

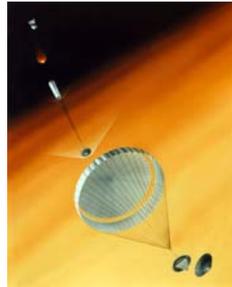
# Certification technology for auto-generated code

## PROBLEM

NASA missions increasingly will use auto-code generation technology for ground/flight software

**But:** this comes with **risk**

- how can the correctness of the generated code be assessed?
- code generators are complex pieces of software themselves that may contain bugs

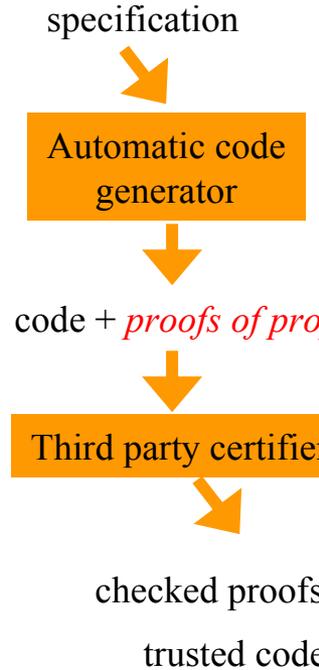


## TECHNOLOGY

Targeting attitude control systems, we have designed an extension for the **Autofilter** code generator to output proofs that the algorithms generated are statistically optimal - a key effectiveness property.

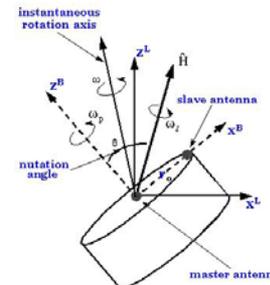
The code generator will produce proofs which are then checked independently by a third party – ideally, a small kernel proof checker that has been formally verified.

## SOLUTION



Too difficult to formally verify the code generator (too complex)

Instead: product-oriented certification → extend the generator to output not only the code but also a proof that key properties hold



# Explanation of Accomplishment

- **POC:** Jon Whittle (ASE group, Code IC, jonathw@email.arc.nasa.gov)
- **Technology:** Autofilter is a code generator geared towards state estimation problems (e.g., attitude estimation, parameter estimation). Given a high-level model of the problem to be solved (in terms of differential and other equations), Autofilter generates highly reliable code that can easily be plugged into an existing architecture. We have designed an extension to Autofilter so that in addition to the code it generates a proof that the algorithm inherent in the code is statistically optimal – specifically, the proof is that the particular representation generated of a Kalman filter algorithm minimizes the mean-squared estimation error. The technology is widely applicable in that proofs can be generated for different variants of the Kalman filter, namely standard Kalman filters, extended Kalman filter and information filters.  
**Accomplishment:** This work was presented at the 2002 International Conference on Automated Software Engineering. The current status is that semi-automatically generated proofs for effectiveness have been certified with a prototype certification engine written in Maude. Other properties previously investigated include safety properties such as consistency of measurement units and consistency of coordinate frames.
- **Benefits:** This technology has the potential to increase the confidence in the use of code generators within and outside NASA. Auto-generated code will come with a certificate of its correctness (with respect to certain key properties that have been proved). These certificates can be independently checked by third parties such as a certification authority.