SCADE: Industrial Success of a Synchronous Language and its Future Challenges

In honour of Gérard Berry and Jean-Jacques Lévy

GGJJ 2011, Gérardmer Feb. 3rd 2011
Amar Bouali
Esterel Technologies
amar.bouali@esterel-technologies.com
Objectives

- Explain why SCADE is having success in the industry
- Share some facts and figures about industrial use-cases
- Highlight some scientific challenges for SCADE
Background
Synchronous Languages

- Created in the early 80’s from a joint research effort by control engineering and computer sciences researchers

- Lustre
  P. Caspi – N. Halbwachs
  (VERIMAG)

- Signal
  A. Benveniste – P. Le Guernic
  (IRISA)

- Esterel
  JP Rigault, JP Marmorat – G. Berry
  (INRIA/Ecole des Mines)
Mid-80’s

- SCHNEIDER Electric develops SAGA as the industrial version of Lustre for control command software for nuclear plants
- AIRBUS develops SAO, a formalism close to Lustre
- Verilog industrializes SCADE in collaboration with Schneider and Airbus.

Fall 80’s:

- AT&T experiments Esterel on models and verify telephone protocols
- DASSAULT Aviation designs embedded applications with Esterel for the Rafale
- CISI, then Simulog, industrializes Esterel Studio in close collaboration with Dassault.
In the 90’s:
- Verilog then Telelogic develops SCADE Suite development environment
- Simulog develops Esterel Studio

1999: Esterel Technologies, starts up born from INRIA, created from Simulog

2002: Esterel Technologies acquires SCADE from Telelogic

2007: ET extends Scade/Lustre with Esterel concepts in collaboration with Verimag and Paris 6
Safety, Standards & Costs
Safety Critical Systems Requirements

- High-level of reliability required
- Minimize the risk of error introduction and maximize the error detection through intensive verification
- Minimize delay to market
- Compliance to safety standards (DO-178B for avionics, EN 50128 for railways, EN 60880 for nuclear, IEC 61508 for industry)
The Process Model

System Requirements

- SW High-Level Design
- SW Detailed Design
- SW Coding

Verification

System Validation

SW Integration Testing
Probabilities and Categories of Failures

- Extremely improbable
- Remote
- Extremely remote
- Extremely improbable
- Probable
- Minor
- Hazardous
- Major
- Catastrophic

- Unacceptable
- Acceptable
### Verification efforts depend on Assurance Levels

<table>
<thead>
<tr>
<th>Level</th>
<th>Effect of anomalous behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Catastrophic failure condition for the aircraft (<em>e.g.</em>, aircraft crash).</td>
</tr>
<tr>
<td>B</td>
<td>Hazardous/severe failure condition for the aircraft (<em>e.g.</em>, several persons could be injured).</td>
</tr>
<tr>
<td>C</td>
<td>Major failure condition for the aircraft (<em>e.g.</em>, flight management system could be down, the pilot would have to do it manually).</td>
</tr>
<tr>
<td>D</td>
<td>Minor failure condition for the aircraft (<em>e.g.</em>, some pilot-ground communications could have to be done manually).</td>
</tr>
<tr>
<td>E</td>
<td>No effect on aircraft operation or pilot workload (<em>e.g.</em>, entertainment features may be down).</td>
</tr>
</tbody>
</table>
Limits of Tradition
Software engineering
Traditional Methods Limits...

- Lack of SW design quality & accuracy
  - Ambiguous and incomplete, especially for control logic
  - Miscommunication between System & SW engineering

- Error-prone manual coding and verification
  - Hard to detect *early* unintended function
  - Late verification upon changes

- Do not scale-up to today’s system size and complexity
The Cost of Error Detection

<table>
<thead>
<tr>
<th>Analysis</th>
<th>Conceptual Design</th>
<th>Programming</th>
<th>Unit Testing</th>
<th>System Testing</th>
<th>Operation</th>
</tr>
</thead>
</table>

