BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF CONTROL AND INSTRUMENTATION

CENTRE FOR APPLIED CYBERNETICS

Automatic Implementation of State Automata into 32-bit RTOS

<u>Pavel Kučera</u>

Ondřej Hynčica, František Zezulka

Content

1. Motivation
2. Formal Methods
3. Strategy of the Control System Design
4. Automation Design Tool
5. Conclusion

Motivation

Failing of the control system causes financial lost or even casualties

1979, USA Pennsylvania, Three Mile Island nuclear power plant. Over 140,000 people evacuated within a 15 mile area.

source: www.atomicarchive.com

1982, Therac-25, a compounding of process design, and implementation failures, software defect caused massive radiation killing 3 people.

spurce: Levenson, Nancy. *Safeware*, Reading, Mass.:Addison-Wesley, 1995

1985, Cement factory, a failure of 8080-based control system caused a large pile of boulders (about 6-8 feet in diameter) to pile up on top of the conveyor (about 80 feet up), eventually falling off and crushing several cars on the parking lot, and damaging a building.

source: Levenson, Nancy. *Safeware*, Reading, Mass.:Addison-Wesley, 1995

Motivation

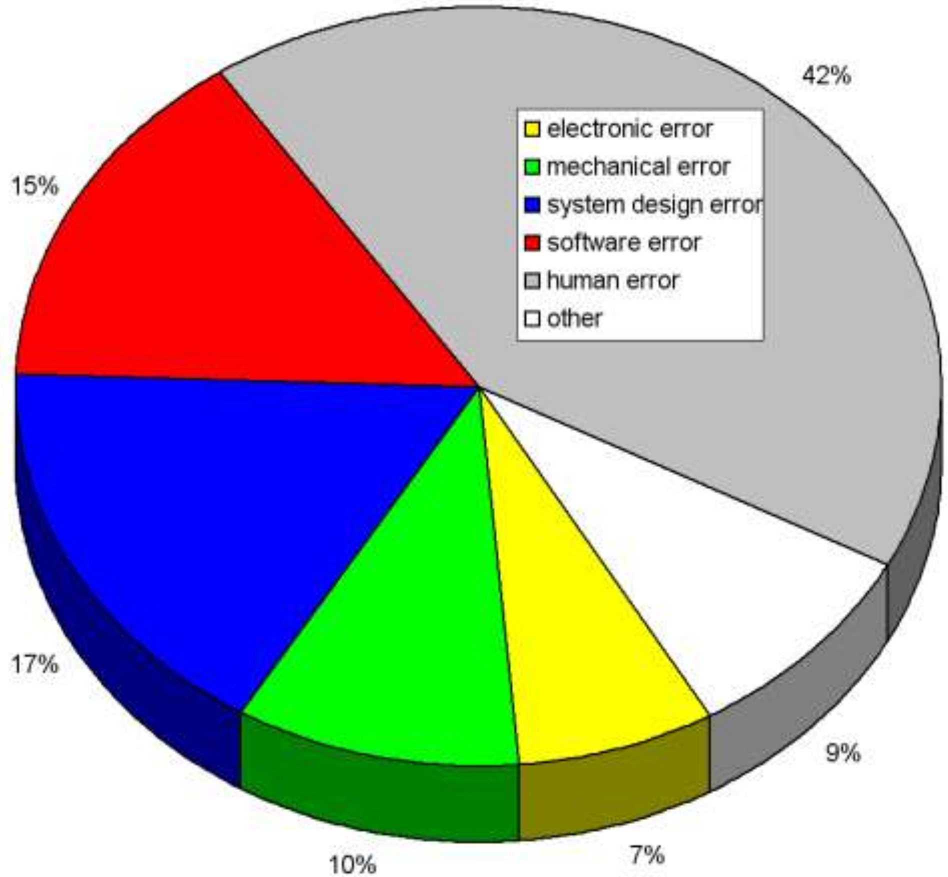
Failing of the control system causes financial lost or even casualties

2008, Trinec Stell, inoperability of the real-time diagnostic system of the continuous casting process caused 2 mil. EUR financial lost in 2008.

