Imperial College London

Failure Modes and Effects Analysis of GNSS Aviation Applications

Carl Milner and W Y Ochieng
Centre for Transport (CTS)
Department of Civil and Environmental Engineering
carl.milner05@imperial.ac.uk

Imperial College London

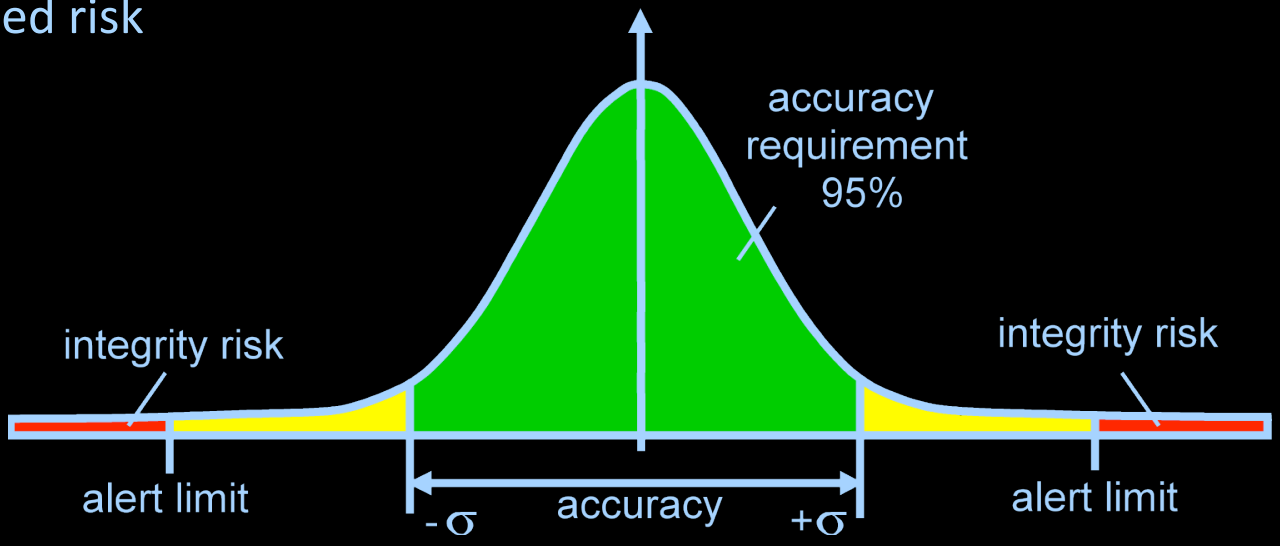
Outline

- Definition and relevance of integrity
  - Challenges
- FMEA Methodology and Structure
- Failure Characterisation
  - Conventional
  - Proposed concept
    - Step
    - Ramp
- Failure Impact on Integrity Risk
  - Weighted-RAIM Integration
  - Numerical Errors
  - VPL Results
  - Bias-RAIM
- Conclusions

carl.milner05@imperial.ac.uk

Definition and Relevance of Failure

- Integrity relates to *safety* criticality → failure alerting function with a prescribed risk



- The system is required to deliver a warning (*alert*) when the user position error exceeds an allowable level (*alert limit*)
- A warning must be issued within a given period of time (*time-to-alert*) and with a given probability (*integrity risk*)

