

Formal Methods in the Development of Highly Assured Software for Unmanned Aircraft Systems

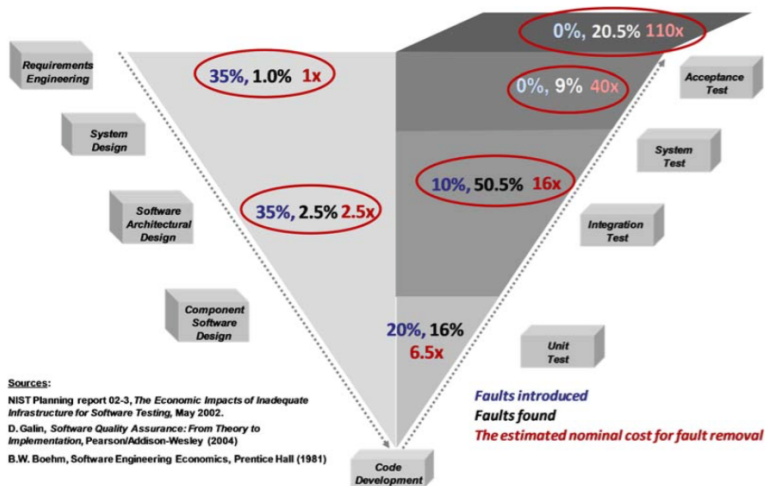
César A. Muñoz¹
cesar.a.munoz@nasa.gov



Sixth International Workshop on Formal Techniques for Safety-Critical Systems
November 16, 2018

¹Formal Methods Team at NASA LaRC and the National Institute of Aerospace.

Error Leakage Rates Across Development Phases²



²Taken from [FGG⁺12].

Notations and Tools Used in DO-178B Projects³

Notation	Sys Req	ICD	HL Sw Req	LL Sw Req	Hw Req
English	39	27	36	32	29
Tables/Diagrams	31	30	30	19	19
Exec. Models	7	1	8	8	1
...					

Tool	Sys Req	ICD	HL Sw Req	LL Sw Req	Hw Req
DOORS	23	13	22	18	12
Word Processor	19	20	18	17	16
Spreadsheet	5	4	5	4	3
...					

³Taken from [Fed09].

Formal Requirements Capture and Analysis

- State of the Art Tools:
 - Analysis of Semantic Specifications and Efficient generation of Requirements-based Tests (ASSERT) [SMD⁺17]; Specification and Analysis of Requirements (SpeAR) [GFH16]; Constrained Language Enhanced Approach to Requirements (CLEAR) [BMH⁺18].
- Benefits:
 - Formal, human-readable, requirement specifications, automated requirement analysis via model-checking and automated theorem proving, automated generation of test cases, etc.
- However:
 - Restricted logics, lack of support for nonlinear arithmetic.

Using Expressive Logics to Specify Requirements

- + Enable the specification and analysis of more complex operational and functional requirements.
- Limited automation. Requires the use of interactive theorem proving.
- Is it feasible?

Using Expressive Logics to Specify Requirements

- + Enable the specification and analysis of more complex operational and functional requirements.
- Limited automation. Requires the use of interactive theorem proving.
- Is it feasible?
- Case studies at NASA LaRC:
 - Detect and Avoid Alerting Logic for Unmanned Systems (DAIDALUS).
 - Polygon Computations for Geofencing (PolyCARP)
 - Independent Configurable Architecture for Reliable Operations of Unmanned Systems (ICAROUS).

Unmanned Aircraft Systems (UAS)

According to the Association for Unmanned Vehicle Systems International (AUVSI) the cumulative impact between 2015 and 2025 to the US economy resulting from the integration of UAS into the NAS will be more than US \$80 billion.⁴

- Agricultural monitoring
- Disaster management
- News coverage
- Environmental monitoring
- Freight transport
- ...



⁴Economic report of AUVSI, March 2013.

UAS are Here

... to stay

THE WALL STREET JOURNAL.

