SYSTEM ENGINEERING
AND
SOFTWARE EXCEPTION HANDLING

Herb Hecht
SoHaR Incorporated
Culver City, California
WHY WE ARE HERE

1. Many failures in critical systems are due to missing or faulty exception handling and we want to change that.
2. They were not tested under the exception conditions.
3. The requirements were not specific about exceptions that had to be tolerated.
4. Comprehensive specification of exceptions that have to be tolerated is difficult – or is it impossible?
“The main line software code usually does its job. Breakdowns typically occur when the software exception code does not properly handle abnormal input or environmental conditions – or when an interface does not respond in the anticipated or desired manner.”

SOME SPECTACULARS

- THERAC-25 FATAL RADIATION OVERDOSES
  - DID NOT SUPPRESS OPERATOR INPUT WHILE MAGNETS WERE REPOSITIONED

- ARIANE 5 CRASHED AFTER LAUNCH
  - DISABLED LANGUAGE PROVIDED EXC. HANDL.
  - PERMITTED SHUT-DOWN OF BOTH NAV SYST.

- MARS POLAR LANDER HARD LANDED
  - FAILURE TO DE-BOUNCE CONTACTS
IMPORTANCE OF EXCEPTION HANDLING - 2

“The main line software code usually does its job. Breakdowns typically occur when the software exception code does not properly handle abnormal input or environmental conditions – or when an interface does not respond in the anticipated or desired manner.”


“Therefore the identification and handling of the exceptional situations that might occur is often just as (un)reliable as human intuition.”

WHY THESE FAILURES?

THE PROGRAMS WERE NOT TESTED UNDER THE CONDITIONS THAT CAUSED THE FAILURES

THERE WERE NO REQUIREMENTS FOR TESTING UNDER THESE CONDITIONS

GENERATING REQUIREMENTS FOR EXCEPTION HANDLING IS DIFFICULT
WHY THE DIFFICULTY?

- Exception conditions arise from several levels.
- Exception conditions are more difficult to understand than main line requirements.
- Exceptions occur infrequently but require disproportionate effort.
SOURCES OF EXCEPTIONS

OPERATIONAL REQUIREMENTS
  LOSS OF POWER, COMMUNICATION, THERMAL CONTROL

IMPLEMENTATION DETAIL
  CALIBRATION ANOMALIES, ACTUATOR STATES, OPERATOR INPUT

COMPUTING ENVIRONMENT
  HARDWARE FAILURES, MEMORY ERRORS, EXECUTIVE, MIDDLEWARE

MONITORING AND SELF-TEST
  OVER-TEMPERATURE SENSORS, SYSTEM PERFORMANCE TEST

APPLICATION SOFTWARE
  ASSERTIONS, VIOLATION OF TIMING CONSTRAINTS, MODE CHANGES
WHO IS RESPONSIBLE?

OPERATIONAL REQUIREMENTS
IMPLEMENTATION DETAILS
COMPUTING ENVIRONMENT
MONITORING AND SELF-TEST
APPLICATION SOFTWARE

SYSTEM ENGINEERING
VEHICLE HEALTH MGM’T
SOFTWARE ENGINEERING
SOFTWARE SPECIALIST
SOFTWARE EQUIPMENT
REQUIREMENT GENERATION

OBJECTIVE
- EXCEPTION CONDITION AND ACTION

ALGORITHM
- QUANTITATIVE CONDITION DESCRIPTION
- TIMING AND RESPONSIBILITY FOR ACTION

ASSIGNMENT
- SPECIFY SOFTWARE IMPLEMENTATION OF ALGORITHM
BUILDING BLOCKS

- EXISTING PRACTICES
- EXPERIENCE
- TOOLS
- INTEREST GROUP
- WORKING GROUP
- RECOMMENDED PRACTICE
CONTACT

herb@sohar.com
Herb Hecht
310/338-0990 X110