- Introduced errors in %
- Detected errors in %
- Cost of an error in K$

Time (not linear)
This is where SCADE has solutions…
Data-Flow for Continuous Control

\[ K_p \varepsilon + K_i \int \varepsilon \, dT \]
Inspired from SynchCharts of [André et al] at I3S (Nice)
Scade 6: Unified Synchronous Paradigms

- A Conservative Extension of Synchronous Dataflow with State Machines, EMSOFT ’05 [Colaço, Pagano, Pouzet]

Specify better, verify less!
Reconcile System and Software Engineers
Certified Flow

- Model Verification
  - Testing and formal verification with model-checking (Prover SAT)
  - Structural coverage of model with MC/DC criteria for Boolean decisions
  - WCET analysis with Abstract Interpretation techniques (AbsInt)

- Automatic code generation with a certified CG, written in Objective CAML
  - First CAML program qualified by authorities for Level A!
  - [Pagano, Chailloux] *Certified Development Tools Implementation in Objective Caml*, PADL 08

What You Prove Is What You Embed!
Safety by construction

No uninitialized variables
Bounded loops and memory
Deterministic code
Predictable execution time
The Industrial Success
SCADE in Aerospace & Defence

**Commercial Programs**
- Airbus A340 & A380
- Boeing 787
- Eurocopter EC135/145/155/225
- Eurocopter AS 350
- Sikorsky S76D
- Dassault Falcon 7X, Falcon SMS
- Sukhoi Superjet 100
- ARJ-21 (Chinese Regional Jet)
- Cessna Citation Mustang
- Cessna Citation Encore+
- Cessna Citation XLS+
- Be200e (Amphibious Jet)
- Eclipse 500
- Embraer Phenom 100/300
- Gulfstream G500
- Mitsubishi MRJ

**Defense Programs**
- Airbus A400M
- Dassault Rafale / Mirage 2000-9
- EADS Astrium M51 Missile
- MBDA FREMM Frigate Missile Launcher
- Eurocopter Super Puma, NH90
- Chinese Helicopters Z8, Z10
- US Air Force F16
- US-101 (Presidential Helicopter)
- Watchkeeper (UAV)
- Neuron (UAV)

**Space Programs**
- ARIANE 5 Launcher
- ATV Launcher
- ESA’s VEGA Launcher
- Shenzhou II Rocket
- CEV Program
SCADE in the Airbus A380

- SCADE is present in the following A380 systems:
  - Flight Control system
  - Flight Warning system
  - Electrical Load Management system
  - Anti-icing system
  - Braking and Steering system
  - Cockpit Display system
  - Part of ATSU (Board / Ground comms)
  - FADEC (Engine Control)
  - EIS2 : Specification GUI Cockpit:
    - PFD : Primary Flight Display
    - ND : Navigation Display
    - EWD : Engine Warning Display
    - SD : System Display

- 8 M LOC automatically generated!
Programs: EC135, EC145, EC155, EC225
Company: Eurocopter
Application: Autopilots
Results:
- 90% of the code generated automatically
- Development time divided by 2
- Turn around cycle performed in less than 48 hours
- EASA certification
- No code review, no unit testing on SCADE Suite generated code
SCADE in Railways

- **Brazil**
  - Sao Paulo subway

- **China**
  - Nanjing subway Line 2
  - Beijing subway Changping Line

- **France**
  - French Railways (RFF) – whole network
  - Paris subway
  - Lyon subway
  - Marseille subway

- **Hong Kong**
  - Hong Kong subway

- **Portugal**
  - Porto subway

- **Russia**
  - Russian Railways (RZD)

- **Singapore**
  - Singapore subway

- **Taiwan**
  - Taipei subway

- **Turkey**
  - Ankara subway

- **UK**
  - British Rail (Cambrian and Ester lines)
  - Eurotunnel
Railways

- **Automatic Train Control & Protection Systems**: ETCS & CBTC...
  - Includes emergency braking, overspeed protection, vehicle speed control, ATP/ATO
  - Door opening & departure interlocks
  - On-board displays
- **Control Centers**: Fault reporting & Interlocking Displays
- **Interlockings**
- **Train detection systems (Axle counters...)**
- **Level Crossing Protection**
CBTC Architecture