[Home](#) [World](#) [U.S.](#) [Politics](#) [Economy](#) [Business](#) [Tech](#) [Markets](#) [Opinion](#) [Arts](#) [Life](#) [Real Estate](#)



At Glencore, Mining Emperor Tries to Save His Realm



Volkswagen Helps Customers Identify Tainted Cars



Coca-Cola Urges FIFA Soccer Chief Blatter to Step Down



Sbarro Seeks New Life Beyond the Mall



[BUSINESS](#)

FAA: U.S. Airliner Nearly Collided With Drone in March

Incident Appears to be First Case of a Big U.S. Airliner Nearly Colliding With an Airborne Drone

By [JACK NICLAS](#)

Updated May 9, 2014 7:56 p.m. ET

[OFFBEAT](#)

Pilot Says Drone Flew Past Jet Nearing J.F.K.

By [PATRICK MCGEEHAN](#) and [JOSEPH GOLDSTEIN](#) MARCH 5, 2013 12:17 PM [61 Comments](#)

[News](#)

Quadcopter drone flew 'deliberately close' to UK passenger plane

The incident occurred at Southend Airport with the pilot telling air traffic control that it was a "remote control helicopter [with a] very small engine"

[James Vincent](#) | [@jjvincent](#) | Monday 27 October 2014 12:36 GMT | [4 comments](#)

See and Avoid

In the case of manned aircraft (14 CFR Part 91 [FAA09]):

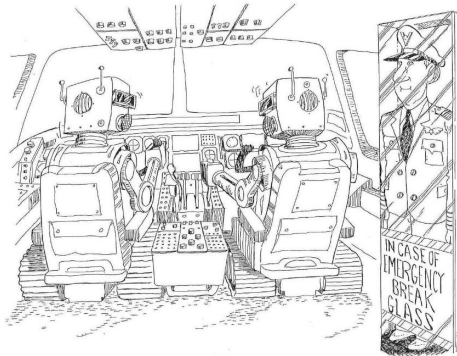
- Pilots may not operate so close to another aircraft as to create a collision hazard.
- Vigilance shall be maintained by pilots so as to see and avoid other aircraft.
- Pilots may not pass over, under, or ahead of another aircraft unless well clear.

Detect and Avoid

- **Detect and Avoid (DAA)** was defined by the FAA as “the combination of UAS Self-Separation (SS) plus Collision Avoidance (CA) as a means of compliance with 14 CFR Part 91”.
- **DAA Requirements:**
 - ① Provide a geometric means to determine well-clear status.
 - ② Interoperate with existing collision avoidance systems.
 - ③ Avoid undue concern for traffic aircraft.
 - ④ Enable self-separation capabilities.

Requirement 1: Geometric Determination of Well Clear

- In the case of of manned aircraft, well-clear status is a subjective determination by the on-board pilot.
- In the case of Unmanned Aircraft System (UAS), determination of well-clear status is made by an on-board system.



FAA DO-365 Definition of Well Clear

- A *loss of well-clear* occurs when:
 - ① Distance at time of closest point of approach is less than HMD and
 - horizontal range is less than DMOD or
 - modified tau is less than TAUMOD; and
 - ② Relative altitude is less than ZTHR or time to co-altitude is less than TCOA,
- where
 - Distance modification threshold (DMOD) = 4000 ft.
 - Horizontal miss distance threshold (HMD) = 0.66 nmi.
 - Modified τ threshold (TAUMOD) = 35 s.
 - Time to co-altitude threshold (TCOA) = 0 s.

Towards a Geometric Definition of Well-Clear

Global positioning systems enable **precise** definitions of distance and time functions.

