Digital Systems Software Requirements Guidelines

Vol. 2 Failure Descriptions

Contract RES-00-037

M. Hecht
H. Hecht

SoHaR Incorporated
Beverly Hills, CA

for

Nuclear Regulatory Commission
Washington, DC

June 2001

Abstract

This document provides descriptions of 45 failures that are linked to software requirements review guidelines listed in Volume I prepared under Contract NRC-00-037. The failure descriptions are "lessons learned" which illustrate why the specific software requirements guidelines are needed.

Table of Contents

List of Tables

Executive Summary

A significant proportion (if not the majority) of all accidents in which software was involved can be traced to requirements errors. Not only do missing, inaccurate, or incomplete requirements lead to flaws in software development, they also prevent these flaws from being detected during V&V. For example, functional testing is based on the requirements; a missing or inaccurate requirement will therefore not be detected. Integration testing sometimes detects the omissions or inaccuracies, but more frequently it is only through failures in actual operation that these defects are made manifest.

This is the second of two volumes prepared under Contract RES-00-037 and contains a set of 45 failures that illustrate the need for and the importance of specific requirements review guidelines. Cross reference tables link the requirements review guidelines to the failure descriptions and the failure descriptions to the guidelines.

List of Acronyms

A/D	Analog to Digital
APU	Auxiliary Power Unit
ARTCC	Air Route Traffic Control Center
CFR	Code of Federal Regulations
CCCH	Central Computing Complex-Host
CCU	Central Control Unit
CPU	Central Processing Unit
D/A	Digital to Analog
DHCP	Dynamic Host Configuration Protocol
EPRI	Electric Power Research Institute
ESFAS	Engineered Safety Function Actuation System
FADEC	Full Authority Digital Engine Controller
FDIO	Flight Data Input Output
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes and Effects and Criticality Analysis
HVAC	Heating, Ventilation, and Air Conditioning System
I&C	Instrumentation and Control
IEEE	Institute of Electrical and Electronics Engineers
LSB	Least Significant Bit
NRC	Nuclear Regulatory Commission
P&ID	Process and Instrumentation Diagram
PLC	Programmable Logic Controller
RTS	Reactor Trip Systems
PDS	Previously Developed Software
PID	Proportional Integral Derivative Control
UPM	Uninterruptible Power Module
SAR	Safety Analysis Report
TRACON	Terminal Radar Approach Control Center
TTL	Transistor-Transistor Logic
V&V	Verification and Validation

1. Introduction

This document is the second volume of the Digital Systems Software Requirements Guidelines. Together with Volume 1, it provides guidance to the NRC for reviewing high-integrity software requirements documents in nuclear power plants.

This volume contains requirements related failures that substantiate and illustrate the requirements guidelines of Volume 1. Chapter 2 of this volume provides an overview of the failure reports and Chapter 3 presents the failure description sheets.

The following appendices of Volume 1 will also be found helpful to the reader of this document:

Appendix A—Glossary of Technical Terms

Appendix B—Reviewers

2. Overview of Failure Descriptions

The failure descriptions contained in this section were selected from sources in the general digital controls field and in digital controls applied to nuclear power plants. The following list summarizes the criteria used to select relevant failure examples.

- The failure resulted from multiple causes.
- The proper definition and implementation of a software requirement would have mitigated or prevented the failure.
- The failure did or could have had safety significance.
- The failure was adequately documented.

Although many hundreds of source failure descriptions were examined, only 30 from the general digital controls field and 15 from nuclear power plants were included. Table 2–1 provides a list of the failure descriptions and cross-references the descriptions to the guidelines in Volume 1. Table 3–2 provides the reverse mapping (i.e., guidelines to failure descriptions). The failure descriptions from the general digital controls field are *anecdotal*. They are not formal failure reports and are intended for the purposes of illustration only. Failure descriptions from the nuclear field were excerpted from licensee event reports (LERs) and tend to be more complete. None of the failure descriptions have been independently verified.

Table 2-1. Failure Reports to Guidelines (Vol. 1) Cross-Reference

Number	Title	Guidelines
0001	Configuration Management on User	2.3.1-1, 2.6-1
0002	Decimalization and Ford Stock Splits	2.1-3, 2.2.1-3
0003	Pentagon Security Gate Malfunction	2.3.3-1, 2.5.2-1
0004	Single Points of Failure and Backup Plans	2.5.2-1, 2.8-4
0005	UPS Backup Failure	2.1-3, 2.9-4, 2.3.4-9
0006	Saturn Limit Logic	2.3.1-6, 2.3.4-2, 2.9-8
0007	A Subtle Fencepost Error	2.3.4-1
0008	Pentium III Chip Flaw	2.5.2-1
0009	Train Door Failure	2.1-1, 2.5.2-3
0010	Failures During Upgrades	2.6-5, 2.7-2
0011	Elevator Software	2.6-6
0012	GPS Clock Problem	2.2.1-2
0013	Electrostatic Discharge	2.9-10
0014	TDWR Crash Failure	2.4-5, 2.6-3
0015	TDWR Communication Failure	2.5.1-1, 2.5.1-2

Number	Title	Guidelines
0016	Weather Failure Due to Telco Circuits	2.5.1-2, 2.6-1
0017	TDWR SW Failure	2.4-5, 2.5.2-1, 2.6-1
0018	Weather Processor Crash	2.5.2-7, 2.6-1
0019	Indianapolis ARTCC Failure	2.4-2, 2.5.1-1
0020	BOS ARTCC Problem	2.5.2-1, 2.6-4, 2.6-5
0021	F 16 Weight on Wheels	2.3.1-6
0022	Bombing While Flying Upside Down	2.3.1-1
0023	747-400 Uncommanded Throttle Closure	2.5.2-1
0024	A320 Article in Science & Vie	2.1-3, 2.9-1, 2.9-2
0025	747 Problems	2.5.2-1
0026	Train Signal System Software	2.1-3, 2.5.2-3
0027	NASDAQ Outage	2.4-5
0028	Subway Doors	2.5.2-1, 2.5.3-3, 2.9-2
0029	London Subway Doors	2.1-1, 2.5.3-3, 2.9-2
0030	747 Engine Shut Down	2.5.2-3
0031	Security Computer Failure	2.3.2-2, 2.5.2-3
0032	Thermal Power Calculation	2.2.1-1
0033	Disabled Function	2.3.1-4
0034	Snubber Inspection Scheduling	2.6-3
0035	Reactor Instrumentation	2.5.1-1
0036	Inspection Procedures	2.3.1-4, 2.6-3
0037	Disabled Alarm	2.1-1
0038	Incomplete Surveillance Software	2.6-3
0039	Monitor Accuracy Error	2.2.1-1
0040	Deficient surveillance Test Procedure	2.3.1-4
0041	Software Maintenance Problem	2.5.3-3
0042	Missed Surveillance Test	2.3.1-4
0043	Date Uncertainty	2.5.3-3
0044	Rod Position Calculation	2.3.1-4
0045	Reactor Power Calculation	2.3.3-2, 2.6-4

Table 2-2. Guidelines (Vol. 1) to Failure Reports Cross-Reference

Guidelines	Failure Report No.	Title
2.1-1	0009	Train Door Failure
	0029	London Subway Doors
	0037	Disabled Alarm
2.1-3	0002	Decimalization and Ford Stock Splits
	0005	UPS Backup Failure
	0024	A320 Article in Science & Vie
	0026	Train Signal System Software
2.2.1-1	0032	Thermal Power Calculation
	0039	Monitor Accuracy Error
2.2.1-2	0012	GPS Clock Problem
2.2.1-3	0002	Decimalization and Ford Stock Splits
2.3.1-1	0001	Configuration Management on User
	0022	Bombing While Flying Upside Down
2.3.1-4	0033	Disabled Function
	0036	Inspection Procedures
	0040	Deficient surveillance Test Procedure
	0042	Missed Surveillance Test
	0044	Rod Position Calculation
2.3.1-6	0006	Saturn Limit Logic
	0021	F 16 Weight on Wheels
2.3.2-2	0031	Security Computer Failure
	0045	Reactor Power Calculation
2.3.3-1	0003	Pentagon Security Gate Malfunction
2.3.4-1	0007	A Subtle Fencepost Error
2.3.4-2	0006	Saturn Limit Logic
2.3.4-9	0005	UPS Backup Failure
2.4-2	0019	Indianapolis ARTCC Failure
2.4-5	0014	TDWR Crash Failure
	0017	TDWR SW Failure

Guidelines	Failure Report No.	Title
	0027	NASDAQ Outage
2.5.1-1	0015	TDWR Communication Failure
	0019	Indianapolis ARTCC Failure
	0035	Reactor Instrumentation
2.5.1-2	0015	TDWR Communication Failure
	0016	Weather Failure Due to Telco Circuits
2.5.2-1	0003	Pentagon Security Gate Malfunction
	0004	Single Points of Failure and Backup Plans
	0008	Pentium III Chip Flaw
	0017	TDWR SW Failure
	0020	BOS ARTCC Outage
	0023	747-400 Uncommanded Throttle Closure
	0025	747 Problems
	0028	Subway Doors
2.5.2-3	0009	Train Door Failure
	0026	Train Signal System Software
	0030	747 Engine Shut Down
	0031	Security Computer Failure
2.5.2-7	0018	Weather Processor Crash
2.5.3-3	0028	Subway Doors
	0029	London Subway Doors
	0041	Software Maintenance Problem
	0043	Date Uncertainty
2.6-1	0001	Configuration Management on User
	0016	Weather Failure Due to Telco Circuits
	0017	TDWR SW Failure
	0018	Weather Processor Crash
2.6-3	0014	TDWR Crash Failure
	0034	Snubber Inspection Scheduling
	0036	Inspection Procedures
	0038	Incomplete Surveillance Software
2.6-4	0020	BOS ARTCC Problem
	0041	Software Maintenance Problem
	0045	Reactor Power Calculation

Guidelines	Failure Report No.	Title
2.6-5	0010	Failures During Upgrades
	0020	BOS ARTCC Problem
2.6-6	0011	Elevator Software
2.7-2	0010	Failures During Upgrades
2.8-4	0004	Single Points of Failure and Backup Plans
2.9-1	0024	A320 Article in Science & Vie
2.9-2	0024	A320 Article in Science & Vie
	0028	Subway Doors
	0029	London Subway Doors
2.9-4	0005	UPS Backup Failure
2.9-8	0006	Saturn Limit Logic
2.9-10	0013	Electrostatic Discharge

3.Failure Descriptions

This chapter presents the failure descriptions and the following additional information:

Date: The date of the description or failure report (not necessarily the date of the occurrence of the failure)

Source: The source of the failure description—LERs are identified by docket number, year, and report number.

Domain: The general application area of the failure (aircraft, ground transportation, etc.)

Function: The function within the domain

Guidelines: The applicable and relevant guidelines from the previous chapter

Description: A description of the failure as presented in its original source—these descriptions have not been edited and sometimes take liberties with grammar and writing style.

Discussion: A brief explanation of how proper application of the requirements guidelines might have prevented or mitigated the consequences of the failure

0001 Configuration Management on User Interface

Date 09/19/2000

Source Risks 21.05 (Neumann, 2001)

Domain HVAC

Function Climate Control

Guidelines 2.3.1-1 2.6-1

Description

Computerized air-conditioning risks
Pere Camps <pere@pere.net>
Tue, 19 Sep 2000 19:45:05 +0100 (BST)

We just moved offices this Monday to a brand new building and the air-conditioning machines were working much too well: we were freezing. This surprised most of us as the new AC system was run by a PC. It looked very robust. After some "debugging," we found out that the control software was buggy. We notified this to the appropriate vendor, which confirmed the bug with us and told us that it would soon be fixed.

