}_{11}\cap\bar{f}_{12} \\ A_{11}=f_{11}\cap\bar{f}_{12} \\ A_{12}=f_{12} \end{cases} \qquad (8.16)$$

So, for example, if predicate f_{11} is true but f_{12} is false, then the state lies in the region A_{11} and a TA is issued.

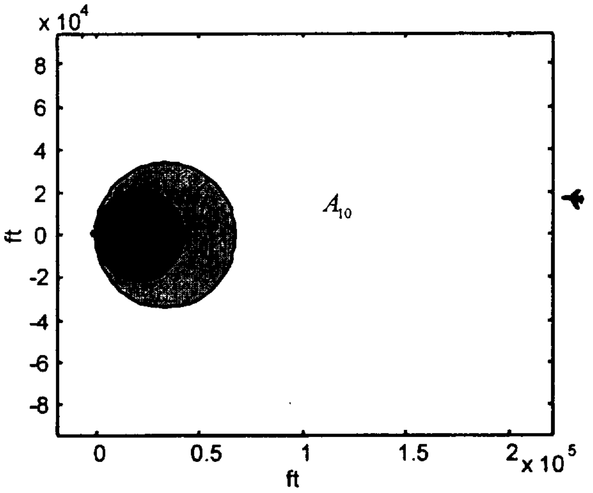


Figure 8.2 Example TCAS Threshold Function and Alert Stages

The formalized TCAS threshold function and alert stages can be visualized for a given aircraft encounter situation. Figure 8.2 shows one example case for two aircraft heading in opposite directions, each at 500 kt. The two alert threshold regions are then shown to scale in the relative frame of one aircraft, with threshold parameter values set assuming the encounter occurs at an altitude of 20,000 ft (RTCA 1983). A given type of alert will occur if the intruder aircraft enters into the regions shown.

The thresholds for ACM are based on four parameters, *PAZ*, *CAZ*, τ_{PAZ}, and τ_{CAZ} (RTCA 2000).

$$\frac{a-\sqrt{CAZ^2-b^2}}{V_r}<\tau_{CAZ} \Leftrightarrow \text{CAZ Alert} \tag{8.17}$$

if there is no CAZ alert, then a PAZ alert is issued according to:

$$\frac{a-\sqrt{PAZ^2-b^2}}{V_r}<\tau_{PAZ} \Leftrightarrow \text{PAZ Alert} \tag{8.18}$$

With ACM, A_{20} corresponds to a no-alert or low level alert condition, A_{21} corresponds to a PAZ alert, and A_{22} represents the space where a CAZ alert is issued. These regions are formally defined by the threshold function T_2:

$$T_2 = \begin{cases} f_{21} : \dfrac{a-\sqrt{PAZ^2-b^2}}{V_r}<\tau_{PAZ} \\ f_{22} : \dfrac{a-\sqrt{CAZ^2-b^2}}{V_r}<\tau_{CAZ} \\ A_{20} = \bar{f}_{21} \cap \bar{f}_{22} \\ A_{21} = f_{21} \cap \bar{f}_{22} \\ A_{22} = f_{22} \end{cases} \tag{8.19}$$

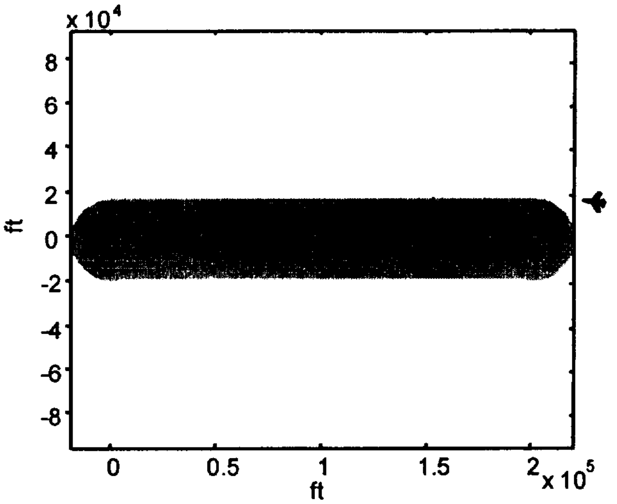


Figure 8.3 Example ACM Threshold Function and Alert Stages

With the same encounter situation shown in Figure 8.2, the formalized ACM threshold function and alert stages can be visualized in Figure 8.3, with threshold parameter values set assuming the encounter occurs at an altitude of 20,000 ft (RTCA 2000).

Equations 8.16 and 8.19 then give a formal basis by which a given state can be translated into an alert stage for each system. By then comparing combinations of alert stages between the two systems, conditions leading to static or dynamic dissonance can be identified.

8.1.3 Conditions for Dissonance

Having set up the basic alert stage regions in state space, we can analyze the two systems together. There are nine possible combinations of alert spaces between TCAS and ACM: $S_{00} = A_{10} \cap A_{20}$, $S_{01} = A_{10} \cap A_{21}$, $S_{02} = A_{10} \cap A_{22}$, $S_{10} = A_{11} \cap A_{20}$, $S_{11} = A_{11} \cap A_{21}$, $S_{12} = A_{11} \cap A_{21}$, $S_{20} = A_{12} \cap A_{20}$, $S_{21} = A_{12} \cap A_{21}$ and $S_{22} = A_{12} \cap A_{22}$.

A more convenient way of visualizing this region is to plot the four alert stages for the two systems (TA, RA, PAZ, CAZ) for a given aircraft encounter situation. Figure 8.4 shows the same encounter situation and same threshold parameter values as we showed in Figure 8.2 and 8.3.

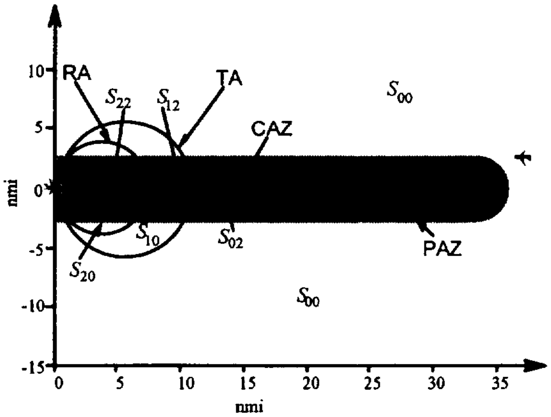


Figure 8.4 Example TCAS and ACM Thresholds

ACM is designed to provide an earlier warning of traffic than TCAS. Should this happen, there is probably no perceived dissonance from the pilot's point of view, even though the alert stage from ACM is at a higher level than that from TCAS. So, alert spaces S_{00}, S_{01}, and S_{02} are not dissonance spaces. If the opposite occurred, however, there may be perceived dissonance because the pilot may not understand why ACM does not rate the traffic as a threat while TCAS does.

For example, a TCAS RA without any prior ACM alert conditions may be perceived as dissonant if pilots become accustomed to ACM advisories occurring before TCAS alerts. This condition is represented by the set $S_{20} = A_{12} \cap A_{20}$, or equivalently in terms of predicates:

$$S_{20} = f_{12} \cap \bar{f}_{21} \cap \bar{f}_{22} \tag{8.20}$$

In terms of the specific state values involved, and because the CAZ threshold is always within the PAZ threshold, equation 8.20 can be rewritten as:

$$\left\{(a-\frac{V_r\tau}{2})^2 + b^2 < DMOD\sqrt{a^2+b^2} + (\frac{V_r\tau}{2})^2\right\} \cap \left\{\frac{a-\sqrt{PAZ^2-b^2}}{V_r} > \tau_{PAZ}\right\} \tag{8.21}$$

As Figure 8.4 shows, the PAZ region extends well in front of the CAZ, TA, and RA regions. This is intentional, to provide the pilots ample time to respond to a potential conflict well before severe maneuvering is required. The CAZ is a significantly thinner region, also extending farther forward than the TA or RA. In this situation, however, note that the TA and RA thresholds do extend laterally beyond the CAZ and PAZ regions. If an intruder were to enter the S_{10} or S_{20} regions, dissonance could be perceived if the pilot was concerned why a PAZ alert did not accompany or precede the TCAS alert. Although regions S_{10} and S_{20} appear to be relatively small in Figure 8.4, they do extend between 3 to 6 nmi laterally and cover an area over 16 nmi^2.

One difficulty in visualizing alerting behavior is that the problem is complex and multidimensional. A change in speed or heading, for example, would change the sizes and orientations of all of the alerting regions in Figure 8.4. Still, such a diagram can be useful for examining specific encounter situations.

