ISWHM: Tools and Techniques for Software and System Health Management

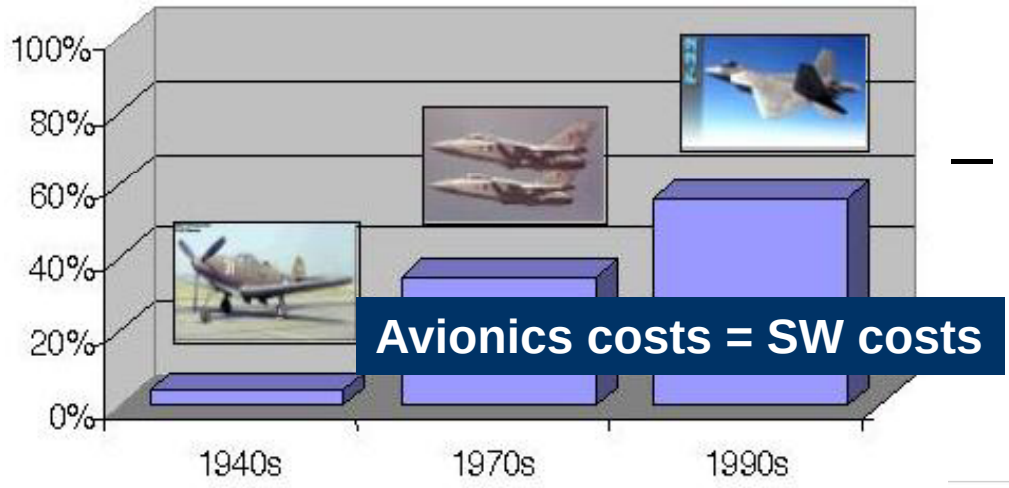
Johann Schumann, RIACS/USRA

NASA Ames

2/11/2009

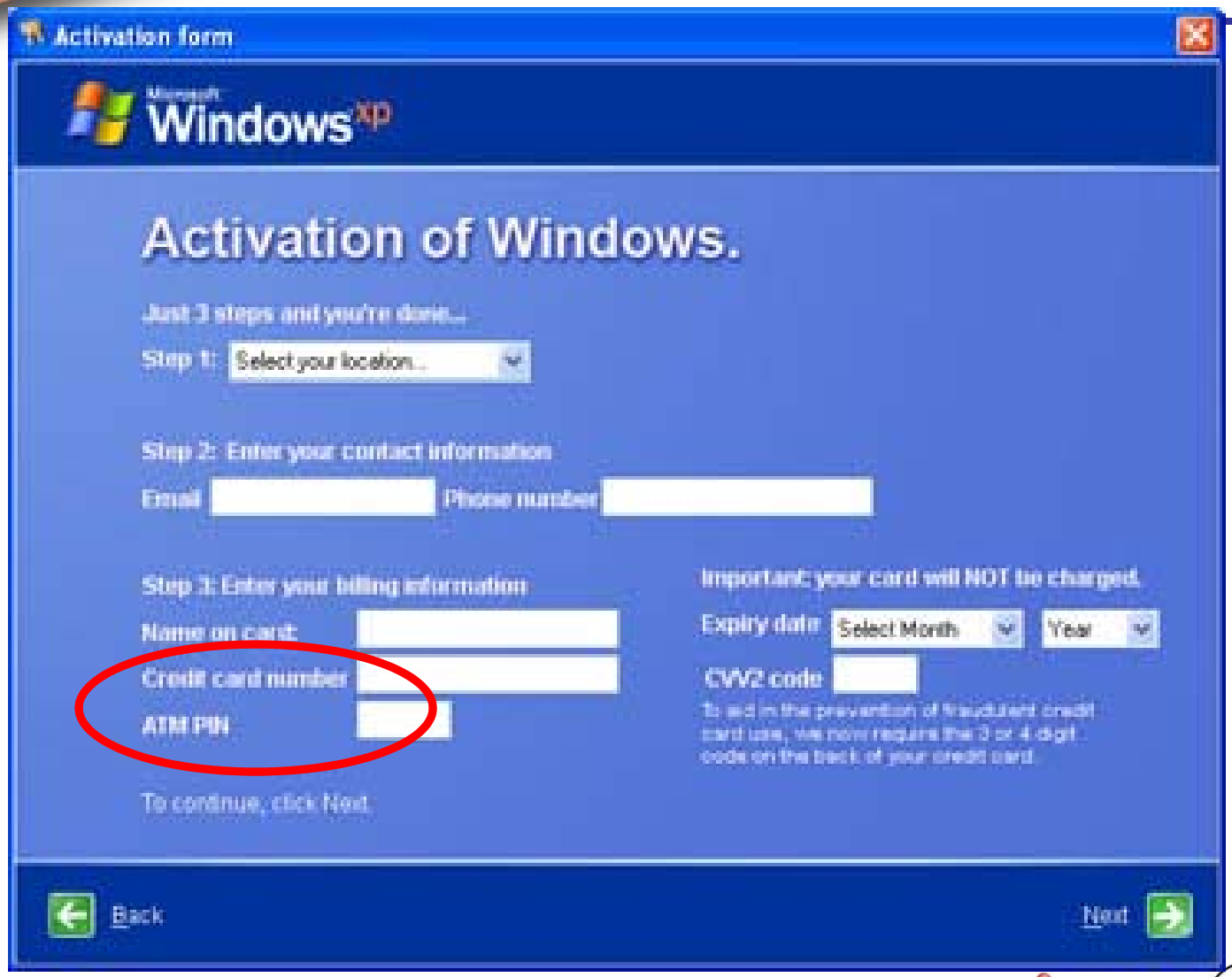
Joint work with O. Mengshoel, ARC/CMU and A. Darwiche, UCLA