- $(\mathbf{s}_o, s_{oz}), (\mathbf{v}_o, v_{oz})$: Ownship's position and velocity vectors.
- $(\mathbf{s}_i, s_{iz}), (\mathbf{v}_i, v_{iz})$: Intruder's position and velocity vectors.
- $\mathbf{s}, \mathbf{v}$: Relative horizontal position and velocity vectors, i.e.,
 $\mathbf{s} = \mathbf{s}_o - \mathbf{s}_i$ and $\mathbf{v} = \mathbf{v}_o - \mathbf{v}_i$.
- $\mathbf{s}_z, \mathbf{v}_z$: Relative vertical altitude and speed, i.e.,
 $s_z = s_{oz} - s_{iz}$ and $v_z = v_{oz} - v_{iz}$.

$$\begin{aligned} t_{\text{cpa}}(\mathbf{s}, \mathbf{v}) &\equiv -\frac{\mathbf{s} \cdot \mathbf{v}}{\mathbf{v}^2} & \tau(\mathbf{s}, \mathbf{v}) &\equiv -\frac{s^2}{\mathbf{s} \cdot \mathbf{v}}, \\ \tau_{\text{mod}}(\mathbf{s}, \mathbf{v}) &\equiv \frac{\text{DMOD}^2 - s^2}{\mathbf{s} \cdot \mathbf{v}} & t_{\text{ep}}(\mathbf{s}, \mathbf{v}) &\equiv \frac{-\mathbf{s} \cdot \mathbf{v} - \sqrt{\Delta(\mathbf{s}, \mathbf{v})}}{\mathbf{v}^2}, \end{aligned}$$

where $\Delta(\mathbf{s}, \mathbf{v}) \equiv \text{DMOD}^2 \mathbf{v}^2 - (\mathbf{s} \cdot \mathbf{v}^\perp)^2$.

A Formal Definition of Well Clear

Two aircraft are in well-clear violation if and only if $WCV(\mathbf{s}, \mathbf{v})$ holds.

$$WCV(\mathbf{s}, s_z, \mathbf{v}, v_z) \equiv \text{Horizontal_WCV}(\mathbf{s}, \mathbf{v}) \text{ and} \quad (1) \\ \text{Vertical_WCV}(s_z, v_z),$$

where

$$\begin{aligned} \text{Horizontal_WCV}(\mathbf{s}, \mathbf{v}) &\equiv d_{\text{cpa}}(\mathbf{s}, \mathbf{v}) \leq \text{HMD} \text{ and} \\ &\quad (\|\mathbf{s}\| \leq \text{DMOD} \text{ or } 0 \leq \tau_{\text{mod}}(\mathbf{s}, \mathbf{v}) \leq \text{TAUMOD}), \\ d_{\text{cpa}}(\mathbf{s}, \mathbf{v}) &\equiv \|\mathbf{s} + t_{\text{cpa}}(\mathbf{s}, \mathbf{v}) \mathbf{v}\|, \\ \text{Vertical_WCV}(s_z, v_z) &\equiv |s_z| \leq \text{ZTHR} \text{ or } 0 \leq t_{\text{coa}}(s_z, v_z) \leq \text{TCOA}, \\ t_{\text{coa}}(s_z, v_z) &\equiv -\frac{s_z}{v_z}. \end{aligned}$$

Formally specified in Prototype Verification System (PVS)

Three Little Lemmas

For all $\mathbf{s}, \mathbf{v}$ representing non-accelerating converging encounters predicted to cross DMOD, i.e., $\mathbf{s} \cdot \mathbf{v} < 0$, $\mathbf{s}^2 > \text{DMOD}$, and $\Delta(\mathbf{s}, \mathbf{v}) \geq 0$,

- **Lemma 1:** $t_{\text{ep}}(\mathbf{s}, \mathbf{v}) \leq \tau_{\text{mod}}(\mathbf{s}, \mathbf{v}) \leq t_{\text{cpa}}(\mathbf{s}, \mathbf{v}) \leq \tau(\mathbf{s}, \mathbf{v})$,

- **Lemma 2:** Let t_{var} be one of $\{t_{\text{ep}}, \tau_{\text{mod}}, t_{\text{cpa}}, \tau\}$,

$$t_{\text{var}}(\mathbf{s}, \mathbf{v}) = t_{\text{var}}(-\mathbf{s}, -\mathbf{v}).$$