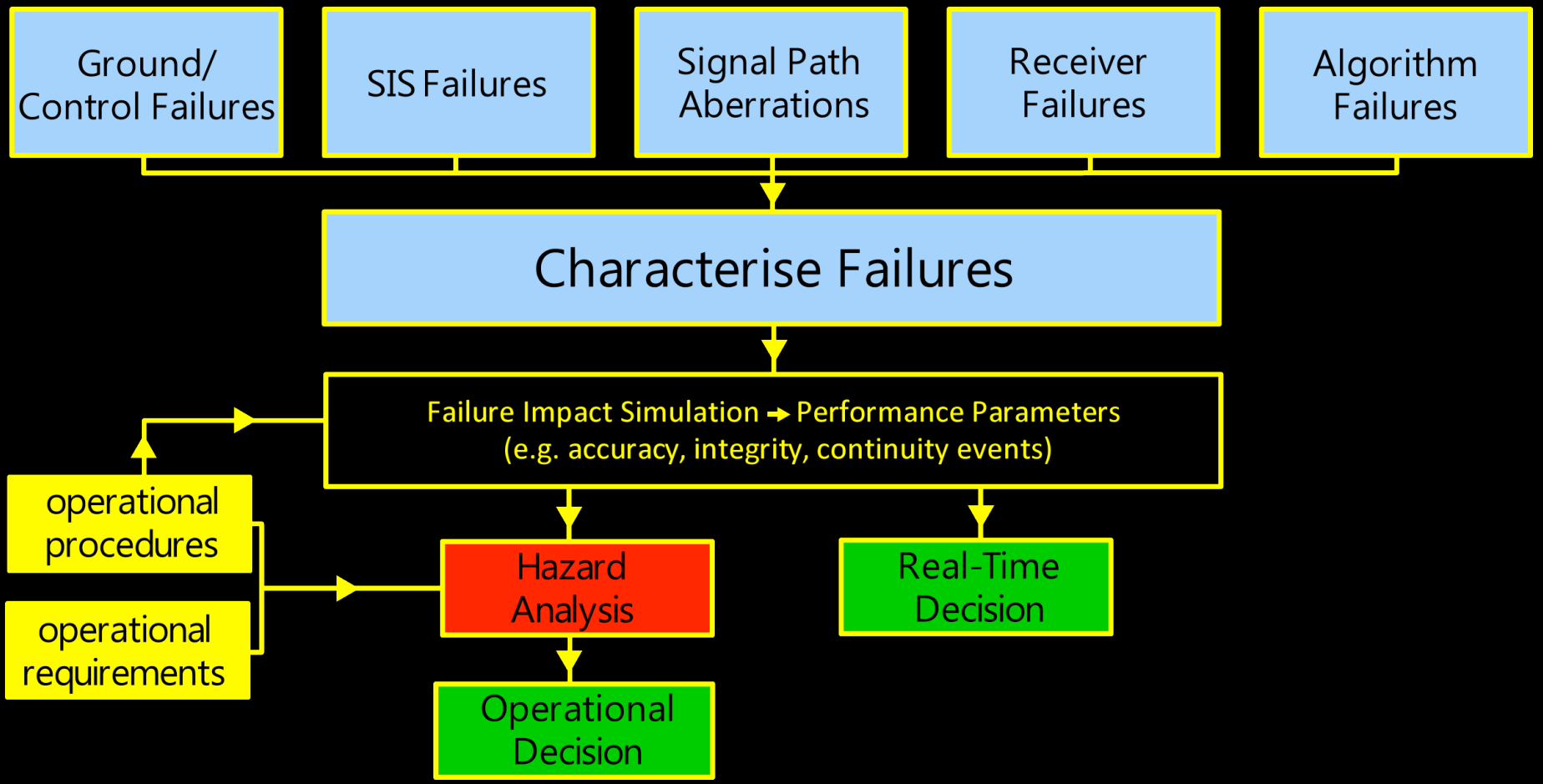
carl.milner05@imperial.ac.uk

Challenges of Integrity

- Integrity risk is the product of the *probability of failure* and *missed alert*
- Integrity monitoring is essential to meet the requirements (RAIM - Receiver Autonomous Integrity Monitoring)
- The application of failure probabilities may not always provide a strong link between reality and algorithm design / performance requirements
- The computation of missed alert probabilities may also incorporate conservative modelling assumptions
- Solution: a state-of-the-art Failure Modes and Effects Analysis (FMEA)

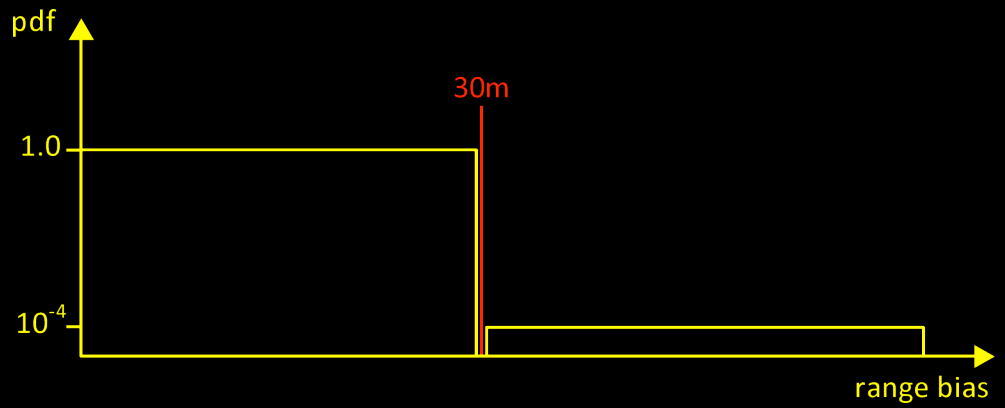
carl.milner05@imperial.ac.uk

FMEA Methodology and Structure



carl.milner05@imperial.ac.uk

Failure Characterisation : Conventional (stand-alone)



