A Formal Model of Lower System Layers

Julien Schmaltz
Saarland University - Computer Science Department
Saarbrücken, Germany
A Motivation Example

- eCall
  - Automatic emergency call system
  - A phone call is automatically emitted when car sensors detect an accident

Formal Proofs of
- Applications
- Operating systems
- Compilers
- Processors
- FlexRay bus
Precise timing parameters
- Metastability
- Analog bit transfer correctness
- Connection between analog and digital

\[ \text{Precise timing parameters} \]
\[ \text{Metastability} \]
\[ \text{Analog bit transfer correctness} \]
\[ \text{Connection between analog and digital} \]
Outline

- Asynchronous communications
- Analog bit transfer correctness
- Connection with a fully digital world
Modeling Principles

- 3-valued logic:
  - 0, 1 for “low” and “high” voltages
  - $\Omega$ for any other voltage
- Signals are functions from time to $\{0, 1, \Omega\}$
- Transition from low (high) to high (low) via $\Omega$
- Clocks are offset/period pairs
  - Initial phase offset
  - Bounded drift of clock periods
  - We note $e_u(c)$ the date of edge $\#c$ of unit $u$
  - Edges have no width
Analog Register

Registers at rising clock edges
Analog Register

Setup and holding times determine a “metastability window”. Metastable means output voltage is neither 0 nor 1.
Analog Register

Input and control signals *defined* and *stable* in this window.
Analog Register

Transition after $t_{p_{min}}$. Final value after $t_{p_{max}}$. 
Sender creates a “safe sampling window”.

\[ e_s(c) \]
Receiver Starting Point

Receiver starting point is the first edge to be “affected”.

\[ e_s(c) \quad e_r(cy(c)) \]
$e_s(c) \quad e_r(c) \times(c)$

cy(c) \text{ defined as } Min \{\xi | e_r(\xi) + t_h \geq e_s(c) + t_{p_{min}}\}$
Good Sampling

\[ e_s(c) \quad e_r(cy(c)) \quad e_r(cy(c) + 1) \quad e_r(cy(c) + 2) \]

Sampling in the sweet spot from \( cy(c) + 1 \) to \( cy(c) + n + 1 \)
Outline

- Asynchronous communications
- Analog bit transfer correctness
- Connection with a fully digital world
Formal Definition of Registers

- Timed registers represented by function $tR_u(c, clk_u, In_u, ce_u, Out_u^0) \equiv tR_u^c$

- $tR$ generates a function of time for cycle $c$
  - $tR_u^{c-1}(e_u(c))$ if $ce$ is low
  - $\Omega$ if $ce$ and $In$ violate setup or holding times constraints
  - $tR_u^{c-1}(e_u(c))$ during $t_{p_{min}}, \Omega$ and $In_u(e_u(c))$ at $t_{p_{max}}$

- See previous diagram!
Safe sampling window large enough to entail \( n \) receiver cycles

\[
\text{BigEnough}(k, n) \equiv \tau_s \cdot (k + 1) \geq \tau_r \cdot (n + 2)
\]

- \( n + 1 \) cycles because of our weak hypothesis
- \( n + 2 \) cycles because of metastability
- \text{BigEnough} = \text{hypothesis on the relationship among clocks}
Correctness Theorem

Under our assumptions, if the sender creates a S.S.W. of length \( k \), receivers sample \( n + 1 \) times properly.

\[
\text{BigEnough Safe Sampling Window} \wedge \text{Correct Analog Control Signals} \\
\text{ce}_s(e_s(c)) = 1 \wedge \forall l \in [1 : k], \text{ce}_s(e_s(c + l)) \\
\wedge \text{Analog Connection} \\
\forall c, \text{In}_r = tR_s(c, \text{clk}_s, \text{ce}_s, \text{In}_s, \text{Out}_s^0) \\
\rightarrow n + 1 \text{ good samples} \\
\forall l \in [0 : n], tR_r^{cy(c) + 1 + l} = \text{In}_s(e_s(c))
\]
Outline

- Asynchronous communications
- Analog bit transfer correctness
- Connection with a fully digital world
Analog and Digital

- Bit lists on the digital side
- Signals, functions of time on the analog side
Analog and Digital

● $\gamma$ converts bit lists to signals

$$\text{bv2sp}(\gamma, l, clk) \equiv \gamma$$  do not generate metastability
 Analog and Digital

- $\zeta$ represents a synchronizer

\[
\zeta(s, t) \triangleq 
\begin{cases} 
  s(t) & \text{if } s(t) \in \{0, 1\} \\
  \epsilon x, x \in \{0, 1\} & \text{else} 
\end{cases}
\]
Analog/Digital Theorem

If the **digital sender** behaves properly, we obtain $n + 1$ good **digital samples** from the **analog transmission**.

\[ \forall c, \text{In}_r = tR(c, \text{clk}_s, \gamma(c\text{e}_s), \gamma(\text{In}_s), \text{Out}_s^0) \]

\[ \land \text{Modeling Hypotheses}(\text{bv2sp}, \text{BigEnough}) \]

\[ \land \text{Digital Sender Behavior} \]

\[ c\text{e}_s[c] = 1 \land \forall l \in [1 : k], c\text{e}_s[c + k] = 0 \]

\[ \rightarrow n + 1 \text{ good digital samples} \]

\[ \forall l \in [0 : n], \zeta(tR_r^{cy(c)+l+1}) = \text{In}_s[c] \]
Conclusion

- Formal model of lower system layers
  - Precise timing parameters and metastability
  - Connection with the digital world
- Embedding in Isabelle/HOL
  - Users concern with the last theorem and modeling principles
  - Part of the Verisoft repository
- Verification of a FlexRay-like Interface
  - Clock drift
  - Sample full messages
THANK YOU!!