- **Lemma 3:** Let t_{var} be one of $\{t_{\text{ep}}, \tau_{\text{mod}}, t_{\text{cpa}}\}$, for all $0 \leq t_1 \leq t_2 \leq t_{\text{cpa}}(\mathbf{s}, \mathbf{v})$,

$$t_{\text{var}}(\mathbf{s} + t_1 \mathbf{v}, \mathbf{v}) \geq t_{\text{var}}(\mathbf{s} + t_2, \mathbf{v})$$

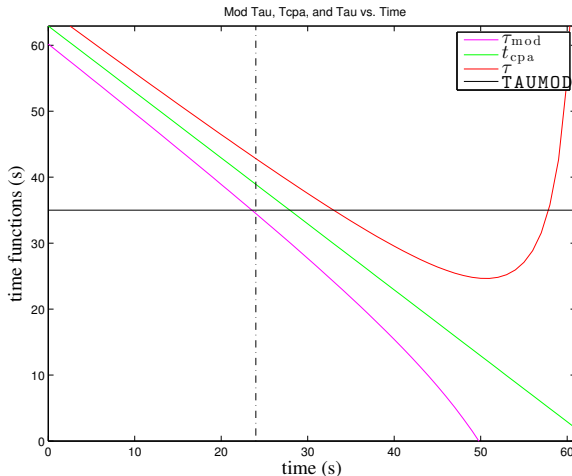


Requirement 2: Existing Collision Avoidance Systems

- Traffic Alert and Collision Avoidance System (TCAS) is a family of systems designed to reduce the risk of mid-air collision between *cooperative* aircraft (i.e., transponder equipped).
- TCAS is mandated in most commercial aircraft.
- TCAS II, the current generation of TCAS, provides: Traffic Alerts (TAs) and Resolution Advisories (RAs).

The Story of Tau

- Tau is an approximation of time to closest point of approach (T_{cpa}) used in TCAS I.
- Tau Mod is a modification of Tau used in TCAS II.



Interoperability with TCAS II RA

For an appropriate choice of threshold values, i.e., DMOD, HMD, ZTHR, TAUMOD, and TCOA, the well-clear volume contains the TCAS II RA volume.

Theorem 1 (Inclusion)

For all $(\mathbf{s}, s_z), (\mathbf{v}, v_z)$,

$$TCAS_II_RA(\mathbf{s}, s_z, \mathbf{v}, v_z) \implies WCV(\mathbf{s}, s_z, \mathbf{v}, v_z).$$



Requirement 3: Avoid Undue Concern for Intruder

In a pair-wise encounter, the ownship and intruder make the same determination of their well-clear status.

Theorem 2 (Symmetry)

For all $(\mathbf{s}, s_z), (\mathbf{v}, v_z)$,

$$WCV(\mathbf{s}, s_z, \mathbf{v}, v_z) \iff WCV(-\mathbf{s}, -s_z, -\mathbf{v}, -v_z).$$



More Theorems

- ① **Extensibility**: A well-clear volume with a given set of thresholds is completely included in another well-clear volume with larger thresholds.
- ② **Local Convexity**: In a pair-wise, non-maneuvering encounter, there is at most one time interval where the aircraft are predicted to be in well-clear violation.
- ③ **Convergence**: In a pair-wise, non-maneuvering converging encounter, the time interval of violation extends at least until the time of closest point of approach



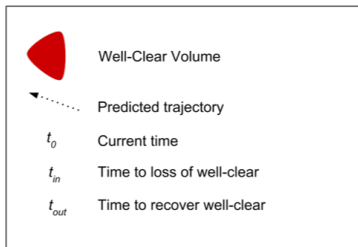
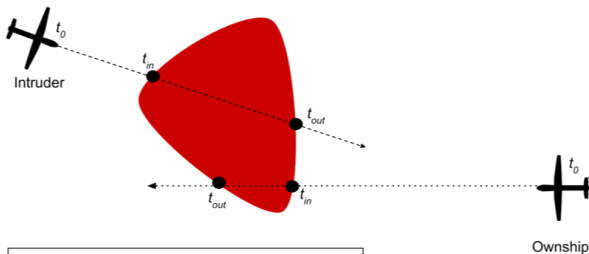
Requirement 4: Detect and Avoid Capabilities

- Detection Logic: Predict whether ownship and intruder will lose well-clear within a lookahead time.
- Alerting Logic: Provide an alert level indicating severity of potential loss of well-clear status.
- Maneuver Guidance Logic: Provide guidance to maintain or recover well-clear status.