2009, D.C. Metro Red Line Crash, a Red Line Metrorail train crashed into a stationary train between Ft. Totten and Takoma stations. Nine people died and more than 70 people were injured. A train control system that should have prevented this deadly Metro crash failed in a test conducted by federal investigators.

source:www.washingtonpost.com

Motivation

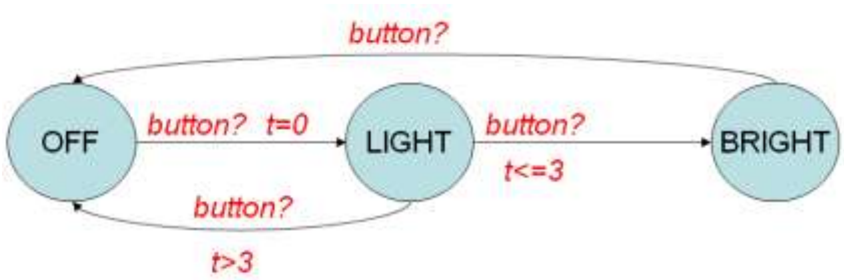


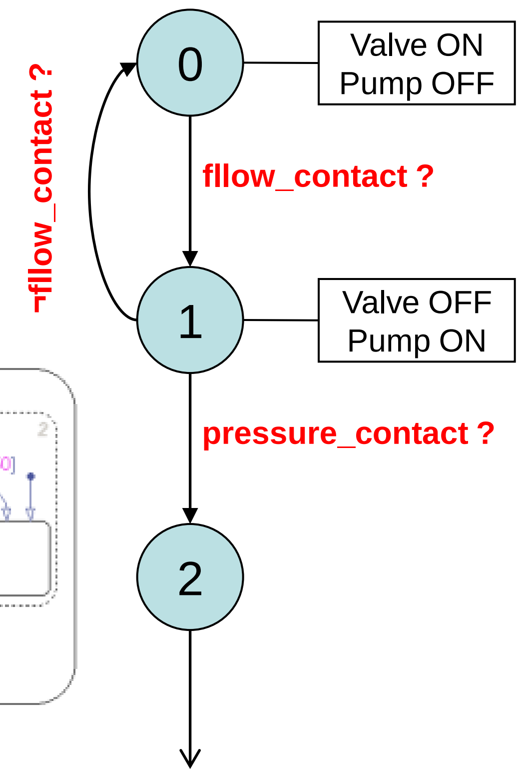
Source: Systems Failure Analysis, Safety and Reliability Society (www.sars.org.uk)

Hypothesis

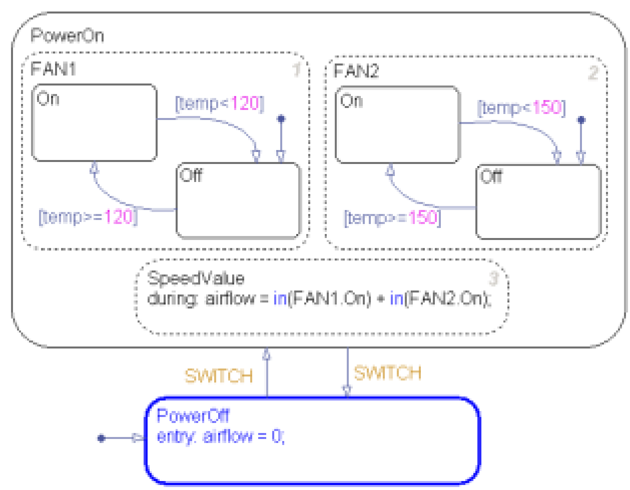
1. Control system is wrongly specified
2. Control system is not entirely specified
3. Implementation of the specification is not complete
4. Implementation of the specification is faulty
5. Unpredictable circumstances

