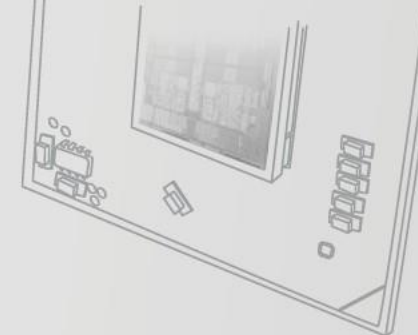




KRONO-SAFE

Safe design in real-time



ASTERIOS Checker: A Verification Tool for Certifying Airborne Software

Amira METHNI (Krono-Safe)

Emmanuel OHAYON (Krono-Safe)

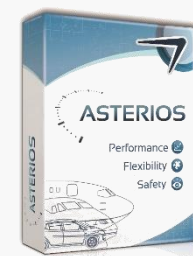
Francois THURIEAU (Safran)

January 30, 2020



Introduction

- **Context**
 - Safety-critical (real-time) software requires a high level of confidence
 - For airborne systems, DO-178C provides guidances to guarantee safety and reliability
 - 5 assurance levels (*Development Assurance level*).
 - Level A: “software whose failure would cause or contribute to a catastrophic failure of the aircraft”
 - Designing safety-critical real-time applications meeting DO-178C is not an easy task
- **Related work**
 - Certified RTOS: VxWorks, PikeOS.
 - ANSYS SCADE (ANSYS), Code inspector (MathWorks)
- **ASTERIOS® technology**
 - Set of tools for the design of safety-critical real-time applications with a small foot-print real-time kernel (RTK) in charge of running the application on the embedded platform.
 - About Krono-Safe:
 - Spin-off of CEA (French Alternative Energies and Atomic Energy Commission)
 - Founded in 2011
 - DO-178C Certification strategy using an automated verification tool called ASTERIOS Checker, qualified in accordance with DO-330.