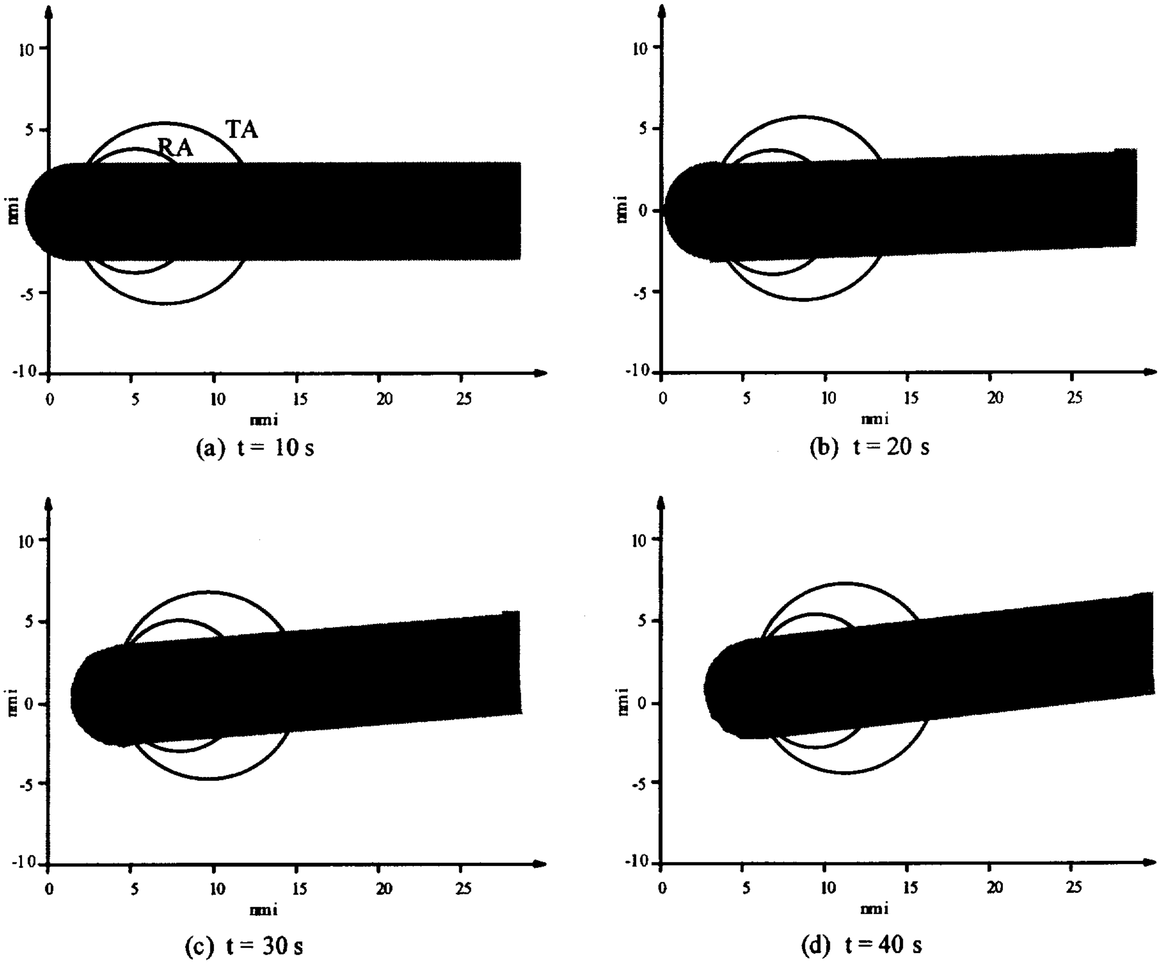
8.1.4 Perceived Dissonance Due to Process Dynamics

In addition to examining the alerting regions to expose areas where alert stage dissonance could be perceived, it is also necessary to examine the process dynamics to see how dissonance may evolve over time. One of the major issues with the integration of ACM and TCAS is how to manage ACM alerts that are later upgraded to TCAS alerts. If action is taken in response to an ACM alert, it is preferable that no TCAS alert occur (RTCA 2000). Accordingly, one issue to examine is what types of ACM resolution maneuvers are required to prevent TCAS alerts from occurring.

As a somewhat extreme example, consider a situation in which a CAZ alert is issued against one aircraft directly in front of another and heading in the opposite direction, with both aircraft at 500 kt. In response to the CAZ alert, assume that one aircraft begins a turning maneuver with a certain response delay, a roll-in to a certain bank angle, and a roll-out at a certain new heading angle.

Figure 8.5 shows four snapshots (spaced every 10 seconds) of the two aircraft and the alert thresholds assuming one aircraft follows a turning avoidance action with a 10 second time delay, 10° bank angle, and 20° final heading change. Figure 8.5(a) shows the situation immediately following the 10 seconds time delay. Approximately 10 seconds later (Figure 8.5[b]), the CAZ region is exited but the aircraft crosses the boundary of the TCAS TA region. Here, dissonance would be perceived since ACM is downgrading the alert stage and TCAS is upgrading the alert stage. Within the next 10 seconds (Figure 8.5[c]), a TA is issued. Finally (Figure 8.5[d]), an RA is issued from TCAS, commanding the pilot to climb or descend. So, in this extreme situation there is a progression from taking action in response to an ACM alert that ultimately ends in a TCAS RA. The RA command itself may also cause some confusion as the pilot must determine whether to continue the turn that has already been initiated, or to execute the climb or descent command.

The same thresholds in Figure 8.5 could also be placed on the second aircraft, which might then also receive and react to alerts. In particular, it may be relatively common for ACM to be installed on one aircraft while TCAS is installed on the other. In that situation, the ACM aircraft would begin maneuvering in response to the PAZ or CAZ alert. Unless that aircraft performed a sufficiently aggressive maneuver, a TCAS TA or RA could still be issued on the second aircraft. If not designed properly, ACM might not able to prevent the second aircraft from having to maneuver in response to TCAS.



(a) t = 10 s

(b) t = 20 s

(c) t = 30 s

(d) t = 40 s

Figure 8.5 TCAS and ACM Thresholds During Avoidance Maneuver

8.2 Management of Dissonance

To address one aspect of the TCAS / ACM compatibility issue, a Conflict Resolution System Priority Matrix has been developed (RTCA, 2000). This matrix proposes suppressing any ACM advisories that are dissonant with TCAS RAs. The main issue here is that the dissonant TCAS RA may occur *after* the ACM alert. ACM may need to be designed with some means for predicting that a TCAS alert will be occurring, and ACM advisories may need to be modified to ensure that they remain in consonance with that future TCAS alert.

An alternate way to mitigate the effect of alerting system conflicts is through operator training. Pilots will be trained, for example, that ACM and TCAS use different decision-making logic, and that alerts from the two systems may not (and in fact probably will not) occur in concert. In extreme situations, however, training should not be relied upon too greatly.

Additionally, it may be possible to modify air traffic operations themselves so that dissonance is less likely. A request to pilots to reduce their vertical speed as the aircraft nears a target altitude, for example, is one operational change that has already been made to help reduce the likelihood of dissonance between TCAS false alarms and air traffic controllers.

Finally, it may be necessary to modify the design of the logic in the new (or existing) alerting system to reduce the potential for dissonance as much as possible. It was suggested by the RTCA subcommittee, for instance, that ACM conflict resolution advisories should allow the conflict to be resolved without triggering any TCAS advisories (RTCA 2000). One means of trying to ensure this is to modify ACM-induced maneuvers so that the likelihood of triggering a TCAS alert is small. That is, through identifying the subset of $\mathbf{F}_{mn}$ $(\mathbf{F}_{mn} - \mathbf{F}_{mn\mathrm{D}})$ for ACM resolution advisories as we suggested in Chapter 6, the dynamic dissonance between TCAS and ACM could be avoided. This issue is examined in more detail in the rest of the section.

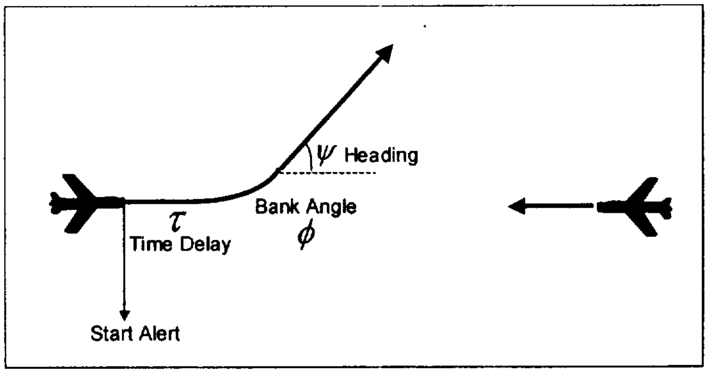


Figure 8.6 ACM Maneuver Model

To address this issue, a point-mass simulation was executed to examine the interaction between aircraft trajectories and the alert stages of ACM and TCAS (Figure 8.6). To run the simulation, an intruder aircraft was placed directly in front of a host aircraft, traveling in the opposite direction, with each aircraft at 500 kt. Upon crossing the PAZ alert threshold, a given time delay was implemented, and then the host aircraft performed a roll-in to a certain bank angle and rolled out at a given heading angle. Time delay, bank angle, and heading change parameters were systematically varied. Depending on the combination of response latency, bank angle, and turn angle, either (i) no TCAS alert would be issued, (ii) a TA would be issued during the maneuver, or (iii) both a TA and RA would be issued.

Figure 8.7 shows the interactions between delay, bank angle, turn heading, and TCAS alert status. The curves that are shown represent boundaries between different TCAS alert behaviors. Two groups of curves are shown. The solid lines represent the boundary between RA and TA (lower solid line) or between TA and no alert (upper solid line) when there is no time delay following the PAZ alert. The dashed lines show similar boundaries when there is a 10 second response delay after the PAZ alert. A combination of bank angle and turn angle toward the lower-left of the plot will result in an RA. Performing a maneuver between sets of curves will result in a TA. Making a large enough turn with a large enough bank angle (upper-right part of the diagram) will avoid any TCAS alert from occurring.