Detection Logic

(Figure is notional)

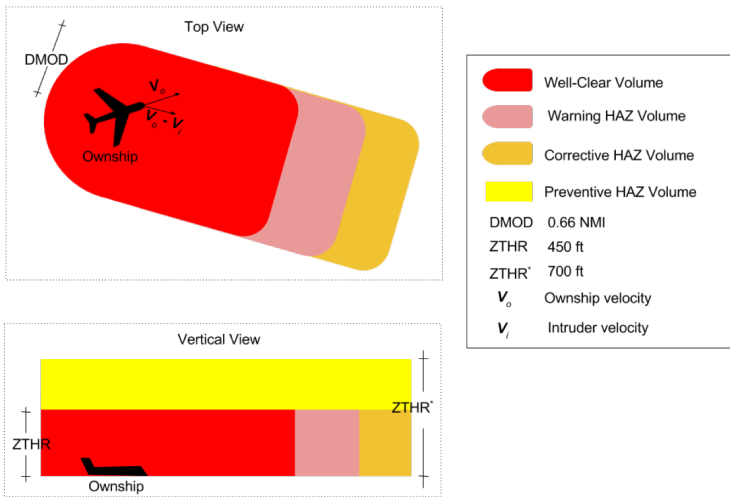
Assuming non-maneuvering trajectories, compute time interval of loss of well-clear, i.e.,



Alerting Logic

(Figure is notional)

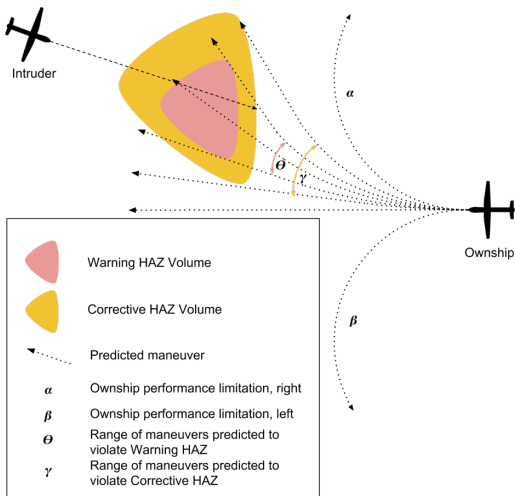
Compute alert level using hazard volumes, i.e.,



Maneuver Guidance Logic

(Figure is notional)

Compute range of maneuvers to maintain/recover from loss of well clear, i.e.,



Operational Requirements for Alerting Logic

In a nominal, pair-wise, non-maneuvering encounter:

- Both aircraft simultaneously compute the same alert level
 $\Leftarrow$ *Well-clear symmetry.*
- Alerts progress according to severity level
 $\Leftarrow$ *Well-clear extensibility.*
- Once an alert is issued, it is continuously issued until threat disappears
 $\Leftarrow$ *Well-clear local convexity.*
- Once an alert is issued, it does not disappear before time of closest point of approach
 $\Leftarrow$ *Well-clear convergence.*



