THE JOURNAL OF NAVIGATION (2013), **66**, 719–735. © The Royal Institute of Navigation 2013
doi:10.1017/S0373463313000337

Introducing Unmanned Aircraft Systems into a High Reliability ATC System

Peter Brooker

(*Aviation Consultant*)
(E-mail: p_brooker@btopenworld.com)

Civil and military unmanned aircraft systems (UAS) operations are currently subject to restrictions that put major limits on their use of airspace. There is considerable debate about how to develop the safe, secure and efficient integration of UAS into non-segregated airspace and aerodromes. This paper examines a *necessary* safety aspect. Airlines and their passengers would obviously ask, "Is it still safe with all these unmanned aircraft around?" The spotlight must be on Air Traffic Control Systems as High Reliability Organizations (HRO). That status comes from industry characteristics: focus on safety, effective use of technological improvements, learning from feedback from accidents/incidents, and an underpinning safety culture. The safety of ATC Systems has improved dramatically: accidents are now the product of rare and complex 'messes' of multiple failures. It is therefore a major challenge to preserve the HRO status by ensuring at least current safety performance. The analysis sketches feasible processes of policy decision-making and safety analyses. Key factors are policies on UAS equipage and airspace usage, implementation of a Traffic Alert and Collision Avoidance System (TCAS)-variant appropriate for UAS, use of an 'Equivalent Level of Safety' philosophy, small datalink latencies, proven HRO safety and learning cultures, and stress testing of system resilience by real-time simulations.

KEY WORDS

1. Unmanned Aircraft Systems. 2. ATC. 3. Air Safety. 4. HRO.

Submitted: 6 January 2013. Accepted: 19 May 2013. First published online: 21 June 2013.

1. INTRODUCTION.

Civil and military unmanned aircraft systems (UAS) operations are currently subject to restrictions that put major limits on their use of airspace. As demand for UAS services increases, there is considerable debate about how to develop the safe, secure and efficient integration of UAS into non-segregated airspace and aerodromes. This paper examines a *necessary* safety aspect – the introduction of UAS into a 'High Reliability' Air Traffic Control (ATC) System. Airlines and their passengers would obviously ask, "Is it still safe with all these unmanned aircraft around?" What feasible processes of safety analyses – to the satisfaction of high-calibre decision-makers – would lead to an answer? This analysis does not examine the effects on General Aviation (GA) in uncontrolled airspace or risks to third parties on the ground.

UAS aircraft or unmanned aerial vehicles (UAV) do not carry a pilot on board. They operate on pre-programmed routes and follow commands from pilot-operated ground control stations; the airframe, power plant, ground control station, communications links, etc, being the "system". An alternative term is a Remotely Piloted Aircraft System (RPAS), highlighting the continuing responsibility of a pilot. The phrase "ATC System" used here covers not only the ground-based services provided by controllers – ATC – but also airspace policies and designs, and collision avoidance based on ground and airborne equipment, aircrew see-and-avoid, and UAV's DSA (Detect – is something there? Sense – is it a threat/target? Avoid – manoeuvre to miss.) For convenience, Traffic Alert and Collision Avoidance System (TCAS) here is the implemented version of the generic Airborne Collision Avoidance System (ACAS) II – TCAS II Version 7.1, TA is a Traffic Advisory, and an RA is a corrective, ie a deviating manoeuvre, Resolution Advisory (http://www.eurocontrol.int/msa/public/standard_page/ACAS_ICAO_Provisions.html).

There is extensive governmental, industry and R&D work on UAS on an international basis, for example, ICAO (2011). The sources here select from these original or authoritative contributions. CAA (2012b) is an example of current guidance material about UAS. Elias (2012) and Dillingham (2012) describe the USA's strategy and work programmes. European Commission (2012) describes current European Union strategy and activities, in particular a European Workshop on UAS.

2. SKETCH OF PROJECTED UAS AIRSPACE-RELATED CHANGES.

UAV operations currently require special airspace arrangements, which necessitate significant planning, resources, and ATC/UAS coordination. There are usually restrictions on the UAV in terms of timeframe, weather, and flight over populated areas. ATC generally needs to segregate UAV from other flights, for example by blocking airspace. Forecasts of increased UAV demands, with commercial and societal benefits, have led to the judgement that UAV need *integration* into civil ATC operations. This would be routine access, rather than the present *accommodation* via special authorizations. The challenge is how to do this safely and efficiently.

The literature on UAS and airspace integration is ever increasing. A very useful recent document is the USA's Federal Aviation Administration framework for Integrating UAS into future air traffic management systems (FAA, 2012). This is the baseline UAS Concept of Operations here. The Concept excludes any integration of small UAV operating by "visual line of sight" of the UAS ground control (GCC) staff into civil (manned) transport traffic. The main thrust is that UAS operations are "look-alike" versions of Instrument Flight Rules (IFR)-based operations as far as technically possible. Figure 1 illustrates UAS elements. These include the Communications link between the ATC centre and the UAS GCC (with a ground or wired interface rather than an ATC relay through the UAV), the Remote pilots working in the station, the control link between GCC and UAV, and DSA facilities on the aircraft, which include both cooperative and non-cooperative elements.

Cooperative and non-cooperative refers to the sensors on the UAV. Aircraft support cooperative surveillance by carrying equipment that provides electronic information supporting their detection, for example, Mode S transponders or