[Added note: The bug with the PC software was so huge (it looks like it only happens with our setup—the vendor claims it is the first time it happened) that what we have is the AC units running continuously, no matter what the thermostat tells the control unit].

Discussion

The vendor had used this program previously ("It only happens with our set-up.") and assumed it to be suitable for a wide range of environments. This assumption was clearly incorrect and would have been discarded if a complete specification of the run-time environment had been generated. This cause for the failure is classified as an inadequate specification of the complete run-time environment (Guideline 2.3.1-1).

The description indicates that neither the software nor the system had been adequately tested prior to being put into operation. This cause of the failure is classified as an example of inadequate online checks of pre-developed software intended for multiple system configurations (Guideline 2.6-1).

0002 Decimalization and Ford Stock Splits

Date 08/07/00

Source Risks 21.05 (Neumann, 2001)

Domain Financial

Function

Guidelines 2.1-3 2.2.1-3

Description

On 7 Aug 2000, Ford completed its Value Enhancement Plan, a somewhat complicated stock transaction where Ford created a new company (Ford Value Company) and issued a new stock. Ford stockholders of record on July 27th had the option of taking the new common or Class B stock plus (1) $20 per share, (2) a fraction of the new common stock that would be the equivalent of $20, or (3) a fraction of cash and fractional shares that would maintain their percentage ownership of all outstanding shares.

For the last two options, the fraction of cash and fraction of shares depended on the total number of outstanding shares of the old company. At the end of the exchange and disbursement, the new company transformed back into the old company, and trades on the NYSE as F. The final numbers wound up such that if you took the full fractional new share with your matching full share, you received an additional 0.748 share.

*Tim Prodin [and other readers of Risk]

Discussion

The description of this failure emphasizes the effect rather than the cause. However, the title "decimalization" suggests that the requirements were formulated in true fractional form whereas the implementation used decimal fractions. This aspect of the failure is classified as an example of incorrect functional requirements (Guideline 2.1-3).

There is also an indication that an inappropriate digital representation was used. This aspect of the failure is classified as an example of requirements did not ensure that data types were appropriate for the variables (Guideline 2.2.1-3).

0003 Pentagon Security Gate Malfunction

Date 08/05/00

Source Risks 21.05 (Neumann, 2001)

Domain Real-time control

Function Barricade access

Guidelines 2.3.3-1 2.5.2-1

Description

In RISKS-19.97, we reported on a Pentagon security system that injured the visiting Japanese defense minister and five others when a barricade was raised at the wrong time in September 1998. That accident was attributed to a faulty sensor and resulted in the installation of a new barricade control system.

On 5 Aug 2000, the same barricade sprang up under the German defense minister, who—arriving for a Pentagon honors ceremony—was injured and briefly hospitalized, along with the German defense attaché and an American security aide. [Source: Reuters item cited in the *New York Times*, 6 Sep 2000]

Discussion

The barricade control system needed to be reviewed not only from perspective of security but also for safety, since it was capable of causing injury. Sensor failures are common occurrences, and provision for the system to remain in a safe state after a sensor failure should have been incorporated at the outset. This cause of the failure is classified as an example of inadequate requirements for handling of sensor data (Guidelines 2.5.2-1).

The requirements should have been reviewed, particularly after the first failure, to provide for safe operation under off-nominal conditions. This cause of the failure is classified as an example of incomplete specification of I/O parameters, including operation under off-normal conditions (Guidelines 2.3.3-1).

0004 Single Points of Failure and Inadequate Backup Plans

Date 09/25/00

Source Risks 21.05 (Neumann, 2001)

Domain Internet

Function DHCP

Guidelines 2.8-4 2.5.2-1

Description

Monday, 25 September 2000 17:00:37 -0400

Last night our cable modem (currently AT&T Roadrunner, name subject to change daily) stopped working, and the constant busy signals from their tech support line led me to believe it wasn't merely Yet Another Outage (TM).

Strangely, my cable modem lights were all doing the right thing, and when I checked with my neighbors, their cable modems were working fine. After a couple of hours of redialing, I finally got a message saying that there were unspecified problems that they were working on (strange, usually they list the affected towns) and after some time on hold I finally talked to a tech support rep who offered to help "if I can."

Turns out the DHCP server for the entire northeast went down, and as people's leases on their IP addresses expired, they were dropped off the network. I asked about the secondary or backup DHCP servers, but apparently there was so much demand due to expired leases that the backup server couldn't respond quickly enough and was getting overloaded with requests.

Discussion

The network requirements did not provide adequate capacity of the backup DHCP to permit handling of demands that would arise from a foreseeable recovery condition. This cause of the failure is classified as an example of inadequate capacity planning in rollback/recovery (Guideline 2.8.2-4).

Even with the insufficient backup capacity, the network could still have recovered much faster if requirements had called for subscribers to be notified of impending loss of service and of the expected recovery time. This cause of the failure is classified as an example of inadequate match of recovery procedures with network characteristics (Guideline 2.5.2-1).

0005 UPS Backup Failure

Date: 10/12/000

Source Risks 21.10 (Neumann, 2001)

Domain Hospital

Function Uninterruptible power supply

Guidelines 2.1-3 2.9-4 2.3.4-9

Description

British newspapers today reported that a baby was born at Eastbourne General Hospital by caesarian section, the operation being performed under torchlight following a power cut caused by a storm. On one account, the standby generators couldn't be started as the computer that controlled them believed they were already on; and when main power was restored after twenty minutes, it could not be switched through to the operating theatre as the computer believed that the generators were still running. On another account, the computer refused to believe that the power had gone off in the first place.

http://www.guardian.co.uk/uk_news/story/0,3604,381054,00.html

The emergency lights above the operating table were not powerful enough for the doctor to work safely, so he sent nurses running to get torches (flashlights) from wherever they could. The nurses held the torches over the patient's abdomen in shifts to prevent their arms becoming stiff.

According to the Guardian, the operation succeeded because the patient required only a local anaesthetic and because the obstetrician had worked for ten years in Africa. He was used to operating not just under torchlight but under candlelight. According to the 'Telegraph', there was also a heart patient who died in an ambulance outside where paramedics were trying to revive him. The hospital denied that the power cut was a contributory factor in his death.

RISKS readers will recognize a number of too-common failings, such as the lack of easily usable manual overrides and a failure to test fallback modes of operation properly. Above all, there seems to have been a violation of the KISS principle. As Christopher Strachey said, 'It's impossible to foresee the consequences of being clever.' Clever failsafe mechanisms should be avoided. By Ross Anderson

Discussion

The requirements for monitoring the line voltage and starting the generators were incorrect and had not been verified. This cause of failure is classified as an example of incorrect and unverified logic (Guideline 2.1-3).

When power was restored, it should have been possible to override the automatic control system and return to normal power. This cause of the failure is classified as an example of inadequate requirements for manual overrides (Guideline 2.9-4).

In a nuclear power environment, the provision of IEEE 279 calling for manual initiation of all plant protective functions would have been applicable. If this installation had been subject to these provisions, the failure would also have been classified as an example of lack of manual initiation (Guideline 2.3.4-9).

0006 Saturn Limit Logic

Date	11/07/00		
Source	Risks 21.09 (Neumann, 2001)		
Domain	Automotive control		
Function	Safety interlock		
Guidelines	2.3.4-2	2.9-8	2.3.1-6

Description

As a safety feature, my Saturn will prevent me from going faster than is safe with my suspension or tires. When I first got the car, I had to try this feature out, so I found a long straight road and floored it. When I got to 105 mph the engine lost power and I slowed down. Experimentation revealed that I couldn't regain power until I dropped below 100, then I could accelerate again.

A couple of days ago I drove through a fairly steep chasm with a road straight down one side and up the other. I figured I needed as much momentum as possible, so I pushed the clutch in and coasted down. Somewhere along the way I hit 105 mph. Just as I was starting up the opposite side I noticed that virtually all of my warning lights were on, and the engine was at 0 RPM. A still engine means no power steering and no power brakes. I'm quite glad there weren't any turns or traffic that might have forced me to turn or brake.

The problem was the assumption that I got to an excessive speed by using the engine to accelerate. The default action works great when the clutch is engaged. In my case, I ended up with a car that suddenly became very hard to control when I was already doing something unsafe.

Discussion

The unsafe condition was due to a faulty assumption in the requirements that high speed was due to use of the engine. The cause of the failure can be classified as examples of:

(a) Forbidden transition; engine running to engine off while automobile at speed (Guideline 2.3.1-6)
(b) Improper specification of interlocks (Guideline 2.3.4-2)
(c) Improper operator interface (Guideline 2.9-8)

0007 A Subtle Fencepost Error

Date 11/19/00

Source Risks 21.05 (Neumann, 2001)

Domain e-Commerce

Function Order entry

Guidelines 2.3.4-1

Description

I recently got email from amazon.com offering me a $50 discount on any order of $100 or more from ashford.com. As it happens, my wife's wristwatch needed repair, and I decided that for $50, I wouldn't mind buying her another watch if I could find one I thought she would like. I found such a watch for exactly $100. When I tried to order it, the ashford.com website wouldn't accept my promotional offer code. More precisely, it accepted it but didn't indicate any discount. So I called them on the phone. The (very pleasant) sales rep said that he could place the order for me. When he tried, though, he also found that their system wouldn't accept the promotional code.

He then told me that he would go ahead and place the order anyway, and once it was in their system, he would make sure that I was charged the right price. It might take a day or two, but he would make it right. I told him to go ahead.

They let you track existing orders on their website. Later that day, the order was there, showing a price of $100.00. The next day, it still showed $100.00. The following day, it showed $50.01.

If you've read this far, I trust that you can figure out what must have happened.

Andrew Koenig, ark@research.att.com, http://www.research.att.com/info/ark

Discussion

The requirements were not specific in that they permitted using > rather than >=. This failure is classified as an example of lack of specificity and completeness (Guideline 2.3.4-1).

0008 Pentium III Chip Flaw

Date 08/29/00

Source Risks 21.04 (Neumann, 2001)

Domain Hardware

Function CPI

Guidelines 2.5.2-1

Description

New Pentium III chip recalled
"NewsScan" <newsscan@newsscan.com>
Tue, 29 Aug 2000 09:45:34 -0700

Intel is recalling its 1.3 gigahertz Pentium III chip, which it has sold to only "a handful" of "power users" running advanced applications because a certain combination of data, voltage, and temperature conditions may cause the chip to fail. The chip is expected to be back on the market in a couple of months. (Reuters cited in the *Washington Post*, 29 Aug 2000, http://www.washingtonpost.com/wp-dyn/articles/A40772-2000Aug29.html; *NewsScan Daily*, 29 August 2000)

Discussion

Robustness requirements must address the potential of hardware failures due to design or other sources. Growing complexity of hardware makes such design failures increasingly likely. Provisions for tolerating hardware failures are incorporated in Guideline 2.5.2-1.

0009 Train Door Failure

Date 01/08/00

Source Risks 21.04 (Neumann, 2001)

Domain Ground transportation

Function Door control

Guidelines 2.5.2-3 2.1-1

Description

Bruised but still a believer: the train fan who became a victim
Date: 01/08/2000
By ROBERT WAINWRIGHT, Transport Writer

As the head of Planet Ark, John Dee sat on the Olympic bid committee, which proclaimed that spectators should be encouraged to use public transport. As a commuter, Mr. Dee almost became a victim of the system he supported when his leg became trapped in a train door as it left Meadowbank Station on Sunday afternoon.