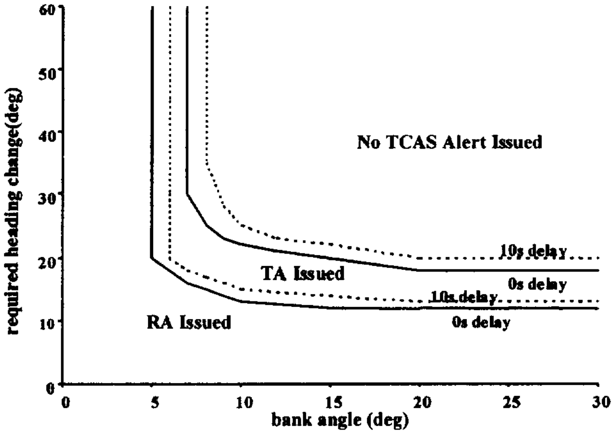


Figure 8.7 Effect of PAZ Avoidance Maneuver on TCAS Alert Status (500 kt opposite direction)

For example, shown in Figure 8.7, with no time delay and a 15 degree bank angle, the host aircraft must turn beyond 20 degrees to avoid triggering a TCAS TA. The host would have to turn at least 12 degrees to avoid triggering a TCAS RA. A 10 second response delay would add several degrees to these turn minima. Thus, relatively significant avoidance maneuvers must be performed following an ACM PAZ alert in order to prevent triggering TCAS TAs or RAs.

It is even more difficult to prevent TAs and RAs following a CAZ alert. In fact, in this 500 kt opposite-direction example, a TCAS TA cannot be avoided without exceeding an extreme maneuver (at least 30 degree bank angle and 60 degree heading change). Figure 8.8 shows the TCAS alerting behavior following a response maneuver to a CAZ alert. Avoiding an RA after a CAZ alert also requires an extreme maneuver. With a 30 degree bank angle, a 32 degree heading change is required without time delay, and 40 degree heading change is required if there is a five second delay.

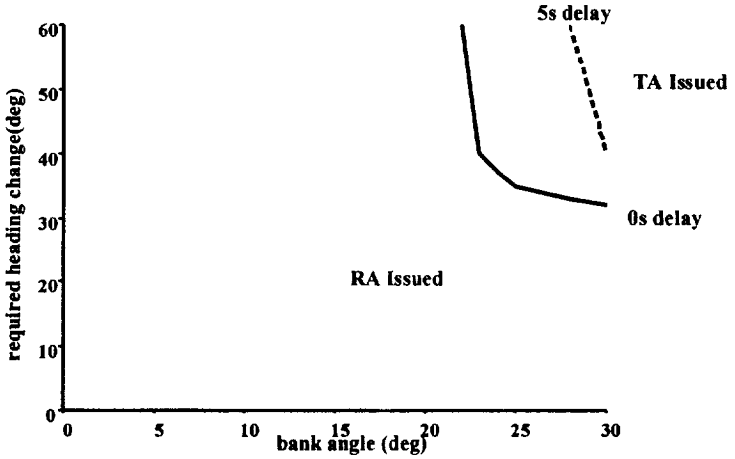


Figure 8.8 Effect of CAZ Avoidance Maneuver on TCAS Alert Status (500 kt opposite direction)

Simulations were also performed for vertical maneuvers following ACM PAZ and CAZ alerts. It was assumed that the aircraft performed a pull-up maneuver at a load factor of 1.2 g to a given vertical rate. Table 8.1 shows the minimum climb rates that are required under these conditions to avoid receiving a TCAS TA or RA alert. Climbs or descents at approximately 400 ft/min are required to avoid a TA if action is started immediately after a PAZ alert is issued. RAs are more easily avoided, with rates less than 100 ft/min required. After a CAZ alert, TAs cannot be avoided without a significantly more extreme maneuver (a load factor of approximately 2.4 g is required). RAs after a CAZ alert could be avoided with vertical rates between approximately 600 and 900 ft/min depending on the response delay of the pilot and aircraft.

Table 8.1

Vertical Maneuver Requirements (ft/min)
to Avoid TCAS Alerts (1.2 g pull-up load factor)

		0 second delay		10 second delay	
		TA	RA	TA	RA
ACM alert	PAZ	380	70	450	80
	CAZ	——	600	——	900

8.3 Summary

In this chapter, conditions for dissonance have been identified by formally describing the threshold functions of TCAS and ACM.

An analysis of the initial specifications for the ACM system in connection with the current TCAS suggest that there may be operating conditions in which TCAS alerts could occur without having first received ACM advisories. The simulations also show that it may be difficult to avoid receiving a TCAS alert even after taking action in response to an ACM alert in certain geometries. These may not be dissonance problems, but need to be investigated further to determine the scope of encounters that may lead to this type of behavior and to examine other human factors issues relating to this problem. Potential solutions include modifying the ACM threshold parameters or ACM resolution maneuvers (or both), or accepting that TCAS alerts may occur in certain geometries and training pilots to understand why that dissonance exists and how it can be resolved.

Sensor error may contribute more dissonance to that originating from the logic difference, especially for pop-up situation, which will make it harder to avoiding receiving a TCAS alert even after taking action in response to an ACM alert in certain geometries. Due to differences in sensor information, another form of dissonance can occur if TCAS rates one aircraft as a threat while ACM rates a different aircraft as a threat.

Finally, some simplification of TCAS and ACM was used to perform this initial analysis. A more detailed study that includes factors such as communication and filtering delays should be performed if higher-fidelity results are desired.

9 Summary and Conclusions

The potential for conflicting information to be transmitted by different automated alerting systems is growing as these systems become more pervasive in process operations. Newly introduced alerting systems must be carefully designed to minimize the potential for and impact of alerting conflicts (or dissonance), but little is currently available to aid this process. The development of a model of alert dissonance would therefore be beneficial in terms of providing both a theoretical foundation for understanding conflicts and as a practical basis from which specific problems can be addressed.

This thesis developed a methodology to model, analyze and mitigate conflicts between multiple alerting systems. The methodology can be used to identify different types of dissonance given two alerting systems, and also articulates the conditions that must be true for each type of dissonance to occur. Based on the formal analysis of the dissonance, several methods are described to address different problems caused by different types of dissonance. The methodology is applied to two different processes with multiple alerting systems to deal with different kinds of dissonance problems.

9.1 Summary

9.1.1 Category of Dissonance Situations

Based on a framework that facilitates articulating the specific information elements that are sensed, processed, and displayed by each alerting system, and the interactions between alerting systems, different types of dissonance are identified, including how the dissonance is connected to differences in alert stage or resolution command information. The *alert stage* specifies the level of threat according to the alerting system.

Dissonance exists when the alert information suggests different threat level and/or actions to resolve the hazard. Dissonance may not be perceived by the human operator even if the dissonance is indicated between alerting systems, if the human operator understands why the dissonance is indicated. Dissonance may be perceived even if there is no indicated dissonance at some time, the human operator can be influenced by other factors, for instance, the dynamics of the process, other nominal information, human mental model, etc.

9.1.2 Major Components Leading to Multiple Alerting Systems Dissonance

By drawing a mapping between process states and the resulting alert stages and resolution commands, two major causes of dissonance are identified: the mapping itself (different threshold functions or resolution logic) and the input (different observable state caused by sensor error).

- When two systems are designed to protect against different hazards or different time scales are used for the same hazard, threshold functions and resolution logic are usually different in order to satisfy different objectives. Thus, dissonance may perceived if the two systems are in dissonant alert stages, the intersection of allowed action spaces by the alerting systems is empty, or the trends of changes of this information is different for the same process state.
- When two systems use different sensors to monitor the process, even if they have the identical alerting thresholds or resolution logic, they may still be dissonant due to sensor error.

9.1.3 Formal Method to Identify the Conditions for Dissonance

A mathematical method is developed to identify when or where the different types of dissonance could occur in a given operation when there are logic differences between two alerting systems. By exposing those situations that lead to dissonance, the system design can be modified, operations can be changed, or the operators can be trained to work around the dissonance.

By defining the alert stages as subsets of the whole state space, combinations of alert stage subsets lead to space that may result in dissonance when two alerting systems operate simultaneously. The boundaries of alert stage subsets (threshold functions) can be defined by a set of predicates (or inequality statements) based on certain parameter values. The conditions for dissonance space can then be mathematically described as the combination of true or false predicates.

9.1.4 Method to Analyze Dissonance Originating from Sensor Error

A formal method to analyze dissonance originating from sensor error is developed. The contribution of sensor error to dissonance is identified through analyzing the effect of sensor accuracy on the probability of dissonance, and is compared against the contribution of logic differences to dissonance.

The mathematical analysis of the probability of dissonance for a given true state or a set of trajectories helps to identify the contribution of sensor error to dissonance for a given dynamic system. By defining the concepts of missed dissonance and false dissonance, it is then possible to contrast the relative contribution of sensor error to dissonance against the contribution of logic differences. This analysis may be used to help the designer decide on the optimal sensor accuracy to minimize dissonance, or it could be used to find the tradeoff between sensor accuracy and logic threshold modifications to decrease the probability of dissonance.

