

Y2K

just months away



It's time for aerodromes to finalise their Y2K contingency programs before the bug bites.

Graham Bailey

I WAS REMINISCING WITH A COLLEAGUE recently. Soon we were well into the technical stuff associated with runway roughness, and the finer points of flexible pavement design.

I was in trouble, having serious memory problems with the first principles of Boussinesq.

Eager to impress, I tried to change the subject, "I've been asked to write an article on the subject of Y2K, as it applies to airports", I told my old friend.

"What's that got to do with airports?" was the dismissive response. "Y2K is something for the airlines and the air traffic system to worry about."

While the experts still differ about the impact the millennium bug is going to have on airport operations, the airport community must be well aware that we are looking at a real threat.

The bug basics: According to one definition, a bug is an ugly insect that crawls about in hidden places.

The year 2000 bug arises from the way dates are stored in computer systems; the four-digit year being represented by the last two digits of that year – so 1997 is represented by the digits 97. Therefore on 1 January 2000 some software or embedded chips could read the date as 1900.

The challenge for airport operators is to hunt down these bugs, then assess and test system ability to continue normal operations.

Problems do not begin and end at 1 January 2000. For instance, 2000 is a leap year whereas 1900 was not, and some programs or chips will not recognise 29 February 2000.

Each airport has its own organisation to consider, and must rely on suppliers, business partners and customers. The bigger the airport, the more complex the relationships and interdependencies.

// Airports that are not ready may find themselves facing a serious business loss. //

What sort of problems? Let's look at three examples: electricity supply, emergency planning and human resources.

Electricity supply: Australian electricity supply businesses have large programs to deal with the bug, and have spent over \$200 million on the problem. The industry peak body, the Electricity Supply Association of Australia (ESAA), has issued a statement advising that most of the individual electricity businesses have dedicated project teams in place to determine and correct non-compliant systems.

The ESAA has established a national forum to improve information sharing on Y2K compliance. Contact the ESAA on: ph 02 9233 7222, fax 02 9233 7244.

Your documented airport emergency plan will outline roles, capabilities and responsibilities, and will address response procedures, including plan activation, notification and coordination. Even where there is no regulatory requirement for an airport emergency plan, it is still a good idea to have one – if nothing else, in the form of basic information, contact numbers and area details.

Emergency planning: You should ask yourself about how the millennium bug could affect your emergency planning:

- What are the functional areas and systems involved?
- Are contact details appropriate and reliable?
- What is the status of preparedness for each stakeholder?
- What is the status of the essential technical facilities, including communications systems?
- Where are the potential weaknesses, and how will they be overcome?

Human resources: Even the human resources manager is at risk. Employment records, pay systems and other HR information are usually computer generated and stored electronically.

Employers are acting outside the law if they fail to pay employees their correct entitlements. In addition, State and Federal legislation requires employers to keep certain employment records for several years.

When you think through this area, there is plenty of incentive to ensure preventative action; at the very least, you should think about the timely creation of hard copy records of essential data.

Legal issues and risk management – such as insurance exposure – should all be part of the airport Y2K preparedness audit. And what about the systems of your creditors and debtors?

IATA year 2000 program: The International Air Transport Association (IATA) is effectively the voice of the world's international airlines, with some 257 member airlines representing 98 per cent of international scheduled traffic.

IATA's \$20 million year 2000 project sets out to create awareness of the problem and to collect and share data. Airlines will be able to access this data in order to plan flights over the year 2000 period. Airports that are not ready may find themselves facing a serious business loss.

IATA has developed a standard methodology in order to assess Y2K readiness. The process involves site visits and a structured walk-through "audit" of high volume airports.

Training seminars are also part of the picture, together with tool kits to facilitate data collection and assist the lesser volume airports with Y2K readiness.

High volume airports, termed Tier 1 airports, include Melbourne, Brisbane and Sydney. Tier 2 are defined as less complex, and include Adelaide, Coolangatta, Alice Springs, Cairns, Canberra, Darwin, Hobart, Perth, Townsville and Launceston.