Though his pro-public transport beliefs have not changed, Mr. Dee, nursing a badly bruised right leg and sprained back, was having second thoughts yesterday about safety levels of the beleaguered rail system. He was the second person in the past four days to be trapped in a train door. Last Thursday, an elderly woman was trapped in the door as a train traveled between Redfern and Erskineville. The official report said the woman's leg was still "protruding from the door" when the train arrived at the next station.

Mr. Dee's ordeal began when he was returning home to Kirribilli after hosting a National Tree Day function. He tried to get off a train about 2.40 pm, just as the station guard was warning that the doors were closing and to stand clear. But Mr. Dee said the door was closing as the guard was speaking. It knocked him backwards, trapping his left foot below the knee inside the train and leaving his right leg dangling between the platform and the train wheels.

"The force of the door closing knocked me off balance. My left leg was trapped and my right foot was down near the wheels and I couldn't move. I was so far down that I had to hold the door with my hand to steady myself," he recalled yesterday. "Luckily, there were two women inside the train. They managed to open the door enough for me to get my left leg out but I was still trapped between the train and the platform."

Mr. Dee said a fellow commuter saved him from being crushed by screaming out to platform staff to stop the train from moving. "He saved me. The guard obviously couldn't see me. If the train had moved off then I would have been dead; it's as simple as that." Mr. Dee said he was worried about passenger safety during the Olympics. "You couldn't get a more pro-public transport group than Planet Ark, but there is something

blatantly wrong with the transport system," he said. "There were no safety buttons in the carriage to warn staff or stop the train, and there was no one on the platform to see me. It was pure chance that the train was prevented from moving." A spokesman for CityRail said both incidents were being investigated.

Discussion

That the trains were allowed to move with doors sufficiently open to trap passengers indicates that requirements for sensor processing (and their verification) were inadequate. This cause of failure is classified as an example of improper sensor data processing requirements (Guideline 2.5.2-3).

Safety considerations for public transport should preclude trains from moving with "body parts protruding." In terms of nuclear reactor safety, this is a "design basis event." This aspect of the failure is classified as an example of incomplete with regard to design basis (Guideline 2.1-1).

0010 Failures During Upgrades

Date 8/01/00

Source Risks 21.01 (Neumann, 2001)

Domain Banking

Function Customer interface

Guidelines 2.7-2 2.6-5

Description

Barclays Internet-banking security-glitch following software upgrade
Pete Morgan-Lucas <pjml@nsgmail.nerc-swindon.ac.uk>
Tue, 1 Aug 2000 09:30:44 +0100 (BST)

Barclays Bank yesterday had a problem within their online banking service—at least four customers found they could access details of other customers. Barclays are claiming this to be an unforeseen side-effect of a software upgrade over the weekend.

See http://news.bbc.co.uk/hi/english/business/newsid_860000/860104.stm for more details.

//Pete Morgan-Lucas// NERC_ITSS Network Security, NERC Swindon.

[Also noted by AllyM at http://www.theregister.co.uk/content/1/12287.html and Andrew Brydon in a BBC item that mentioned seven complaints. PGN]

Discussion

The upgrade requirements failed to provide the assurance of access control that had existed previously. This cause of failure is classified as an example of lack of access control (Guideline 2.7-2).

The failure description also indicates that requirements did not provide a defined methodology for performing software upgrades ("…we will not relaunch until totally confident this cannot happen again"). This cause of failure is classified as an example of lack of upgrade support (Guideline 2.6-5).

0011 Elevator Software

Date 11/12/98

Source Risks 20.07 (Neumann, 2001)

Domain Elevator

Function Floor announce

Guidelines 2.6-6

Description

Talking elevator with off-by-one error?
George Michaelson <ggm@dstc.edu.au>
Thursday, 12 November 1998 11:19:10 +1000 (EST)

New building. Seven floors labeled [1..7]

Enter lift [elevator]. Select floor 1.

Arrive at floor 1. Lift announces: "Floor eight."

My guess is that the software is generic and is loosely coupled to the real "I know where I am" function the lift has innately, talking or not. I have a mild concern that a lift this [is] confused—maybe doesn't want to be used.

Shades of Douglas Adams.

-George

Discussion

The software requirements for interfacing with "the real world" were issued and not verified. This cause of failure is classified as an example of lack of requirements for checking for completeness of interface (Guideline 2.6-6).

0012 GPS Clock Problem

Date 10/23/98

Source Risks 20-07 (Neumann, 2001)

Domain Aircraft

Function Time sync

Guidelines 2.2.1-2

Description

GPS internal clock problem
"Bob Nicholson" <lattice@popmail.dircon.co.uk>
Wed, 11 Nov 1998 08:20:39 +0000
[This has been reported earlier, beginning in RISKS-18.24, but is still a problem. PGN]

As a licensed aircraft engineer, I regularly receive "AIRWORTHINESS NOTICES" from the British CAA. Here is one (verbatim) that may be of interest.

CIVIL AVIATION AUTHORITY: AIRWORTHINESS NOTICE

No. 7, Issue l, 23 October 1998

"The Potential Resetting Of Global Positioning System (GPS) Receiver Internal Clocks"

1.1 The timing mechanism within GPS satellites may cause some GPS equipment to cease to function after 22 August 1999 due to a coding problem. The GPS measures time in weekly blocks of seconds starting from 6 January 1980. For example, at midday on Tuesday 17 September 1996, the system indicates week 868 and 302,400 seconds. However, the software in the satellites' clocks has been configured to deal with 1024 weeks. Consequently on 22 August 1999 (which is week 1025; some GPS receivers may revert to week 1—i.e., 6 January 1980).

1.2 Most airborne GPS equipment manufacturers are aware of the potential problem and either have addressed the problem previously or are working to resolve it. However, there may be some GPS equipment (including portable and hand-held types) currently used in aviation that will be affected by this potential problem.

2.0 Action to be taken by aircraft operators who use GPS equipment (including portable and hand-held types) as additional radio equipment to the approved means of navigation should inquire from the GPS.

Discussion

The software requirements did not consider the range of the data to be processed. This cause of failure is classified as an example of error in data size and precision requirements (Guideline 2.2.1-2).

0013 Electrostatic Discharge

Date 11/19/00

Source AMBRIEFS (FAA, 2000)

Domain Air traffic control

Function Communications

Guidelines 2.9-10

Description

At 9:53 AM EST, an electrostatic discharge (ESD) occurred, causing the V-3 East Arrival Integrated Communications Switching System (ICSS) position to fail. The controller felt the ESD through her headset. She filed a CA-1 form, but elected not to have a medical exam.

The specialist replaced several components and remapped the position to restore the V-3 position at 1:54 PM. The ESD was attributed to low humidity in the Terminal Radar Approach Control (TRACON). The carpet will be sprayed with anti-static material after the TRACON closes on 11/19. The headset was removed from service by Air Traffic for further inspection.

[TRACON: The facility at which controllers direct aircraft in the immediate vicinity of the airport, primarily for take-off and landing.

ICSS: The means by which flight data messages are sent to and from the approach control facility.]

Discussion

The requirement died not consider the effects of electrostatic discharge. This cause of failure is classified as an example of avoiding harm to operator at the human-computer interface. (Guideline 2.9-10).

0014 TDWR Crash Failure

Date 11/19/00

Source AMBRIEFS (FAA, 2000)

Domain Air traffic control

Function Weather radar

Guidelines 2.6-3 2.4-6

Description

At 11:10 PM CST, the Terminal Doppler Weather Radar (TDWR) failed during clear weather. The Low Level Windshear Alert System (LLWAS) was available.

A specialist was called out and performed a remote system reset and software reload via the Maintenance Data Terminal (MDT) at the tower. The system was returned to service at 12:55 AM.

Discussion

There had been repeated failures of this type (e. g., See Failure Description Nos. 3.15 and 3.16). The requirements did not mandate that conditions surrounding a system crash be completely described and recorded to support attacking the root causes. In the absence of such requirements, the technician concentrated on restoring operation as fast as possible. This cause of failure is classified as an example of lack of offline diagnostic requirements (Guideline 2.6-3).

When recurring problems are encountered, a failure rate should be determined to support management decision making and to help in the evaluation of fixes (e.g., Did a corrective measure reduce the failure rate?). This contribution to the failure is classified as an example of lack of failure rate calculation and assessment of conformance with quantitative requirements (Guideline 2.4-5).

0015 TDWR Communication Failure

Date 11/18/00

Source AMBRIEFS (FAA, 2000)

Domain Air traffic control

Function Weather radar

Guidelines 2.5.1-1 2.5.1-2

Description

DETAILS: On 11/18 at 9:11 PM MST, the Terminal Doppler Weather Radar Service (TDWRS) failed in clear weather due to a communications problem. The Wind Measuring Equipment (WME) was available.

RESOLUTION: MCI-Worldcom investigated under ticket #1119-0210 and reported that numerous channel banks were interrupted when a contractor caused a flood in the U.S. West main central office in Salt Lake City. Telco restored the circuit using an alternate path, and the service was restored on 11/19 at 2:05 A.M.

Discussion

The long recovery time was partially due to lack of requirements for dealing with anomalous conditions. Manual switchover to alternate commercial lines or satellite communications would have reduced the outage time. This cause of the outage is classified as an example of lack of requirements for error handling (Guideline 2.5-1).

Also, redundant communication channels shared a single weak link. The requirements should have called for identification and avoidance of correlated failure probability. The cause of this communication failure is classified as an example of lack of independence and redundancy requirements at both the system and software levels (Guideline 2.5.1-2).

0016 Weather Failure Due to Telco Circuits

Date 11/19/00

Source AMBRIEFS (FAA, 2000)

Domain Air traffic control

Function Weather radar

Guidelines 2.5.1-2 2.6-1

Description

DETAILS: At 7:30 AM EST, the Terminal Doppler Weather Radar Service (TDWRS) failed due to a Telco circuit interruption. The weather was clear, and the Wind Measuring Equipment (WME) was available.
[Note: Telco circuits are required to be redundant. The failure indicates that redundant circuits shared a common element]

RESOLUTION: Specialists notified MCI Worldcom, who investigated under ticket #1119-0562. Verizon dispatched a technician to the site, who replaced a faulty card in a T-1 circuit, but the problem persisted. Troubleshooting continues.

Discussion

Redundant communication channels shared a single weak link. The requirements should have called for identification and avoidance of correlated failure probability. The cause of this communication failure is classified as an example of lack of independence and redundancy requirements at both the system and software levels (Guideline 2.5.1-2).

Inability to identify the cause of the failure indicates lack of diagnostic requirements. This cause for extending the time for restoration of service is classified as an example of inadequate requirements for diagnostics (Guideline 2.6-1).

0017 TDWR SW Failure

Date 11/14/00

Source AMBRIEFS (FAA, 2000)

Domain Air traffic control

Function Weather radar

Guidelines 2.6-1 2.5.2-1 2.4-5

Description

DETAILS: At 9:36 AM EST, the Terminal Doppler Weather Radar (TDWR) failed in clear weather due to a Radar Products Generator (RPG) fault. The Low Level Windshear Alert System (LLWAS) was available.

RESOLUTION: The specialist reloaded the software and reset the TDWR. Diagnostics were then performed and the system was monitored before being returned to service to assure system reliability. The TDWR was returned to service at 11:00 P.M.

Discussion

Diagnostics in this case supported testing (monitoring) prior to placement of unit back into service. Although not a cause of failure, the event emphasizes the need for offline diagnostics (Guideline 2.6-1).

The RPG fault was a foreseeable event and requirements for exception handling might have prevented it from causing failure of the service. This cause of failure is classified as an example of incomplete requirements for exception handling leading to software failure (Guideline 2.5.2-1).