9.1.5 Ways to Identify Dangerous Dissonance Space

A hybrid model is developed to accurately describe the dynamic behavior of the process incorporating multiple alerting systems, in which the continuous and discrete dynamics coexist and interact with each other. Using the hybrid model, dangerous dissonance space is identified through backward reachability analysis.

The hybrid automation model developed in this thesis describes the evolution of a collection of discrete and continuous variables as a sequence of continuous dynamics and discrete transitions. While following continuous dynamics, discrete variables remain constant and continuous variables evolve according to a vector field (like a usual control system). At discrete transition times, both continuous and discrete variables change value instantaneously, according to a transition function.

Transition functions model the human operator's response to alerting system commands, including response delay and the discrete control being applied to the process. So, transition functions on the boundaries of alert stage subset combinations act as a random processor, which randomly chooses a governing differential operator based on some probability density function (PDF) of the allowed action space in that subset. Crossing boundaries of these subsets drives the activation of transition functions.

Given the hazard space of the process, dangerous dissonance space can be identified using backward reachability analysis with the hybrid model we developed. The human operator's possible response in dangerous dissonance space could lead the process to some hazard space. So, methodologies must be developed to at least avoid the dangerous dissonance space.

9.1.6 Methods to Avoid or Mitigate Dissonance

Several ways to avoid or mitigate dissonance are suggested, including prioritization, modification of system design, modification of operational procedures, modification of control strategy, and modification of procedures under dissonance. Mitigation methods should be chosen based on the advantages and disadvantages of each method, specific performance requirements of each alerting system, and the different types of dissonance that may be encountered.

- Alerting systems can be prioritized. If more than one alerting system is triggered, the lower priority alerts may be inhibited or only displayed passively. Prioritization is the simplest way to deal with dissonance and can help reduce sensory and cognitive overload of the human during a time of high stress. However, prioritization can reduce safety if two alerts are both valid but the operator is only receiving or responding to one. Also, it may be difficult to "undo" an earlier alert if a higher-priority system acts later.
- It may be necessary to modify the design of the logic in the new (or existing) alerting system to reduce the potential for dissonance as much as possible. Different from prioritization, modification of system design avoids dissonance or at least the dangerous effect of dissonance by eliminating dissonance space (those subsets of the whole state space in which dissonance occurs) or at least the dangerous dissonance space (part of the dissonance space in which the human operator's possible response

could lead the process to hazards). In general, the elimination of dissonance space may compete with a system's other performance requirements, and it may be hard to find a global optimal solution for this multi-objective optimization problem.

- It may be possible to modify operational procedures of the process so that dissonance is unlikely to be triggered (through preventing the alert that may cause dissonance with other alerts) as long as we know the conditions for the dissonance. This is a way to avoid dissonance without changing alerting system design or adding a filter to inhibit one or more alerting systems. But the modification of operational procedures may largely decrease the operating space of the whole process or induce other workload on the operators.
- Modification of control strategy of alerting systems can be used to mitigate dissonance when the dissonance is already exposed, if the dissonance cannot be avoided through the previous methods. It could be done either by modifying alerting system commands to avoid entering dangerous dissonance space, or by restricting the control to avoid hazard space once in dangerous dissonance space. But these control strategies may be hard to implement or may not exist for some situations.
- A final way to mitigate dissonance is through modifying procedures under dissonance. The operators may be trained to know the decision-making logic of each alerting system, or they could be trained to take certain control of the process once exposed to dissonance. Training alone will not affect any system design. But dissonance may still exist if the logic or sensor error differences result in situations different from the trained situation, and training may fall short in more severe cases.

9.1.7 Application of the Framework

The methodology developed in this thesis is applied to analyze two different processes with multiple alerting systems; each has different types of dissonance. These examples serve to demonstrate the flexibility of the methodology.

In-Trail Separation Example

Two different alerting systems are used to monitor an In-Trail separation process, one for safety and the other for efficient operation. A region of dissonance space exists due to an empty intersection of allowed action spaces (one system commands the operator to accelerate while the second system commands a deceleration).

The mathematical method developed in Chapter 3 is used to identify the conditions required for this dissonance to occure. The formal method developed in Chapter 4 is used to analyze the dissonance originated from sensor error. Probability of dissonance contours are computed for the whole state space given the sensor accuracy, so that the probability of dissonance for any given true state can be viewed. An example trajectory is examined to analyze the cumulative probability of dissonance, which describes the overall opportunity to trigger dissonance for the given trajectory. Finally, for a given example set of uncertain trajectories, the contribution of the sensor error to dissonance is compared to the dissonance contributed by logic differences. It is observed that there may be some benefit from sensor error to decreasing probability of dissonance for some values of sensor accuracy. But this benefit may not be good for the overall safety of the process.

The hybrid model developed in Chapter 5 is used to fully describe the hybrid phenomenon of this In-Trail separation process. The dangerous dissonance space, which is the largest part of the dissonance space in this example, is identified using backward reachability analysis of the hybrid process.

The ways to avoid or mitigate dissonance suggested in Chapter 6 are outlined in this example to demonstrate the advantages and disadvantages of each method. The optimal design of the threshold functions of two alerting systems are suggested in this example, which may increase 5% of safety compared to the original design by decreasing the percentage of trajectories entering dangerous dissonance space.

Air Traffic Separation Example

To demonstrate the application of the methodology to a real air traffic control problem, the dissonance between two traffic alert and collision avoidance systems, the existing Traffic Alert and Collision Avoidance System (TCAS) vs. the proposed Airborne Conflict Management (ACM), are modeled and analyzed.

An analysis of the initial specifications for the ACM system in connection with the current TCAS suggest that there may be operating conditions in which TCAS alerts could occur without having first received ACM advisories. The simulations also show that it may be difficult to avoid receiving a TCAS alert even after taking reasonable action in response to an ACM alert in certain geometries.

It was suggested by an RTCA subcommittee that ACM conflict resolution advisories should allow the conflict to be resolved without triggering any TCAS advisories (RTCA 2000). One means of trying to ensure this is to modify ACM-induced maneuvers so that the likelihood of triggering a TCAS alert is small (modify alerting system command to avoid dissonance).

A simulation was run for one encounter with two aircraft traveling in the opposite direction, with each aircraft at 500 kt. Upon crossing the Protected Aerospace Zone (PAZ) alert threshold, a given time delay was implemented, and then the host aircraft performed a roll-in to a certain bank angle and rolled out at a given heading angle. The simulation result shows that relatively significant avoidance maneuvers must be performed following an ACM PAZ alert in order to prevent triggering TCAS Traffic Advisories or Resolution Advisories. It is even more difficult to prevent a TCAS alert following Collision Avoidance Zone (CAZ) alert. In fact, in this 500 kt opposite-direction example, TCAS Traffic Advisories cannot be avoided without exceeding an extreme maneuver (at least 30 degree bank angle and 60 degree heading change).

Simulations were also performed for vertical maneuvers following ACM alerts. It was assumed that the aircraft performed a pull-up maneuver at a load factor of 1.2 g to a given vertical rate. The simulation result shows that climbs or descents at approximately 400 ft/min are required to avoid a TCAS Traffic Advisory if action is started immediately after a PAZ alert of ACM is issued. Resolution Advisories are more easily avoided, with rates less than 100 ft/min required. After a CAZ alert from ACM, Traffic Advisories cannot be avoided without a significantly more extreme maneuver (a load factor of approximately 2.4 g is required). Resolution Advisories from TCAS after a CAZ alert of

ACM could be avoided with vertical rates between approximately 600 and 900 ft/min depending on the response delay of the pilot and aircraft.

9.2 Conclusions

The primary contributions of this thesis are discussed below.

1. A representation of the process with multiple alerting systems has been generalized, including major components of each alerting system and interactions between alerting systems. The representation has been used to identify the major causes of dissonance and different types of dissonance between two given alerting systems.

2. A mathematical method has been developed to identify when or where different types of dissonance could occur in a given operation when there are logic differences between two alerting systems. Given the conditions for dissonance, the dissonance problems can be addressed practically.

3. A probabilistic analysis methodology has been developed to estimate the probability of dissonance originating from sensor error. The methodology also provides ways to compare the contribution of sensor error to dissonance against the contribution of logic differences, through defining the concepts of missed dissonance and false dissonance.

4. A hybrid model has been developed to fully describe the hybrid phenomenon in the process with multiple alerting systems. The model has been used to identify dangerous dissonance space through backward reachability analysis of the hybrid process. Dangerous dissonance must be avoided or mitigated either through modifying alerting system logic design or through modifying the control strategy of the process. The model can also be used to identify other parts of dissonance space with negative consequences, e.g., inefficient operation.

5. Five different methods to avoid or mitigate dissonance have been outlined. The advantages and disadvantages of each method have been described. All these methods have been applied in the In-Trail Separation example to demonstrate the feasibility of each method.

6. In the analysis of dissonance between two real traffic alert and collision avoidance systems (the existing Traffic Alert and Collision Avoidance System (TCAS) vs. the proposed Airborne Conflict Management (ACM)), the benefit to expose and mitigate dissonance is shown using the methodology developed in this thesis. Using the methodology, the conditions for dissonance where TCAS alerts occur without having first received ACM advisories are identified, and dynamic dissonance where a TCAS alert is triggered after taking action in response to an ACM alert is determined for certain geometries. One of the suggested mitigation methods, modifying the alerting system command to avoid dissonance, has been recommended to avoid this dynamic dissonance.