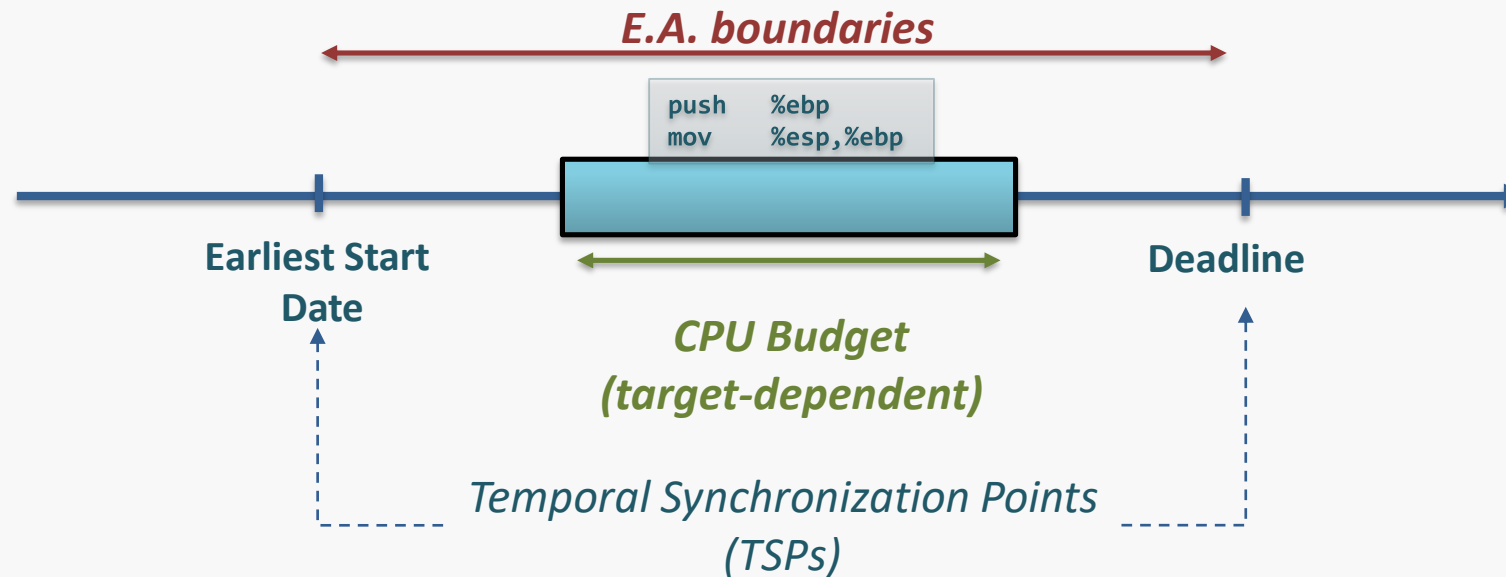
The Psy (*Parallel Synchronous*) model

- Parallel and Multi-tasking programming model
- Originally created for OASIS technology
- Time-Triggered paradigm
 - System observes its environment at predetermined instants
 - No lock/semaphore/mutex
 - enables predictable and reproducible behaviors
- Offers an abstraction for the design of the real-time application



Elementary action (EA)

- A real time task = 1 sequential execution unit
- *TSPs define the cadence of tasks*
- Psy model is implemented by the PsyC programming language
 - An application is a static set of Agents
 - Agent is a sequence of EAs

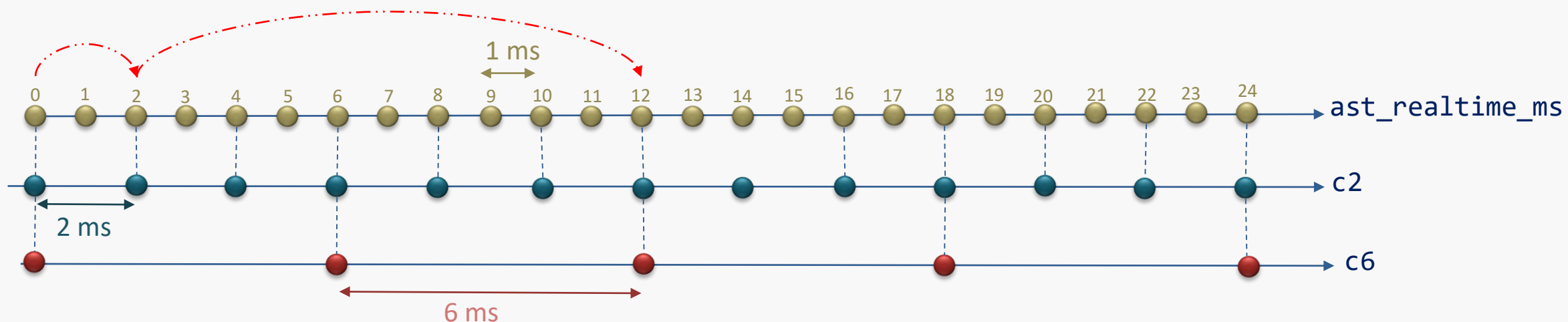




Basic concepts of PsyC

- **Source (*HW-dependent part*):** provides base tick thanks to HW resource (e.g timer)
- **Clock definition (*HW-independent part*)**
 - A tool for measuring time: a set of ticks based on a source
 - Can derive from either other clocks or a source
- **Advance semantic:**
 - Grammar: `advance <n> with <clockname>;`
 - Advance from the current time up to the *n*th tick of `<clockname>`
- **Examples:**

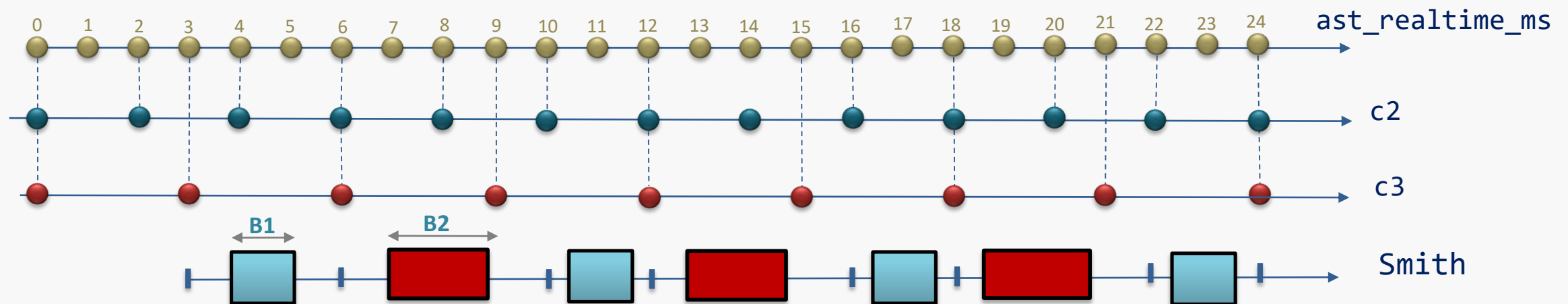
```
advance 1 with c2; // from t = 0
advance 2 with c6; // from t = 2
```





