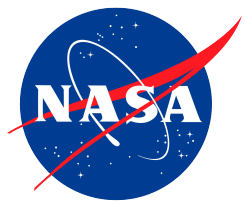
Formal Methods in Air Traffic Management: The Case of Unmanned Aircraft Systems

César Muñoz[1]
cesar.a.munoz@nasa.gov



12th International Colloquium on Theoretical Aspects of Computing (ICTAC 2015)

[1] In collaboration with the NASA Langley Formal Methods Team.

The First "A" in NASA

"To serve the future needs of aviation by conducting research into, and developing solutions for, the problems of flight, . . ."

- Safe, Efficient Growth in Global Operations
- Real-Time System-Wide Safety Assurance
- Assured Autonomy for Aviation Transformation

NextGen: Develop and demonstrate future concepts, capabilities, and technologies to support expected increase in capacity and mobility while maintaining safety.

This Talk

How formal methods enable discovery in Air Traffic Management (ATM)

Air Traffic Management

Three competing objectives:

- Performance
- Capacity
- Safety

Air Traffic Management in the World

The International Air Transport Association (IATA) predicts that passenger numbers are expected to reach 7.3 billion by 2034 (4.1% average annual growth).[2]

[2] IATA Press Release No. 57, 16 October 2014.

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 billions.[3]

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

[3] Economic 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 NICAS

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 occured 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

UAS in the National Airspace System (NAS)

A NASA Project

Develop key capabilities to enable routine and safe access for public and civil use of UAS in non-segregated airspace operations.

The Main Challenge

Michael Huerta, Administrator, Federal Aviation Administration:[4]

> *A bedrock principle of aviation is see and avoid. And if you don't have a pilot on board the aircraft, you need something that will substitute for that, which will sense other aircraft, and we can ensure appropriate levels of safety.*

[4] `http://www.pbs.org/newshour/bb/drone-industry-grows-faster-flick-joystick-regulation-lag`.

14CFR Part 91

- 91.111 (a) No person may operate an aircraft **so close to another aircraft as to create a collision hazard.**
- 91.113 (b) General. When weather conditions permit, regardless of whether an operation is conducted under instrument flight rules or visual flight rules, **vigilance shall be maintained by each person operating an aircraft so as to see and avoid other aircraft**. When a rule of this section gives another aircraft the right-of-way, the pilot shall give way to that aircraft and **may not pass over, under, or ahead of it unless well clear**.

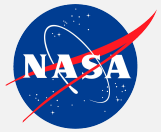
Detect and Avoid

(Formerly Known As Sense 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 14CFR Part 91, §91.111 and §91.113.[5]
- DAA Requirements: DAA shall
  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

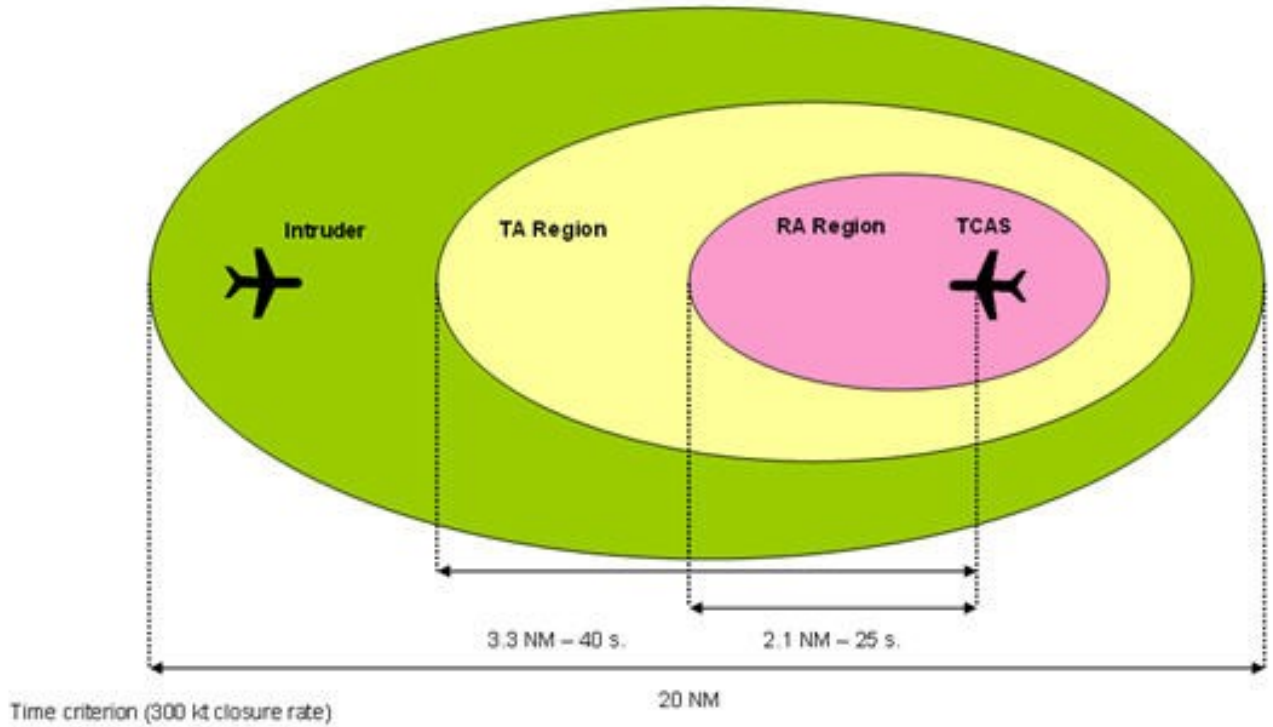
[5] SAA for UAS Workshop Final Report, October 9, 2009.