Formal Methods

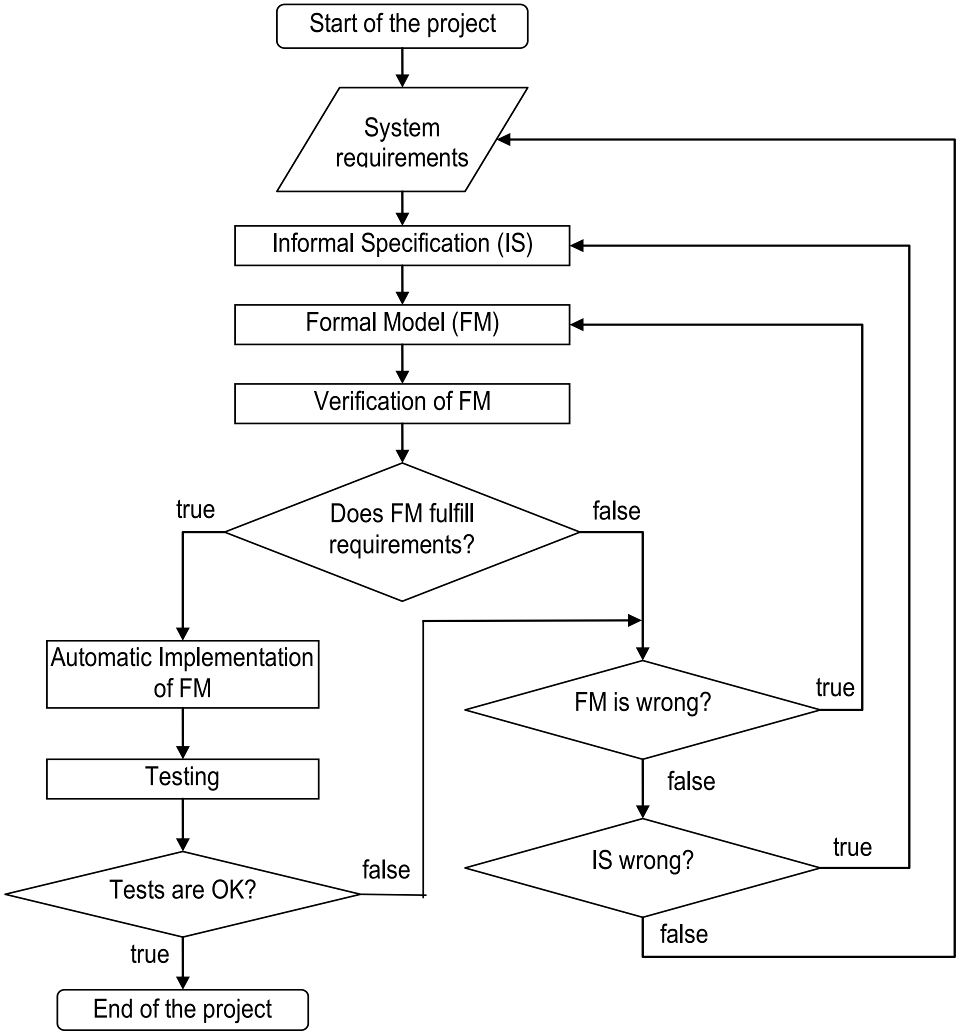




- IAR Visual State
- UPPAAL
- Automaton Laboratory
- FSM Library
- Ptolemey II
- Grapher
- Autograph
- StateFlow