What a PsyC application looks like

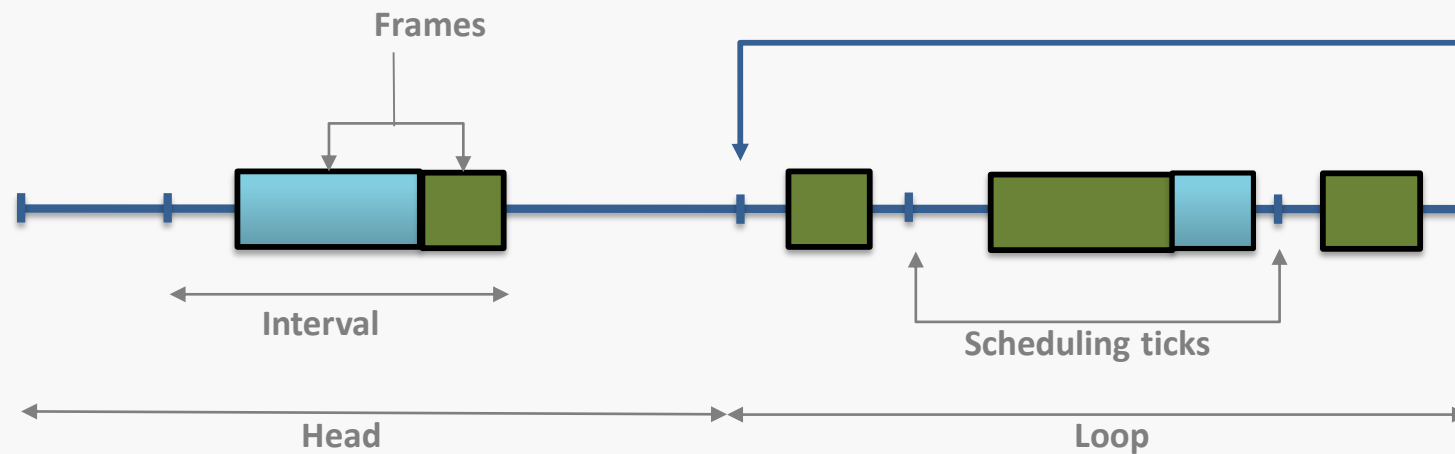
```
source ast_realtime_ms;  
clock c2 = 2 * ast_realtime_ms;  
clock c3 = 3 * ast_realtime_ms;  
  
agent Smith(uses realtime, starttime=1 with c3) // advance from 0  
{  
  body start // infinite loop  
  {  
    f1();  
    timebudget B1, advance 1 with c3;  
    f2();  
    timebudget B2, advance 2 with c2;  
  }  
}
```