9.3 Recommendations

Because of its generalized nature, the methodology developed in this thesis can be applied to model and analyze the interactions between any decision support systems. Advanced decision support systems that are currently under consideration in the aerospace industry would benefit from this work. For example, the Center TRACON Automation System (CTAS), which is being developed at the NASA Ames Research Center, generates air traffic advisories designed to increase fuel efficiency, reduce delays, and provide automation assistance to air traffic controllers. CTAS itself includes several automation functions, all of which must be well integrated not only within CTAS itself, but also with other ground-based systems and airborne systems. The methodology in this thesis can be applied to determine interaction issues among automation functions within CTAS, between CTAS and other ground-based systems, and between CTAS and airborne decision support systems. The hybrid model developed in this thesis can be applied to model CTAS functions, examine the dissonance space to verify the safety and reachability specifications, and discover ways to optimize the CTAS design or operational procedure to minimize potential dissonance.

In addition, the application of the methodology developed in this thesis is not restricted to the aerospace industry; it can also be applied to automobiles, chemical and power control stations, and medical monitoring systems, where automated alerting systems are becoming increasingly pervasive.

References

[1] Abeloos, A., Mulder, M., and Paassen, R. V. (2000, September 27-29), "Potential Co-operations Between the TCAS and the ASAS", International Conference on Human-Computer Interaction in Aeronautics, Toulouse, France.

[2] Altman, E. and Gaitsgory, V. (1997), "Asymptotic optimization of a nonlinear hybrid system governed by a Markov decision process," SIAM Journal of Control and Optimization, 35(6):2070-2085.

[3] AMIA 2000 Panel Presentation (2000), "Advanced Clinical Alerting systems: Do they Impact Patient Outcomes?".

[4] Asarin, E. , Bournez, O. , Dang, T. , Maler, O. , and Pnueli, A. (2000, July), "Effective synthesis of switching controllers for linear systems," Proc. IEEE, vol. 88, pp. 1011-1025.

[5] Automatica (1999, March), "Special issue on hybrid systems," vol. 35, no. 3.

[6] Berson, B., Po-Chedley, D., Boucek, G., Hanson, D., Leffler, M., and Wasson, H. (1981, January), "Aircraft Alerting Systems Standardization Study, Vol. 2: Aircraft Alerting System Design Guidelines", DOT/FAA/RD-81/38/II, National Technical Information Service, Springfield, VA.

[7] Boucek, G., Po-Chedley, D., Berson, B., Hanson, D., Leffler, M., and White, R. (1981, January), "Aircraft Alerting Systems Standardization Study, Vol. 1: Candidate System Validation and Time-Critical Display Evaluation", DOT/FAA/RD-81/38/I, National Technical Information Service, Springfield, VA.

[8] Branicky, M. S. (1995, June), "Studies in Hybrid Systems: Modeling, Analysis, and Control," Doctor of Science thesis, dept. of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, Massachusetts.

[9] Brudnicki, D., Lindsay, K., and McFarland, A. (1997, October 26-30), "Assessment of Field Trials, Algorithmic Performance, and Benefits of the User Request Evaluation Tool (URET) Conflict Probe", *16th Digital Avionics Systems Conf.*, Irvine, CA.

[10] Carrick, I. (1997, March), "Incorporating Human Factors into Safety Systems in Scottish Nuclear Reactors", Proceedings of the Workshop on Human Error and Systems Development, pp. 27-33, Glasgow, Scotland.

[11] DeCelles, J. L. (1992, January), "Delayed Response to GPWS Warnings", *Air Line Pilot*, Vol. 61, No. 1.

[12] Endsley, M. R. (1995), "Toward a Theory of Situation Awareness in Dynamic Systems", *Human Factors*, Vol. 37, No. 1, pp. 32-64.

[13] German BFU Web (July, 2002). German Federal Bureau of Aircraft Accidents Investigation [On-Line], Available: http://www.bfu-web.de/aktuinfo-e28.htm.

[14] Hawkins, F. H. (1987), *Human factors in flight*, Aldershot, England: Ashgate.

[15] IEEE Trans. Automat. Contr. (1998, April) "Special issue on hybrid control systems," vol. 43.

[16] Isaacson, D. and Erzberger, H. (1997, October 26-30), "Design of a Conflict Detection Algorithm for the Center/TRACON Automation System", *16th Digital Avionics Systems Conf.*, Irvine, CA.

[17] Kelly, W. E. (1999, October), "Conflict Detection and Alerting for Separation Assurance Systems", 18th Digital Avionics Systems Conference, pp. 6.D.1-1 – 6.D.1-8, St. Louis, MO.

[18] Koutsoukos, X. D. , Antsaklis, P. J. , Stiver, J. A. , and Lemmon, M. D. (2000, July), "Supervisory control of hybrid systems," Proc. IEEE, vol. 88, pp. 1026-1049.

[19] Kremer, H, Bakker, B, and Blom, H. (1997, June 17-20), "Probabilistic versus Geometric Conflict Probing," Air Traffic Management Seminar, Saclay, France.

[20] Krozel, J., Peters, M., and Hunter, G. (1997, April), "Conflict Detection and Resolution for Future Air Transportation Management," NASA CR-97-205944.

[21] Kuchar, J. K. and Carpenter B. D. (1997), "Airborne Collision Alerting Logic for Closely-Spaced Parallel Approach", *Air Traffic Control Quarterly*, Vol. 5, No. 2, pp. 111-127.

[22] Kuchar, J. K., and Yang, L. C. (2000), "A Review of Conflict Detection and Resolution Modeling Methods," *IEEE Transactions on Intelligent Transportation Systems*, Vol. 1, No. 4.

[23] Lygeros, J., Tomlin, C. , and Sastry, S. (1999, March), "Controllers for reachability specifications for hybrid systems," Automatica, pp. 349-370.

[24] Lynch, N., Segala, R., Vaandrager, F., and Weinberg, H.B. (1996), “Hybrid I/O automata,” Hybrid Systems III. New York: Springer-Verlag, no. 1066 in LNCS, pp. 496-510.

[25] Momtahan, K., Tetu, R., and Tansley, B. (1993), “Audibility and Identification of Auditory Alarms in the Operating Room and Intensive Care Unit”, *Ergonomics*, Vol. 36, No. 10, pp. 1159-1176.

[26] Najm, W., Koopmann, J., and Smith, D. (2001, June), “Analysis of Crossing Path Crash Countermeasure Systems”, Paper No. 378, 17th International Technical Conference on the Enhanced Safety of Vehicles, Amsterdam, Netherlands.

[27] Pritchett, A. R. & Hansman, R. J. (1997, January), “Pilot Non-Conformance to Alerting System Commands During Closely Spaced Parallel Approaches”, MIT Aeronautical Systems Laboratory Report, ASL-97-2, Cambridge, MA.

[28] Pritchett, A. R. & Yankosky, L. J. (2000, August), "Pilot Performance At New ATM Operations: Maintaining In-Trail Separation And Arrival Sequencing", *AIAA Guidance, Navigation, and Control Conference*, Denver, CO.

[29] Pritchett, A., Vandor, B., and Edwards, K. (2002, February), “Testing and Implementing Cockpit Alerting Systems”, *Reliability Engineering and System Safety*, Vol. 75, Issue 2, , Pages 193-206.

[30] Proc. IEEE (2000, July) “Special issue on hybrid systems: Theory and applications,”, vol. 88.

[31] Radio Technical Committee on Aeronautics (RTCA) (1983, September), “Minimum Performance Specifications for TCAS Airborne Equipment”, Document No. RTCA/DO-185, Washington, D.C..

[32] Radio Technical Committee on Aeronautics (RTCA) (2000, December), “Application of Airborne Conflict Management: Detection, Prevention, and Resolution”, Document No. RTCA/DO-263, Washington, D.C..

[33] Samanant, P., Jackson, M., Haissig, C. and Corwin, W. (2000, March), “CASPER/AILS: An Integrated DGPS/ADS-B Airborne Alerting System for Closely Spaced Parallel Approaches”, AIAA/IEEE PLANS Conf..

[34] Sarter, N. , and Woods, D. (1995), "How in the World Did We Ever Get Into That Mode? Mode Error and Awareness in Supervisory Control", *Human Factors,* Vol 37, No. 1, pp. 5-19.

[35] Sheridan, T. B. (1992), *Telerobotics, Automation, and Human Supervisory Control,* MIT Press, Cambridge, MA.

[36] Skafidas, E. , Evans, R.J. , and Mareels, I.M. (1997), "Optimal controller switching for stochastic systems," IEEE Conference on decision and control, pp 3950-3955, San Diego, CA.

[37] Song, L., and Kuchar, J. K. (2001, June 11-12), "Describing, Predicting, and Mitigating Dissonance Between Alerting Systems", 4th International Workshop on Human Error, Safety, and System Development, Linköping, Sweden.

[38] Syst. Control Lett. (1999, October), "Special issue on hybrid systems," vol. 38, no. 3.

[39] Swiss Aircraft Accident Investigation Bureau (2001, June), "Final Report of the Aircraft Accident Investigation Bureau", Bern.