- On-board computers: ATP / ATO
- On-ground computers: IOC, ZC
Speed & Braking Profile with SCADE

map<<SegmentsNumber>>

GetMinOver3

SL1
SL2
SL3

TSL

V1
V2
V3

Min

SL1
SL2
SL3
TSL

int

int

bool

int

int

int
- Standard component models for signals and points as State Machines
- A station is a network of such, with precise route reconfiguration rules
- Alstom built a 20,000 state machine components for an SNCF station!
- Challenging formal verification problem
SCADE Successes in Nuclear I&C Software

- Armenia
  - METZAMOR
- Belgium:
  - TIHANGE
- Bulgaria:
  - KOLZODUY
- China:
  - QIN SHAN
- Czech republic:
  - DUKOVANY 1,2,3,4
- Lithuania:
  - IGNALINA
- France:
  - BUGEY 1,2,3,4
  - FESSENHEIM 1, 2
  - CELESTIN (Experimental reactor)
  - CATTENOM 1,2,3,4

**21 Reactors (PWR & VVER) in Production using ESTEREL SCADE!**
- AREVA NP (France)
- CEA (France)
- DS&S (France, USA, UK)
- Hollysys (China)
- KAERI (Korea)
- Korea Power (Korea)
- NPIC (China)
- Rolls Royce Marine (UK)
- Schneider (France)
- AREVA TA (France)
SCADE offers ways to improve SW design quality and reliability
   - SW Engineers switch from SW coding to SW design, focusing more on their problem and IP

Early verification raise up the confidence and reduce verification costs

Certified automatic code generation reduces risks of error introduction and removes verification effort
Next Challenges
Joint initiative with the French CEA LIST laboratory

SysML framework Papyrus connected to SCADE

Bring formal semantics to SysML diagrams
  - Clean definition of interfaces and modularity
  - Clean refinement rules from SysML to SCADE
Language Extensions

- Richer Iterative schemes and data-types (ranges, sized integers, float)
- Object-orientation for *dynamic* control?

The goal of the USAF is to develop UASs that are increasingly automated, modular, and sustainable. In addition the expansion of capabilities and theatres of operation for the UASs means that there is a requirement for the UASs to operate in environments with both military and commercial aircrafts. Here FAA insists that UAS operations have an equivalent level of safety to those of manned aircrafts."
Scaling & Optimizations

- Code Generation
  - Optimization of large data-structures handling and program rewriting for control structure factorization
  - Distributed control over networks of ECUs

- User interface
  - Handling of large structures and arrays
More powerful techniques for verification with data
  - Mix model-checking, static analysis, and other theories
  - Information on data ranges, control points reachability
  - Floating-point decision procedures

Proof generation for verification in Theorem Provers

Assume-Guarantee reasoning
  
  *Assuming P is true, prove that Q is true*
Integration in Real-Time Environment

- Networks of distributed control (GALS models)
  - Relaxed synchronous hypothesis keeping the desirable properties
  - [Halbwachs and Mandel] *Simulation and verification of asynchronous systems by means of a synchronous model*, ASCD 06
  - [Camus] *A verifiable architecture for multi-task, multi-rate synchronous software* ERTS 08
- Integration in Time-Triggered Architectures
  - [Capsi, Le Sergent] *Applications From Simulink™ To SCADE/Lustre To TTA: A Layered Approach For Distributed Embedded*
ET has been successful in providing SCADE as a synchronous approach for the safety-critical embedded market.

ET is grateful to the many men years of fruitful research from YOU!

ET continuously works in close collaboration with academics and is involved in several funded R&T projects (*Pôle de compétitivité*, European projects, etc.)
But success, really, is this!

- Terex, world-wide leader in fixed and mobile cranes
- We presented SCADE to Terex Italy last June
- During a corporate meeting, the Italians suggested to their German and American colleagues to select and buy a French technology!
Thank you!

Questions ?