When recurring problems are encountered (See Failure Description Nos. 14 and 16), a failure rate should be determined to support management decision making and to help in the evaluation of fixes (e.g., Did a corrective measure reduce the failure rate?). This contribution to the failure is classified as an example of lack of failure rate calculation and assessment of conformance with quantitative requirements (Guideline 2.4-5).

0018 Weather Processor Crash

Date 11/14/00

Source AMBRIEFS (FAA, 2000

Domain Air traffic control

Function Weather processing systems

Guidelines 2.6-1 2.5.2-7

Description

DETAILS: At 3:00 P.M. EST, the Aviation Weather Processor Service (AWPS) was interrupted due to a system trap-out. All users were transferred to Salt Lake City (SLC) at 3:15PM.

RESOLUTION: Specialists performed a software reload and completed a flight database rebuild to restore service. At 4:42 P.M., the users were transitioned back to Atlanta AWPS.

UPDATE: 1114/0217Z: Service "A" transmit process ($AT0) trap-out occurred due to a "process invalid condition" in CPU 0. The preliminary examination of the "save" files by Operational Support (AOS) revealed that the trap-out occurred while attempting to transmit the non-hourly weather reports to WMSCR when the non-hourly portion of the service "A" transmit queue became full.

Atlanta AWP was requested to submit a PTR and forward the "save" files on tape and the service "A" line monitor system history file to AOS-540 for further analysis. No change in AWP procedures has been recommended at this time.

Discussion

Diagnostics in this case supported timely restoration of service. Although not a cause of failure, the event emphasizes the need for offline diagnostics (Guideline 2.6-1).

Buffer overflow during attempt to transmit caused by full queue indicates lack of requirements for accurate estimation of maximum queue size. This cause of failure is classified as an example of insufficient requirements for estimating the maximum queue size (Guideline 2.5.2-7).

0019 Indianapolis ARTCC Outage

Date 11/13/00

Source AMBRIEFS (FAA, 2000)

Domain Air Traffic Control

Function En route systems

Guidelines 2.5.1-1 2.4-2

Description

DETAILS: At 4:05 PM EST, the Indianapolis, IN (ZID) Air Route Traffic Control Center (ARTCC) experienced a loss of critical power that interrupted all air/ground communications, radar displays, and automation systems. Operations declared ATC Zero and activated the ATC contingency plan. The Air Traffic Control System Command Center (ATCSCC) coordinated a national ground stop for traffic to and through ZID airspace.

RESOLUTION: The CMOS chips in each of the circuit cards were weakened or faulty due to exposure to electrostatic discharge (ESD). This "damage" was confirmed through comparison/probing of the circuitry before and after the cards that contain the CMOS chips were replaced.

All the UPMs (uninterruptible power modules) have been tested. They will now have the defective cards replaced and be retested and aligned individually and as a combined system.

All 51 cards are bad; 45 in the UPMs and 6 in the Bypass Transfer Control System were verified [as] bad through comparison testing of the voltages and waveforms from the first UPM repaired.

Yes, the facility has used the energized but offline systems as the test bed.

Discussion

Requirements did not deal with detection of this correlated failure mechanism. This cause of failure is classified as an example of lack of requirements for independence of failure detection and recovery mechanisms (Guideline 2.4-2).

The use of an energized system for testing by substitution represents a hardware analog to inadequate exception handling in software. This cause of failure is classified as an example of inadequate requirements for exception handling (Guideline 2.5.1-1).

0020 Boston ARTCC Outage

Date	11/13/00		
Source	AMBRIEFS (FAA, 2000)		
Domain	Air traffic control		
Function	En route		
Guidelines	2.6-4	2.5.2-1	2.6-5

Description

DETAILS: At 2:27 AM EST, the installation of a Flight Data Input/Output (FDIO) Electronic Equipment Modification (EEM) to add Central Control Unit (CCU)-3 was completed. This EEM provides equipment diversity and required hardware and software changes to the FDIO and Central Computer Complex-Host (CCCH) adaptation changes. End-to-end testing was successfully completed.

At 5:30 AM, the host was configured for daytime operation, and error printouts started to appear indicating "time message timeouts" and undetermined errors for Nantucket (ACK) ATCT and Falmouth (FMH) TRACON. At 1:38 PM EST, the host experienced a slowdown of flight plans and General Information (GIs).

RESOLUTION: Initially the issue appeared to be a modem problem. After further investigation by the host specialist, it was determined CCU-3 would not switch and the secondary CCU seemed to be inoperative; the EEM installation was causing the problem. The specialists coordinated a host shutdown from 2:45 to 3:30 PM, removed CCU-3, and reverted to the previous version of software.

Operations continued using Direct Access Radar Channel (DARC) only. A ground stop and Mile-In-Trail (MIT) restrictions were implemented. Air Traffic completed the transition back to normal operations at 4:00 PM. AOS personnel arrived onsite to assist in the investigation during the 11/04 midshift. The preliminary assessment indicated a combination of factors were responsible for the host error messages, slowdown, and abort. One of the sites interfacing the CCU, Falmouth, has been a source of intermittent interruptions for several months. This alone has not caused a host operational problem. However, a LAN hardware problem in CCU-3, combined with the Falmouth circuit problem, caused a host queue buildup, and this buildup is suspected to have caused the saturation warnings leading to the host abort. The core dump from the abort will be analyzed by AOS on 11/04 to determine whether the abort was caused by the queue buildup. Also, preliminary analysis indicates a specialist was attempting to manually switch control units to work around the error messages at the same time the host was sending commands to also switch. This worsened the queue buildup problem and is believed to have led to the abort.

1107/1537Z: Bus connector and interface cards were replaced to restore the CCU-3 LAN. CCU-3 will remain out of the system until all testing has been successfully completed. A post-mortem report should be completed by 11/9.

Discussion

Technician action to reconfigure an air traffic control computer at the same time the system was trying to reconfigure itself exacerbated the problem. This cause of failure is classified as an example of lack of requirements to address proper functionality of system to support maintenance actions (Guideline 2.6-4).

The communication errors in the channel from Nantucket were part of the initiating events. This cause of failure is classified as an example of lack of requirements for exception handling in communication channels (2.5.2-1).

Requirements for testing the software upgrade were also inadequate. This cause of failure is classified as an example of lack of requirements for software upgrade support (Guideline 2.6-5).

0021 F-16 Weight on Wheels

Source Neumann, 1986

Domain Flight control

Function Landing gear retraction

Guidelines 2.3.1-6

Description

[During early flight testing] one of the first things the Air Force test pilots tried was to tell the computer to raise the landing gear while standing still on the runway. Guess what happened? Scratch one F-16.

Discussion

Requirements should have prevented raising the landing gear while the aircraft was on the ground. The aircraft being on the ground is normally sensed by the "weight on wheels switch." This very easily incorporated signal would have prevented the failure. This cause of failure is classified as an example of lack of requirements for conditions under which mode changes are permitted (Guideline 2.3.1-6).

0022 Stores Management

Date 10/1/86

Source Neumann, 1986

Domain Flight control

Function Stores management

Guidelines 2.3.1-1

Description

[In the F16] the onboard computer system has a weapons management system that will attempt to keep the plane flying level by dispensing weapons and empty fuel tanks in a balanced fashion. So if you ask to drop a bomb, the computer will figure out whether to drop a port or starboard bomb in order to keep the load even. One of the early problems with that was the fact that you could flip the plane over and the computer would gladly let you drop a bomb or fuel tank.

Discussion

This potential failure mechanism could be avoided by complete specification of the conditions for releasing stores. This cause of failure is classified as an example of lack of complete definition of the hardware and software runtime environment (Guideline 2.3.1-1).

0023 747-400 Uncommanded Throttle Closure

Date 4/11/90

Source Risks 10.04 (Neumann, 2001)

Domain Flight control

Function Autothrottle

Guidelines 2.5.2-1

Description

Boeing 747-400 Autothrottle problems
Martyn Thomas <mct@praxis.UUCP>
Wed, 11 Apr 90 17:26:41 BST

This week's Flight International reports:

"British Airways (BA) Boeing 747-400s have experienced uncommanded inflight closure of all four throttles on six separate flights between 6 October 1989 and 19 February 1990, 'several times' on one of those flights alone, according to formal reports. Several other airlines have suffered the same incident, Northwest reporting it first….

In most of the events the power levers retarded rapidly to idle, but sometimes the reduction was partial, followed by automatic reset….

All incidents have occurred in the climb or cruise, and an IAS of more than 280 knots is believed to be fundamental to the even….

Evidence indicates that the event is caused by a spurious signal to the full authority digital engine control from the stall-management module. The 'single-word' spurious command says that the undercarriage [gear] is down or the flaps are at setting 1, so if the IAS exceeds the maximum speed for these configurations, the autothrottles close to reduce IAS to limiting speed, then reset to maintain it.

The modification [to correct the problem—issued on February 22nd] assumes that the fault was in the processing logic of the appropriate universal logic card (a printed-circuit software unit [sic]) and adopts a standard technique for reducing digital oversensitivity: there is now a delay (a few microseconds) built into the software by requiring it to receive an 'eight-word' command before acting. Power spikes of other spurious commands should not produce a reaction.

So far the latest modification has proved effective. Early corrections, though, had assumed the reaction was associated only with main gear selection, so although software changes had reduced the incident rate, spurious flap signals continued to set engines to idle. BA has not reported any further events since

February.”

Discussion

The need to “de-bounce” switch indications is widely recognized to mitigate the effects of spurious switch operation (e. g., due to acceleration) or electric transients that simulate switch closure. A frequently used de-bounce technique is to require that the signal be present for a given number of clock cycles before it is accepted as valid. The cause of this failure is classified as an example of improper sensor data processing requirements (Guideline 2.5.2-1).

0024 A320 Article in Science & Vie

Date	6/2/90		
Source	Risks 10.02 (Neumann, 2001)		
Domain	Flight control		
Function	A320		
Guidelines	2.9-2	2.9-1	2.1-3

Description

This article appeared in the "Aeronautique" section of the French science magazine "Science & Vie," in the April 1990 issue. A rebuttal from Bernard Ziegler, technical director of Airbus Industrie, may be found in the following May issue.

LES CRISES DE NERFS DE L'A320

Translation of article by Bertrand Bonneau:

THE A320'S ATTACKS OF NERVES

The first aircraft in the history of the world to be totally "managed" by computer—Has the A320 been put into service before it is ready?

The excessive number of incidents during its first year of use can only make one think so. How could the willingness to declare the pilots responsible for major accidents, even before the judges have returned their verdict, appear other than suspect? Even so, as everyone wished, the verdict whitewashed the aircraft.

At the start of 1988, the French authorities and Airbus Industries congratulated themselves on the certification of the A320 only one year after the first flight of the prototype. In less than one year, the manufacturer had demonstrated the reliability of this new generation aircraft to the authorities of four of the states of the European Community.

However, controversy surrounding the aircraft would not be slow to surface…at the time of the inaugural flight of the Air France A320, on 28th March 1988 over Paris, with the Prime Minister of the time on board. This flight was marked by a series of technical incidents, notably by the untimely setting off of alarms. New controversies were to arise when an aircraft was destroyed in the forest of Habsheim in Alsace (26th June 1988), and when an Indian Airlines A320 crashed before reaching the runway in Bangalore last February. In both of the last two cases, the aircraft was whitewashed, as far as public opinion was concerned, before the slightest preliminary accident report was published.

Although what have come to be called the “Chirac flight” and the “Habsheim affair” are the two facts most known to the public, the first year of operation of the A320 has been marked by numerous incidents which have directly called into question certain systems on the airplane. Often badly received by the first crews qualified on this aircraft, and sometimes vigorously denied by the technical directors of the launching companies, these incidents lead one to ask if the manufacturers and the certification authorities have not proceeded a little too quickly.