Functional Specification of Detection Logic

The following algorithm returns the time interval of loss of well-clear within a lookahead time T .

```
detection_WCV( $\mathbf{s}, s_z, \mathbf{v}, v_z, T$ )  $\equiv$   
  let  $[t_1, t_2] = \text{detection\_VWCV}(s_z, v_z, T)$  in  
    if  $t_1 > t_2$  then  $[T, 0]$   
    elsif  $t_1 = t_2$  and  $\text{Horizontal\_WCV}(\mathbf{s} + t_1\mathbf{v}, \mathbf{v})$  then  $[t_1, t_1]$   
    elsif  $t_1 = t_2$  then  $[T, 0]$   
    else let  $[t_{\text{in}}, t_{\text{out}}] = \text{detection\_HWCV}(\mathbf{s} + t_1\mathbf{v}, \mathbf{v}, t_2 - t_1)$  in  
       $[t_{\text{in}} + t_1, t_{\text{out}} + t_1]$   
    endif,
```

where

```
  detection_VWCV( $s_z, v_z, T$ )  $\equiv \dots$   
  detection_HWCV( $\mathbf{s} + t_1\mathbf{v}, \mathbf{v}, t_2 - t_1$ )  $\equiv \dots$ 
```

Theorem 3 (Soundness and Completeness)

For all $(\mathbf{s}, s_z), (\mathbf{v}, v_z)$, $T > 0$, and $t \in [0, T]$,

$$\begin{aligned} WCV(\mathbf{s} + t\mathbf{v}, s_z + tv_z, \mathbf{v}, v_z) &\iff \\ t \in \text{detection_WCV}(\mathbf{s}, s_z, \mathbf{v}, v_z, T). \end{aligned}$$



Proofs in the Real Field

```
[-1]  eps = 1 OR eps = -1
[-2]  v'y*eps <= 0
[-3]  rd'y*eps < 0
[-4]  ((v'x = 0 AND v'y = 0) IMPLIES rd'x >= 0)
[-5]  ((v'x /= 0 OR v'y /= 0) IMPLIES rd'x > v'x)
[-6]  rd'x*v'y*eps-rd'y*v'x*eps <= 0
[-7]  mps'y*eps+rd'y*eps < 0
[-8]  v'x >= 0
[-9]  (dv'x /= 0 OR dv'y /= 0)
[-10] mps'x*rd'y*eps-mps'y*rd'x*eps <= 0
[-11] -1*(dv'x*mps'y*eps)-dv'x*rd'y*eps+ dv'y*mps'x*eps+dv'y*rd'x*eps < 0
[-12] ((rd'x*mps'x+rd'x*rd'x+rd'y*mps'y+rd'y*rd'y < 0 AND
      dv'x*rd'y*eps-dv'y*rd'x*eps < 0) OR (rd'x*mps'x+rd'x*rd'x+
      rd'y*mps'y+rd'y*rd'y >= 0 AND dv'x*mps'x+dv'x*rd'x+dv'y*mps'y+
      dv'y*rd'y > rd'x*mps'x+rd'x*rd'x+rd'y*mps'y+rd'y*rd'y
      AND dv'x*rd'y*eps-dv'y*rd'x*eps <= 0))
|-----
[1]  (dv'x /= 0 OR dv'y /= 0) AND dv'y*eps < 0 AND ((v'x = 0 AND v'y = 0)
      IMPLIES dv'x >= 0) AND ((v'x /= 0 OR v'y /= 0) IMPLIES dv'x > v'x)
      AND dv'x*v'y*eps-dv'y*v'x*eps <= 0
```