[40] Tomlin, C. J. , Lygros, J. , and Sastry, S. (2000, July), "A game theoretic approach to controller design for hybrid systems," Proc. IEEE, vol. 88, pp. 949-969.

[41] Tsai, C. (1998), "Composite stabilization of singularly perturbed stochastic hybrid systems," International Journal of Control, 71(6):1005-1020.

[42] UK AAIB Web (October, 1999). United Kingdom Air Accidents investigation Branch Bulletins [On-Line], Available: www.aaib.dtlr.gov.uk/bulletin/oct99/dabek.htm.

[43] Veitengruber, J., Boucek, G., and Smith, W. (1997, May), "Aircraft Alerting Systems Criteria Study, Vol. 1: Collation and Analysis of Aircraft Alerting Systems Data", FAA-RD-76-222, National Technical Information Service, Springfield, VA.

[44] Ververs, P. M., Good, M. D., Rogers, W. H., Riley, V., and Dorneich, M. C. (1999, September), "Alerting and Notification of Conditions Outside the Aircraft: Concept Defined and Prototyped", Final report, Honeywell Technology Center.

[45] Waller, M. and Scanlon, C., eds. (1996, December), "Proceedings of the NASA Workshop on Flight Deck Centered Parallel Runway Approaches in Instrument Meteorological Conditions", NASA Conference Publication 10191, Hampton, VA.

[46] Wickens, C. D. (1992), *Engineering Psychology and Human Performance*, Harper Collins.

[47] Winder, L. F., Kuchar, J. K. (2000, August), "Generalized Philosophy of Alerting with Applications for Parallel Approach Collision Prevension", Document No. ICAT-2000-5, Cambridge, MA.

[48] Yang, L., and Kuchar, J. K. (1998, August), "Using Intent Information in Probabilistic Conflict Analysis", Proc. 1998 AIAA Guidance, Navigation, and Control Conf., AIAA-98-4237, Boston, MA, pp. 797-806.

Appendix

Hazard Avoidance Alerting with Markov Decision Processes

Lee Winder & James Kuchar
International Center for Air Transportation
Massachusetts Institute of Technology

A.1 Overview

Alerting systems for hazard avoidance are increasingly prevalent and complex. Newer alerting logics often use many input state variables, are able to produce a variety of alert signals, and can take years to fine tune for desired behavior. Some of these not only cue the human to the hazard's presence, but give explicit guidance for resolving the situation. To speed the design process for such logics, efforts were made in recent years to describe the structure and goals of alerting in general mathematical terms (e.g. Kuchar & Yang[1,2]). The resulting theory identifies False Alarms and Safe Alerts, couched in probabilistic terms, as a set of outcome categories adequate for characterizing overall system performance. Time has revealed some limitations in this theory. Among these are that it fails to explain how Nuisance Alerts are distinct from False Alarms and how they can be minimized,[*] and that it assumes post-alert guidance will follow a fixed, planned trajectory even though dynamic replanning is often desired. Of particular interest, for example, is whether an alert should be delayed until more complete information is attained, or whether action should be taken at the current time even though there are significant unertainties. The objective of this work is to develop and illustrate new methods for alerting system design that address such limitations of the existing theory.

The proposed solution is to design the alerting logic as a kind of "rational agent" (rational in that it makes the most of available information to achieve given goals). The agent maintains a model of its operating environment, consistent with observations and prior information, and applies it along with an outcome utility model to choose actions

[*] Nuisance Alerts are alerts the human considers incorrect. These may be distinct from False Alarms, defined as alerts where the incident of concern would not have occurred otherwise.

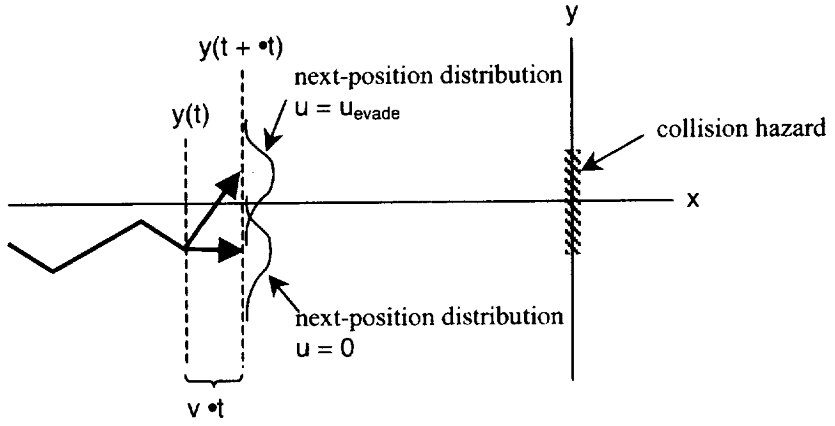
that maximize the benefit to itself. In particular we are developing decision theoretic alerting agents (using the theory of Markov decision processes (MDP) and partially observable Markov decision processes (POMDP)),[3] where probability theory provides the modeling language. An expected benefit of this approach is alerting behavior that can follow idealized human judgment with a proper utility model, tending to avoid nuisance alerts and perceived late alerts. Another benefit is that dynamically planned evasion guidance comes naturally from the MDP model, while current methods usually require ad hoc design of guidance dynamics for a given threshold.

The MDP-based alerting concept has been applied to a simple hazard avoidance process that resembles some problems of current interest (e.g. terrain avoidance for aircraft). In future work these methods will be extended to cover more complex problems such as tactical collision avoidance between aircraft pairs. Future work will also include a more formal mathematical description of the decision theoretic alerting framework. The remainder of this appendix describes some work accomplished up to this point and outlines a plan for future research.

A.2 Initial Work with a Testbed System

As an initial step in modeling Markov decision processes, experimentation was carried out for the simple collision avoidance process shown in Fig. 1. This example has been intentionally generalized and abstracted; later work will link this general model with more concrete applications. The x and y axes describe the position of a "vehicle" in a plane. As shown, the vehicle approaches from the left and moves at constant speed in the positive x direction, with y position varying according to a first-order discrete-time Markov process. If the vehicle crosses the y axis within the highlighted region near the origin, a collision occurs. An alerting system affects the process dynamics through the control variable u, which can take either of two discrete values, 0 and u_{evade}, where $u_{evade} > 0$. When $u = 0$ the process is a discrete random walk or Brownian motion process, and this is defined as the nominal behavior of the process. When $u = u_{evade}$ there is a bias on the distribution mean of the next y position, as illustrated. Nominally the alerting system defers alerting by choosing $u = 0$ (the "nominal action"). When an evasion maneuver is deemed necessary to avoid the hazard, the alerting system sets $u =$

u_{evade}. This marks the beginning of an alert and the process dynamics change accordingly. Afterward the alerting system is still free to set $u = 0$ if this is the best choice available, at which point the process will return to its nominal dynamics.



$x(t + \bullet t) = v \bullet t$ 　　 u = Alert input = $\begin{cases} 0, & \text{nominal (defer alert)} \\ u_{evade}, & \text{constant bias} \end{cases}$

$y(t + \bullet t) = y(t) + u + w$ ← w = Gaussian white sequence

Fig. 1 First-order Markov System with Hazard

Note that because the process is a Markov process and the alerting system is assumed able to make exact observations of the entire process state, $\{x, y\}$, this decision problem is a regular Markov Decision Process (MDP). In more complex problems to be studied later, the process state will not be fully observable by the alerting system, for example due to sensor limitations. Such decision problems are referred to as Partially Observable Markov Decision Processes (POMDP).

The alerting system is modeled as a rational agent that classifies possible outcomes of its actions in terms of utility it would gain. A simple utility structure was defined for this example as illustrated in Fig. 2. If the vehicle reaches the y axis without colliding with the hazard and without any alert from the alerting system, the alerting system realizes a positive utility of U_o. If no alert is issued but a collision occurs, the utility is zero. If after receiving an alert the vehicle misses the hazard then the utility is U_1, which is assumed to be positive and less than U_o. If a collision occurs following an alert, the utility is zero. This classification reflects competing desires to avoid both collisions and unnecessary alerting interventions. The closer U_1 is to U_o, the less important alert avoidance is relative to collision avoidance, and the earlier alerts would tend to occur. In truth the requirements of the human, and therefore of the alerting system, may imply a different or more complex description of utilities. For example, this utility scheme would not penalize high frequency switching between the two u values, which could result in control sequences that are difficult for a human to follow, but a penalty for such switching could be injected into the utility model if desired.