Traffic Alert and Collision Avoidance System (TCAS)



- Family of airborne systems designed to reduce the risk of mid-air collisions between *cooperative* aircraft (i.e., transponder equipped).
- Mandated in the US for aircraft with greater than 30 seats or a maximum takeoff weight greater than 33,000 pounds.
- Current version, TCAS II, provides:
  - **Traffic Alerts** (TAs).
  - **(Vertical) Resolution Advisories** (RAs).

TCAS II TA and RA Volumes



Example of ACAS Protection Volume between 5000 and 10000 feet

Deconstructing TCAS II RA Detection Logic (I)

- Pairwise logic: ownship and intruder aircraft.
- TCAS volumes are based on distance and time functions on aircraft relative states:
  - Range r and relative altide r_z.
  - Time Tau:

$$\tau \equiv -\frac{r}{\dot{r}}.$$

  - Time to co-altitude (t_{coa}):

$$t_{\text{coa}} \equiv -\frac{r_z}{\dot{r}_z}.$$

Deconstructing TCAS II RA Detection Logic (II)

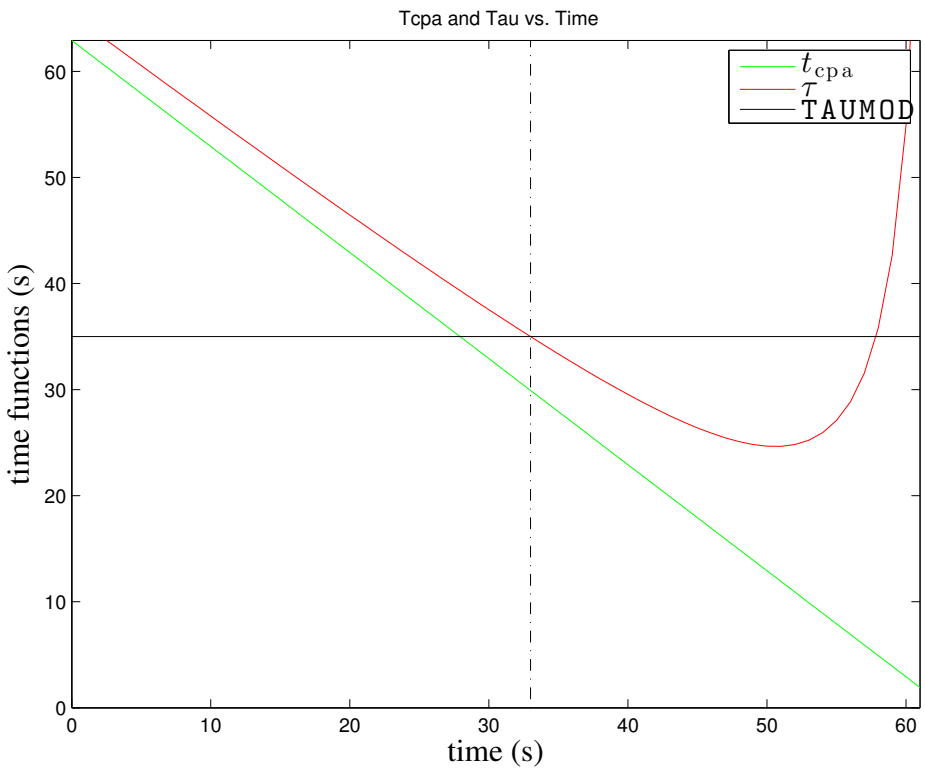
Times and distance functions are compared against a set of thresholds, whose values depend on ownship's altitude:

- `DMOD`, `ZTHR`: Horizontal and vertical distance thresholds compared to r and r_z, respectively.
- `TAUMOD`: Time threshold compared to τ and t_{coa}.

$$\begin{aligned}\texttt{TCASII\_RA} \equiv (r \leq \texttt{DMOD} \ \texttt{or} \ (\tau \leq \texttt{TAUMOD} \ \texttt{and} \ \ldots)) \ \texttt{and} \\ (r_z \leq \texttt{ZTHR} \ \texttt{or} \ t_{\text{coa}} \leq \texttt{TAUMOD}).\end{aligned}$$

The Story of Tau

- Tau is an approximation of time to closest point of approach (Tcpa).
- Tau is not necessarily a good approximation.
- In a non-accelerating encounter, Tcpa decreases linearly with respect to time.