[For example, there have been] twelve times more incidents than were foreseen. In his statement on the first year of operation of the A320 in the Air France fleet, a statement addressed to the general department of civil aviation (Direction Generale de l’Aviation Civile—DGAC) on the 11th July 1989, the technical sub-director of operations management of the national company remarks that the first exercise has been marked by “a greatly increased number of technical incidents altogether” (page 12). Whereas the target set was one incident per thousand hours of flight, the year 1988 ended with an incident rate of twelve per thousand hours of flight. For comparison, this rate was 5/1000 at the time of the first year of operation of the Airbus A300.

The frequency of these incidents that have marked the A320 going into service within Air France, Air Inter, and British Airways has forced the manufacturer to publish no fewer than 52 provisional flight notices (Operations Engineering Bulletins or OEBs) between April 1988 and April 1989. The launch of a new aircraft requires on average four times fewer [notices]. OEBs are temporary notices sent out by the manufacturer to the users. They form a list of anomalies or simply functional features of the aircraft that do not appear in the user’s manual for the equipment (FCOM, Flight Crew Operation Manual): they are only revealed in the course of operation. In the case of Air France, these provisional records are provided to the crews in the form of a volume of supplementary technical information notices (Renseignements Complementaires Techniques—RCTs).

For the A320, the number of OEBs alone gives an account of the problems of putting the aircraft into service. At the technical level, around twenty of the fifty main computers of the first A320s coming off the production lines in Toulouse have had to undergo modifications, for the A320 is the first aircraft in the world to be completely computerized. Computers control the function of all the systems of the airplane (motors, ailerons, but also the cabin lighting, etc); it [sic] processes raw data, converts them, and transmits them to the pilot. Now, the application of numerous modifications defined by the manufacturer in order to correct defects in the systems or to enhance them has been the origin of new breakdowns. These new problems have obliged the manufacturer to publish new OEDs before drawing up final modifications.

During service, companies have had to modify certain procedures once or several times for operating their aircraft. Also, with the exception of Air Inter, which reported only good results, the increased number of incidents was the origin of poor availability and bad technical readiness of the first A320s delivered. “Of 7,334 stopovers [landing + take-off’s (?)] carried out up to April 1989,” states the report of the technical sub-director of Air-France, “one lists on technical grounds [i.e., something went wrong (?)]: 4 acceleration-stops on take-off, 36 about-turns on the ground, 10 about-turns in the air, 1

emergency descent procedure, the cabin altitude being on the increase (without violent decompression), 1 engine stop in flight."

I think an about-turn on the ground is an aborted take-off, and an about-turn in the air is a return to the departure port. I'm not sure what the difference is between an about-turn on the ground and an acceleration-stop. Presumably the latter means the engines raced or cut-out during approach to take-off. 'Cabin *altitude* being on the increase' is a literal translation: I think it means the cabin atmosphere was below pressure, since they came *down*. Anyone with access to a dictionary of French avionic terms, or who knows the correct English avionic terms is welcome to correct me! It is advisable to add to these outcomes the grounding of aircraft due to suspect behavior and 74 cancellations of flight before even starting up the engines.

Reliability in question. For the aviation companies, the most serious problem would seem to have been that of the reliability of the information given to the crew by the various systems of the A320. The operating assessment by the technical sub-director of Air France is edifying on this subject. One discovers there, for example, that "certain inconsistencies of piloting information have led to certain confused and very distracting situations, where the information presented to the pilots on the control screens during flight was in contradiction to the physical reality of the equipment, not always verifiable in flight" (report already cited, page 18). [Presumably this means: "The instruments were lying, but the pilots couldn't get out and walk around to check this at 30,000 feet!" Nice to know that French technical officialese is as obscure as British or American!]

Without a doubt, Captain Claude Dalloz and First Officer Patrick Vacquand share the views of the technical sub-director of Air France. On the 25th August 1988, while taking off from Roissy on a flight to Amsterdam (flight AF 914), they had the disagreeable surprise of seeing the message "Man pitch trim only" appear in red on their control screens. In plain terms, this message informed the pilots that the controls activating the pitch control mechanism were no longer in a functional state. In this case, the only means of ensuring the longitudinal stability of the aircraft is to manually move the trimmable horizontal stabilizer by means of the pitch trim wheels.

Meanwhile, the copilot who was at the controls felt not the slightest difficulty in controlling the aircraft. Then the crew witnessed a display of imaginary alarms ("fire in the toilets," for example), and noticed new signaling anomalies on the screens concerning the flight control systems, the position of the landing gear, and also the situation of the automatic pilot.

It was therefore decided to return, but, during the approach, the gear at first refused to come down normally. Given the uncertainty, three passes at low altitude were made in front of the control tower to ascertain the real position of the gear after having carried out safety maneuvers. As the information provided to the crew ("gear partially down") did not correspond to the observations of the controllers at Roissy (gear down), the passenger cabin was prepared for an eventual crash, which, very fortunately, did not occur. The same incident recurred on another plane on 29th November 1988. It finally required nine months of operation before a new, more reliable, version of the Flight Warning Computer (FWC) called into question by these two cases was made available to users.

A temperamental altimeter. A good many problems, due to the design of certain systems, have revealed themselves since the start of operation. The most spectacular for the passengers would have been the vagaries of the integrated cabin communication system (CIDS), which modified explanations or illuminating announcements in an eccentric fashion. More seriously, the crews discovered that the temperature regulation of the passenger cabin could interfere with the functioning of the engine power control computers (FADEC), generating breakdowns and alarms. To avoid these interferences, crews were asked not to "reinitialise" the cabin temperature regulation system while the engines were running.

However, the most worrying phenomenon for the crews has been the untimely alterations to the setting of the altimeters during flight. Having reached a certain altitude, the pilots set their altimeters in a standard way, calculated in relation to the theoretical atmospheric pressure at sea level (1 013 hPa), in order that all aircraft using the airspace should have the same reference for altitude (QNH base). Relative to this base, the altimeter indicates a pressure altitude, which is a "QNE" altitude. While the aircraft is descending, at a predetermined height, the crew must set their altimeters in relation to the altitude of the destination airport (QFE base). Apart from some very rare landing strips situated below sea level, airports are above this [sea] level. Since pressure diminishes with altitude, the value of QFE is generally less than 1 013 hPa. The sudden alteration of the altimeter setting by the flight programming computer (Flight Control Unit, FCU) sometimes occurs in uncomfortable conditions. So, in July 1988, during an approach to Roissy, the untimely alteration of the altimetric setting, which conveyed itself as a reversal of the altimeter reading, provoked an automatic delivery of fuel in order to compensate for the false deviation in altitude generated by the defaulting computer and detected automatically by the safety systems of the aircraft. This delivery of fuel occurred while the aircraft was being flown manually on its descent. The rapid intervention of the pilot could not avoid the aircraft going into overdrive for several seconds.

Untimely alterations of altimetric settings showed up on at least the first three planes delivered to Air France, among them the aircraft that crashed at Habsheim. The commission of inquiry has revealed in its final report that such an incident had taken place on the plane several hours before its crash, concluding immediately that this anomaly due to a design error had played no part at all in the accident. Moreover, the flight report (CRM, compte-rendu materiel) of a crew concerning a third aircraft of Air France made mention of vagaries of the altimeter.

It is therefore surprising that the report of the technical sub-director of Air France limits this type of incident to a single A320 of his fleet (the aircraft registered F-GFKB), when it has also occurred on at least two other planes (registered F-GFKA and F-GFKC). But the most amazing thing remains that this functional anomaly should cease without anyone being able to identify its origin!

Recording of parameters. In an indirect manner, these two types of incidents have revealed another potential source of problems in the level of the recording of parameters by the "black box recorder" (DFDR, Digital Flight Data Recorder). In effect, each piece of information given to the pilot is handled by a cascade of computers. Now, this "black box" records the majority of its information on the intermediate computers and not at the start or end of the processing chain. When examining this data,

therefore, there is nothing that allows one to know precisely what the pilots had for information, since there is no recording at the output of the symbol generator [DMC] for their screens.

The problems posed by the flight data recording system can be illustrated by referring to the two incidents mentioned. If the Paris/Amsterdam flight recalled above had ended in a crash, the "black box recorder," which captures a large part of its information from the flight warning computer (FWC), would have revealed that the crew no longer had pitch control available. In fact, all the flight controls were functioning, but the flight warning computer, which is one of the principal sources of information of the "black box recorder," had failed (diagram, p.98).

Equally, if the untimely alterations of the altimeter readings had ended in a crash, the "black box recorder" would have revealed no malfunction of the altimeter assembly, since the recording of pressure altitudes (QNE), which was correct, is affected by equipment located upstream of the failing computer. This computer (FCU) incorrectly processed the information that had been sent to it, and an erroneous indication of altitude was sent to the control screens (diagram above, p. 99).

Modification Campaigns. Before the A320s went into service, the launch companies' instructors—who cannot be accused of bias since they were all volunteers—complained of having had no contact with the test pilots of Airbus Industries. The report of the technical sub-director of Air France, for its part, confirms this worry by revealing that it had, at last, been possible to establish a "frank relationship" (page 17) after six months. The adaptation of failing systems has been progressively integrated in the course of several modification campaigns begun at the start and middle of 1989 as problems were found and listed. It was necessary to wait until the end of last year to obtain the definitive version of certain pieces of equipment, that is to say, eighteen months after the certification and entry into commercial service of the A320.

At the end of last year, the dossier of supplementary technical notices (RCTs) distributed to A320 crews already comprised eleven pages, whereas the RCTs of other aircraft in the Air France fleet rarely went beyond three pages.

Contrary to the fears expressed many times in the course of these last years, not only by certain pilots' unions, but also by the American certification authorities (Federal Aviation Authority, FAA), the electrical flight controls and the electronic engine control system, which constitute the two great technological innovations of the A320, would never be the direct cause of any significant incident, notably in stormy conditions. During test, just as in service, the A320 was struck by lightning several times without the least influence on the flight controls.

The majority of the teething troubles and design faults of the A320 therefore concern more classical systems. The report of the technical sub-director of Air France is once again definitive: "Pressurization, management of cabin communications (CIDS), pneumatic generation, auxiliary power units (APU) … have been for a long time an unacceptable reliability. Everything is still not under control to this day (NDLR: 11th July 1989)." (Report already cited, page 17).

Industrial secret. It could therefore be thought that the certificator has turned his attention above all to the innovative elements (flight controls, FADEC, etc.) of the A320. However, this explanation, although not completely without foundation, does not take into account the fact that the systems called classical are also subject to major innovations, since they practically all require computer automation.

Discussion

Spurious data indications by the flight warning computer may be due to lack of de-bounce as described under Failure Description No. 23) but in any case indicate that requirements for vital operator displays ignored essential characteristics. This cause of failure is classified as an example of incomplete HCI requirements (Guideline 2.9-2).

The number and ordering of event notifications on the display obviously made the pilots' task more difficult. Warning displays should recognize that operators can only perform a limited number of actions and must prioritize the displays so that the most important actions will be taken first. This cause of failure is classified as an example of event notification and display requirements inadequacies (Guideline 2.9-1).

The incorrect warning of the outage of automatic pitch trim caused the operators to take improper actions. For vital indications there must be independent means of distinguishing between failures of the monitored system (here, flight controls) and the monitoring system (the flight warning computer). This cause of failure is classified as an example of incorrect requirements for control and indication (Guideline 2.1-3).