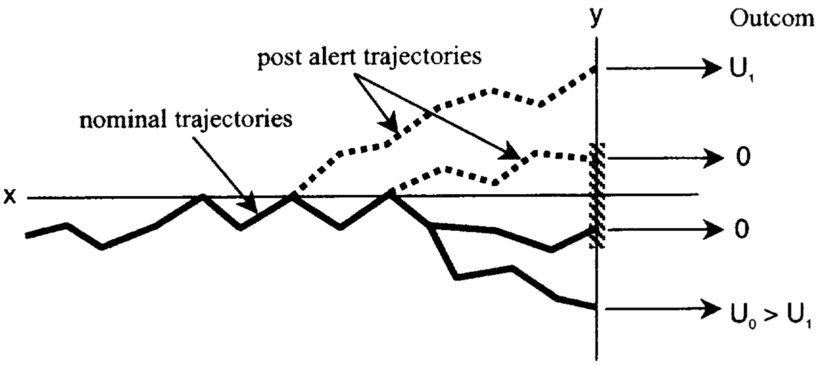
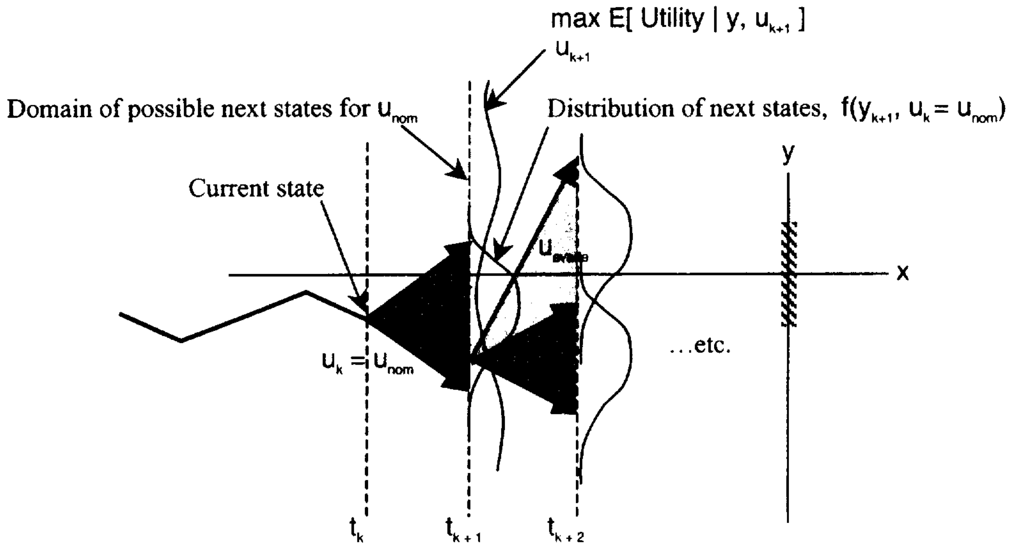


Fig. 2 Outcome Utility Definitions

Due to process uncertainty the alerting system must make control decisions based on expected rather than exact outcome utilities. By the Maximum Expected Utility principle, the preferred action is the one with the highest expected utility. Mathematically speaking, the expected utility of a given alert action u_k at time step k (in this case $u_k = 0$ or $u_k = u_{evade}$) can be stated as an integral of the product of the maximum expected utility of a state and likelihood of arriving at that state over all possible next states. For this example:

$$E[\text{ Utility} \mid u_k\,] = \int \max_{u_{k+1}} E[\text{ Utility} \mid y, u_{k+1}\,]\, f(y_{k+1}, u_k) dy$$

For each possible next state the maximum expected utility is the then greatest of the expected utilities over possible actions that could be taken from there. Each of those expected utilities is determined in the same way just described for the current state. Thus, the expected utility (and maximum expected utility) follows from a recursive calculation. The recursion eventually terminates where the maximum expected utility becomes trivially determined—in this case, when the y axis is reached the maximum expected utility is U_1, U_0 or 0, depending on the endpoint and trajectory taken to get there. These ideas are illustrated in Fig. 3 for the testbed process.



max E[Utility | y, u_{k+1}]
u_{k+1}
Domain of possible next states for u_{nom}
Distribution of next states, $f(y_{k+1}, u_k = u_{nom})$
y
Current state
u_{evade}
x
...etc.
$u_k = u_{nom}$
t_k
t_{k+1}
t_{k+2}

Fig. 3 Recursive Computation of Expected Utility at {x_k, y_k} for the Nominal Action

Though imagined easily enough, in general a pure recursive calculation of this sort is not practical beyond a few steps into the future, and more efficient methods must be found to estimate expected utilities. In this particular example it was noted that values of expected utility for each alert action could be computed offline over the state space of the process (the x, y plane), and stored in table form. The utility functions are smooth, so utilities at arbitrary positions can be approximated through interpolation on a discrete matrix of stored values. The function values follow directly from required boundary values and the defined process dynamics, and can be determined numerically.

Fig. 4 shows contours of the resulting utility functions. Expected utility is highest in the outermost regions (approaching U_0 for the Deferred Alert case, and U_1 for the Alert case), and decreases to zero toward the innermost regions.

Prior to alert the decision logic is to compare the Deferred Alert with the Alert utility at successive observed states, and to choose the action with the highest utility. In other words if the difference { E[Utility | Defer] – E[Utility | Alert] } is positive the alert is deferred, and if it is negative an evasion command is issued. The alert threshold is represented as a contour of zero expected utility in Fig. 5.

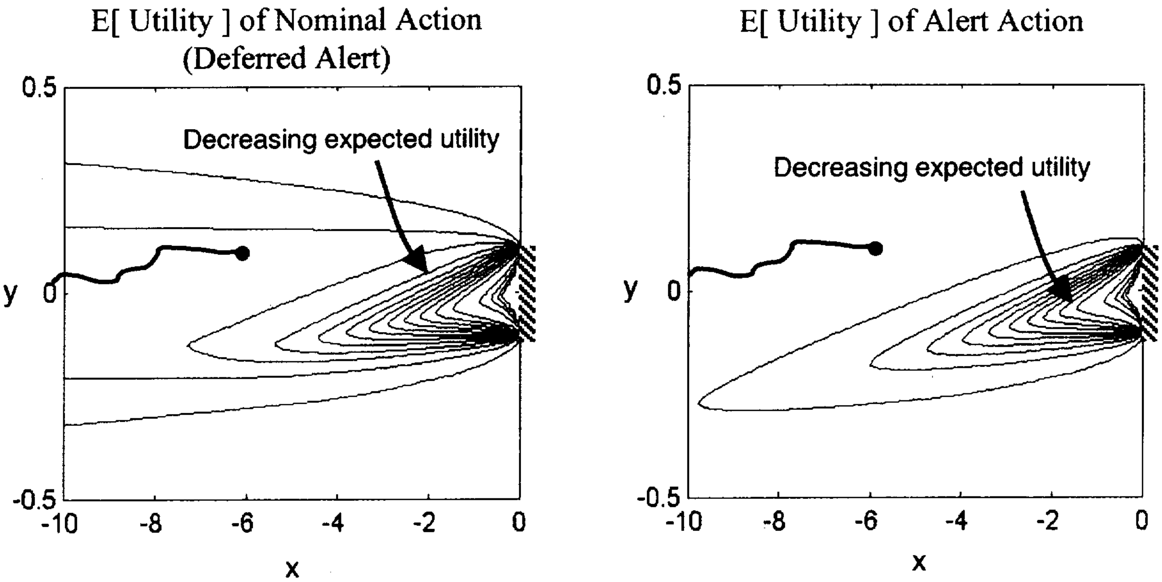


Fig. 4 Contours of Expected Utility for Each Alert Action (prior to alert)

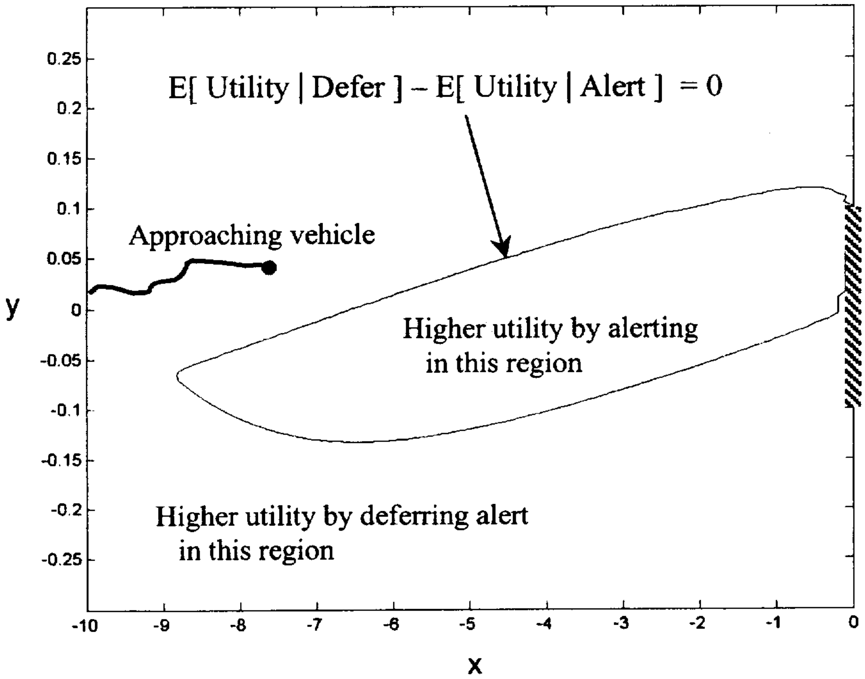


Fig. 5 Utility-based Alert Threshold for Testbed System

After an alert is initiated the Nominal Action expected utility function can be discarded because it no longer applies. It may now be necessary to introduce a new utility function at that time in order to judge the utility of the $u_k = 0$ option.