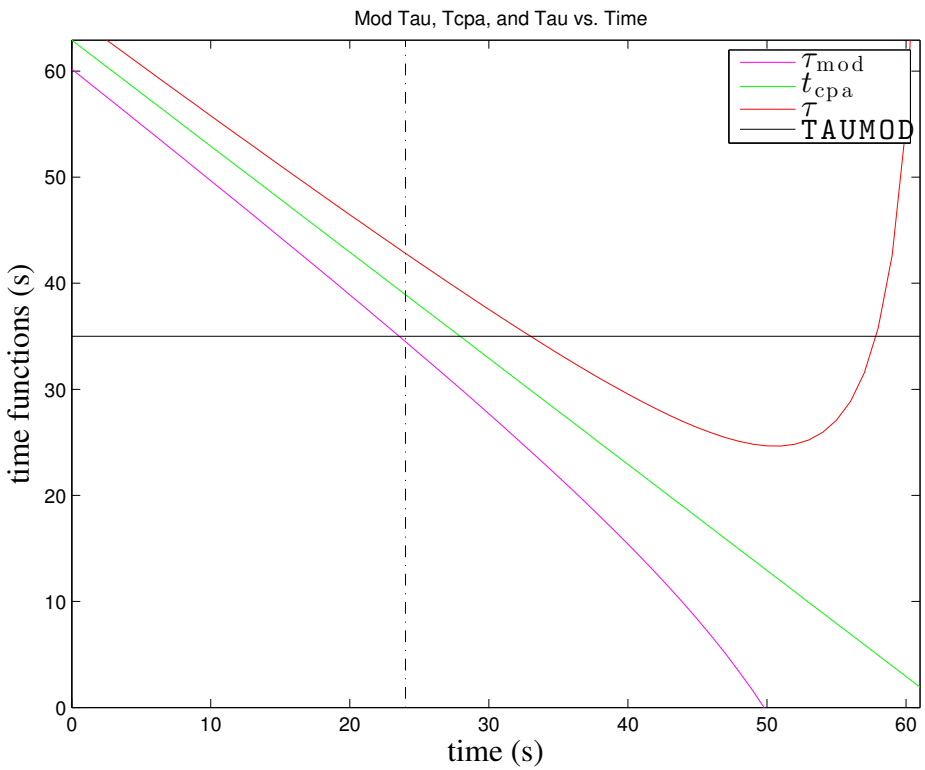


Modified Tau

- TCAS II Version 7.1., uses Modified Tau:

$$\tau_{\text{mod}} \equiv -\frac{r^2 - \text{DMOD}^2}{r\dot{r}}$$

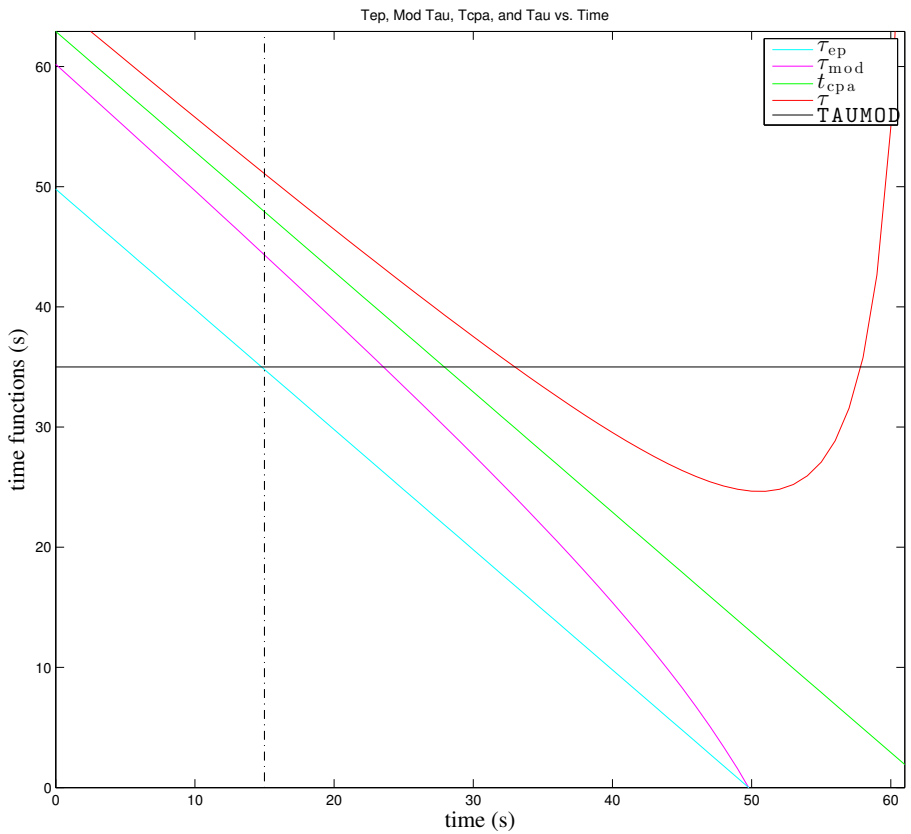
- Modified Tau is a more conservative approximation of Tcpa:



Time to DMOD

(Also known as Time to Entry Point)

Time to DMOD, i.e., t_{ep},is more conservative than Modified Tau and it decreases linearly with time for non-accelerating encounter:



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 $v_z = v_{oz} - v_{iz}$.

$$t_{\text{cpa}}(\mathbf{s}, \mathbf{v}) \equiv -\frac{\mathbf{s} \cdot \mathbf{v}}{\mathbf{v}^2} \qquad \tau(\mathbf{s}, \mathbf{v}) \equiv -\frac{\mathbf{s}^2}{\mathbf{s} \cdot \mathbf{v}},$$

$$\tau_{\text{mod}}(\mathbf{s}, \mathbf{v}) \equiv \frac{\texttt{DMOD}^2 - \mathbf{s}^2}{\mathbf{s} \cdot \mathbf{v}} \qquad t_{\text{ep}}(\mathbf{s}, \mathbf{v}) \equiv \frac{-\mathbf{s} \cdot \mathbf{v} - \sqrt{\Delta(\mathbf{s}, \mathbf{v})}}{\mathbf{v}^2},$$