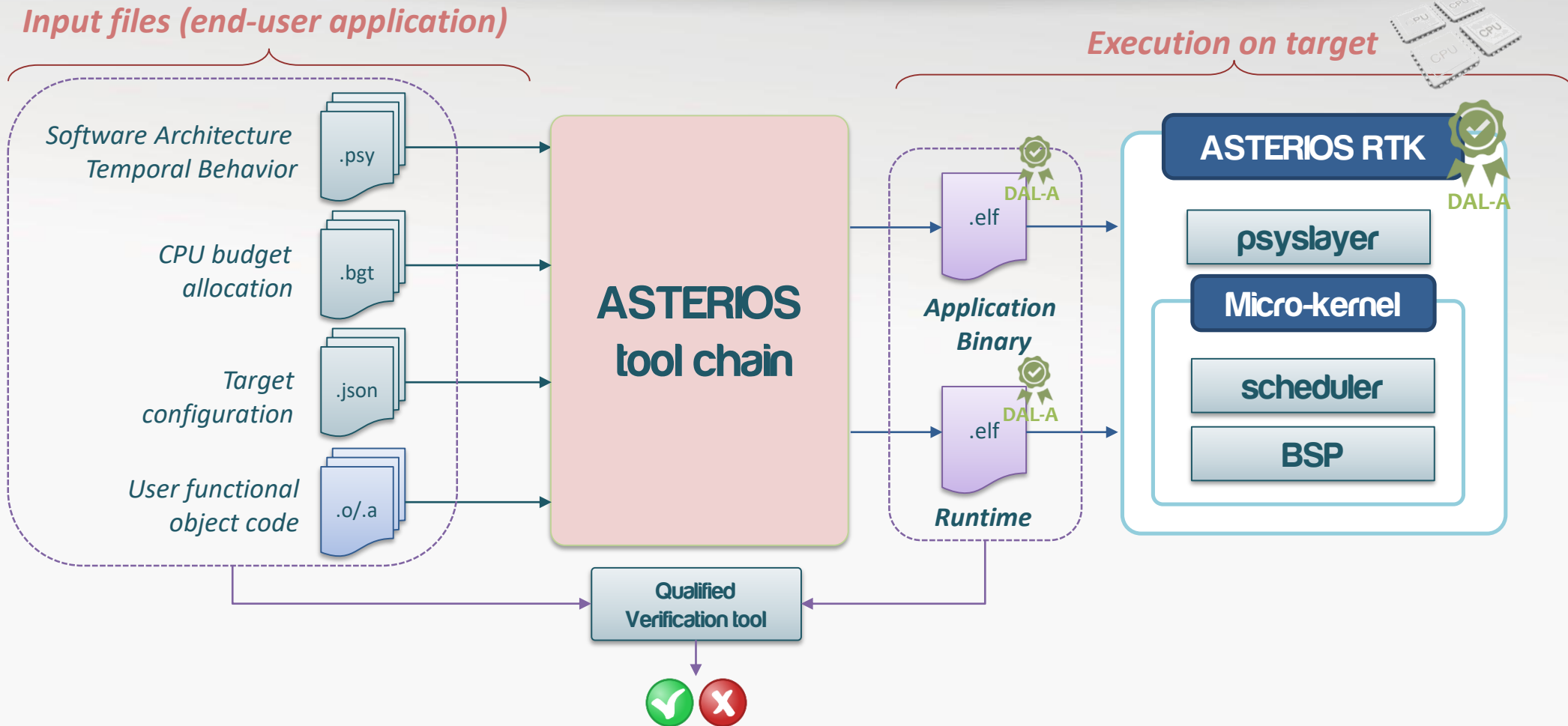


Repetitive Sequences of Frames (RSF)

- Offline, preemptive, periodic and fully static scheduling plan composed of frames:
Static time allocation for one task
 - Frame defined by a quota (part of the budget)
- Ensures that all CPU budget requirements are satisfied



ASTERIOS suite and certification strategy



- **Tool qualification (DO-178C §12.2.1):**

“it is used to *eliminate, reduce or automate software life cycle processes*”, without its output being itself verified



Tool qualification

- Tool Qualification Criteria and levels (DO-178C §12.2)