IVHM in Aircraft



- Modern aircraft
  - Have IVHM for major electrical/mechanical subsystems
    - Important for safety, reliability, environmental impact, economical considerations
  - Rely heavily on SW
    - no Software health mgmt
    - but many software problems

State-of-the-art



Health Management

- The top-level functionality of HMS includes
  - detection: something is wrong
  - diagnosis: identify potential causes of the anomaly
  - prognosis: provide estimated time until total failure
  - mitigation: provide solution to fix/work-around the anomaly

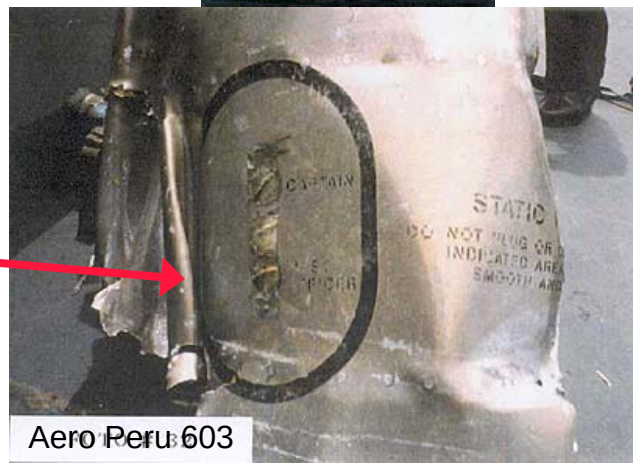
K.I.S.S.: Attach SW to IVHM

is not that easy...

- Software problems don't develop over time
  - they come in during all phase of SW life cycle
  - they "don't go away"
- SW failures mostly occur instantly–HW often fails gradually (e.g., an oil leak)
- SW problems occur due to problematic interoperation with HW
- SW IVHM is a piece of software itself

HW-SW Interaction

- HW (e.g., sensors) can behave differently than expected (and causes a SW failure)
  - on purpose: use same SW for different HW
    - Ariane V failure
  - accidentially during development
    - DART: new GPS system just before launch
    - wrong orientation of gyro-box in aircraft
  - HW failure
    - broken cable
    - disabled sensor (e.g., covered static pressure port)
  - gradual degradation
    - increase of sensor noise
  - unexpected environmental sensor readings



Aero Peru 603

SW IVHM is SW

Quis custodiet ipsos custodes?