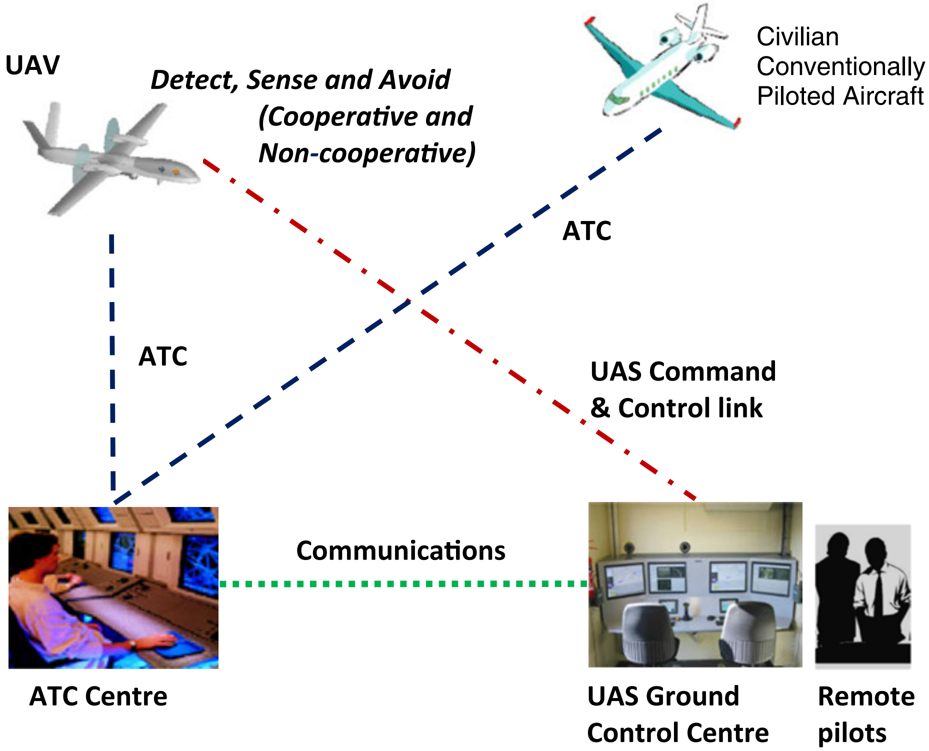
UAV
Detect, Sense and Avoid (Cooperative and Non-cooperative)
Civilian Conventionally Piloted Aircraft
ATC
ATC
UAS Command & Control link
Communications
ATC Centre
UAS Ground Control Centre
Remote pilots

Figure 1. Some Integrated UAS elements.

Automatic Dependent Surveillance – Broadcast (ADS-B). Non-cooperative traffic covers air vehicles not fitted with such equipment – GA, gliders, balloons, parachutes – so the UAV needs new sensors to replace visual acquisition. Candidate sensors include electro-optical, thermal, laser/LIDAR, radar, and acoustic. Dillingham (2012) notes the lack of current suitable technology for DSA but is positive about near term "potential solutions".

To meet the "look-alike" requirement in FAA (2012), UAS operations must comply with existing, adapted, and/or new operating rules or procedures, not require new classes/types of airspace, file and fly IFR flight plans, and comply with ATC separation minima in controlled airspace. Each UAS has a flight crew, including a Pilot in Control, who controls only one UAV and complies with all ATC instructions; and autonomous operations are not permitted. UAS have to meet the necessary performance and equipage requirements (including Mode S transponder and ADS-B (Out)), the UAV must have an appropriate airworthiness certificate, and the necessary communications spectrum must be available. ATC is responsible for separation services as required by class of airspace and type of flight plan for both manned and unmanned aircraft, with no direct link to the UAV for flight control purposes.

3. ATC SYSTEMS – A HIGH RELIABILITY TRACK RECORD.

UAS are to integrate into a "High Reliability" ATC System. This and the next section

https://doi.org/10.1017/S0373463313000337 Published online by Cambridge University Press

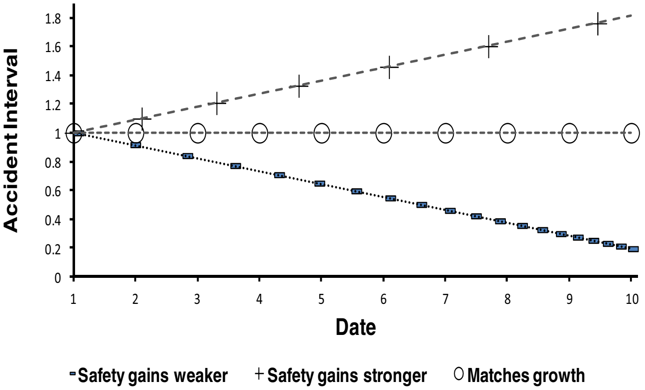

Figure 2. Illustration of “Safety Progress” chart.

examine the reasons why it is appropriate to categorize ATC Systems as a High Reliability Organization (HRO). The starting point is an examination of the track record of ATC Systems. The simplest way of measuring aviation-related safety is by accident rates. Traditionally, this examines activity-related data, for example, rates per annum, per flight, per passenger, and per passenger kilometres flown. The approach here focuses on how well safety improvements are dealing with *growth* in traffic. In Figure 2 the horizontal axis is the date of a particular type of accident, assumed here as regular events (in reality, accident timings have large statistical fluctuations.). The vertical axis measures the time from event i to the next event i + 1, i.e. it is the accident interval – “the time between failures”. If traffic grows and step-by-step safety improvements match traffic growth, then the trend is a horizontal line with constant intervals between points. If the improvements do not overcome traffic growth, the trend of event intervals would be downward. The Figure shows the line for traffic growth exceeding safety improvements by a constant amount, which leads to the interval between events reducing over time. If, in contrast, safety improvements overcome traffic growth effects, then the trend line would be upward – Figure 2 shows annual safety improvements exceeding traffic growth by a constant amount, with the interval between events increasing over time.

The “safety progress” chart in Figure 2 does not require activity data or averaging. It is effective if the policy interest is in the difference between the improvement rate and the traffic growth rate. However, to provide information about safety there must be actual traffic growth. If traffic declines, then an increasing interval between events might simply reflect the reduced pressure on safety produced by lower activity. In fact, in only five years in 1950–2011 have worldwide passenger numbers declined.

Figures 3 and 4 show the safety progress charts for “Collision in Flight” accidents for 1950–2012 with respectively ⩾1 fatality (a “fatal aircraft accident”) and ⩾10 fatalities in at least one of the aircraft. The source is the Aviation Safety Network (2013) (ASN), a database managed by the reputable Flight Safety Foundation. This database covers airliners, military transport planes and corporate jets. No aviation database is perfect, for example, countries may not publicise details of accidents or publish inaccurate accounts. 1950 is the starting point, simply because earlier years would include the 1939–1945 War and special post-War economic recovery operations. Wholly military collisions are excluded, because such operations often

https://doi.org/10.1017/S0373463313000337 Published online by Cambridge University Press

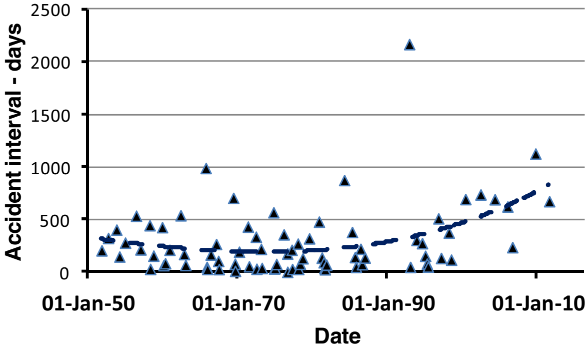

Figure 3. Safety progress chart for all mid-air collisions with ⩾1 fatalities in a civil (non-GA) aircraft, source ASN (2012).