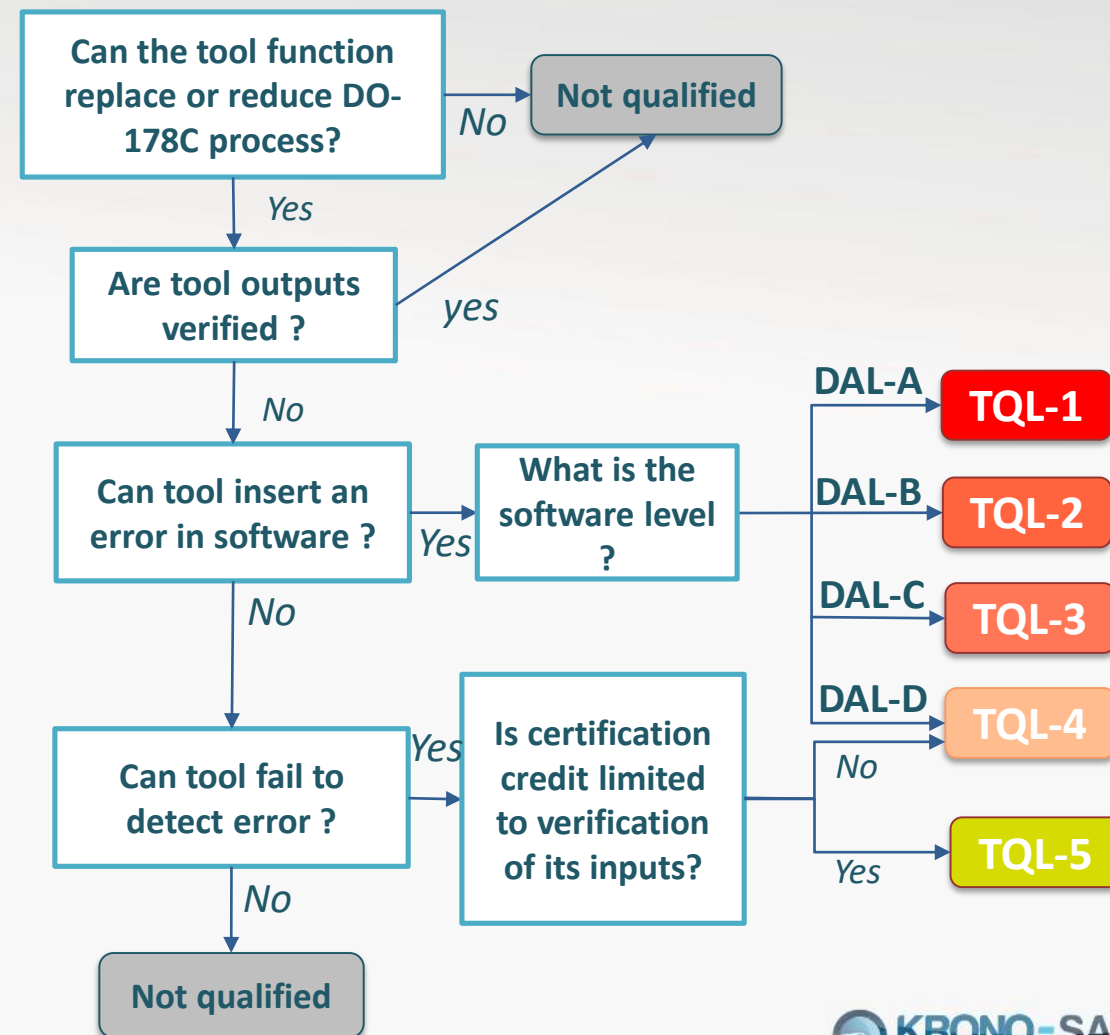
- a. Criteria 1: A tool whose output is part of the airborne software and thus could insert an error.
- b. Criteria 2: A tool that automates verification process(es) and thus could fail to detect an error, and whose output is used to justify the elimination or reduction of:
 - 1. Verification process(es) other than that automated by the tool, or
 - 2. Development process(es) that could have an impact on the airborne software.
- c. Criteria 3: A tool that, within the scope of its intended use, could fail to detect an error.

Software Level	Criteria		
	1	2	3
A	TQL-1	TQL-4	TQL-5
B	TQL-2	TQL-4	TQL-5
C	TQL-3	TQL-5	TQL-5
D	TQL-4	TQL-5	TQL-5

- ASTERIOS Checker is qualified at TQL-5
- Once the TQL is determined, the Tool Qualification Document Guidance (DO-330/ED-215) applies

January 30, 2020

- Identifying the TQL [*]