Strategy of the Control System Design



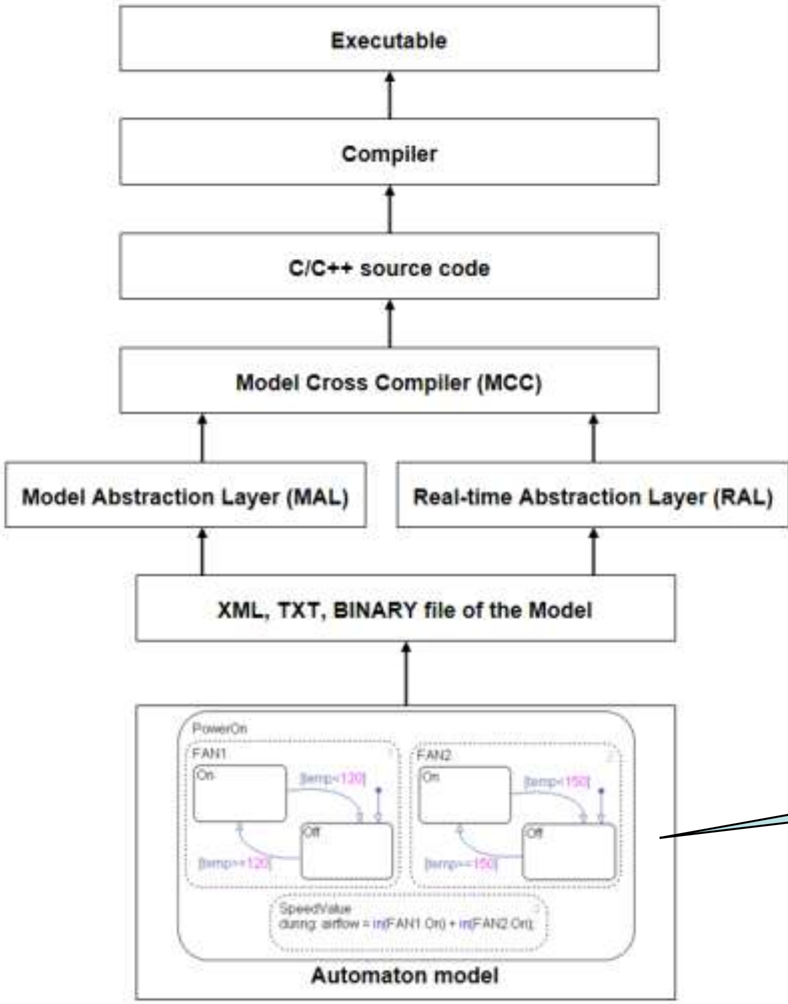
Automation Design Tool

Automation design tool for real-time embedded system design solves step *Automatic Implementation of FM.*

Formal model of the system is based on automata created in a designing and verification tool.

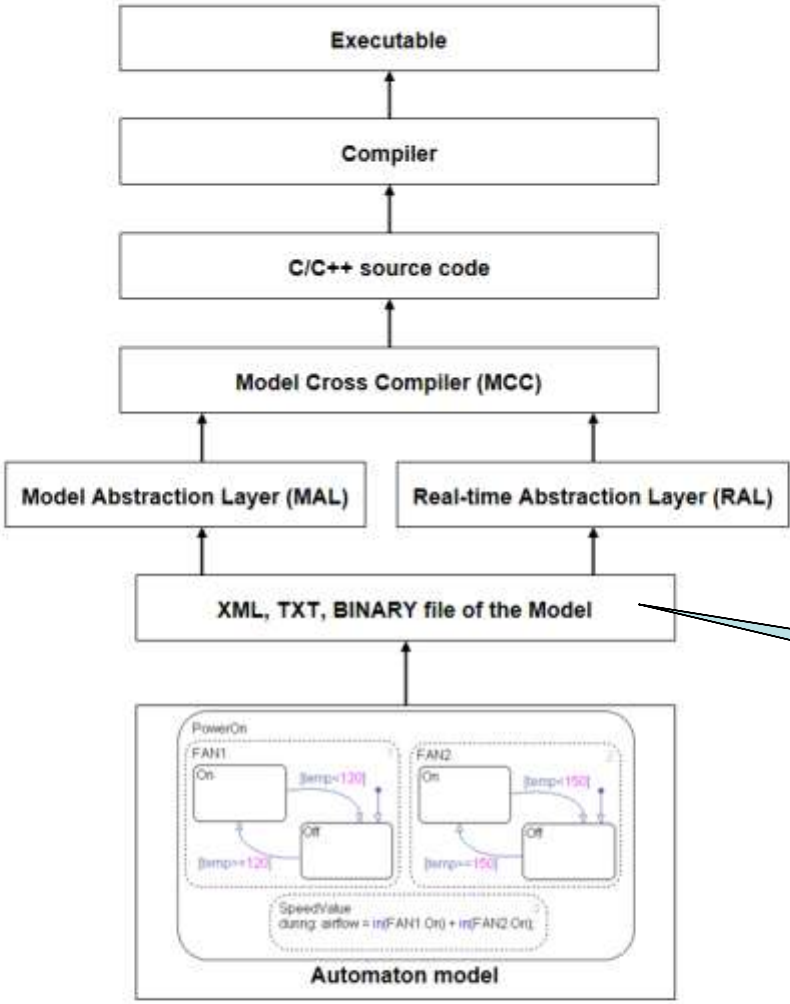
This formal model can be automatically converted into the objects that are easy to implement in 32-bit real-time operating systems and these objects results in executable code.