Juvenal

- The IVHM system that monitors the SW system must be at least reliable as the SW under scrutiny
  - false alarms are not an option (repeated alarms tend to be ignored - nuisance alarms)
  - un-detected failures are a safety hazard
- Rigorous V&V of IVHM system necessary, state-of-art testing not sufficient

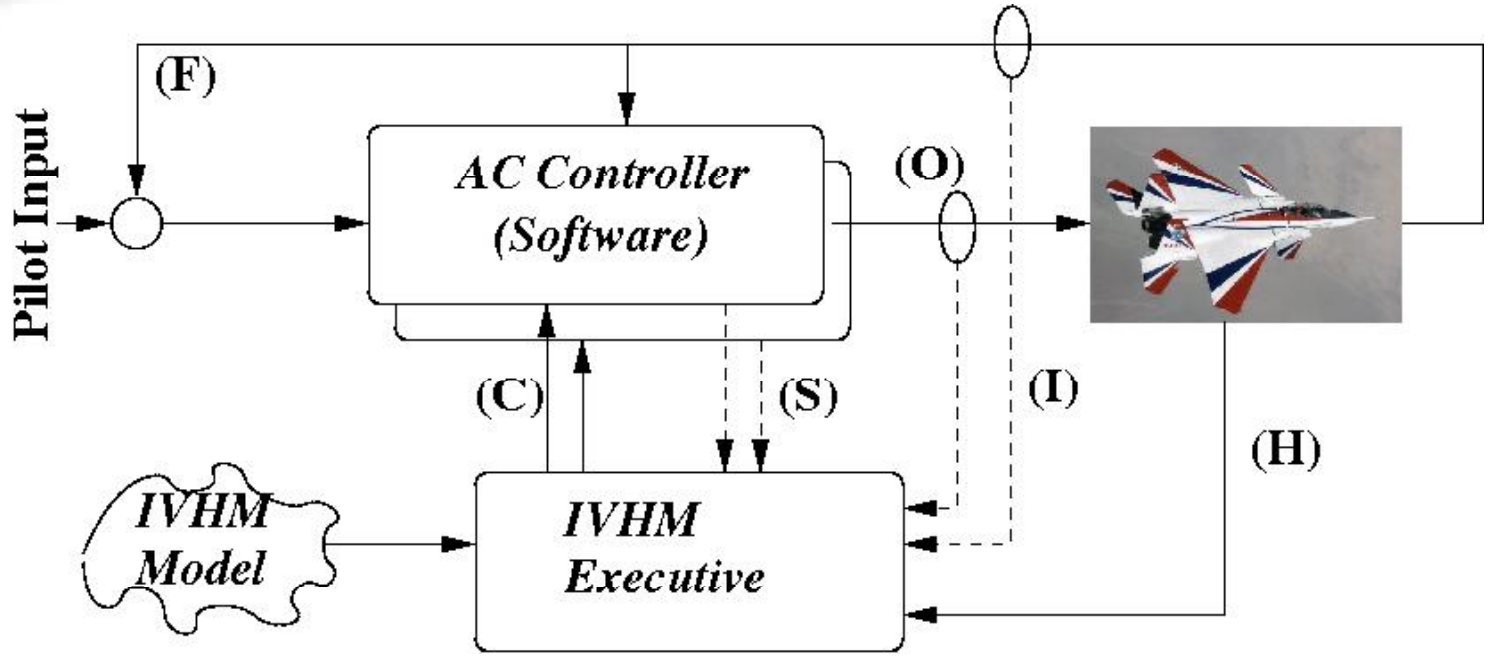
IVHM V&V

1) IVHM model analysis: completeness & consistency of model
   - model-based testcase generation, parametric testing & analysis
2) V&V of IVHM engine and algorithm
   - correctness of translation (“compiler-style”)
3) IVHM engine code V&V
   - Model Checking, WCET, code-based test-case generation, static analysis
4) Support for construction of safety cases
   - putting the pieces together