Detect and Avoid Alerting Logic for Unmanned Systems



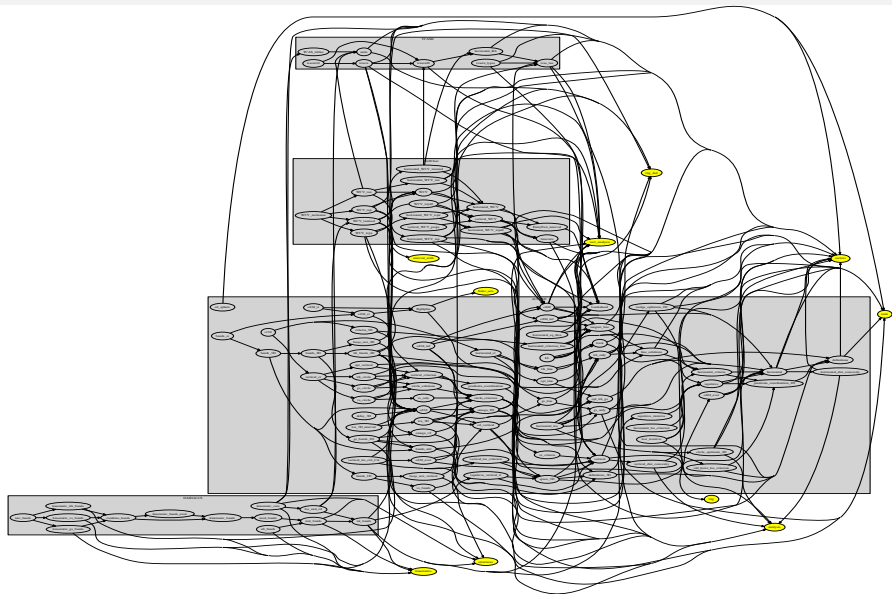
- Reference implementation Minimum Operational Standard Requirements of Detect and Avoid for Unmanned Aircraft Systems (FAA DO-365).
- Specifications and software (Java and C++) released under NASA Open Source Agreement (<http://github.com/nasa/wellclear>).
- Further information:
<https://shemesh.larc.nasa.gov/fm/DAIDALUS>.

DAIDALUS in the Prototype Verification Systems (PVS)

- Formally proved in PVS that WC satisfies high-level requirements: inclusion, symmetry, local convexity.
- Formally specified WC algorithms: detection, self-separation bands, and alerting.
- Formally verified correctness of the algorithms against functional requirements.

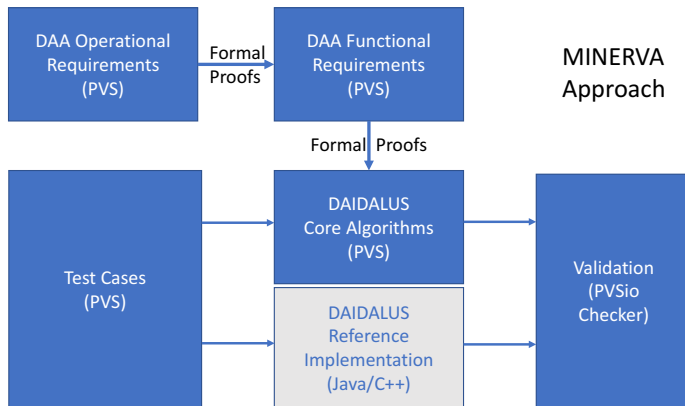
PVS Library	#Theories	#Proofs	#Lines of Spec.
ACCoRD	77	1,211	8,601
TCASII	9	142	784
WellClear	19	236	1,244
DAIDALUS	21	385	3,509
Total	126	1,974	14,138

DAIDALUS in Theory



DAIDALUS Code Validation

Mirrored Implementation Numerically Evaluated against Rigorously Verified Algorithms

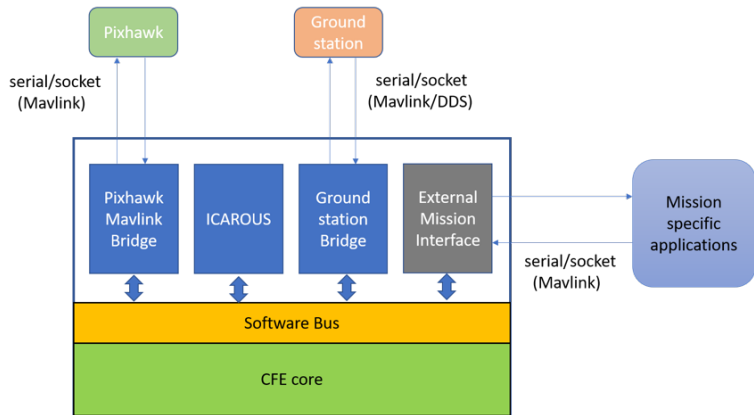


Independent Configurable Architecture for Reliable Operations of Unmanned Systems



- On-board software architecture that integrates formally verified, highly assured core algorithms for building safe, autonomous UAS applications.
- Released under NASA Open Source Agreement (<http://github.com/nasa/icarous>).