- Binary function (GPS SPS Performance Standard)
  - No information for failures < 30m
  - Ambiguity in size of bias beyond 30m

- Defined per time period (per year → per hour)
  - Performance requirements derivation
  - Failure rate factored to operation time period (per hour)
    e.g. Integrity Risk 10^{-7} = 10^{-4}(failure rate) × 10^{-3}(missed alert)
  - Algorithms apply quantities on an epoch-by-epoch basis

carl.milner05@imperial.ac.uk

Imperial College London

Failure Characterisation :SBAS

- WAAS Integrity Threat Model
  - Greater detail for ramp errors
  - Step errors defined from 3.6m yet definition is still vague

- One step towards a more detailed model is taken

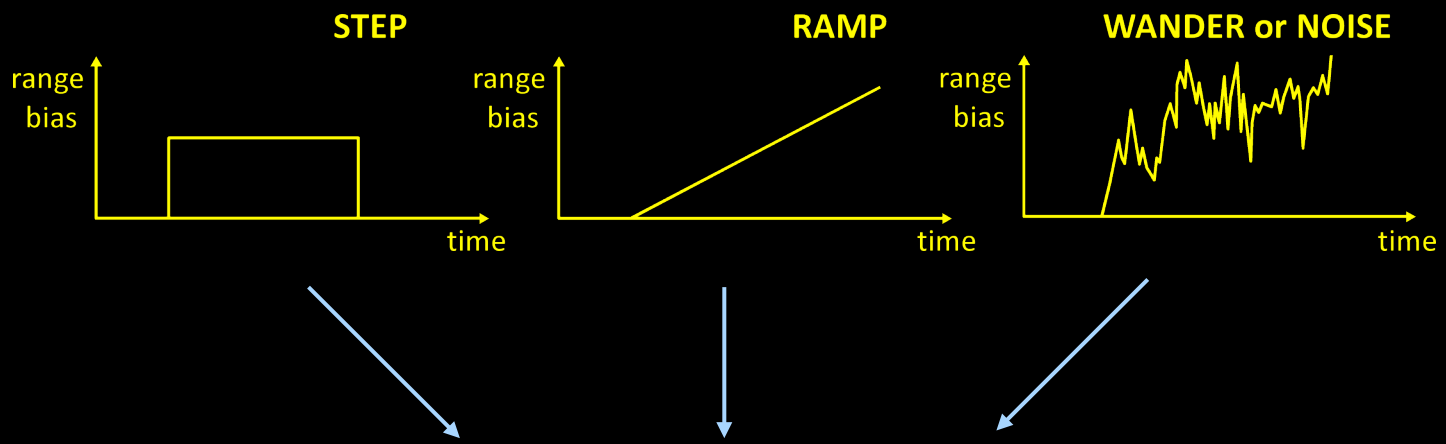
- Failures are not defined in an instantaneous manner nor utilise exposure time

- Proof that a drive towards a more sophisticated model can be achieved in a certified application

Error	Magnitude	Probability
STEP	**>3.6m**	**10^{-4} /h**
RAMP	0.001m/s to 0.05m/s	10^{-6} /h
RAMP	0.05m/s to 0.25m/s	10^{-6} /h
RAMP	0.25m/s to 0.75m/s	10^{-6} /h
RAMP	0.75m/s to 2.5m/s	3.5×10^{-6} /h
RAMP	2.5m/s to 5m/s	4.1×10^{-6} /h
RAMP	**0.001m/s +**	**10^{-4} /h**

carl.milner05@imperial.ac.uk

Failure Characterisation : Proposed Concept



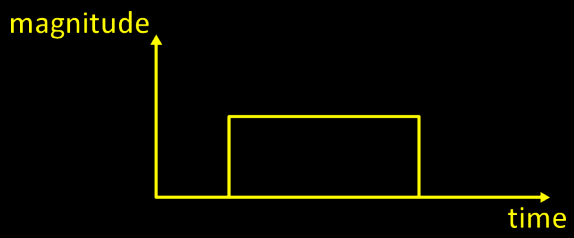
$$probability = f(bias, t_{now})$$

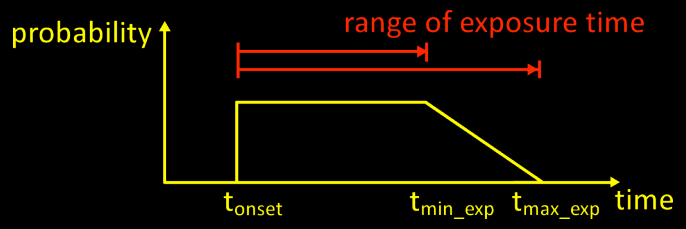
- Failure model is a detailed function of bias
- Failure model is defined on an instantaneous epoch-by-epoch basis

carl.milner05@imperial.ac.uk

Imperial College London

Failure Characterisation: Proposed Concept Step:





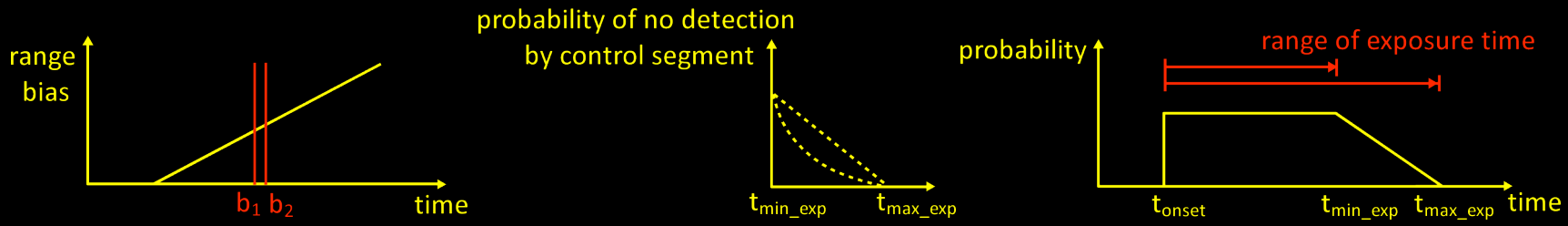
- Magnitude remains constant over time
- Step errors over a range are processed identically
- Area under the graph is normalised:

$$p(\text{failure mode}, t_{now}) = p(\text{failure mode, time period}) \times \frac{\text{area under graph}}{t_{max\_exp} - t_{onset}}$$

carl.milner05@imperial.ac.uk

Imperial College London

Failure Characterisation: Proposed Concept Ramp



- Must consider the time the failure mode lies between b_1 and b_2
- Use a linear bound on the no detection probability after t_{min_exp}
- Reasonable to assume remaining failure probability decreases exponentially

carl.milner05@imperial.ac.uk

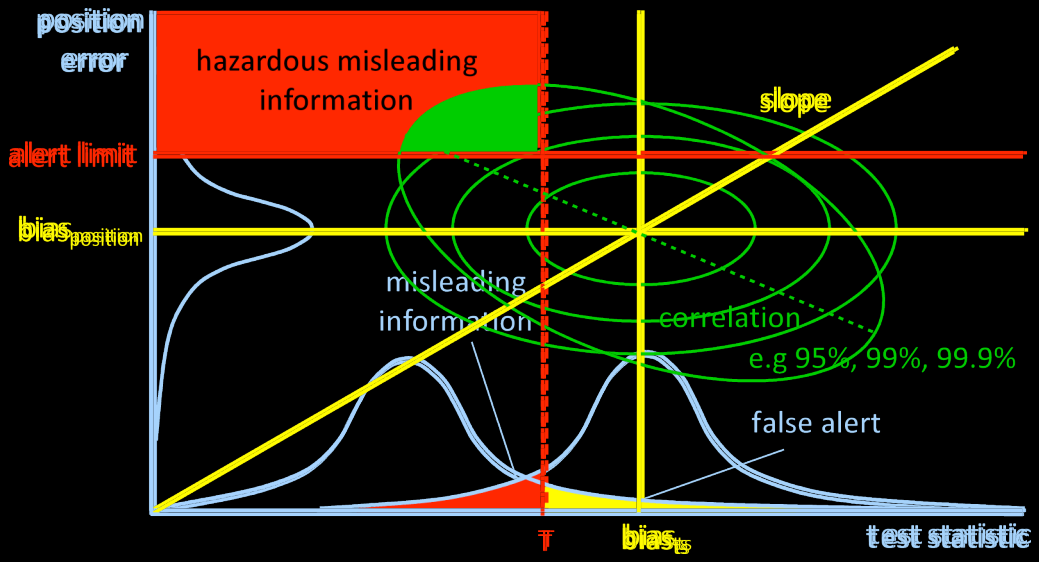
Failure Characterisation : Conclusions

- P(30<B) = 9.6e-06 / sample (New)
- P(30<B) = 1.25e-5 / hour (Trad.)