Automation Design Tool



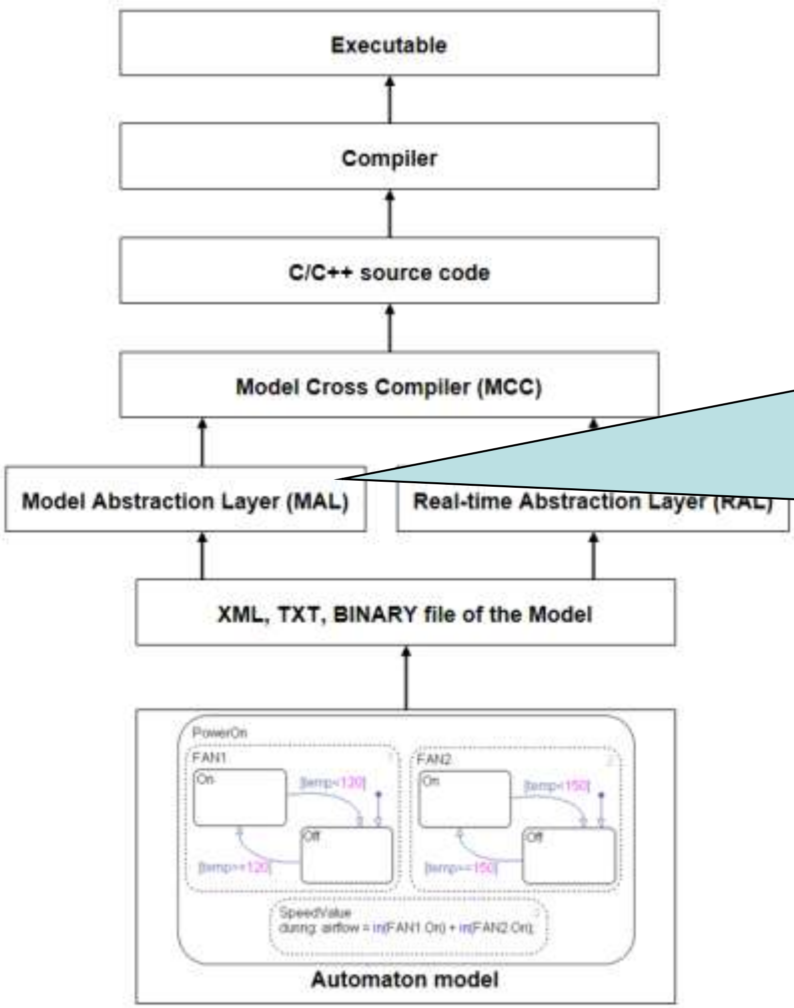
Formal model is created, simulated and verified using automaton diagrams.

Automation Design Tool



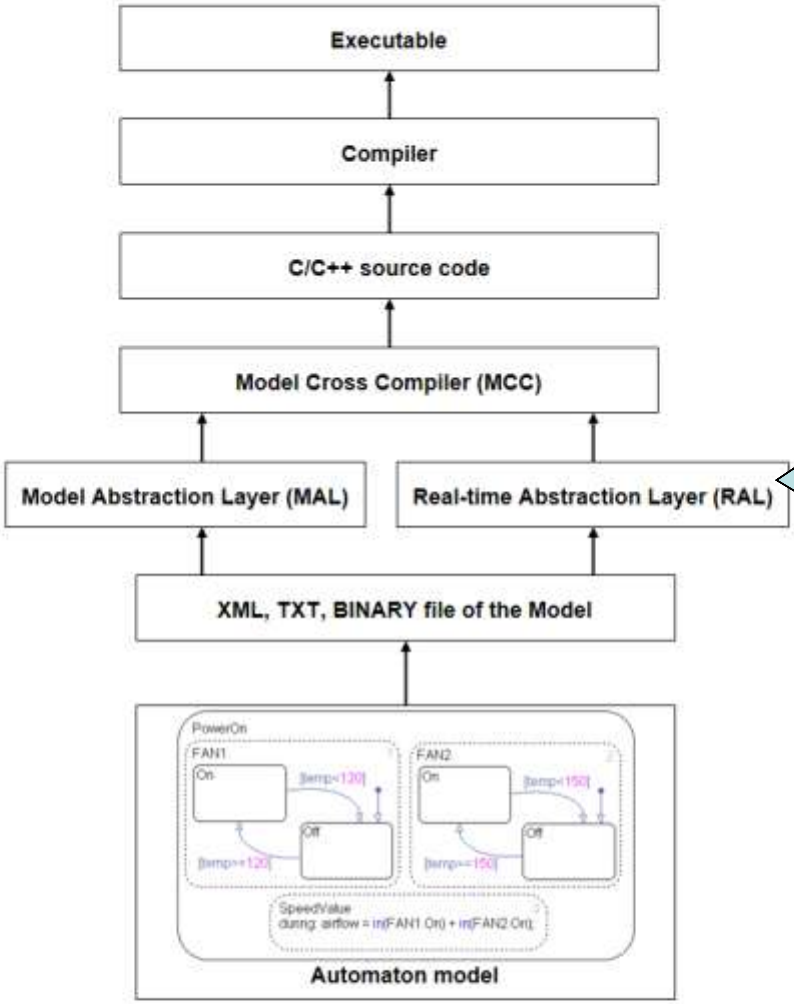
Formal model is represented in a relevant form.