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

Three Little Lemmas

For all $\mathbf{s}, \mathbf{v}$ representing non-accelerating converging encounters predicted to cross DMOD, i.e., $\mathbf{s} \cdot \mathbf{v} < 0$, $\mathbf{s}^2 > \mathtt{DMOD}$, 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 $0 \leq t_1 \leq t_2 \leq t_{\text{cpa}}(\mathbf{s}, \mathbf{v})$,

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

A Formal Definition of Well Clear

Requirement 1: WC shall provide a geometric means to determine well-clear status

Let t_{var} be one of $\{t_{\text{ep}}, \tau_{\text{mod}}, t_{\text{cpa}}, \tau\}$, two aircraft are in t_{var}-well-clear violation if and only if $\texttt{WCV}_{t_{\text{var}}}(\mathbf{s}, \mathbf{v})$ holds.

$$\begin{aligned}\texttt{WCV}_{t_{\text{var}}}(\mathbf{s}, s_z, \mathbf{v}, v_z) \equiv\ & \texttt{Horizontal\_WCV}_{t_{\text{var}}}(\mathbf{s}, \mathbf{v}) \ \texttt{and} \\ & \texttt{Vertical\_WCV}(s_z, v_z),\end{aligned} \tag{1}$$

where

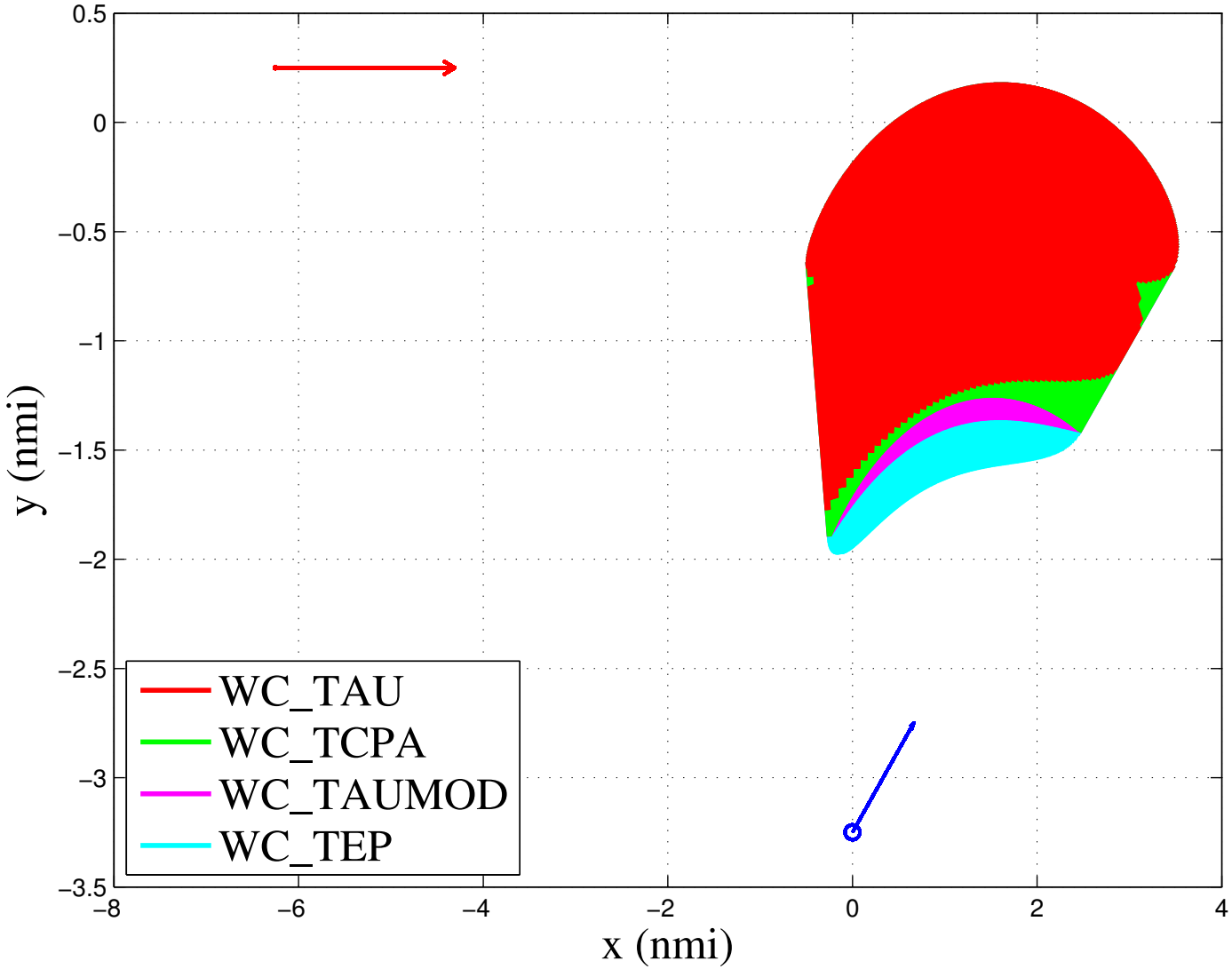
$$\begin{aligned}\texttt{Horizontal\_WCV}_{t_{\text{var}}}(\mathbf{s}, \mathbf{v}) \equiv\ & \|\mathbf{s}\| \leq \texttt{DMOD} \ \texttt{or} \\ & (d_{\text{cpa}}(\mathbf{s}, \mathbf{v}) \leq \texttt{DMOD} \ \texttt{and} \ 0 \leq t_{\text{var}}(\mathbf{s}, \mathbf{v}) \leq \texttt{TAUMOD}),\end{aligned}$$

$$d_{\text{cpa}}(\mathbf{s}, \mathbf{v}) \equiv \|\mathbf{s} + t_{\text{cpa}}(\mathbf{s}, \mathbf{v})\,\mathbf{v}\|,$$

$$\texttt{Vertical\_WCV}(s_z, v_z) \equiv |s_z| \leq \texttt{ZTHR} \ \texttt{or} \ 0 \leq t_{\text{coa}}(s_z, v_z) \leq \texttt{TCOA},$$

$$t_{\text{coa}}(s_z, v_z) \equiv -\frac{s_z}{v_z}.$$

A Family of Well-Clear Volumes



Well-Clear Properties: Inclusion

Requirement 2: WC shall interoperate with existing collision avoidance systems

Theorem 1 (Inclusion)