- Includes empirical orbit modelling failure mode
- Natural model for a sample based assessment of integrity risk
- Number of independent samples per hour
- Important consideration for Galileo – openness of information

carl.milner05@imperial.ac.uk

Failure Impact on Integrity: Weighted RAIM



- Weighting will [illegible] of the test statistic and position error
- Approximate by 2D Gaussian – Use Schur Matrix to define conditional pdf

carl.milner05@imperial.ac.uk

Failure Impact on Integrity : Numerical Errors

- 2D Gaussian Approximation
- Numerical Errors must be accounted
  - Gaussian approximation of test statistic domain from non-central chi-square distribution
  - Analytic approximations to Gaussian curves
  - Numerical Integration Errors
    - Integration procedure truncation error (E)
    - Functional round off error

$$\int_a^b f(x)dx = \sum_{i=1}^{n} w_i f(x_i) + E$$

- Included either at the point of computation or as global errors
- Integration procedure therefore both *conservative* and *worst-case*

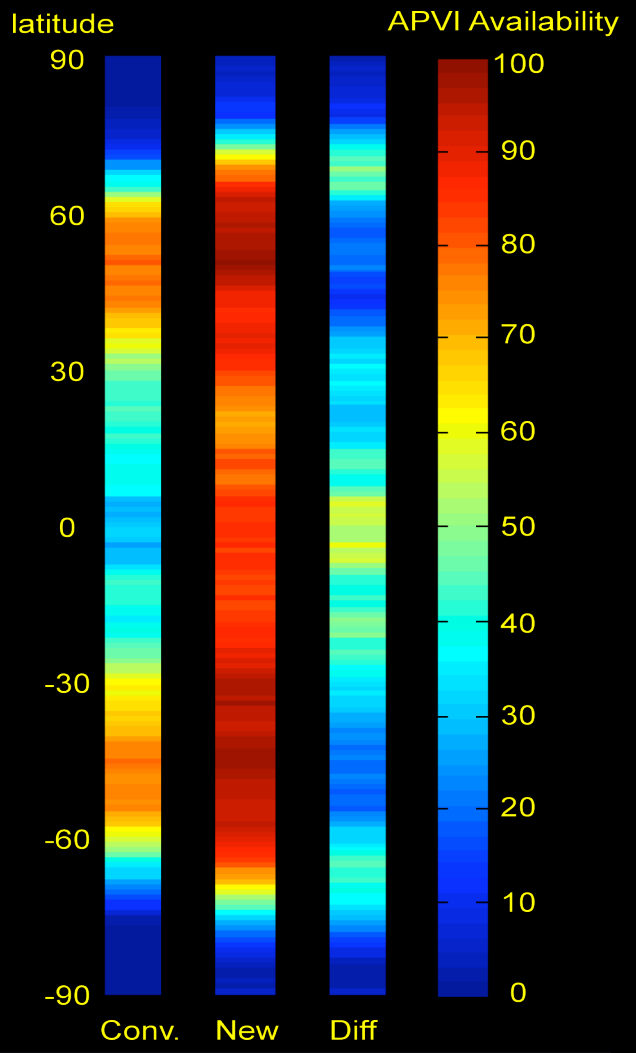
carl.milner05@imperial.ac.uk

Imperial College London

Failure Impact on Integrity :VPL Results

Aerodrome	APVI Availability (%) Conventional	New
Gatwick	73	93
JFK	64	83
Sydney	58	89

- 5 minute samples
- APVI Availability improved by ~30%
- Processing time of < 2 seconds
- Validation procedure:
  - VPLs compared to ideal Monte Carlo



carl.milner05@imperial.ac.uk

Failure Impact on Integrity :Bias - RAIM

Aerodrome	APVI Availability (%)		
	Conventional	New WRAIM	Bias RAIM
Gatwick	73	93	94
JFK	64	83	90
Sydney	58	89	91

- Unsurprisingly lower VPL in most cases due to lack of ambiguity
- Must be integrated over all biases due to the way model is defined
- Leads to problems at low biases < 30m in some cases
- Further tests required

carl.milner05@imperial.ac.uk

Conclusions

- Challenge exists to model integrity risk realistically through
  - capturing accurately failures and their probabilities
  - evaluating the failures' impact on the integrity monitoring functions
- Novel 'Total Failure Model' concept shows there exists a means to link failure modelling to performance requirements and RAIM
- Accelerated integration of weighted-RAIM integrity risk is able to improve APVI availability considerably
- Bias-RAIM is an example of how a more sophisticated failure model may be used
- *Extended Concept:* Assessing the augmented system would require a more sophisticated model of ionospheric error probabilities

carl.milner05@imperial.ac.uk

Imperial College London

Thank you

carl.milner05@imperial.ac.uk

w.ochieng@imperial.ac.uk

www.imperial.ac.uk/cts
www.geomatics.cv.imperial.ac.uk