Automation Design Tool



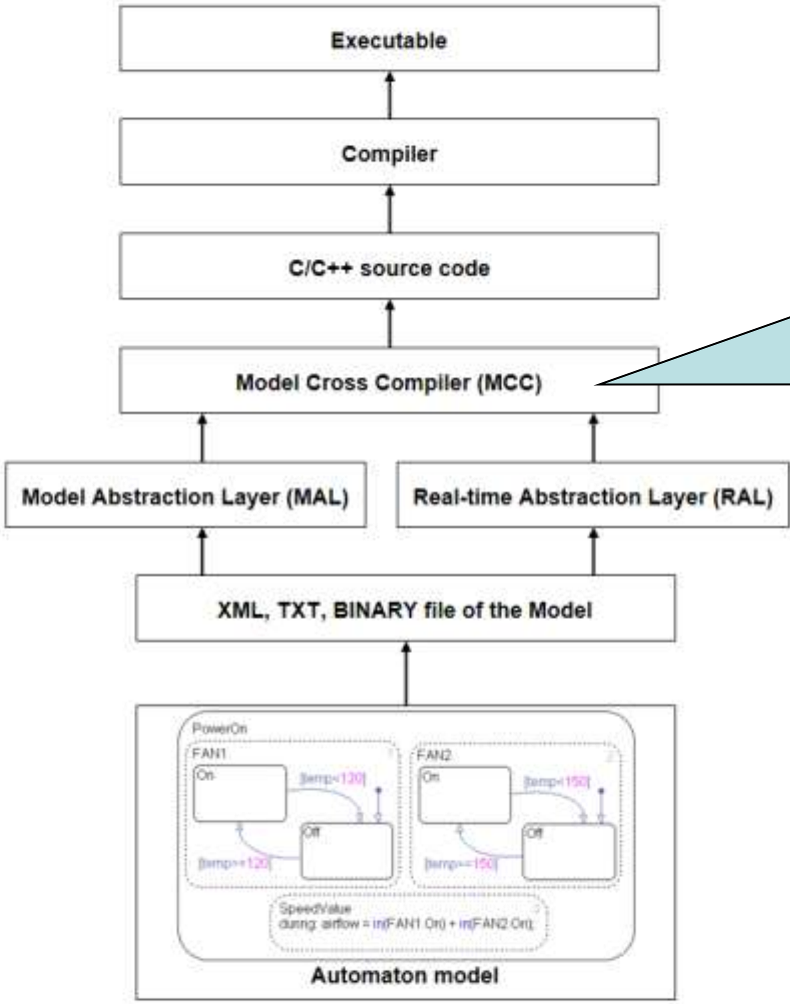
The purpose of the MAL (Model Abstraction Layer) is to create an independent interface between timed automata model and real-time entities (processes, threads, synchronizations, IPC) that will be automatically implemented. MAL is independent on the target HW and target operating system.

Automation Design Tool



The purpose of the RAL (Real-time Abstraction Layer) is to create a unified structure describing real-time behavior of the system. RAL is also independent on the target HW and target operating system.
It is also responsible for auto verifying feature – RTOS will be permanently check time behavior of the process.