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

$$\begin{aligned} WCV_{\tau}(\mathbf{s}, s_z, \mathbf{v}, v_z) &\implies WCV_{t_{cpa}}(\mathbf{s}, s_z, \mathbf{v}, v_z) \implies WCV_{\tau_{mod}}(\mathbf{s}, s_z, \mathbf{v}, v_z) \\ &\implies WCV_{t_{ep}}(\mathbf{s}, s_z, \mathbf{v}, v_z). \end{aligned}$$

For an appropriate choice of threshold values, i.e., `DMOD`, `ZTHR`, `TAUMOD`, and `TCOA`, the violation volumes determined by $\texttt{WCV}_{\tau_{\text{mod}}}(\mathbf{s}, s_z, \mathbf{v}, v_z)$ and $\texttt{WCV}_{t_{\text{ep}}}(\mathbf{s}, s_z, \mathbf{v}, v_z)$ are larger than the TCAS II RA volume.

Well-Clear Properties: Symmetry

Requirement 3: WC shall avoid undue concern for traffic aircraft

Theorem 2 (Symmetry)

Let t_{var} *be one of* $\{t_{ep}, \tau_{mod}, t_{cpa}, \tau\}$, *for all* $(\mathbf{s}, s_z), (\mathbf{v}, v_z)$,

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

In any encounter, the intruder aircraft makes the same determination as the ownship about the well-clear status.

Well-Clear Properties: Local Convexity

Requirement 4: WC shall enable self-separation capabilities

Theorem 3 (Local Convexity)

Let t_{var} *be one of* $\{t_{ep}, \tau_{mod}, t_{cpa}\}$, *for all* $(\mathbf{s}, s_z), (\mathbf{v}, v_z)$, $t_1 \leq t_2 \leq t_3$,

$$WCV_{t_{var}}(\mathbf{s} + t_1\mathbf{v}, s_z + t_1 v_z, \mathbf{v}, v_z) \text{ and } WCV_{t_{var}}(\mathbf{s} + t_3\mathbf{v}, s_z + t_3 v_z, \mathbf{v}, v_z) \implies WCV_{t_{var}}(\mathbf{s} + t_2\mathbf{v}, s_z + t_2 v_z, \mathbf{v}, v_z).$$

In a non-accelerating encounter, there is at most one time interval where the aircraft are in well-clear violation.

Well-Clear Algorithms: Detection

The following algorithm returns the time interval of t_{var}-well-clear violation within a lookahead time T.

$$
\begin{aligned}
&\texttt{detection\_WCV}_{t_{\text{var}}}(\mathbf{s}, s_z, \mathbf{v}, v_z, T) \equiv \\
&\quad \texttt{let } [t_1, t_2] = \texttt{detection\_VWCV}(s_z, v_z, T) \texttt{ in} \\
&\qquad \texttt{if } t_1 > t_2 \texttt{ then } [T, 0] \\
&\qquad \texttt{elsif } t_1 = t_2 \texttt{ and } \texttt{Horizontal\_WCV}_{t_{\text{var}}}(\mathbf{s} + t_1\mathbf{v}, \mathbf{v}) \texttt{ then } [t_1, t_1] \\
&\qquad \texttt{elsif } t_1 = t_2 \texttt{ then } [T, 0] \\
&\qquad \texttt{else let } [t_{\text{in}}, t_{\text{out}}] = \texttt{detection\_HWCV}_{t_{\text{var}}}(\mathbf{s} + t_1\mathbf{v}, \mathbf{v}, t_2 - t_1) \texttt{ in} \\
&\qquad\quad [t_{\text{in}} + t_1, t_{\text{out}} + t_1] \\
&\qquad \texttt{endif},
\end{aligned}
$$

where

$$
\begin{aligned}
\texttt{detection\_VWCV}(s_z, v_z, T) &\equiv \ldots \\
\texttt{detection\_HWCV}_{t_{\text{var}}}(\mathbf{s} + t_1\mathbf{v}, \mathbf{v}, t_2 - t_1) &\equiv \ldots
\end{aligned}
$$