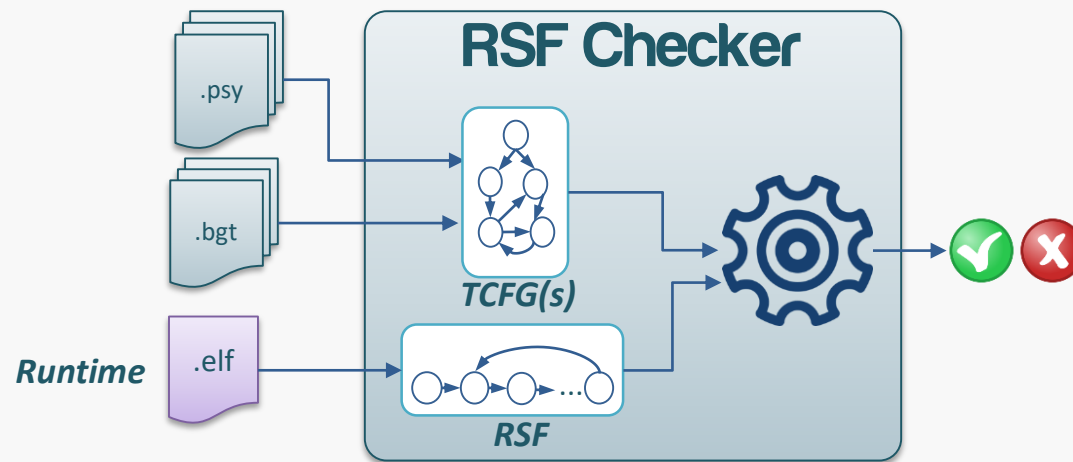


ERTS'20



RSF Checker

- Ensures that the scheduling plan produced by ASTERIOS tool chain is correct.
 - Property: for each agent, the RSF provides the CPU time for all EAs with respect to the input budget files.

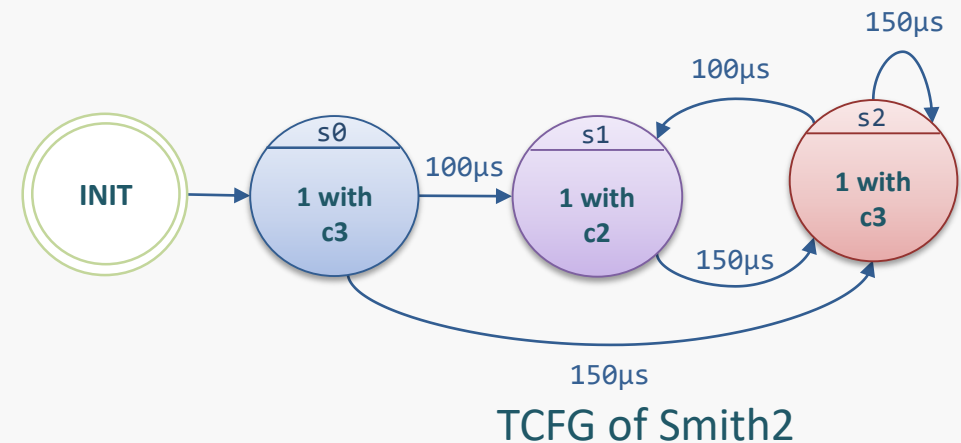


Formalization of a Psy agent

- **Temporal Control Flow Graph (TCFG):** cyclic directed graph (S, T)
 - S : set of states, where s corresponds to a temporal constraint, i.e., an **advance** statement (including INIT state)
 - $T \subseteq S \times B \times S$: set of transitions, where
 - $B \subseteq \mathbb{N}^*$: budget values (as defined by .bgt file(s))
 - $tr \in T$ is identified by (s_i, b, s_j) with $b \in B$: EA containing the functional C code between two **advance** statements (i.e. s_i and s_j) requiring the CPU budget b .

```
source ast_realtime_ms;
clock c2 = 2 * ast_realtime_ms;
clock c3 = 3 * ast_realtime_ms;

agent Smith2(uses realtime, starttime=1 with c3) // node s0
{
  body start
  {
    f1();
    if (condition) {
      f2();
      timebudget B1, advance 1 with c2; // node s1, B1=100µs
    }
    f3();
    timebudget B2, advance 1 with c3; // node s2, B2=150µs
  }
}
```