0025 747 Problems

Date 6/25/90

Source Risks 10.12 (Neumann, 2001)

Domain Flight control

Function Flight management, Maintenance

Guidelines 2.5.2-1

Description

747-400 computer problems cause excess departure delays
Jon Jacky, University of Washington <JON@GAFFER.RAD.WASHINGTON.EDU>
Mon, 25 Jun 1990 17:33:41 PDT
Here are excerpts from the Seattle *Post Intelligencer*, March 22, 1990, p. B7:

BOEING TASK FORCE TACKLES PROBLEMS WITH THE 747-400 by Bill Richards

After a year on the job, Boeing's newest jumbo jet, the 747-400, has piled up more mechanical delays at the departure gate than any of the company's jetliners since the first 747 went into service 20 years ago. Boeing officials said yesterday they knew about problems with two especially troublesome pieces of equipment—a computerized power unit used to start the plane's engines and a computer that spots maintenance problems—but decided to sell the jumbos anyway.

[Boeing official Robert A.] Davis said the problem with the 400's engine power unit was caused by unusual sensitivity in the unit's digital monitoring system. If the plane switches from ground power to auxiliary power to engine power in the wrong sequence, the engines shut down and must be restarted, which results in a delay at the gate, he said. Boeing engineers were aware of the problem during the plane's flight tests, said Davis, but decided to maintain the plane's sales schedule and troubleshoot later.

Boeing also discovered a problem with the plane's central maintenance computer during flight tests. The computer, which keeps track of equipment malfunctions in 75 separate systems when the plane is on the ground, was not "fully debugged" when Boeing began delivering its first 400s last year, Davis said.

The 400's performance record lagged so badly behind previous jetliner models that the company formed a special task force last month to whip the plane into shape. Davis, who heads the task force, said the unit has started improving the 400's "dispatch reliability rate," the measure of how frequently the planes are delayed more than 15 minutes at the boarding gate because of mechanical malfunctions. Davis said none of the problems encountered in the 400 could cause the plane to be unsafe to operate. But Boeing has received complaints "across the board" from airlines that own the jetliner, Davis said.

Boeing said it expects to cure the glitches in the 400 by making changes on its production line next month. So far, about 20 of the (57) 400s already in operation have been retrofitted since October.

Discussion

The problems in the power control computer and in the maintenance computer may need separate corrective measures, but they share a common root cause in that requirements for sensor data processing were incorrectly stated and not verified. The common aspect of these failures is classified as an example of incorrect sensor data processing (Guideline 2.5.2-1).

0026 Train Signal System Software

Date 7/23/90

Source Risks 10.15 (Neumann, 2001)

Domain Train control

Function MMI

Guidelines 2.1-3 2.5.2-3

Description

Pete Mellor <pm@cs.city.ac.uk>
Mon, 23 Jul 90 20:00:44 PDT
>From the *Guardian*, Mon. 23rd July, front page:

Headline: BR signalmen 'worked blind'
Subhead: Computer software problems admitted at key commuter train center
By-line: Patrick Donovan, Transport Editor

British Rail has admitted that computer software problems have been uncovered at a signal center, which controls London's busiest commuter lines. They left operators "working blind" after train movements were wiped off control screens on at least one occasion over the last five weeks. A BR spokesman said newly installed software, responsible for flashing up the position of trains on the indicator screens of signal operators at Wimbledon, has been found to contain two technical faults. The Wimbledon center controls 90 mph services south of Waterloo and includes the Clapham Junction area, where 35 people died in a train accident in December 1988. Faulty wiring on a signaling modernization program was found to have caused the crash.

BR said one of the faults uncovered on the indicator screen software has not yet been fully rectified. An internal investigation began after an operator found that the system was providing "the wrong information." Realizing that he had lost track of train movements, the operator immediately turned all signals to red.

A spokesman said that at no time was any train at risk. "What happened caused concern to the signalman." But he stressed that the mechanical signal equipment and all other equipment worked normally, bringing all trains to an immediate standstill after the problem was discovered.
"The problem was caused by computer software fault in the signal box. [sic—PM] It gave the wrong indication to the signal man. All the trains froze where they were. The lights told him that something was different to what was happening [outside]."

BR conceded that the faulty equipment served a vital function, “This little piece of software tells the signalman what is happening outside.” The software faults were found inside the panel in the train indicator box in a system responsible for operating the lights.

Alastair Wilson, contracts and production director of E. B. Signal, the manufacturers, said: “The system is under test. I do emphasize that things are going through a testing stage. It is not unusual to have minor software bugs.”

A spokesman for the National Union of Railwaymen said that any operational shutdown of train indicator screens would “at best create a major disruption and at worst could create alarming safety hazards. If everything goes to red it puts enormous pressures on an individual signalman.”

Discussion

The description shows that sensor data were not correctly processed, at least under some conditions, and that this led to incorrect information being displayed to the operator. This cause of failure is classified as an example of inadequate correctness requirements (Guideline 2.1-3).

That the software furnished wrong information to the operator indicates lack of requirements for internal checks. This contribution to the failure is classified as an example of failure to provide for validation of inputs and outputs (Guideline 2.5.2-3)

0027 NASDAQ Outage

Date 12/1/00

Source Copeland, 2000

Domain Stock trading

Function Online trading system

Guidelines 2.4-6

Description

Software glitch forces 11-minute shutdown of NASDAQ

By Lee Copeland, Computerworld
http://www.infoworld.com/articles/hn/xml/00/12/01/001201hnnasdaq.xml?p=br&s=7?1207thpm

A SOFTWARE GLITCH in the NASDAQ's price quote engine caused the stock exchange to halt trading for 11 minutes on Wednesday. It is the third time this year that the stock exchange has experienced a slowdown or halt in trading due to problems with its order-routing system. Analysts said temporary outages and technology glitches are recurrent problems that online brokerages and trade exchanges haven't yet been able to lick. "NASDAQ will have glitches, as will NYSE and other full-service and online brokerages, because no one is operating in a fail-safe mode," said Dan Burke, an analyst at Gomez Advisors in Lincoln, Mass. "They are all spending tremendous amounts of resources to ensure 100 percent uptime, but there's no real way to ensure it yet."

According to NASDAQ stock market officials, Wednesday's halt was caused by a software problem in its Small Order Executive System and its quote update system by Carlsbad, Calif.-based SelectNet. NASDAQ officials said they noticed the problem at 3:40 p.m. EST and suspended trading at 3:49 p.m. EST. Technicians had restored the system incrementally by 4 p.m. EST. "We shut down on our own, so that folks were not trading on stale quotes," said NASDAQ spokesman Andy MacMillan. "It was a unique combination of circumstances that caused the problem, but the problem was fixed by after-hours trading."

Until the problem was fixed, NASDAQ traders were unable to update and view new quotes. The exchange also handled a higher-than-usual trade volume of approximately 2 billion trades. NASDAQ's average share volume is 1.65 billion trades per day.

Problems with the order-routing system have caused delays on two other occasions this year. The SelectNet system experienced 75 minutes of update delays on April 4. That day investors traded 2.9 billion shares on the exchange and requested 6.5 million quote updates. On Feb. 18, a communication line malfunction disrupted the dissemination of last-sale-price data on NASDAQ for two hours.

“Technology is brittle,” said Jaime Punishill, an analyst at Forrester Research in Cambridge, Mass. “Considering it was down for less than 20 minutes and it has only happened twice this year, I say the NASDAQ has done a pretty good job of keeping its technology up to snuff.”

Discussion

The description does not provide sufficient information to assign a specific cause in the program, though there are indications that failures are volume related (meaning insufficient capacity planning). However, when repeated failures are encountered it should be possible to state whether quantitative reliability or availability requirements were defined and whether they were being met. This aspect of the failures is classified as an example of importance of quantitative reliability and availability requirements (Guideline 2.4-6).

0028 Subway Doors

Date	1/10/91		
Source	Risks 10.77 (Neumann, 2001)		
Domain	Ground transportation		
Function	Automatic doors		
Guidelines	2.5.2-1	2.5.3-3	2.9-2

Description

[SMH Home | Text-only index]
From Risks 10.77.

Vicious Subway Cars (was: Vicious Elevators)
Unix Guru-in-Training <elr%trintex@uunet.UU.NET>
Thu, 10 Jan 91 12:42:54 EST

Here's a quick rundown on RISKS of stepping through the doors on a New York City subway car: each of the twin doors can be as much as 3 inches open when the train starts moving, giving you a maximum gap of 6 inches. Although an interlock prevents the train from starting while the doors are open (called the "indication" by the train crew), the sensors aren't too precise. People can (and do) get dragged by moving cars when they're stuck in the doors. Usually it's their own fault—hyped up New Yorkers who won't wait the next three or five minutes for the next rush hour train (or ten or twenty minutes off peak) blocking the doors open in the vain hope the conductor will re-open and let them in. As a previous RISK poster noted, this all depends on the conductor's mood and if s/he is in a hurry or not. It also depends on their line supervisors: some managers emphasize speed, others passenger safety.

A few years ago the Transit Authority had a problem with "doors opening enroute" on the older (pre-1976 or so) cars—an individual door would open while the train was in motion, once on a speeding express train (thankfully, no one was hurt). The TA rewired all their newer trains with an interlock so that the emergency brake would activate if the doors opened while the train was in motion.

You can experiment with this safety interlock by attempting to force one of the doors open while the train is moving. One day I observed two teenagers on the way to Brooklyn doing exactly that, thrilling over pushing open a door two inches as the train sped through the tunnel. When I warned them that they would kick in the emergency brake if they went too far they had a spell of enlightened self-interest (it can take ten or fifteen minutes for the crew to reset the emergency brake) and left the poor door alone.

Ed Ravin, Prodigy Services Company, White Plains, NY 10601 elr@trintex.UUCP

Discussion

That opening of a door would not bring a moving train to an immediate stop indicates lack of requirements for tolerating sensor failure. This cause of failure is classified as an example of lack of requirements for handling input/output hardware failures (Guideline 2.5.2-1).

That forcing a door open will cause an emergency stop that can only be manually reset by train personnel indicates a need to review requirements for response to temporary conditions. This cause of potential failures is classified as an example of cancellation of partially completed operations (Guideline 2.5.3-3).

The description indicates that people can be trapped in partially open doors, and that the response to such events is up to the individual operator. Proper requirements would identify a response to such situations. This cause of potential failures is classified as an example of response to events (Guideline 2.9-2).

0029 London Subway Doors

Date	1/10/91		
Source	Risks 10.77 (Neumann, 2001)		
Domain	Ground transportation		
Function	Automatic doors		
Guidelines	2.1-1	2.5.3-3	2.9-2

Description

Vicious Doors on London Underground/Network South-East
Pete Mellor <pm@cs.city.ac.uk>
Thu, 10 Jan 91 21:33:56 PST

I was interested in Olivier M.J. Crepin-Leblond's two mailings (RISKS-10.75) regarding the recent train crash and the behavior of tube train doors. I am also a victim (sorry, commuter! :-) of "Network South-East," the bit of what used to be British Rail that serves East Anglia and the area southeast of London. They are a byword for discomfort and overcrowding, even where the rolling stock is new, as it is on the lines from Peterborough and Cambridge into London King's Cross. It was recognised at the enquiry into the Clapham rail disaster that a large proportion of the deaths and serious injuries in a crash can be attributed to passengers having to stand in the aisles between the seats. Even a low-speed impact means that standing passengers who insist on obeying Newton's first law of motion will continue their journey along the carriage until brought to rest by their fellow passengers or by the door to the adjoining carriage.

Even so, it does not appear to be cost-effective to supply adequate numbers of carriages to cope with the rush hour. After all, the management has to show a profit so that privatization will attract investors, and a yearly season ticket between Stevenage and London only costs 1744 pounds sterling.