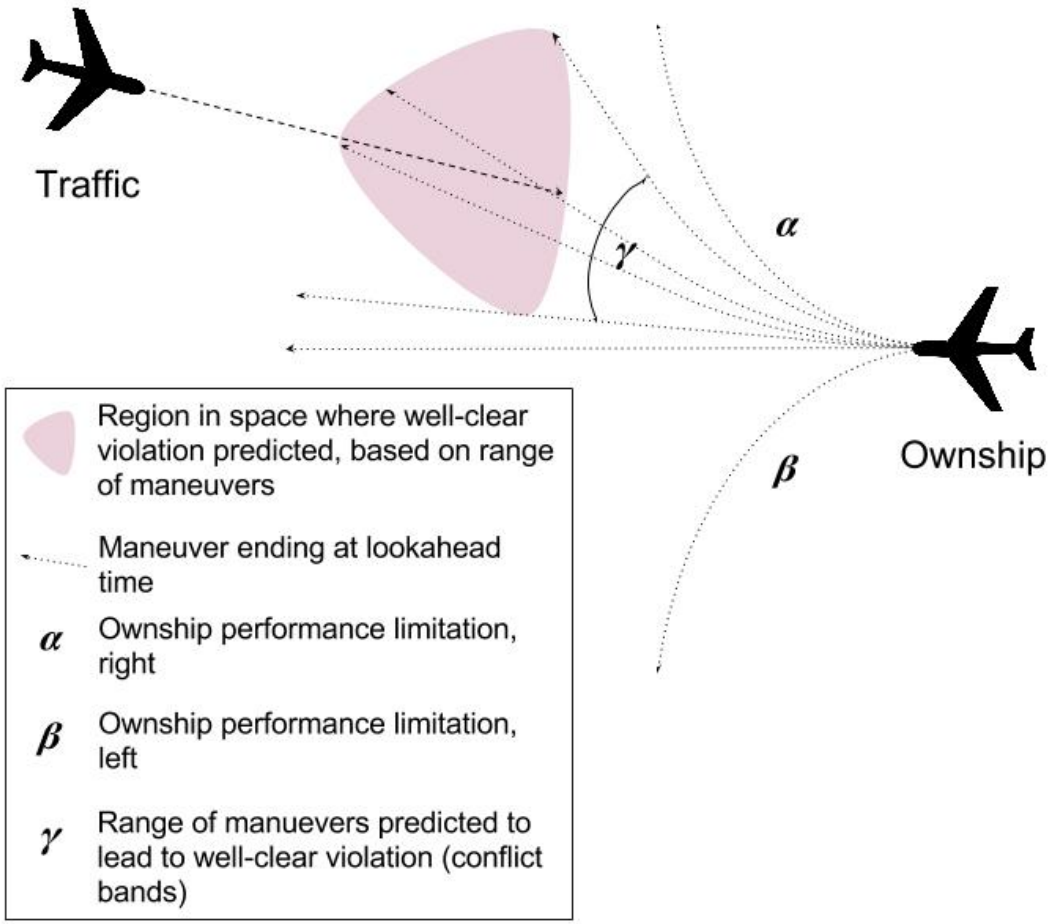
Theorem 4 (Soundness and Completeness)

Let t_{var} *be one of* $\{t_{ep}, \tau_{mod}, t_{cpa}\}$, *for all* $(\mathbf{s}, s_z), (\mathbf{v}, v_z)$, $T > 0$, *and* $t \in [0, T]$,

$$WCV_{t_{var}}(\mathbf{s} + t\mathbf{v}, s_z + tv_z, \mathbf{v}, v_z) \iff$$
$$t \in detection\_WCV_{t_{var}}(\mathbf{s}, s_z, \mathbf{v}, v_z, T).$$

Well-Clear Algorithms: Self-Separation Bands

Bands are ranges of track, ground speed, and vertical speed that lead to well-clear.



DAIDALUS: **D**etect and **A**vo**id** **A**lerting **L**ogic for **U**nmanned **S**ystems[6]

- Open source implementation in Java and C++ of formally verified DAA algorithms.
- Considered for inclusion as DAA reference implementation in RTCA Minimum Operational Performance Standards (MOPS) for Unmanned Aircraft Systems.

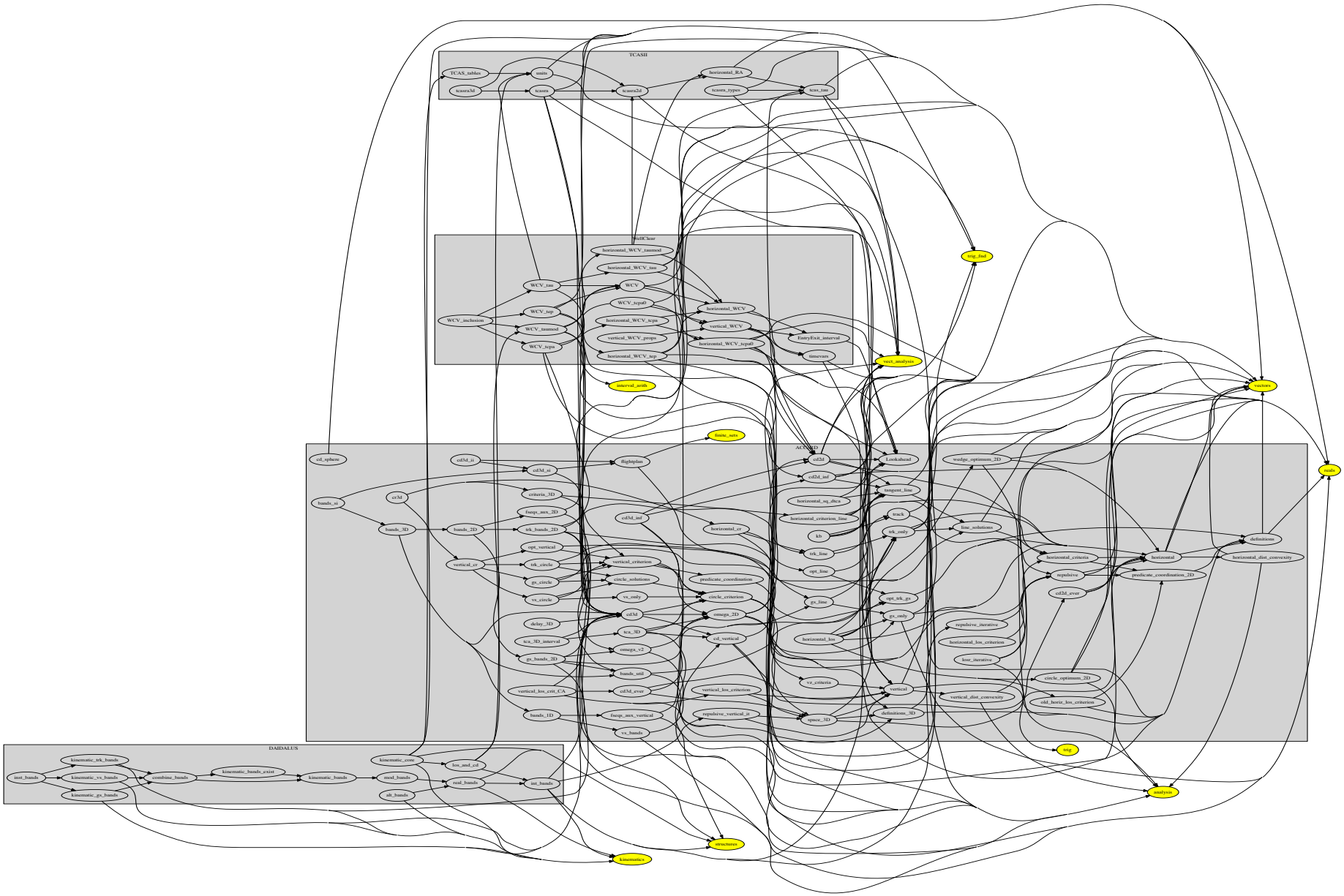
[6] Logo was designed by Mahyar Malekpour (NASA).