Note: For the four accidents where the numbers of fatalities is not identified by ASN, it is assumed that there were two crew plus 60% of the passenger capacity.

Technical note: The trend lines on this and Figure 4 are least-squares cubic fits to the data. As the underlying distribution of events is probably a Poisson process, the distribution of intervals would be expected to be exponentially distributed, rather than homescedastic (constant variance error terms), so the fit is simply a rough guide. In fact, if the vertical points are variance stabilised by a logarithmic transform, the curve has a similar shape.

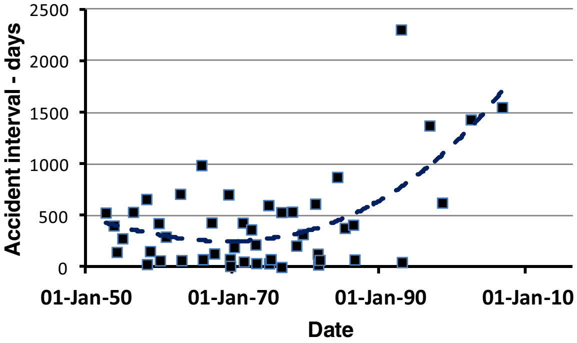

Figure 4. Safety progress chart for mid-air collisions with ⩾10 fatalities in a civil (non-GA) aircraft, source ASN (2012).

do not take place in controlled airspace and because details about them can be very imprecise, but a military aircraft can be one of the pair. The arbitrary choice of ⩾10 fatalities is to focus on civilian conventionally piloted aircraft (CCPA) – generally passenger-carrying aircraft handled by ATC. Wholly freight flights are included in Figure 3, but unlikely in Figure 4. The trend lines shown on Figures 3 and 4 are illustrative least-squares cubic fits. The charts show a marked positive improvement compared with traffic growth both for the ⩾1 fatality and – much more so – for the ⩾10 fatalities data set. Both show a stronger curve upwards than the most common type of aviation accident – “crash out of control”.

4. HRO CHARACTERISTICS AND COLLISION RISK IN ATC SYSTEMS.

LaPorte (1988) was probably the first to state that the USA’s ATC

https://doi.org/10.1017/S0373463313000337 Published online by Cambridge University Press

Table 1. Necessary attributes of HROs for ATC Systems (not in a priority order).

Complex high risk environments
Consequences of error would be serious
Positive safety culture
Continuous improvement – a learning culture
Highly trained and well-rewarded staff
Collective mindfulness across organization:
preoccupation with failure
sensitivity to operations
commitment to resilience
deference to expertise
reluctance to simplify interpretations of issues/risks.

system was a 'High Reliability Organization' (HRO). USA ATC safety has remained high, and *worldwide* performance has improved. There is a huge literature on HROs – Lekka (2011) is a good general review. An influential paper is Weick et al., (1999). An incisive critique is by Hopkins (2007), who makes salient points about ATC Systems. However, few novel papers cover ATM and HRO. Marais et al. (2004) is an exception; noting "…[ATC], for example, is as safe as it is precisely because the system design is deliberately decoupled in order to increase safety."

Table 1 summarises some of the important attributes of HROs for ATC Systems (Lekka, 2011). For example, safety culture includes such things as management's involvement in safety, while learning culture includes systems to collect and analyse data on hazardous incidents. HROs with "collective mindfulness" (Weick et al., 1999) features are believed necessary when facing unexpected situations. The list of attributes is hardly surprising for ATC Systems – complex high-risk environments, with failures having potentially tragic consequences. In open societies this has led to a safety-focused and service-orientated culture, with capable personnel operating at high levels of standardized organizational/technical expertise.

The decisive conceptual advances for avoiding collisions were by Morrel (1958). He concluded that "the proper sphere of ground-based control appears to be in the prevention of occurrence of risk situations" and that "[t]he preferable combination would be a preventive ground-based system, and a curative airborne apparatus, each supplementing the other" – the Short Term Conflict Alert (STCA) and the Traffic Alert and Collision Avoidance System (TCAS) concepts used now. Strangely, Morrel's, and colleagues' efforts to introduce effective safety defences often seem to be credited to later academics.

There are several technological enablers for the collision risk improvements since the mid-1970s and particularly from the 1990s onwards – the 'modern era' in many senses (eg see Mozdzanowska and Hansman, 2008). The major change was the use of Mode C/S transponders and high accuracy Secondary Surveillance Radar (SSR). Those technologies permitted the introduction of ground- and air-based collision avoidance systems–STCA and TCAS. "Softer" changes were very important, for example, better controller displays and input devices, resulting from wider R&D activities and ergonomic analyses. Simultaneously, there was increased attention to a positive safety culture. There is a long history of ATC System continuous improvement – a learning culture in HRO terms – in particular from work on hazardous incidents.

https://doi.org/10.1017/S0373463313000337 Published online by Cambridge University Press

For a collision to occur, TCAS must somehow have "failed", but in the same sense that a soccer goalkeeper is always responsible for a goal being scored. For TCAS to make a safety-critical intervention, the ground-based ATC system must have "failed". For four recent major accidents (Table 3): TCAS was not fitted in two cases; used incorrectly once, and essentially disabled once. Figure 4 indicates how many accidents did *not* happen. Up to 1993, the ⩾10 fatalities collision interval was typically under a year, compared with the four collisions in the last two decades. Thus, modern era developments have probably prevented around sixteen collisions.

The nature of ATC System safety decision-making has changed considerably over the last few decades. There have increasingly been more formal processes and added roles for safety regulators and policy agencies. Statistical terminology is useful for describing Implementation decisions: a Type 1 error is not introducing something new when it would in fact markedly improve safety; a Type 2 error is implementing when the technology, etc, is insufficiently mature. For Type 1s, the risk is of a "known to be preventable" accident – so the decision-makers will be criticised for inaction. For Type 2s, the risk is that the inadequacies of new equipment, pilot/controller usage, etc, will contribute a novel kind of accident – so the decision-makers will be criticised for a premature decision. These were vital considerations when deciding *when* to introduce STCA and TCAS. HRO safety performance will tend to make decision-makers more concerned about Type 2 errors.