Another bit of cost cutting is to use driver-only trains. There is no guard to check the doors before the train pulls out. This is so on most rail and underground services. There is usually a TV monitor, which the driver can use to check the length of the platform. This does not seem to be particularly effective, judging by the number of incidents I have personally witnessed over the last few years, such as:

A driver closing the automatic doors and pulling away after a mother got out but before her children had time to leave the train. (Frantic waving and shouting by other people on the platform made him stop.) - Network Southeast. An elderly woman boards the train (Underground: Piccadilly Line), and the driver closes the doors and moves off before her equally elderly husband can get on.

I leaped onto a crowded tube train (Underground: Metropolitan Line) carrying a shoulder bag just as the doors were closing. I got on, but my bag didn't. The doors closed around the strap, and the train

moved away with the bag hanging outside the carriage, and me pinned to the door by the strap around my shoulder, just waiting for the first obstruction to snag the bag. Fortunately, someone pulled the emergency handle, and the train stopped before it entered the tunnel.

What has this got to do with computers? Not a lot! All these incidents occurred with a human in the loop (just one human, and obviously not very firmly in the loop!). I think that less, not more, automation is the answer to safety here. Bring back the guard! (I went through King's Cross on the Circle Line while the fire was raging a few years ago. They're gonna get me one day!)

Discussion

Safety considerations for public transport should preclude trains from moving when articles of attire are protruding on the outside. In terms of nuclear reactor safety this is a "design basis event." This aspect of the failure is classified as being incomplete with regard to design basis (Guideline 2.1-1).

Separation of mother from children or other dependents indicates a need to review requirements for response to temporary conditions. This cause of potential failures is classified as an example of cancellation of partially completed operations (Guideline 2.5.3-3).

The description indicates that scanning the platform for unsafe conditions is up to the individual operator. Proper requirements would identify a response to such situations. This cause of potential failures is classified as an example of response to events (Guideline 2.9-2).

0030 747 Engine Shut Down

Date 10/3/90

Source Risks 10.10 (Neumann, 2001)

Domain Aircraft

Function Engine control

Guidelines 2.5.2-3

Description

BA 747-400 Engine Failure
Martyn Thomas <mct@praxis.co.uk>
Wed, 3 Oct 90 15:21:58 BST

Flight International (3-9 October) reports that a British Airways Boeing 747-400's No. 1 engine electronic controls failed on takeoff at London Heathrow, causing the engine to shut down. The crew [two pilots, there is no flight engineer] reported the status message "engine controls" and asked their technical support staff, by radio, for advice. They were told, "You've obviously lost control of that engine. It's a FADEC failure" (FADEC = Full Authority Digital Engine Controller).

BA says that the problem was a spurious signal from the electronic "thrust reverse resolver." If so, the early diagnosis of FADEC failure could be wrong. There has been a number of instances of spurious signals causing 747-400 engines to throttle back or shut down, according to Flight (This may be a reference to the earlier reports of spurious signals from flap and gear sensors, reported in an earlier RISKS). Flight International adds that a FADEC failure is extremely unusual.

Martyn Thomas, Chairman, Praxis plc. Software Engineers.

Discussion

Sensor failure caused engine shutdown in a critical flight regime. Requirements for redundant sensors and data processing would have avoided the problem. This cause of failure is classified as an example of validity checks on input (Guideline 2.5.2-3).

0031 Security Computer Failure

Date 1/14/98

Source LER 206 1998 001

Domain Nuclear Power

Function Security Computer

Guidelines 2.3.2-2 2.5.2-3

Description

On January 14, 1998 [discovery date], Southern California Edison (SCE) prepared to install a chart recorder on the primary security computer for system diagnostic testing. At about 9:25 A.M., before starting the installation, SCE had conservatively posted compensatory guards for the appropriate plant areas, as specified in Station Procedures SO123-IV-6.8, "Protected Area and Vital Area Barrier Patrols," for a complete loss of security computers. SCE switched to the backup security computer, removed the primary computer from service and installed the chart recorder. When returning the primary computer to service, a computer network server software error occurred, causing the primary computer to initialize incorrectly. At about 10:26 A.M., the backup computer also failed as a result of this error.

The primary and backup computers were restarted at about 10:32 A.M. and 10:36 A.M., respectively. The cause of this event was an equipment failure. During the reboot of the primary computer, the network server function for the security computers did not start. However, the “boot” sequence continued until the main security program started on the primary computer. Without the network server function, the two computers could not completely communicate and consequently could not fully function. The main security program was not capable of recognizing that the network server function had not started and tried to regain the primary role in the security monitoring system. As a result, a conflict arose and the backup program became unstable and failed to function. Since the primary had no network server function, it could not communicate properly, leaving both primary and backup down.

Discussion

The original cause of the failure was that initialization requirements did not cover start-up from unusual conditions (Guideline 2.3.2-3), causing a communication link to be dropped. The problem was compounded by lack of robustness in that requirements for neither the primary nor the back-up computer provided for verification of the presence of the communication link (Guideline 2.5.2-3).

0032 Thermal Power Calculation

Date 1/14/98

Source LER 220 1998 003

Domain Nuclear power

Function Reactor thermal power

Guidelines 2.2-1

Description

On March 4, 1998, at approximately 1600 hours, with the reactor mode switch in the RUN position, Nine Mile Point Unit 1 (NMP1) exceeded 100 percent rated core thermal power and exceeded the power/flow relationship of Technical Specification (TS) 3.1.7.d. Specifically, the eight hour average for reactor thermal power at 1600 hours read 1851 Megawatts Thermal (MWt) on the control room hourly typer, which exceeded the licensed maximum power level of 1850 MWt. Shift personnel failed to recognize that reactor power was at rated and increasing slowly during the shift due to the reactivity conditions of the core at this point in the operating cycle. Investigation has determined that the thermal power limit had been exceeded on multiple previous occasions.

Shift average power, computer point C873, is calculated by the process computer. The computer extracts a value of instantaneous core thermal power, computer point C875, once each 10 minutes starting at 0000, 0800, and 1600 hours each day. The computer then averages the C875 values to create C873. The C873 value is displayed on the hourly typer in the Trend 7 position. [It was determined that the 10 minute sampling interval did not provide sufficient accuracy].

Discussion

Several means of determining thermal power are available to control room personnel; the most accurate ones show fluctuations, while the C873 computer point has a stable display and is also available in typed form. The requirements for the C873 data did not foresee that this would be the preferred means of establishing thermal power output and did not provide sufficient accuracy (Guideline 2.2-1)

0033 Disabled Function

Date 10/28/99

Source LER 247 1999 019

Domain Nuclear power

Function Position deviation alarm

Guidelines 2.3.1-4

Description

On October 28, 1999, with the unit at 99% power during surveillance testing, the alarm limits for the control rod position deviation (rod-vs-bank) alarm were discovered to be plus or minus 24 steps. The design alarm limits are plus or minus 12 steps. The rod position monitoring system had erroneously been allowed to be disabled due to lack of proper software configuration control of software upgrades related to the Y2K issue. [The contractor performing the upgrade had been allowed to disable functions that were thought to be obsolete, and Con Edison assumed responsibility for determining disposition.] Due to an oversight, that [review of disabled programs] was never completed. As a result, the unit was placed in operation with the RODLOW program disabled.

Discussion

The overall software requirements apparently contained no provision to assure that all required functions were present (Functional completeness of software requirements, Guideline 2.3.1-4).

0034 Snubber Inspection Scheduling

Date 7/16/98

Source LER 270 1998 004

Domain Nuclear power

Function Scheduling software

Guidelines 2.6-3

Description

On July 16, 1998, as part of Oconee's Recovery Plan for Technical Specification (TS) Initiative, it was recognized that some TS snubber surveillances were incorrectly coded in the scheduling software. On July 22, 1998, with Units 1, 2, and 3 at 100% full power, a review of past snubber surveillance dates on all three units determined that Unit 2 had exceeded the snubber surveillance frequency from approximately February 13, 1998, until the unit was shutdown for a refueling outage on March 13, 1998. The surveillance was satisfactorily completed on March 18, 1998. The root cause of this event is a weak process to control changes to the frequency in the scheduling software. A contributing cause is the potentially confusing wording of several TSs.

Discussion

Scheduling software is part of the offline monitoring functions. Guideline 2.6-3 for these functions states, "Requirements should specify for each of the system surveillance and monitoring operations….The frequency of execution of the offline monitoring functions, by sensor or channel, if applicable."

0035 Reactor Instrumentation

Date 3/20/99

Source LER 275 1999 002

Domain Nuclear power

Function Power and temperature instrumentation

Guidelines 2.5.1-1

Description

On March 20, 1999, at 1753 PST, with Unit 1 in Mode 1 (Power Operation) at 92 percent power, Technical Specification 3.3.1, "Reactor Trip System Instrumentation," Table 3.3-1, Action 6, was not met when two channels affecting over-power delta temperature and over-temperature delta temperature were placed in bypass on three occasions, instead of keeping one channel in the tripped condition. The condition lasted less than one hour; therefore, Technical Specification 3.0.3 was met. On March 21, 1999, at 0136 PST, Channel 1 was being tested in the tripped condition. When the testing software detected an electronic communication error, the test automatically aborted. The aborting process changed the condition of the channel from tripped to normal. Technicians returned the channel to tripped within 2 minutes and operators requested the event be evaluated for reportability as a TS violation.

Discussion

The abort process should have restored the channel status to its previous (tripped) condition rather than to normal. Guideline 2.5.1-1 states, "Requirements should identify all foreseeable exceptions and system errors and specify how they are to be handled."

0036 Inspection Procedures

Date 1/8/99

Source LER 282 1999 002

Domain Nuclear power

Function Circuit breaker inspection

Guidelines 2.3.1-4 2.6-3

Description

On January 8, 1999, while Prairie Island Nuclear Generating Plant (PINGP) Unit 1 was at hot shutdown (due to the 1M transformer fault) surveillance procedure (SP) 1016, "RCP Breakers Test," was being performed. Per the SP, the 11 Reactor Coolant Pump (RCP) was stopped and Bus 11 was de-energized. At 0852, during the execution of SP 1016, 12 RCP tripped and the 11 Turbine Driven Auxiliary Feedwater Pump (TDAFWP) auto-started. This event was reported via the Emergency Notification System on the basis of entry in PINGP Technical Specification 3.0.C (due to loss of both RCPs) and on the basis of ESF actuation of the 11 TDAFWP. SP 1016 (and corresponding Unit 2 SP 2016) will remain quarantined until the procedures are appropriately revised.

A step to lift a wire that was in a previous revision of SP 1016 would have prevented trip of the 12 RCP. The missing step in the SP was apparently due to an electronic document management system (EDMS) software error when the SP 1016 file was converted to the new EDMS system in 1996. The loss of the SP step upon conversion was not identified during post-typing or engineer review.

Discussion

The surveillance procedure requirements apparently contained no provision to assure that all required functions were present (Functional completeness of software requirements, Guideline 2.3.1-4)

Surveillance procedure software is part of the offline monitoring functions. Guideline 2.6-3 for these functions states, "Requirements should specify for each of the system surveillance and monitoring operations….Interlocks to prevent operation when systems are being maintained."