DAIDALUS in Theory

- Family of well-clear volumes defined in the Program Verification System (PVS).
- Formally proved in PVS that WC volumes satisfy 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.

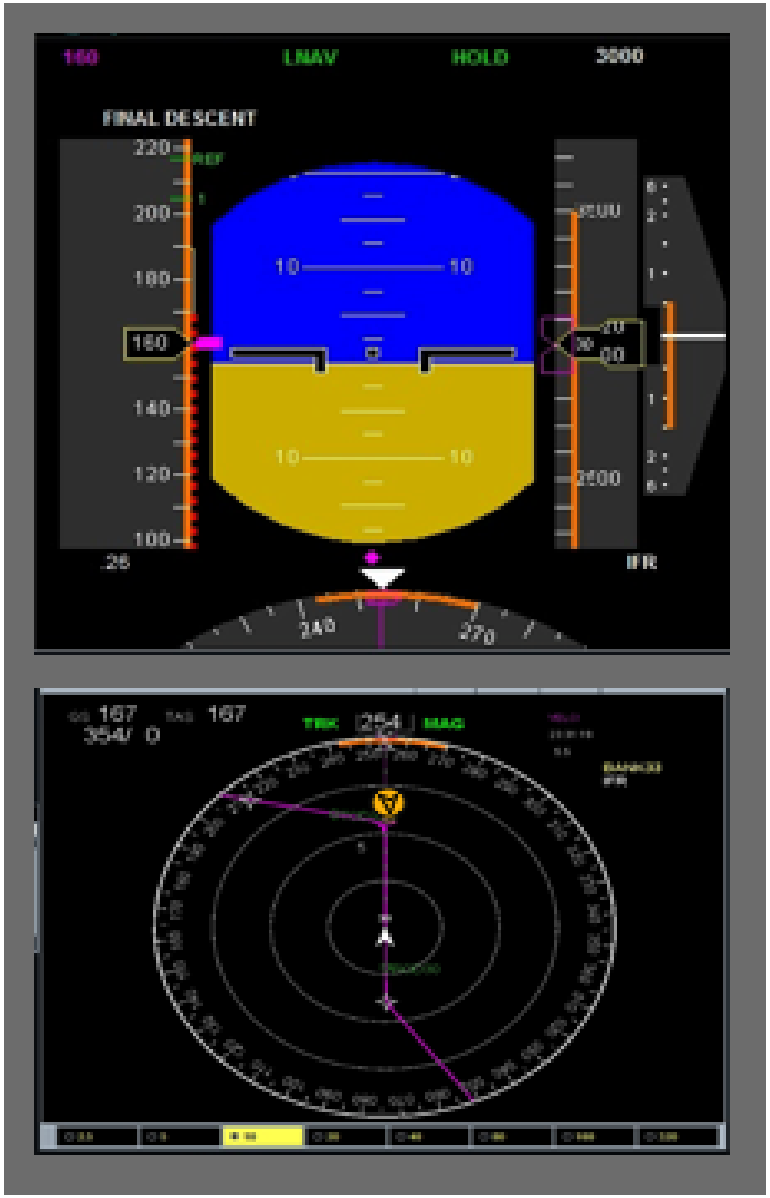
PVS Library	**#Theories**	**#Proofs**	**#Lines of Spec.**
ACCoRD	77	1,211	8,601
TCASII	9	142	784
WellClear	19	236	1,244
DAIDALUS	21	385	3,509
Total	126	1,974	14,138