ISWHM Architecture

- integrated IVHM model of SW and interacting HW (sensors)
  - e.g., statistical Bayesian IVHM model
- instrumentation of SW and sensors
  - What can be instrumented?
  - Instrumentation with assertion properties for discrete components (e.g., state machines)
  - How can we instrument hybrid (discrete mode logic and continuous code (control))?
- powerful/efficient IVHM engine
  - e.g., Bayes nets translated arithmetic circuits (Darwiche, UCLA)

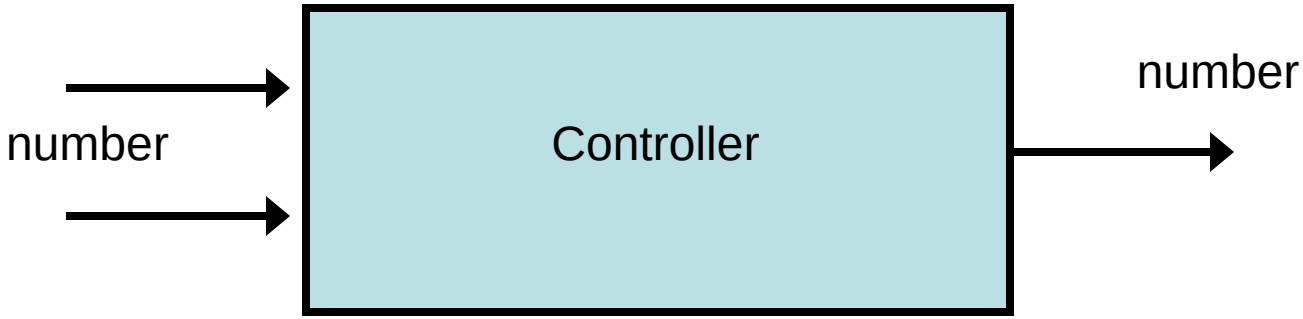
ISWHM for GN&C



- Probabilistic quality metric and runtime-verification for (hybrid) controller
- Advanced (Bayesian) IVHM system

Health Metric

- Traditionally, an algorithm (e.g., control system) takes numerical data and produces numerical data.

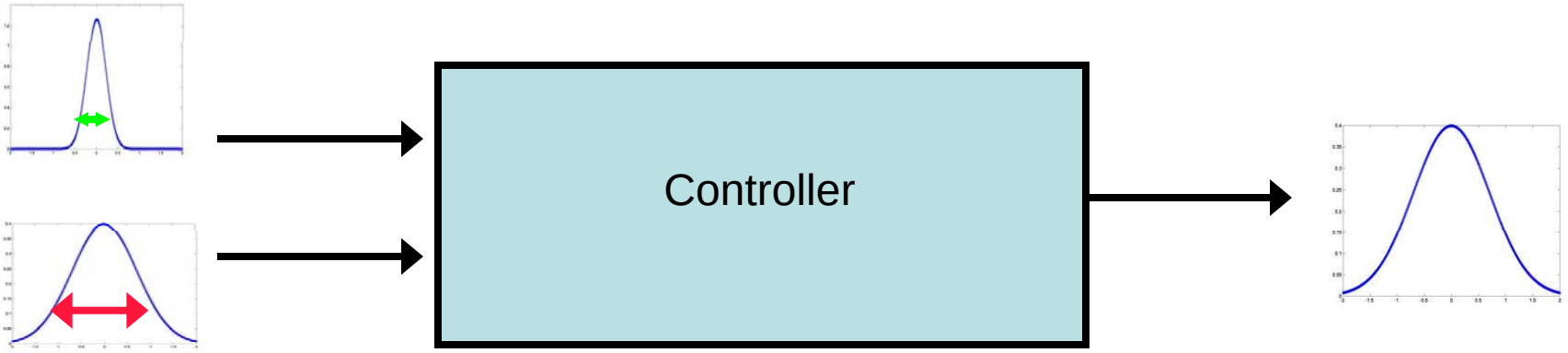


The output produced can contain go/nogo information (e.g., error code) but does *not* contain any notion of

- quality of input data (e.g, are the sensor data OK or noisy?)
- quality of calculation (big round-off errors?)
- quality of internal parameters (are we at the stability limit of the controller)?