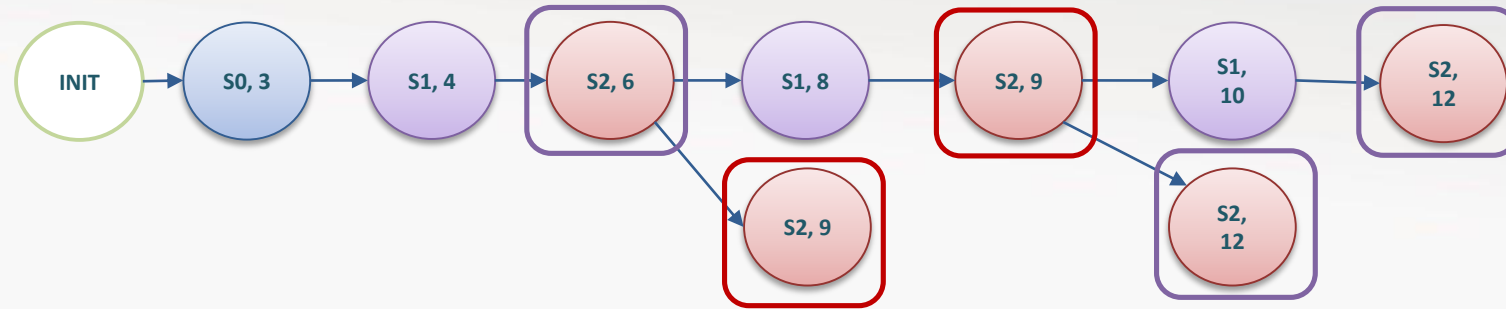


Verification of CPU budgets

- **Simultaneous exploration of the *TCFG* and the *RSF*.**

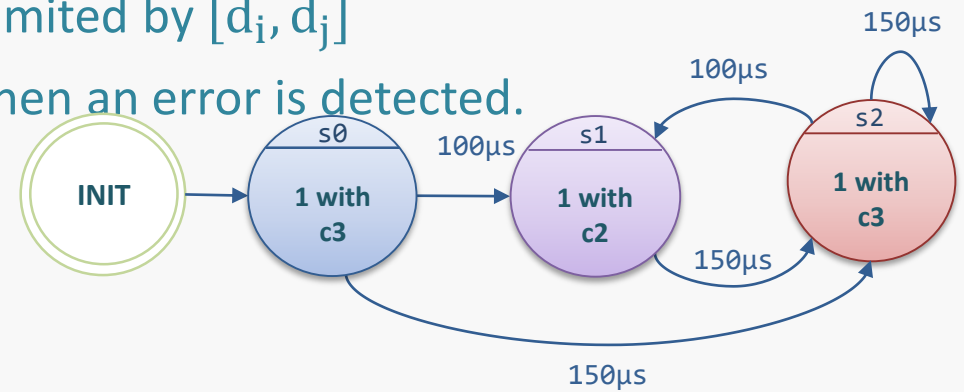
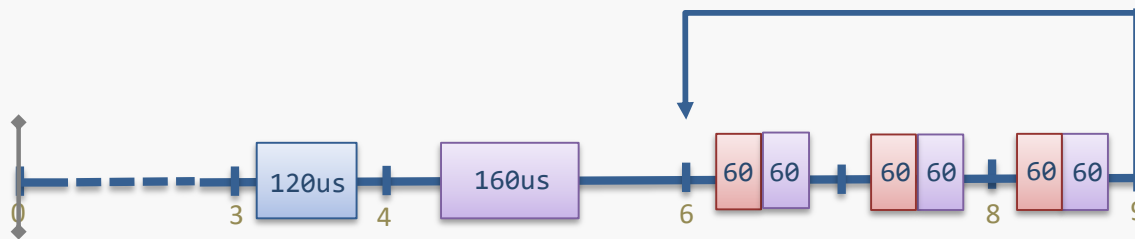
- Compute execution paths

- Sequence of (s_i, d_i) where $s_i \in S$ and d_i the exploration date of s_i , starting from INIT



- and check $b \leq \sum f_1, f_2, \dots, f_m$ of the interval(s) delimited by $[d_i, d_j]$

- and stop when exploring “equivalent states” or when an error is detected.





Experience feedback of Safran Electronics & Defense

- In-house development of verification tools for third-party non-qualified code generators is difficult and costly
- ASTERIOS Checker performs more complex verification than those implemented by a verification tool that enforces a set of coding rules, or syntactic transformations.
- Use of ASTERIOS toolchain:
 - landing system, engine regulation, etc.
 - Typical applications 700k LOC (dozen periodic tasks)
 - No state explosion issue for RSF Checker
- Final qualification is planned for the end of the year



Conclusion

- **ASTERIOS tool-suite and its certification strategy**
 - Non-qualified tool chain
 - DO-330 qualified tool **ASTERIOS Checker (TQL-5)**
- **Perspective**
 - Enable incremental certification of ASTERIOS application: multi-DAL applications



KRONO-SAFE

Safe design in real-time



Thank You

Questions

visit our website krono-safe.com

January 30, 2020