5. COLLISION RISK MODELLING AND SAFETY DEFENCES.

Decision-makers will need several analyses to be made about the integration of UAS into non-segregated airspace. Zeitlin et al. (2006) explains the components of UAS Safety Cases. The main element of a UAS Safety Case is Collision Risk modelling. This section sketches out some important aspects, focusing on safety defences.

Collision risk estimation for CCPA subject to ATC starts from the premise that a mid-air collision follows a succession of failures or absences. A collision occurs between controlled aircraft if – *and only if* – protection layers fail:

(1) A "safety breach": an aircraft is on a flawed flightpath or deviating unexpectedly from its clearance and there is a potential conflict;
(2) *and* controller(s) *fails* to recover system safety before conflict alerts;
(3) *and* STCA plus controller action *fails* to recover system safety before TCAS alerts;
(4) *and* pilot action following TCAS alert *fails* to recover system safety;
(5) *and* the chance orientation of flightpaths *fails* to avoid the collision.

The phrase "recover system safety" is a real-life concept that would be very meaningful to an experienced controller – "situation resolved – normal ATC now." The word "fails" means that people do not always achieve perfection in estimations and choices, and some complex problems cannot be resolved in time to prevent serious conflicts. Term item (1) the "Propensity" R, a rate of occurrence (events per so many flying hours). Items (2) to (5) are then probabilities – p_2 to p_5.

If all breaches were the same then a risk calculation would simply be:

$$\text{Collision Risk C} = \text{R} \times p_2 \times p_3 \times p_4 \times p_5$$

https://doi.org/10.1017/S0373463313000337 Published online by Cambridge University Press

But the ease of resolution of breaches varies, so it is useful to break down Propensity into R_i values, where the subscript means that category i of breach (circumstances, configuration, etc). Using the same subscript for the associated probabilities and summing for all the categories gives:

$$\begin{aligned} \text{Collision Risk C} &= \sum C_i \\ \text{Collision Risk C} &= \sum R_i \times p_{i2} \times p_{i3} \times p_{i4} \times p_{i5} \end{aligned} \tag{1}$$

Equation (1) actually conceals complexity, because it does not show the dependence of the R_i and p_i values on the 'State' of the ATM system at the time that risk is assessed, that is the characteristics of the various human and technological factors at that time. It is likely that the values of later p_is in each sequence will have some statistical dependence on earlier ones. Most of the components of Equation (1) are intrinsically difficult to estimate reliably. Estimated R_i and p_i values have come from somewhere – from incident data, human factors models, simulations, etc, but in many instances there would need to be large statistical confidence bands about any estimate. Some of the C_i could represent extremely serious and difficult conflicts, but might have little effect on C, thanks to very small R_i values.

Figure 5 illustrates a selection of propensity categories, highlighting a major causal factor in each case. The circle marked 'Controlled airspace operations' includes all flights, events, etc, for aircraft subject to ATC over a long period (in Classes A to E airspace – see CAA (2012a)):

Ia: A *Normal* Acute (short duration) increase in risk, for example because people make mistakes and/or judge situations incorrectly – "normal" performance variations.

Ib: An *Abnormal* Acute increase in risk, as individuals sometimes do strange things under stress conditions – a feature in Controlled Flight Into Terrain accidents – or a sudden technical failure or response.

II: Chronic (long-lasting) risk increase in controlled airspace, in particular major weaknesses in delivering a Safety Management System (SMS).

III: An "unknown unknown" category for conflicts between controlled flights: safety modellers are not omnipotent.

IV: A CCPA is operating in Class G – "uncontrolled" – airspace. ATC does not provide separation services in this airspace. Some nearby aircraft may not have transponders – so STCA and TCAS may not function. (See Annexes 1,2 to Chapter 4 of CAA (2011).)

V: Complement of IV: an aircraft, possibly without a transponder, "leaks" from Class G to controlled airspace – an airspace infringement. Again, STCA and TCAS may not function. This category poses serious questions, for example, Eurocontrol (2009) lists 76 "Safety Improvement Actions".

VI: An IFR/Visual Flight Rules (VFR) possible conflict in Class E airspace, where IFR flights (with an ATC service separating from other IFR flights) and VFR flights (not subject to ATC clearance) can both take place. STCA and TCAS will not function if the conflicting VFR aircraft has no transponder (Class E airspace volumes are large in the USA, small in the UK.)

https://doi.org/10.1017/S0373463313000337 Published online by Cambridge University Press

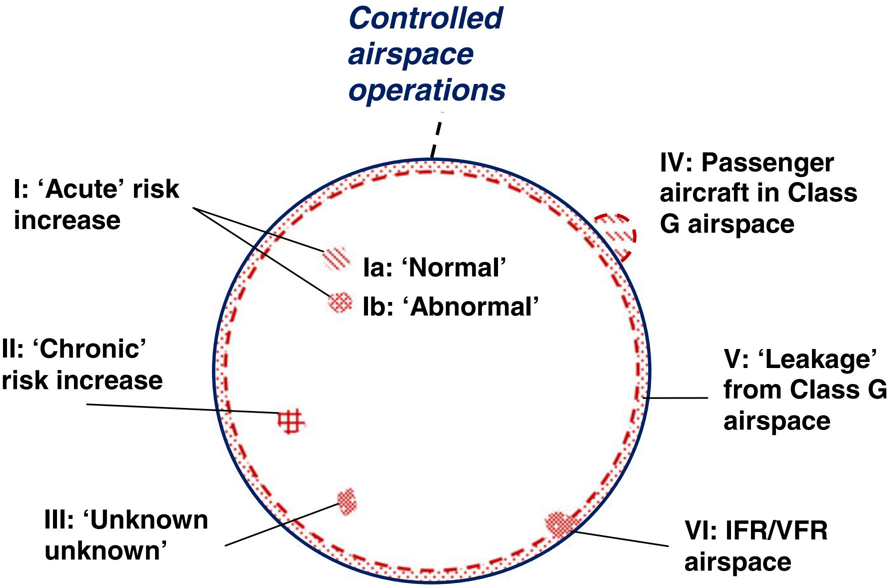
Controlled airspace operations
I: 'Acute' risk increase
Ia: 'Normal'
Ib: 'Abnormal'
IV: Passenger aircraft in Class G airspace
II: 'Chronic' risk increase
V: 'Leakage' from Class G airspace
III: 'Unknown unknown'
VI: IFR/VFR airspace

Figure 5. Illustration of Factors in Collision Categories.