Health Metric

- An algorithm with built-in health metric takes probability variables as inputs and outputs.
- Shape and width of the Probability density function comprises the health metric
- In many cases, the PDF can be easily calculated in addition to the output value using Bayes



Narrow Gauss curves = good quality/health
Wide gauss curves = bad quality/health

Why Bayesian?

- Bayesian statistical theory provides a solid formal basis for calculations with probability distributions

Well-known *Kalman filters* use a Bayesian approach. Our technology is based on similar concepts and will be developed toward selected algorithms in the area of GN&C.

• Traditionally, Kalman filters provide quality of estimates, based upon quality of the input signals. In most cases, this metric is used to “reset” the filter, if the quality gets too poor, but the current quality of the estimates is rarely used for other purposes. Other issues, like numerical stability and round-off errors have been analyzed, but are not handled explicitly by the algorithms

• Our Confidence Tool, developed within the IFCS project dynamically calculates the quality of the neural network using a Bayesian statistical approach. As the NN is trained during the flight, the Confidence tool output can be used to early detect poor performance and detect diverging NN learning.

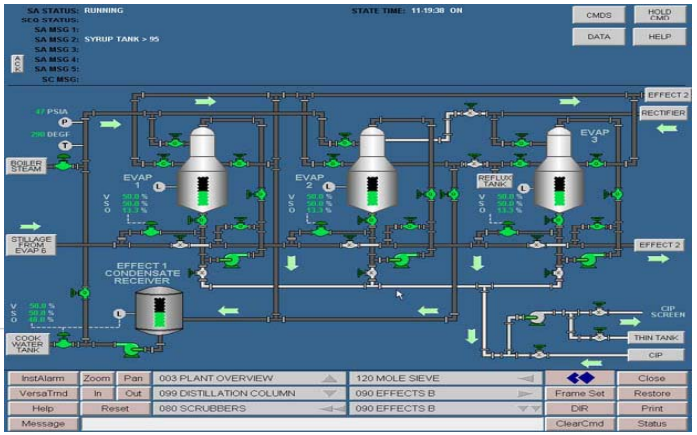
So What? 1

- ISWHM is not just error handling, dynamic bug-finding, self-healing code, or patch upload
- existing techniques (only) fulfill part of the SWHM requirements (DETCT/ID/PROG/MIT)
- existing SW techniques
  - focus on SW aspects only (not SW-HW interaction)
  - no explicit/external model
  - no prognostics (“Your Vista system will have to reboot in 5 minutes...”)

So What? 2

- NRA project will demonstrate ISWHM on GN&C
  - ARC (USRA, CMU), UCLA, 3years, started 10/2008
- Is SWHM useful for LARGE and complex systems?
  - HM models on various level of abstraction for various levels of granularity
  - powerful IVHM engines to handle large sets of sensors
  - seamless spectrum between low-level discrete health information (e.g., mode=45) and statistically defined health metrics for a larger system (e.g., network load, trends in memory usage, etc.).
  - better integration with human intervention system

Why such a display not for a big SW system?



Conclusions

I. *Software Health Management integrated seamlessly into IVHM*

II. *Statistical Quality Metric for continuous components combined with Runtime Verification/Monitoring of discrete SW*

III. *IVHM reasoner/executive verification*

IV. *ISWHM provides additional arguments for Dependability and Safety Cases and can be used for in-situ V&V*

V. *ISWHM should not replace V&V*

Project Team

- NASA Aeronautics NRA,
- start 10/2008 (3 years)

- RIACS/USRA (RSE group NASA ARC)
  - Johann Schumann, PI
  - NN, summer student
- UCLA
  - Prof. Adnan Darwiche
  - Knot Pipatsrisawat, graduate student
- CMU (IVHM group NASA ARC)
  - Ole J. Mengshoel
- Collaboration with
  - Corina Pasareanu, CMU (NASA ARC)
  - NASA IVHM and RSE groups