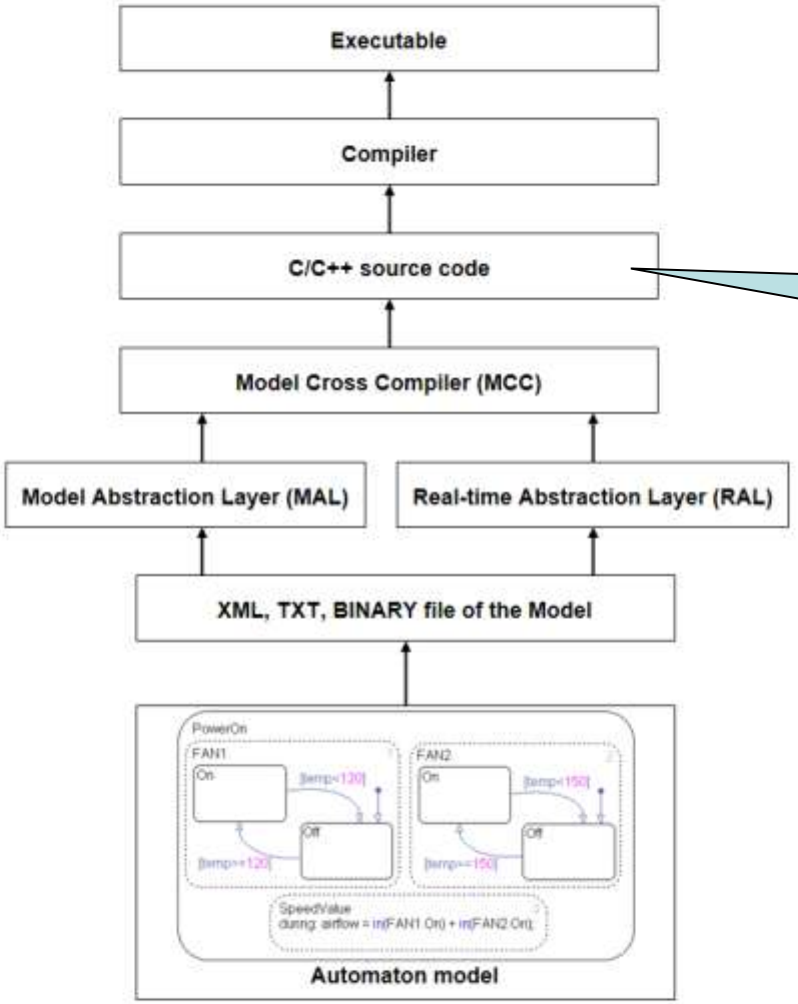
Automation Design Tool



The Model Cross Compiler (MCC) is an interface for MAL and RAL transferring formal model of the system from the description tool into C/C++ source code.

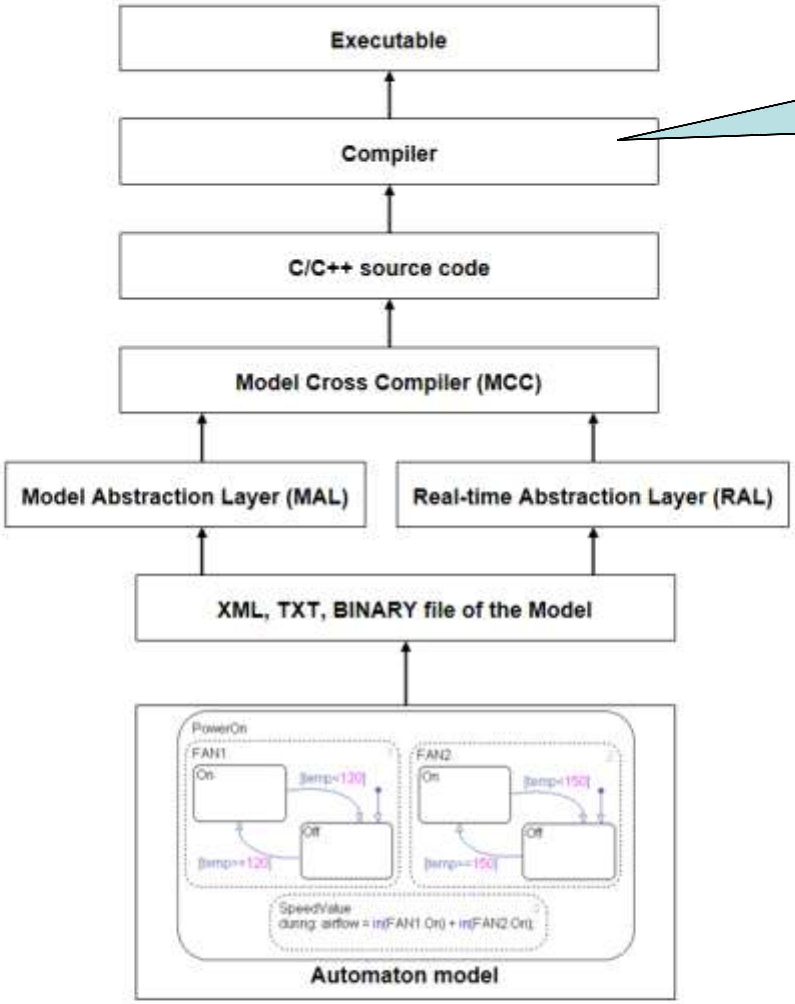
MCC strictly depends on the selected real-time operating system and programming language .