Categories I to III all assume that STCA and TCAS are normally in operation. The other three categories IV to VI allow for the possibility – even probability – that conflicting aircraft are not transponder equipped, so two of the defences are missing (and SSR does not help the controller), and risk reduction relies on unaided visual acquisition and see-and-avoid.

6. UAS AND COLLISION RISKS.

UAVs added to existing or projected air traffic produce changes to some of the collision risks for CCPA. Conceptually, the category-based elements of Equation (1) will change in some instances, and there would be contributions from potential new categories. Collision risks can be *modelled*, but the question is about the extent to which they can be quantitatively *estimated with the necessary reliability*. The distinction is a fundamental one: it is comparatively easy to construct complex mathematical models or computer simulations of particular types of collision risk, but it is extremely difficult to make valid statements about the accuracy of estimates produced by such models. Alas, sophisticated and complex mathematical/simulation models cannot compensate for a lack of empirical data about failure probabilities.

Amalberti (2006) put the problem very clearly: "The processing of in-service experience needs an increasingly complex recombination of available information to imagine the story of the next accident" (Table 2). Fifty years ago a single equipment failure, mistaken data entry, or isolated poor decision might lead to a collision, but now it would necessarily be the product of several factors. To model fully that complexity requires a large number of small probabilities to be estimated with some accuracy – but incident data is sparse, generic probabilities (for example for human errors) are too imprecise, and "expert" judgements cannot be fully trusted (Brooker, 2010; 2011). No collision risk models predicted the precise characteristics of the two

https://doi.org/10.1017/S0373463313000337 Published online by Cambridge University Press

Table 2. Evolution of the prediction model based on past accidents (Amalberti, 2006).

Risk category	Up to 10^{-3}	10^{-3} to up to 10^{-5}	10^{-6} or better
The next accident…	will repeat the previous accidents	is a recombination of part of already existing accidents or incidents, in particular using the same precursors	has never been seen before. Its decomposition may invoke a series of already seen micro incidents, although most have been deemed inconsequential for safety

Note: the risk category numbers are illustrative.

Table 3. Brief summaries of the four TCAS aspects of ⩾10 fatalities collisions since 1993 (the Investigation Reports should be studied for a full picture).

12 Nov 1996: "The root and approximate cause of the collision was the unauthorised descending by the Kazak aircraft to FL-140 and failure to maintain the assigned FL-150." Indian Civil Aviation Authorities made it mandatory for all aircraft flying in and out of India to be TCAS-equipped.

30 July 1998: "Cessna 177 was equipped with a transponder that was not in operation. TCAS in Beech 1900D was removed because not approved in France. TCAS equipment should be fitted in aircraft engaged in public transport operations." (Rough translation from Report)

01 July 2002: Complex mess of causal factors. TU154M crew followed the ATC instruction to descend and continued to do so even after TCAS advised them to climb, ie contrary to the generated TCAS RA.

29 September 2006: Inadvertent inactivation of a transponder, so TCAS could not detect the other aircraft.

Note: the two previous reported collisions on this criterion were in Libya (1992) and Iran (1993), both involving military aircraft.

recent major collisions (Table 3). Both were complex system failures of safety protective layers.

The classic ICAO (1998) reference offers Safety Assessment alternatives:

- "TLS Method" Evaluation of proposed system risk against a threshold: an absolute method where explicit relation between system characteristics and collision risk is compared with a maximum "acceptable" risk: – Target Level of Safety (TLS, for example, Brooker, 2004). This is required when a radical and unproven change is planned. Risk estimates are *synthetic*, ie estimate all the propensities and probabilities in Equation (1).
- "Relative Method" Comparison of proposed system risk with a reference system risk, thus comparing proposed system with one judged acceptably safe. The reference system must be "sufficiently similar" to the proposed system. Risk estimates focus on *changes* to propensities/probabilities in Equation (1).

There are various ways of measuring risk. The most common accident-rate metrics are in terms of the number of accidents with fatalities (with ⩾1 or ⩾10 deaths, or some other criterion) per an activity measure (commonly aircraft hours flown or each year). Decision-makers set the numerical value of a TLS as the achieved accident-rate in the recent past (for example, based on the number of collisions in the last decade), or an improving accident-rate that just matches traffic growth (the horizontal line in Figure 1), or a feasible extrapolation of current performance improvements (for example, a trend line).

https://doi.org/10.1017/S0373463313000337 Published online by Cambridge University Press

An important point about TLSs is that they anchor to the performance of the *current* ATC System – hence covering all the categories of accident postulated in Figure 5. STCA and TCAS reduce collision risks. In the past, some authors and organizations, including ICAO, have said that future ATC Systems designs would only be acceptable if they could demonstrate compliance with the TLS *without* STCA and TCAS in operation. Presumably, the idea would be to ensure that ground-based ATC operated with high efficiency. However, without STCA/TCAS, there is no reason to suppose that it would be feasible to achieve current safety levels, let alone the even higher performance demanded through an improving-safety TLS.

The TLS method has proved to work very well for sub-system or safety parameter (for example, separation minimum) changes. Unfortunately, while it is feasible to construct a TLS for UAS introduction, it is not generally possible to estimate overall collision risks with good predictive accuracy. The intrinsic problem is that the risk processes involve multiple failure modes with human factors, management components, etc. Some authors do view such a TLS approach as essentially mandatory for UAS, for example Zeitlin et al. (2006): "UAS usage involves not only a collision mitigation technology but also introduces an entirely new class of operations." This is obviously important for UAVs operating in *un*controlled airspace needing DSA equipment *equivalent* to see-and-avoid. However, for the case examined here there is comparatively little change in either operational ATC concept or system technologies.

The obvious conceptual problem with the Relative method is that it refers only to a proposed system, not one that has additional aircraft with different characteristics. Additional UAVs would necessarily increase the collision risk rate, simply because the number of potential conflicts will generally increase for the same passenger flight hours (UAVs do not contribute to civil passenger hours). Given the nature of UAV tasks, usually in Class G airspace, there would probably be a high proportion of *de facto* segregation. However, this would not be the case for some High Level Long Endurance UAVs (which will need sequencing with CCPA etc when climbing and descending though their levels) and Medium Level Long Endurance UAVs (which will cruise and loiter – discussed in Section 8 – at CCPA altitudes).