A point worth noting is that the MDP-based alerting method produces a reactive action "policy" for all possible states rather than updating a planned trajectory repeatedly as do many other alerting and conflict resolution methods. Those other methods are effectively ignoring information that is available to the decision maker, namely the impact of future observations on future decisions. A policy is a logical result of directly considering possible future observations as well as possible future actions.

A.3 Outline of Thesis

The following is an outline of planned future work in this area. The MDP-based decision-theoretic alerting philosophy will be developed more fully and formally. Future case studies will attempt to solve more complex hazard avoidance problems where the process must be modeled as a POMDP rather than a standard MDP. In that case it may be difficult or impossible to determine the complete policy solution. An example is collision avoidance alerting for pairs of aircraft on parallel approach, where aircraft may behave differently depending on unobservable dynamic modes.

1) Introduction

   a) Background

      Introduce alerting systems for hazard avoidance. Alerting systems warn operators of some hazard and may simply warn of a hazard condition, or also indicate the need for prescribed evasion maneuvers, or accompany dynamically planned guidance for avoiding the hazard.

   b) Rational agents for alerting

      Notion that certain kinds of alerting systems should be designed in the form of "rational" monitoring agents with knowledge and goals consistent with those of the system operators.

   c) MDP-based alerting

Markov decision processes are an established means of modeling rational sequential decisions in a world with stochastic dynamics. Based on probability and utility theory and the maximum expected utility principle.

d) Thesis roadmap

2) Alerting systems background

a) Purpose

Discuss the purpose of alerting systems.

Can think of alert either as conveying some information that the operator can use in replanning, or as signal from a virtual co-pilot or controller with full knowledge and authority to intervene with guidance.

i) Detection/Provide state information
ii) Intervene and provide guidance

b) Generalizations about system structure, inputs, outputs

Discuss the structure and environment of an alerting system, the input and output relationships and influences.

i) Environment
ii) Hazards/Incidents
iii) Humans
iv) Alert stages
v) Maneuver guidance
vi) Noise, Disturbances
vii) Training, protocol
viii) Experience

c) Alerting system performance

Aspects of alerting system performance relevant to the design process. Safety and false alarms are defined relative to the incident or hazard of concern. Nuisance alerts and perceived late alerts are defined with respect to the operator's perception of the need for an alert. There should also be a means of judging whether evasion maneuvers or guidance are appropriate. Perceived failures of the alerting system may result in operator non-conformance to future alerts, making safety and false alarm metrics difficult to predict or control.

i) Safety
ii) False alarms
iii) Nuisance alerts

iv) Perceived late alerts
v) Evasion maneuvers
vi) Operator conformance to alerts

d) Probabilistic metrics

Probabilistic threshold-specific measures of safety and false alarms have been suggested as better than traditional subjective judgment and global Monte Carlo metrics. SOC analysis method and assumptions.

i) P(SA), P(FA)
ii) SOC plots

3) Design methods

a) Traditional methods (state-space design)

Traditional design involves refining alert criteria in state space through iterative testing and adjustment using Monte Carlo simulation for global metric calculation, and examination of the behavior of the logic for individual scenarios. SOC analysis is a more recent tool.

i) Candidate logic
ii) Trajectory simulations
iii) Monte Carlo simulations
iv) Global probabilistic metrics
v) SOC analysis: Threshold probabilistic metrics

b) Probabilistic (SOC) design space

Defining the alert threshold directly in the space of probabilistic performance metrics is another option meant to produce an alerting threshold with desirable properties in a more direct way.

c) Issues with probabilistic design

The probabilistic design method does not explicitly address nuisance alerts that may lead to operator non-conformance. Only incident and false alarm probabilities are directly controlled and the rest is left to designer judgment. There has also typically been a restrictive assumption of fixed, planned maneuvers and therefore no explanation of dynamic evasion guidance planning as used in some systems (TCAS).

i) Make alerting decision in terms of P(SA), P(FA) only
ii) Trajectory assumptions when calculating metrics

iii) Nuisance and late alerts
iv) Ad hoc guidance design

4) Alerting system as rational dynamic decision maker

Some have stated that nuisance alerts and perceived late alerts result from a mismatch between the mental alert threshold of the operator and the threshold used by the logic, or occur when the operator deems the alert & guidance unjustified by circumstances. One option is to force conformance through training. Another is to try to bring the alert logic in line with the human's thinking (or at least ideal thinking that the human would agree with). This notion is generalized in this work in that the logic's guidance behavior is determined by the same process as the alert threshold.

a) Nuisance and perceived late alerts issue with P(SA), P(FA)-based logic

i) Pritchett experiments and conclusions
ii) Use of training to improve conformance
iii) Making the logic agree with the human operator

b) Operators as "rational" decision makers

"Rational" decision making by an agent in an uncertain world involves some model of the world state and dynamics, a means of representing uncertainty and incorporating observations into beliefs about the world state, and a description of the goals of the agent. It also requires understanding the way anticipated future observations can affect behavior by reducing uncertainty.

c) Alerting system as a decision maker parallel to operators and having the same goals (virtual copilot or ATC), and the nuisance alert hypothesis

5) Theory of Markov Decision Processes (utility-based sequential decision theory)

There are many ways to model "rational" decision making. We focus on one.

Markov decision processes (MDP) and partially observable Markov decision processes (POMDP) are a very general mathematical representation of decision processes in uncertain stochastic environments. This theory will be discussed in the context of alerting and guidance systems for hazard avoidance.

MDP theory uses state variables and probability distributions to model an agent's beliefs about the world. Observations of the world result in updates to the distribution over possible states. Agent goals can be modeled in terms of the utilities or values of different outcomes. The agent chooses successive actions to maximize the expected utility that can be achieved (Maximum Expected Utility principle). In general this theory results in a reactive "policy" that maps each possible world belief distribution into the action the agent would take. There is no planning of a single future action sequence. This policy can be computed exactly in some cases, but usually one must resort to approximate methods.

a) Modeling rational decision processes
b) Markov process state
c) Observations
d) Actions
e) Belief distribution over state ("sufficient statistic" for prediction)
f) Belief updating
g) Expected utility of action
h) Utility definitions
i) Maximum expected utility principle
j) Policies
k) Importance of anticipated future observations in choosing actions
l) Solving MDPs
   i) Exact policy solutions
   ii) Policy approximation
m) Solving partially observable MDPs (POMDPs)

6) Case study: Basic Markov process (MDP problem)

Alerting using MDP concepts is explored using a simple example with a fully observable environment. A simple problem like this could represent encounters between non-cooperative vehicles, terrain avoidance, or encounters with uncertain weather phenomena.

Demonstrate goal modeling methods, policy generation, other basic MDP concepts with an alerting example. Show the importance of considering all future actions that might be taken. Look at implications for SOC-based threshold.

a) Utility structure
b) Policy derivation
c) Discussion

   i) Like an en route alerting problem , CFIT avoidance, weather?
   ii) Demonstrate value function and policy concepts with alerting
   iii) Relationship of utility threshold to SOC threshold
   iv) Effects of anticipating future observations?
   v) Effects of allowing "replannable" maneuvers

7) More case studies:

The following include more complex problems with unobservable world state variables (different dynamic modes), where POMDP methods must be used. Must generate and maintain a belief distribution over possible states, and the effects of anticipating future observations and of flexible evasion maneuvers may be more pronounced.

Case study: Parallel approaches

a) Alerting application with unobservable state variables ("modes")
   i) Requires POMDP solution methods
b) Demonstrate belief state updating
c) Necessary state variables
d) Value of replannable maneuver over fixed planned maneuver
e) Comparison to PRM, AILS thresholds
   i) Similarities and improvements

Case study: TCAS-like logic

a) Alerting application with unobservable state variables ("modes")
   i) Requires POMDP solution methods
b) Demonstrate belief state updating
c) Necessary state variables
   i) Is there a benefit to additional state dimensions over r, h in TCAS?
d) Value of replannable maneuvers
e) Comparison to TCAS threshold and maneuver behavior
   i) Similarities and improvements

Case study: Automotive Collision Avoidance

a) e.g. Rear-end collisions, intersection collisions, head-on collisions

8) Summary & Conclusions

Anticipated contributions:
a) Classification of alerts into information and intervention types
b) Alerting threshold methodology that
   i) directly tries to minimize nuisance alerts and perceived late alerts
   ii) directly accounts for possibility of deferred alerts and future choices
   iii) directly accounts for effects of anticipated future observations on threshold placement
c) Framework for generating dynamic evasion guidance
   i) Current methods are ad hoc additions to some alert threshold
d) Single theory to determine threshold and guidance logic
e) Insight into applicability of SOC theory
f) Insight into selection of state variables for alerting
   i) e.g. Are "higher derivatives" useful?

Appendix References

[1]Kuchar, James K. *Methodology for Alerting System Evaluation.* Journal of Guidance, Control, and Dynamics. Vol. 19, No. 2. March-April 1996. p. 438-444.

[2]Yang, Lee C. & James K. Kuchar. *Performance Metric Alerting: A New Design Approach for Complex Alerting Problems.* IEEE Transactions on Systems, Man and Cybernetics--Part A: Systems and Humans, Vol. 32, No. 1. January 2002.

[3]Russell, Stuart & Peter Norvig. *Artificial Intelligence: A Modern Approach.* 2nd Ed. Prentice Hall. 2003.