ICAROUS Architecture

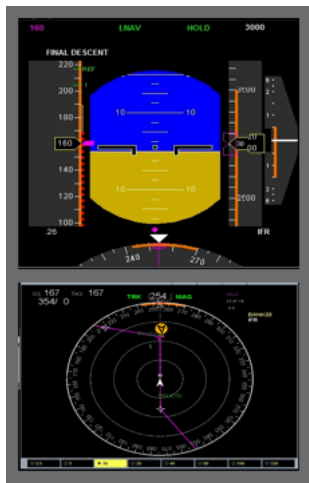


Core Capabilities

- Detect and Avoid (DAIDALUS) – PVS.
- Geofencing (PolyCARP) – PVS.
- Path Planning (Rapid Random Tree Exploration, A*) – PVS.
- Merging and Spacing – PVS.
- Autonomous Decision Making (PLEXIL) – Maude.

DAIDALU & ICAROUS in Practice

DAIDALUS and ICAROUS are currently being used in several projects at NASA involving manned aircraft, remotely piloted aircraft, and autonomous aircraft.



Conclusion

- Rich specification language (PVS) makes it possible to reason about *family* of complex high-level properties and fine tune *specific* operational and functional requirements.
- Higher-order logic enables safe re-use of functional requirements by functional parameter instantiation.
- Higher-order logic enables powerful but practical model validation approaches, e.g., MINERVA.

No Silver Bullet

- DAIDALUS/PolyCARP/ICAROUS highly assured software is possible because of major initial development on theorem proving technology (non-linear arithmetic, model animation, etc.) and formal libraries (kinematics, conflict detection, and resolution, separation assurance, aircraft trajectories, etc.)
- Major advances are still needed on areas such as
 - Proof automation.
 - Readability and usability by non-experts.
 - Verification of non-deterministic behavior.
 - Verification of numerically intensive systems.

Acknowledgements

- DAIDALUS Team: Anthony Narkawicz (NASA), Aaron Dutle (NASA), Jason Upchurch (formerly NASA).
- ICAROUS Team: María Consiglio (NASA), Swee Balachandran (NIA), Marco Feliú (NIA).

References I



Devesh Bhatt, Anitha Murugesan, Brendan Hall, Hao Ren, and Yoganada Jeppu.

The CLEAR way to transparent formal methods.

In Proceedings of the 4th Workshop on Formal Integrated Development Environment (F-IDE 2018), Oxford, UK, July 2018.



FAA Sponsored Sense and Avoid Workshop.

Sense and avoid (SAA) for Unmanned Aircraft Systems (UAS), October 2009.



Federal Aviation Administration.

Requirements engineering management findings report.

Final Report DOT/FAA/AR-08/34, Air Traffic Organization NextGen & Operations Planning Office of Research and Technology Development, Washington, DC 20591, May 2009.

References II



Peter H. Feiler, John B. Goodenough, Arie Gurfinkel, Charles B. Weinstock, and Lutz Wrage.

Reliability validation and improvement framework.

Special Report CMU/SEI-2012-SR-013, Software Engineering Institute, November 2012.



Kerianne H. Gross, Aaron W. Fifarek, and Jonathan A. Hoffman.

Incremental formal methods based design approach demonstrated on a coupled tanks control system.

In *2016 IEEE 17th International Symposium on High Assurance Systems Engineering (HASE)*, pages 181–188, Jan 2016.

References III



Kit Siu, Abha Moitra, Michael Durling, Andy Crapo, Meng Li, Han Yu, Heber Herencia-Zapana, Mauricio Castillo-Effen, Shiraj Sen, Craig McMillan, Daniel Russell, Sundeep Roy, and Panagiotis Manolios. Flight critical software and systems development using ASSERT. In *2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC)*, number 978-1-5386-0365-9/17, pages 1–10, Sept 2017.