The Relative Method can produce useful results by adopting the "Equivalent Level of Safety" (ELOS) philosophy, that is the system can be shown to deliver, at a minimum, a level of safety equivalent to that currently exhibited by CCPA (JAA/Eurocontrol, 2004). Such a principle has mainly been considered for UAV airworthiness aspects. There are different formal definitions of ELOS in the literature, but in the present mid-air collision risk context, an ELOS criterion would be on the lines:

> "An additional UAV operation must not increase collision risk to current CCPA any more than an additional CCPA operating on similar routeings."

(There would similarly be an ELOS for UAVs in Class E and G airspace, that is their safety implications would match general aviation flights.) This definition presupposes that an additional CCPA would not pose unacceptable risks, such that the airspace is not operated within its current safe ATC capacity. If the concern is with the safety effects for CCPA, is it reasonable to argue that the existing reference system – the present ATC System – is sufficiently similar to the proposed system, with the addition of non-segregated UAV? Safety estimates from collision risk models are the starting

https://doi.org/10.1017/S0373463313000337 Published online by Cambridge University Press

point for the safety analysis, not the complete answer. The execution of the analysis process must provide "justified belief" to the decision-maker that the changed system is acceptably safe. The decision-maker must judge how comprehensive is his/her understanding of the failure mechanisms generating the ATC System's predicted safety performance. The following two sections examine different aspects of the ELOS process, the focus being on CCPA/UAV conflicts in controlled airspace.

7. ACAS DEVELOPED FOR UAS.

TCAS was developed for CCPA, not UAV. UAV can have very different performance characteristics, for example, the Global Hawk has a relatively low air speed but a high climb rate – future cargo-carrying aircraft might be the exception. It does not appear that a UAV using TCAS can be guaranteed to be as effective as TCAS on a CCPA. Moreover, if either TCAS or more likely a developed TCAS were to be used, then there would still be latency effects in communications with the remote pilot, plus other factors that might increase response times compared with airborne pilots.

There is considerable debate on these topics, some of which appears to mix issues in using TCAS TAs to support DSA for VFR traffic with TCAS RA operation for IFR flights. A very interesting source is the FAA Report (TCAS on UAS Team, 2011), which examines various options for functions for TCAS on UAV. The report is very negative about the use of TCAS's Collision Avoidance Function, most especially for any manoeuvre in response to a TCAS RA. It sets down safety assessment needs:

> "… should address (1) lack of visual acquisition, (2) response to RAs (time and vertical acceleration), (3) the distributed nature of the system architecture over a data link-TCAS processor to display, and pilot interface with the UA[V], (4) dependencies with other systems on the aircraft that are certified to applicable 14 CFR airworthiness standards, and (5) other design aspects of the system that would be uncovered during the system safety assessment."

These criteria would generally require complex safety analyses, and hence make it extremely difficult to justify any claim that the TCAS RA aspects of UAS would 'be as safe'. *Are they all relevant here – eg does visual acquisition play a significant part in reducing the incidence of and/or resolving potentially serious IFR aircraft conflicts?*

Fortunately, there is some very encouraging recent work to develop from TCAS to a version appropriate for UAV. The FAA is developing "Airborne Collision Avoidance System X" (ACAS X). This uses "computer-optimized threat resolution logic derived from a probabilistic model of aircraft behaviour and a set of costs that represent safety, operational suitability, and acceptability considerations." In contrast, TCAS uses a deterministic model to predict where aircraft will be in the future and a set of heuristic rules to issue alerts (Holland, 2012). The UAV version of this is ACAS Xu. ACAS Xu features include an automated response to an RA (hence mitigating the impact of delayed or lost data links), and there would be maximum commonalities with TCAS II in order to minimize the certification burden. The performance of ACAS Xu and TCAS logics can be compared using the tracks from a very large number of actual TCAS RA encounters. Thus, it is easier to address the bulk of the safety assessment needs noted above.

Is the lack of "visual acquisition" by the remote pilot a critical issue? For TCAS, the existing ICAO operational approval explicitly prohibits manoeuvres that are solely reliant on TCAS traffic symbology. In general, when aircrew visually acquire a target,

https://doi.org/10.1017/S0373463313000337 Published online by Cambridge University Press

the pilot should manoeuvre to miss *only* if the target is a "threat". If TCAS does not issue an RA in IFR-only airspace, then is such a target a genuine threat? If there is an RA, then ICAO regulations instruct the operating pilot to follow it. No exception is made for situations when aircrew visually acquire a nearby aircraft (which may not be the RA-inducing threat). The role of visual acquisition in TCAS operation therefore seems minor at best.

How can an automatic response be justified? Would there be regulatory problems? There is important current work in this area (Loscos, 2012). Currently, CCPA rely on the pilot to commence the RA manoeuvre, although pilots do not always respond to the triggered RAs exactly as expected by TCAS – negatively affecting safety benefits. However, TCAS can be linked with the autopilot for automatic RA response. Loscos notes that Airbus has already developed, certificated and implemented this solution on some aircraft. Moreover, the European Aviation Safety Agency (EASA) certificated Rockwell-Collins ACAS on Eurocopter long-range helicopters (EC225 Super Puma) for which the autopilot automatically flies the RA. Note that TCAS is not currently a requirement for helicopters, but has successfully been fitted and certificated for some operators. Hence, there is a precedent for automatic RA responses, and the indications are that this would improve safety markedly (Loscos, 2012). So, *prima facie* the ACAS Xu with automatic RA responses is feasibly safe. However, if the envisaged ACAS Xu cannot meet the required criteria, then the task of demonstrating performance "at least as effective as TCAS" becomes a very difficult proposition.

8. IF UAV CONFLICT ALERTING IS AT LEAST AS GOOD AS A CCPA'S . . . If the development work on ACAS Xu is successful, then UAVs will be at least as well protected by conflicting alerting mechanisms as CCPA – a *necessary* ELOS requirement. STCA should *prima facie* have the same performance, as the function simply relies on aircraft having Mode S transponders. Performance might well improve markedly when ADS-B data is incorporated. UAVs are not "VFR threats" to CCPA. Categories IV to VI of the CCPA conflicts with VFR traffic are eliminated for UAV intruders, as they are flying IFR with flight plans and ATC clearances. Category Ia meets the ELOS criterion because the ground ATC aspects are presumably the same – in what circumstances would they not be?