The remaining airports served by IATA members are known as Tier 3. Tier 1, 2 and 3 airports have been asked to complete the "tool kit" worksheets and forward the data back to IATA for inclusion in the IATA database.

It's time: With time fast running out, priorities become an issue. When you have ascertained the systems and equipment that are likely to be affected (see box at right), you should ask yourself how critical they are to your operation. Criticality ratings suggested by IATA are:

Vital

- Mandatory regulation.
- Injury or death.
- Emergencies.
- Deemed as vital.
- More than one day of failure equates to ruinous loss.

Critical

- High public/political visibility.
- Basic to organisation goals.
- Forms basis of other systems.
- Devastating loss but survival for 1 + days.

Important

- Subordinate to more critical systems or functions.
- No effect to safety, health, political economic or penalty damage.
- A service agreement will be voided if failure occurs).
- High financial loss but survival for 1+ weeks.

Discretionary

- System can be performed manually without impact.
- No impact on other systems.
- Bothersome but no financial loss.

These ratings will not necessarily appeal to all airports. But the ideas are useful; particularly as a guide for those airports developing their own criticality ratings.

Assessment questions: According to IATA, the basic questions you need to ask about the equipment you have inventoried and prioritised are:

- What is the main function of the equipment reviewed?
- Is the system "date aware"?
- Who is the vendor?
- Do you have any documentation/verification of the Year 2000 status of the equipment or vendor?
- What are the components of the system?
- Does the equipment/system interface with others?
- Does the equipment/system depend on others?
- Have you tested the component?

With 1 January 2000 only months away, it is time to complete your Y2K readiness status audit. I am suggesting a four step approach (see box, below).

For those Tier 2 and 3 airports well advanced towards Y2K readiness, it might be useful if you still do the audit, using independent (fresh start) people, concentrating on the lateral thinking part of Step 1 (below); that is, "What have we forgotten?"

Try putting "the blinkers" on – see nothing

Airport systems to check

- Airport access control.
- Badging system.
- Closed circuit TV.
- Automated sliding doors.
- Escalators.
- Baggage handling systems.
- Cargo systems.
- Local area network.
- Communications systems.
- Air monitoring system.
- Chiller and air conditioning.
- Fire suppression.
- Terminal lighting systems.
- Fire alarms.
- Back-up power generation systems
- Security alarm systems
- Flight information display system (FIDS)
- Baggage information display system (BIDS)
- Common use terminal equipment (CUTE system)
- Fuel services
- Gate operation
- Ground control systems
- Navigational aids
- Security/public safety systems
- Airfield lighting.

Source: IATA Year 2000 toolkit.

This list is incomplete and is intended to "get the thinking going". Airports of basic functionality are likely to have fewer Y2K concerns due to the nature of services provided. For example, many aerodromes will not have airfield lighting or may have equipment which is switched manually upon request.

but computer systems and embedded chips. Approach this as you would a safety audit.

When you do this, you probably use the "what if?" scenario; applied to various combinations of otherwise benign single events, for example, "What if event A occurs at the same time as event B, with the pilot preoccupied with the workload of final approach?"

Each airport must analyse the extent of its own Year 2000 exposure and find the solutions. For many of the smaller airports, the audit will hopefully confirm a status of readiness.

Graham Bailey is a Canberra based aerodrome engineering and operations consultant.

Step 1: Find the potential problems.

Find out where the millennium bug may cause problems.

Make sure this inventory extends to the activities of suppliers and customers, where those activities or systems impact on your operation.

The following IATA toolkit material is available to get you started:

- Functional area and system listing (three pages).
- Airport systems glossary (six pages).

- Year 2000 information technology glossary (six pages).

These are available from CASA's Y2K Info-line on 131 757.

Step 2: How critical?

Make your own judgements, and set the priorities for each item on your inventory of items of equipment at risk.

Step 3: Where are we at?

This is the crux of the entire exercise,

working through the list, making informed judgements on things like:

- Action already undertaken; issue marked off.
- Action required, by priority.
- Specific contingency planning.

Step 4: Document

Use the results to document the responsibilities and effective use of resources which will maximise Y2K readiness in the time remaining.