Automation Design Tool



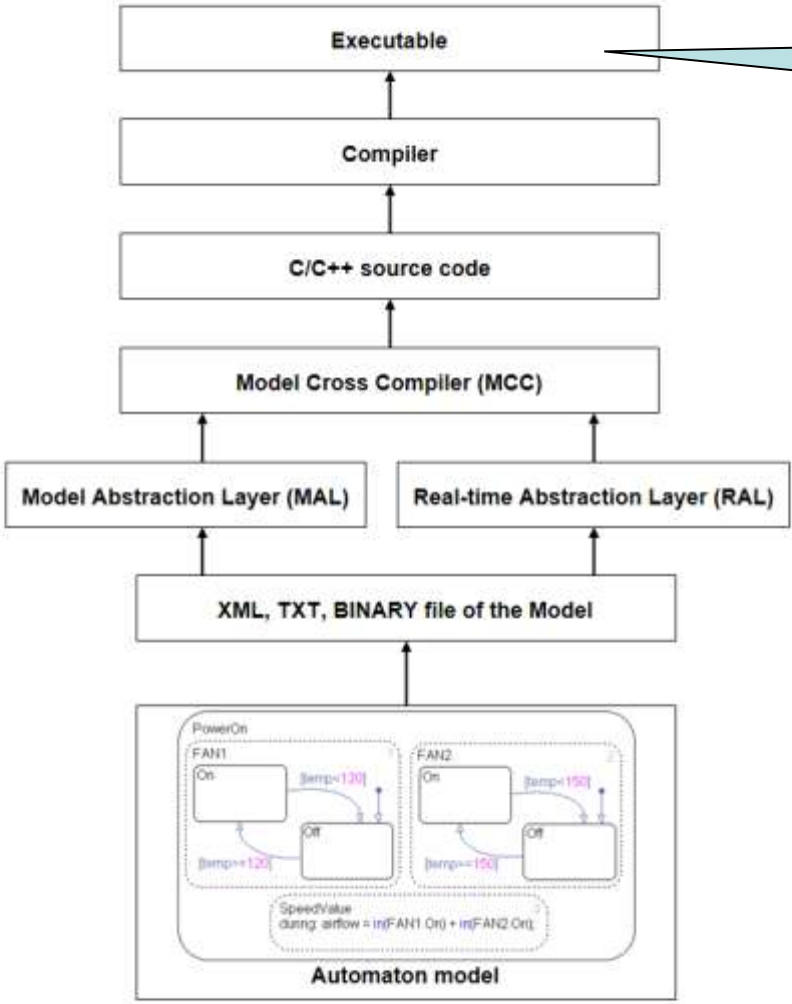
The source code is automatically generated by the MCC.

Automation Design Tool



The source code can be included into the corresponding compiler and executable code for the target HW platform is generated.

Automation Design Tool



Executable code was created automatically without human intervention.

Target platforms

POSIX (IEEE 1003.1) standard based on UNIX OS
Win32 not standardized but a lot of users

32-bits Real-time operating systems

- QNX
- RTLinux
- VxWorks
- Windows CE
- Windows RTX

32-bits characteristic

- Computational power
- Robustness
- Designing tools
- Interfaces
- Cost
- Developers

Current state

RAL and MAL layers are specified in UML.

RAL and MAL layers with limited features are realized for XML source from UPPAAL.

KUČERA, P.; HONZÍK, P. Automation of Real- time Embedded System Design. In *The 13th World Multi-Conference on Systemics, Cybernetics and Informatics.* WMSCI. Orlando: WMSCI, 2009. s. 23-26. ISBN: 978-1-934272-59- 6.

KUČERA, P.; HYNČICA, O.; HONZÍK, P.: PCI- 1710 RTX; *RTX Driver model for PCI1710 DAQ*. ÚAMT. (software).

KUČERA, P.; HONZÍK, P.; HYNČICA, O.: PCI- 1002 RTX; *RTX Driver model for PCI1002 DAQ*. ÚAMT. (software).

KUČERA, P.; HYNČICA, O.; HONZÍK, P.: RTDSBP; *Real- time diagnostiský systém pro detekci nebezpečí průvalu*. Třinecké železárny, a.s.. (ověřená technologie)

Questions