0037 Disabled Alarm

Date 1/18/99

Source LER 302 1999 001

Domain Nuclear power

Function Control rod alarm

Guidelines 2.1-1

Description

On January 18, 1999, Florida Power Corporation's (FPC) Crystal River Unit 3 (CR-3) was in MODE 1 (Power Operation) at 99.9 percent Rated Thermal Power (RTP). FPC personnel discovered that a Surveillance Requirement (SR) had not been performed within the time specified in Improved Technical Specifications (ITS) when a regulating control rod computer alarm became inoperable without operator knowledge. ITS SR 3.2.1.2 requires verification that the regulating rod group position meet the insertion limits specified in the Core Operating Limit Report (COLR) once every 12 hours when the regulating rod insertion limit alarm is operable and once every 4 hours when the regulating rod insertion limit alarm is inoperable. FPC determined that the rod insertion limit alarm on the plant computer was bypassed for power below 15% RTP. Plant procedures did not reflect that the rod insertion limit alarm is inoperable below 15% RTP and did not require the increased surveillance frequency of once per 4 hours.

Currently, a Plant Integrated Computer System (PICS) is being installed to replace the ModComp. During testing of alarm software for the PICS, it was determined that the rod index alarm, quadrant power tilt alarm, and axial power imbalance alarm were bypassed below 15% RTP. This was discovered due to the more extensive testing of alarm software for the PICS than had been performed on the ModComp. [It was subsequently found that] this same bypass existed in the operating ModComp software.

Discussion

Disabling the alarm below 15% RTP (without putting alternative surveillance methods into effects) violated the Technical Specification. This condition would have been avoided by conforming to Guideline 2.1-1, "Software requirements should address all system functions allocated to the software…necessary to fulfill the system's safety intent."

0038 Incomplete Surveillance Software

Date 3/12/98

Source LER 315 1998 015

Domain Nuclear power

Function Ice bucket surveillance

Guidelines 2.6-3

Description

On March 12, 1998, with Unit 1 and Unit 2 in Mode 5, plant personnel identified that the Ice Condenser Technical Specification required ice basket weights were not being adequately maintained. The Ice Condenser absorbs thermal energy released during a coolant leak inside Containment to limit the peak pressure and consists of 1944 ice baskets each filled with a required minimum of 1333 pounds of borated ice. The inability to maintain the required amount of ice in each ice basket, if it had been found during operation, may have resulted in the plant being in an unanalyzed condition, and, in accordance with 10CFR50.72(a)(2)(i), an ENS notification was made at 1930 hours EST that day.

ICEPICK, a computer software random number generator, is utilized to pick the initial 144 ice basket sample. The minimum 144 ice basket sample is required to be expanded for 20 additional ice baskets for each ice basket determined to be below the T/S average weight. The expanded sample is performed in the same bay as the discrepant basket and is considered to be representative of the ice baskets. The 20 baskets, however, are selected by the lead test engineer, as ICEPICK has no capability to perform the sample expansion of 20 additional ice baskets. [The selection by the lead engineer is based on accessibility, thus not random selection.]

The cause of this condition was determined to be work practices in that computer code programmers failed to adequately incorporate Technical Specification requirements in the software code used to identify for refilling those ice baskets with a weight significantly below the Technical Specification requirement. The software used to support the Ice Condenser surveillance program will either be revised or replaced.

Discussion

Surveillance procedure software is part of the offline monitoring functions. Guideline 2.6-3 for these functions states in part, “Requirements should specify for each of the system surveillance and monitoring operations the actions to be taken for each anomaly detected by the system monitoring function.” A basket below T/S average weight is an anomaly that is to be expected, and failure to select the additional 20 baskets, therefore, is not in compliance with the guideline.

0039 Monitor Accuracy Error

Date 6/28/2000

Source LER 316 2000 007

Domain Nuclear power

Function Rod deviation alarm

Guidelines 2.2.1-1

Description

With [Cook] Unit 2 at 79.6 percent rated thermal power (RTP), a shutdown was initiated due to failure to meet Limiting Conditions of Operation (LCO). Two Individual Rod Position Indicators (IRPIs) deviated from the group step counter by more than the 18-step allowed deviation. During the event the Rod Position Deviation Monitor (RPDM) failed to annunciate when the 18-step limit had been reached. The cause for this was that the plant computer software (installed in the early 1990s) contained an error such that the alarm was generated from a "greater than" condition rather than "greater than or equal."

Discussion

The failure of the RPDM to annunciate is due to a frequently encountered problem in distinguishing between "greater than" and "greater than or equal." The corresponding requirement is addressed in Guideline 2.2.1-1, "Accuracy requirements should be stated explicitly."

0040 Deficient Surveillance Test Procedure

Date 9/9/1999

Source LER 334 1999 011

Domain Nuclear power

Function Axial flux difference alarm

Guidelines 2.3.1-4

Description

On September 9, 1999, it was identified that the Operations Surveillance Test 1OST-5A.1, "Delta Flux Alarm Program Operability Check" was inadequate to support the Beaver Valley Power Station (BVPS) Unit 1 Technical Specification (TS) 3/4.2.1. The Axial Flux Difference (AFD) monitor alarm has not previously been sufficiently proven to be operable by a suitable periodic surveillance test and thus, the AFD monitor alarm had been inoperable. The periodic AFD monitor alarm test procedure did not fully test all possible combinations of potential operating conditions. The failure to perform the required more frequent AFD monitoring when the AFD monitor alarm was inoperable constitutes noncompliance with the TS.

The apparent cause of the event was that the subject Operations Surveillance Test procedures, 1OST-SA.1 and 2OST-5A.1 (previously), lacked the information necessary to successfully perform the task from its initial development. Verification that two channels being out of the target band would cause the Axial Flux Difference monitor to alarm were not included in the surveillance procedure.

Discussion

The problem could have been avoided by application of Guideline 2.3.1-4, "Functional completeness of software requirements." The guideline states in part, "All functions allocated to software from the system requirements document should be documented in the software requirements."

0041 Software Maintenance Problem

Date 7/31/00

Source LER 336 2000 013

Domain Nuclear Power

Function Core Monitoring Program

Guidelines 2.5.3-3 2.6-4

Description

With the plant in Mode 1 at 100% power, it was determined that the in-core monitoring computer software program (INPAX) had not run the required calculation for azimuthal power tilt for a period exceeding 12 hours. The surveillance requirement to calculate the tilt at least once per 12 hours was not met and this constituted a condition prohibited by the plant's Technical Specification.

The core monitoring program runs in two modes: full and mini. The latter executes only INPAX, while the full mode includes other functions as well. The mini mode executes automatically every 8 hours. The full mode (which has priority over the mini mode) executes when there is a power change of more than 2.5%. During a down-power test, the full mode was invoked but did not run to completion due to a software error introduced by a recent change. This blocked execution of the mini mode.

Discussion

A program that executed only partially (due to a software error, see below) was allowed to block the execution of a required program and there were no alarms to announce this condition. Guideline 2.5.3-3 states in part, "Requirements should specify which functions can be cancelled prior to completion…and how the operator will be notified."

The initiating condition was improper execution of a software change and lack of a complete test. This could have been avoided by adherence to Guideline 2.6-4, "Requirements to Allow Technician Maintenance."

0042 Missed Surveillance Test

Date 6/29/98

Source LER 353 1998 005

Domain Nuclear power

Function Scheduling software

Guidelines 2.3.1-4

Description

On 06/29/98, the Surveillance Test (ST) coordinator discovered that procedure ST-6-107-887-2, which has a weekly frequency, had exceeded its Technical Specifications (TS) surveillance period with the applicable TS action not being met. Operations personnel were notified and the ST procedure was satisfactorily completed on 06/29/98.

A weakness exists in the use of the ST scheduling software program (i.e., Primavera, P3). The program is utilized differently for STs having weekly frequencies. Specifically, the automatic updating interface process between the Plant Information Management System (PIMS) and Primavera is bypassed to accommodate the shorter window for processing and rescheduling of weekly STs. This results in weekly STs demanding a higher degree of human intervention than STs with frequencies greater than 7 days, which are scheduled automatically by PIMS.

Discussion

The problem could have been avoided by application of Guideline 2.3.1-4, “Functional Completeness of Software Requirements.” The guideline states in part, “All functions allocated to software from the system requirements document should be documented in the software requirements.”

0043 Date Uncertainty

Date 5/3/2000

Source LER 362 2000 002

Domain Nuclear power

Function Leakage rate determination

Guidelines 2.5.3-3

Description

The NRC resident inspector questioned the data used for calculating the Reactor Coolant System leakage for Unit 3. Southern California Edison (SCE) determined that the data were, in fact, incorrect.

The cause of the data error was a latent Y2K-related problem in the way the computer program handled year 2000 dates. If the data collection date and the calculation date are the same, the program considers the dates consistent and performs the leakage rate calculation. If the collection date and the calculation date are different (as was the case here) the program replaces the input data with data taken at the time of the calculation. As a result, all volume differences were incorrectly stated as zero.

Discussion

Aside from the apparently faulty date algorithm, the program occurred because of insufficient validity checks on the data. Guideline 2.5.3-2 states in part, “The requirements should specify that all incoming values are checked and that a response is provided for each out-of-range condition.” That all computed volume differences were zero should have been considered an out-of-range condition.

0044 Rod Position Calculation

Date 5/20/98

Source LER 368 1998 003

Domain Nuclear power

Function Control element assembly position

Guidelines 2.3.1-4

Description

ANO-2 determined that the surveillance of Control Element Assembly (CEA) position was not being performed for one CEA group as required by Technical Specifications. A software change was implemented in 1989 to create a report from the plant computer that calculated CEA position deviations to satisfy the requirement to verify each 12 hours that each CEA is within seven inches of all other CEAs in its group. Errors in developing and implementing that change resulted in Group "P" deviations being determined for each of the two sub-groups but not for the entire group. In the root cause evaluation, it was noted that inconsistencies in documentation at the time this condition originated may have caused some individuals to conclude that each of the Group "P" sub-groups constituted a separate group of CEAs and thereby have contributed to either the error or failure to detect the software change error.

Discussion

The problem could have been avoided by application of Guideline 2.3.1-4, "Functional Completeness of Software Requirements." The guideline states in part, "All functions allocated to software from the system requirements document should be documented in the software requirements."

0045 Reactor Power Calculation

Date 12/16/99

Source LER 440 1999 007

Domain Nuclear Power

Function Feedwater temperature compensation

Guidelines 2.3.3-2 2.6-4

Description

Personnel at the Perry Nuclear Power Plant discovered an error in the calculation of reactor thermal power. A database that provides numeric input to thermal power calculations had been modified by setting specific inputs to zero. This effectively removed the feedwater temperature compensation function from the Integrated Computer System, producing non-conservative values for reactor power.

The cause of the event was identified as program and process weakness in the development of software change. Insufficient administrative controls existed for the review of the software revision. This allowed the software change to be implemented without review of potential impact on plant systems. In addition, the program design description was insufficiently detailed.

Discussion

The licensee's description puts major emphasis on change control, and that aspect is covered by Guideline 2.6-4, "Requirements to Allow Technician Maintenance." In addition, the functionality aspects of the requirements appear to have been deficient with respect to Guideline 2.3.3-2, which states in part: "In the course of reviewing software requirements, it should be demonstrated that data from all sensors needed for monitoring and control of safety functions are identified and the number and location of sensed parameters is adequate."

4.References

Copeland, L. “Software glitch forces 11-minute shutdown of NASDAQ,” *Computerworld*, http://www.infoworld.com/articles/hn/xml/00/12/01/001201hnnasdaq.xml?p=br&s=7?1207thpm

FAA, Federal Aviation Traffic Management Center, Daily Morning Briefing Summaries Database, 2000.

Neumann, Peter, “Risks to the Public,” *ACM Software Engineering Notes*, Vol. 11, No. 5, P. 6, October 1986.

Neumann, Peter, *Risks to the Public*, Electronic newsletter available at http://www.csl.sri.com/~risko/risks.txt and http://catless.ncl.ac.uk/Risks, 2001.