The remaining ELOS questions are with categories Ib, II and III. How might UAS produce additional risks in these categories? These higher collision risks would have to derive from the *nature* of UAS, for example how aircraft fly, keeping to flight paths, interactions with ground ATC, comparing CCPA and UAV pilots. They would be *effects that increase the propensity rate and/or reduce the effectiveness of the successive protective layers*. Examples would be anything that, that tended to make STCA or TCAS fail, and/or weakened ground ATC by among other things, extra controller workload. Where there are recognised differences, what mitigations can be put in place to negate extra risk? Are the existing mitigating safety features equally sufficient – or what else would be needed?

A full analysis of the remaining ELOS questions obviously requires a formal description of the changes to ATC System components, including a rigorous Functional Hazard Assessment (for example, Evans and Nicholson, 2007) and collision risk estimation. Such assessment methodologies are similar to those used in the development and certification of manned aircraft, but with some modifications to

https://doi.org/10.1017/S0373463313000337 Published online by Cambridge University Press

the hazard identification process. Two illustrations of HRO-related aspects are briefly discussed here: Contingency Routeing and Safety/Learning Culture.

Contingency Routeing is one of several navigational aspects of future UAS examined by Paczan et al. (2012): "Contingency routes… are flight plans to be flown in the event that an emergency, failure, or other off-nominal set of conditions are met. Contingency routes are typically pre-programmed into an aircraft's flight management computer…[eg] loss of C2 communication link… there are currently no existing or planned mechanisms for storing and/or processing contingency routes." Future routeings could commence with loitering patterns, such as circle or racetrack circuits. Such routeings would not be conflict-free in terms of other traffic. Pastor et al. (2010) usefully assess UAS flight planning and contingency management. Ground ATC already has well-established procedures and guidelines dealing with emergencies (CAA, 2012a) – but the UAV would be operating autonomously. Assuming that flight data processing can be developed to handle such routes, would they lead to increased risk, for example from markedly higher controller workload? It is very unlikely that datalink delays adding seconds to the communications loop between UAV operators and ATC would be acceptably safe. Neither would a rate of emergencies for UAVs – arising perhaps from easier certification of design and UAS maintenance – that is markedly greater than the CCPA rate. However, if UAVs generally behave more predictably than CCPA, UAS emergencies might generally be easier to handle.

Safety and learning cultures are intrinsic HRO characteristics. They are certainly *necessary ingredients* in reducing the likelihood of risks in categories II and III (Figure 5 and text). However, knowledge of cultural performance cannot be established *a priori*: it requires empirical evidence of incidents and safety management and operational processes. For ground ATC, a key reference is Eurocontrol (2006). An important part of understanding culture in ATC Systems is the collection and analysis of safety incident data. Airlines have analogous interests in safety/learning culture, with particular attention to effective teamwork between aircrew members. The two most recent major mid-air collisions (see Table 3) raised safety culture concerns. Safety culture is a vital element in SMS. The obvious question is whether operations in GCCs exhibit HRO cultural behaviours. The evidence is that there is some way to go. The onus will be on UAS operators to demonstrate that their SMS is as effective as a typical airline.

However, aviation safety analyses and evaluation methods cannot be completed simply by "ticking the boxes". The Ib, II and III categories in Figure 5 are to varying degrees open-ended. An important way forward is to use high fidelity Human in the Loop Simulations (HITLS) (Brooker, 2010) in safety decision-making, to generate confidence in system *resilience* (Hollnagel et al., 2006). HITLS – real time simulations – put controllers and pilots into accurately simulated environments. A HITLS is an experimental replicated control room, and the controllers carry out the same tasks that they would for real traffic, while CCPA/UAS HITLS are linked cockpit simulators (note the need to test GCC handovers).

HITLS would test how *resilient* the evolving system is to a comprehensive set of errors, blunders, etc. The aim is to build up rational belief in the system's capacity to deal with gross abnormalities. Resilience tests have to *attack* the HITLS, to expose its weak points, to show where defences are thin, insufficient, etc. These would include seeded errors, penetration testing, and stress testing. The HITLS process is *aggressive*,

https://doi.org/10.1017/S0373463313000337 Published online by Cambridge University Press

rather than a routine evaluative simulation of normal operations. The tests would generally compare UAVs with CCPA, for example using Airproxes as the starting point for potential conflict situations. For *unknown unknowns* the kinds of exploratory thinking examined by de Jong (2004) are essential ingredients to HITLS.

9. SUMMARY.

The aim is to introduce Unmanned Air Systems (UAS) into controlled airspace without special segregation arrangements. It is necessary that airlines and their passengers not be exposed to higher risks of mid-air collision. The analysis here sketches processes of policy decision-making and safety analyses that should lead to a reasoned conclusion. Air Traffic Control (ATC) Systems are High Reliability Organisations (HROs), whose characteristics include: focus on safety, effective use of technological improvements, learning from accidents/incidents, and an underpinning safety/learning culture. Accidents are now the product of rare and complex "messes" of multiple failures, and hence it is a continuing challenge to preserve the HRO status.

The different ways of safety analysis for UAS introduction are Target Level of Safety (TLS) methods, modelling absolute risk synthetically and comparing with a target derived from current safety performance, and Relative methods, comparing a new system with an existing one. It is very difficult to use TLS for whole-system changes, as there are problems in actually estimating the currently achieved or projected level of safety with precision. Such estimates need many statistical assumptions about a model's failure structures, human factors and managerial failure conditions. The Relative method will work if the new system is sufficiently similar. A proposed specific "Equivalent Level of Safety" is: "An additional Unmanned Air Vehicle (UAV) operation must not increase collision risk to current civilian conventionally piloted aircraft (CCPA) more would than an additional CCPA operating on similar routeings."

If ATC handles UAS exactly the same as CCPA, the fundamental need is for UAV to have Airborne Collision Avoidance System (ACAS) Xu equipment, at least as effective as CCPA Traffic Alert and Collision Avoidance Systems (TCAS). ACAS Xu Resolution Advisories (RAs) are linked to the Flight Management System, ie an automatic response. Hazard analysis has then to concentrate on potential CCPA/UAS differences. Two important components are contingency routeing when the UAV/Ground Control Component (GCC) datalink fails (causing eg marked increases in ATC workload), and safety/learning culture of GCC managers/staff. Knowledge of cultural performance is not available *a priori*: it requires empirical evidence of hazardous incidents and safety processes. Safety analysis must also include stress testing of system resilience by real-time simulation of novel events.

