INTEGRATED SOFTWARE HEALTH MANAGEMENT FOR AIRCRAFT GN&C
Johann Schumann, Ole Mengshoel

Software Can Fail
Despite careful SW development and V&V, safety-critical SW can fail.

F-22 Raptors crossing the date-line: SW bug caused loss of navigation and communication

Harrier Autolander: buggy radar-altimeter integration caused near-crash during landing (NASA)

SPIRIT: overfull on-board file system caused reboot-loop after landing

Ariane-V: SW reused from Ariane IV caused overflow and destruction of rocket

A Bayesian ISWHM
We are using Bayesian networks (BN) to construct a model of the software and its behavior in nominal and failure cases. BNs can be used to:
• detect failure(s), and to
• perform detailed reasoning on the root cause of the problem

Example: low oil pressure and vibration indicates a likely problem with a bearing.

Results for Example Scenario
Writes to almost full on-board file system can cause delays in the control loop (if “badly” implemented), which can result in aircraft oscillations similar to dangerous PIO (pilot induced osc.). ISWHM can detect situation →.

Software Health Management monitors the system and software during operation to:
• reliably detect faults
• diagnose most likely root cause(s) while minimizing the number of false alarms and missed adverse events

References