DAIDALUS in PVS



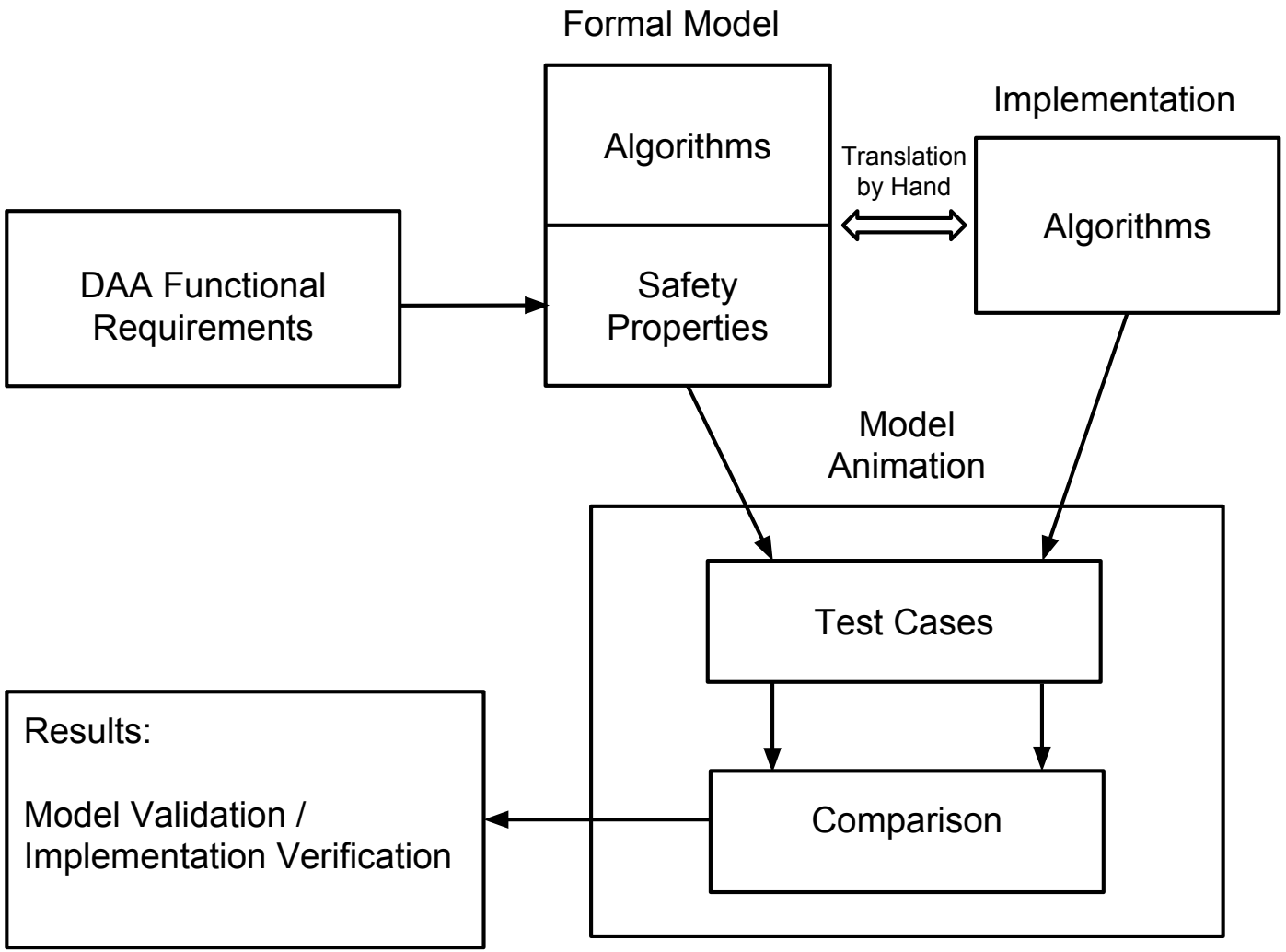
DAIDALUS in Practice

- Code released under NASA Open Source Agreement:
  - Java: 34,371 (loc).
  - C++: 40,445 (loc).
- DAIDALUS is currently being used in human-in-the-loop experiments independently conducted at NASA and FAA.



DAIDALUS Verification and Validation

(On going work)



- Most modern verification systems have limited support for continuous mathematics.
- Algorithms are long, statements are longer, and proofs are even longer.
- Developed PVS decision and semi-decision procedures based on interval arithmetic, affine arithmetic, Bernstein polynomials, Sturm and Tarski theorems. More are needed.
- The elephant in the room: floating point numbers.

Formal 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
```

ATM is a non-traditional formal methods domain:

- ATMer: Formal what? – FMist: Air Traffic what?
- ATM is more than software and avionics systems.
- ATM is a *real globally* distributed system.
- Revolutionary approaches vs. Evolutionary approaches.
- Theoretical solutions vs. Practical solutions.

To Bring Home

As for the future, your task is not to foresee it, but to enable it.

Antoine de Saint-Exupery (1900-1944)

Formal methods are enabling the worldwide evolution of the Next Generation of Air Traffic Systems.

Acknowledgments

- Joint collaborative work:
  - From the Safety-Critical Avionics Systems Branch: Ricky Butler, Aaron Dutle, George Hagen, Jeff Maddalon, César Muñoz, Anthony Narkawicz, and Jason Upchurch.
  - From the Crew Systems and Aviation Operations Branch: María Consiglio and James Chamberlain.
- NASA Langley Formal Methods team:
  `http://shemesh.larc.nasa.gov/fm`
- FM research on UAS in the NAS:
  `http://shemesh.larc.nasa.gov/people/cam/UAS_NAS`