If policy makers prefer not to opt for the strong decisions here – on UAV equipage, implementation of ACAS Xu, use of Equivalent Levels of Safety (ELOS), small datalink latencies, safety/learning cultures – then the process of safety analysis to justify UAS non-segregated use of airspace would be markedly more complex.

REFERENCES

Amalberti, R. (2006). Optimum System Safety and Optimum System Resilience: Agonistic or Antagonistic Concepts? *Chapter 16 of Hollnagel et al. – see below*.

https://doi.org/10.1017/S0373463313000337 Published online by Cambridge University Press

ASN [Aviation Safety Network] (2013). *Database: (Contributory) cause index.* http://aviation-safety.net/database/events/. Accessed 1st January 2013.

Brooker, P. (2004). Consistent and up-to-date aviation safety targets, *Aeronautical Journal*, **108**(1085), 345–356.

Brooker, P. (2010). SESAR safety decision-making: Lessons from environmental, nuclear and defence modelling, *Safety Science*, **48**, 831–844.

Brooker, P. (2011). Experts, Bayesian Belief Networks, Rare Events And Aviation Risk Estimates, *Safety Science*, **49**, 1142–1155.

CAA (2011). *Requirements and Guidance Material for Operators*. CAP 789. UK Civil Aviation Authority, 18 February 2011.

CAA (2012a). *Manual of Air Traffic Services Part 1*. Civil Aviation Publication CAP 493. 15 November 2012.

CAA (2012b). *Unmanned Aerial Vehicle Operations in UK Airspace – Guidance*. Civil Aviation Publication CAP 722, 10 August 2012.

Dillingham, G. L. (2012). *Unmanned Aircraft Systems. Measuring Progress and Addressing Potential Privacy Concerns Would Facilitate Integration into the National Airspace System*. GAO-12–981. USA Government Accountability Office.

Elias, B. (2012) *Pilotless Drones: Background and Considerations for Congress Regarding Unmanned Aircraft Operations in the National Airspace System, R42718*. Congressional Research Service.

Eurocontrol (2006). *Understanding Safety Culture in Air Traffic Management*. Eurocontrol Experimental Centre EEC Note No. 11/06.

Eurocontrol (2009). *European Action Plan for Airspace Infringement Risk Reduction*.

European Commission. (2012). *Strategy for unmanned aircraft systems in the European Union*.

Evans, A. and Nicholson, M. (2007). *Safety Assessment & Certification for UAS*. 22nd International UAV Systems Conference.

FAA (2012). *Integration of Unmanned Aircraft Systems into the National Airspace System Concept of Operations V2*. Federal Aviation Administration.

Holland, J. E. (2012). *Safety and Suitability Performance Assessment of ACAS Xa*. Federal Aviation Administration. Aeronautical Surveillance Panel, Working Group Meeting 13, Washington, DC.

Hollnagel, E., Woods, D. D., Leveson, N. (Eds.), (2006). *Resilience Engineering: Concepts and Precepts*. Ashgate.

Hopkins, A. (2007). *The problem of defining high reliability organisations*. Working Paper 51. The Australian National University.

ICAO (1998). *Manual on Airspace Planning Methodology for the Determination of Separation Minima*. ICAO, Doc 9689-AN/953.

ICAO (2011). *Unmanned Aircraft Systems (UAS)*. ICAO Circular 328 AN/190.

JAA/Eurocontrol (2004). *A Concept for European Regulations for Civil Unmanned Aerial Vehicles (UAVs)*. UAV Task Force Final Report.

de Jong, H. H. (2004). *Guidelines for the identification of hazards: How to make unimaginable hazards imaginable?* Eurocontrol Contract NLR-CR-2004–094. http://www.nlr-atsi.nl/downloads/guidelines-for-the-identification-of-hazards.pdf

LaPorte, T. (1988). *The United States Air Traffic System: Increasing Reliability in the Midst of Growth*. in T. Hughes and R. Mayntz, eds., The Development of Large Technical Systems. Boulder, Westview Press. 215–244.

Lekka, C. (2011). *High Reliability Organisations: A Review of the Literature*. Health and Safety Executive Research Report RR 899, HSE Books, UK.

Loscos, J.-M. (2012). *Information Paper at ANCONF/12 related to Airborne Collision Avoidance*. Aeronautical Surveillance Panel (ASP) 13th WG Meeting.

Marais, K., Dulac, N., Leveson, N. G. (2004). *Beyond normal accidents and high reliability organizations: the need for an alternative approach to safety in complex systems*. In: Engineering Systems Division Symposium. MIT, Cambridge, MA.

Morrel, J . S. (1958). Mathematics of collision avoidance in the air, *Journal of Navigation*, 11, 18–28; Use of self-contained range and azimuth measuring apparatus to detect collision courses, *Journal of Navigation*, **11**, 318–321.

Mozdzanowska, A. and Hansman, R. J. (2008). *System Transition: Dynamics of Change in the US Air Transportation System*. MIT Report ICAT 2008–3.

https://doi.org/10.1017/S0373463313000337 Published online by Cambridge University Press

Paczan, N. M., Cooper, J., Zakrzewski, E. (2012). *Integrating Unmanned aircraft into Nextgen Automation Systems*. 31st Digital Avionics Systems Conference.

Pastor, E., Prats, X., Delgado, L., Barrado, C., Lopez, J. and Santamaria, E. (2010). *An Assessment for UAS Traffic Awareness Operations*. 27th International Congress of the Aeronautical Sciences.

TCAS on UAS Team (2011). Evaluation of Candidate Functions for Traffic Alert and Collision Avoidance System II (TCAS II) On Unmanned Aircraft System (UAS). Version 1.0. FAA/AFS-407. Federal Aviation Administration.

Weick, K. E., Sutcliffe, K. M.,and Obstfeld, D. (1999). *Organizing for High Reliability: Processes of Collective Mindfulness*. R. S. Sutton and B. M. Staw (eds), Research in Organizational Behavior, Volume 1. Stanford: Jai Press, 81–123.

Zeitlin, A. D., Lacher, A., Kuchar, J. and Drumm, A. (2006). *Collision Avoidance for Unmanned Aircraft: Proving the Safety Case*. MP060219, The MITRE Corporation.

https://doi.org/10.1017/S0373463313000337 Published online by Cambridge University Press