A Formal Model of Lower System Layers

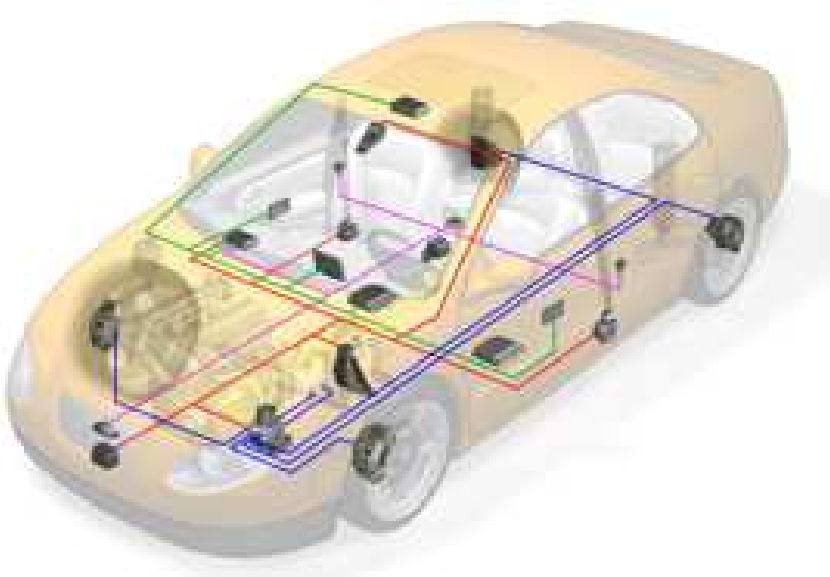
Julien Schmaltz

Saarland University - Computer Science Department

Saarbrücken, Germany

A Motivation Example

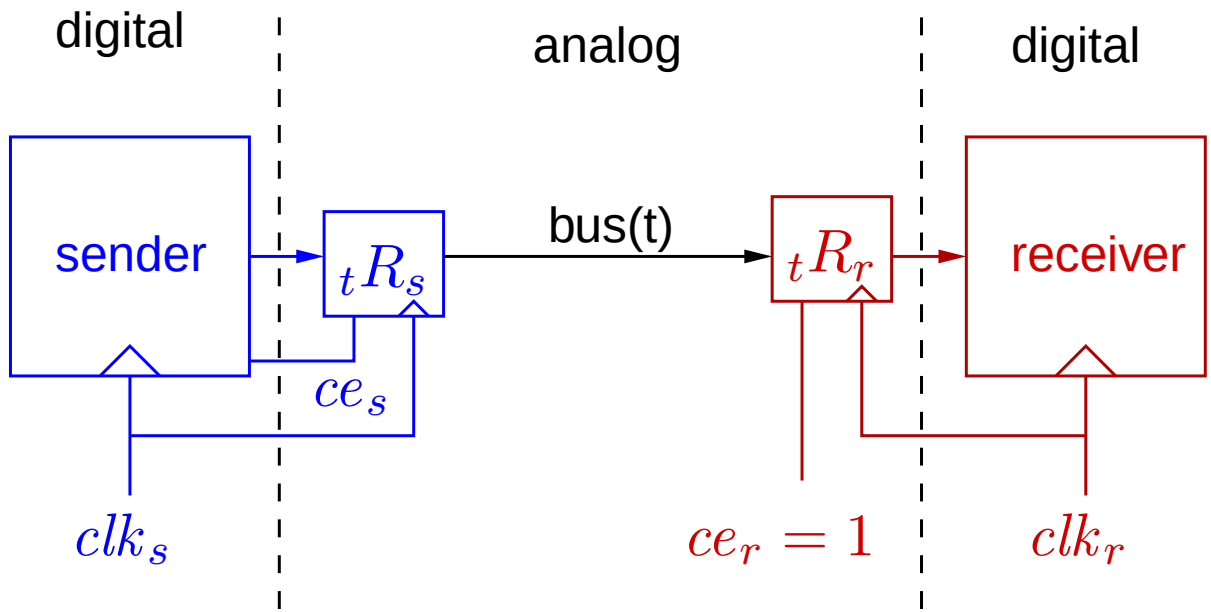
- eCall
  - Automatic emergency call system
  - A phone call is automatically emitted when car sensors detect an accident



Formal Proofs of

- Applications
- Operating systems
- Compilers
- Processors
- FlexRay bus

Contribution



- Precise timing parameters
- Metastability
- Analog bit transfer correctness
- Connection between analog and digital

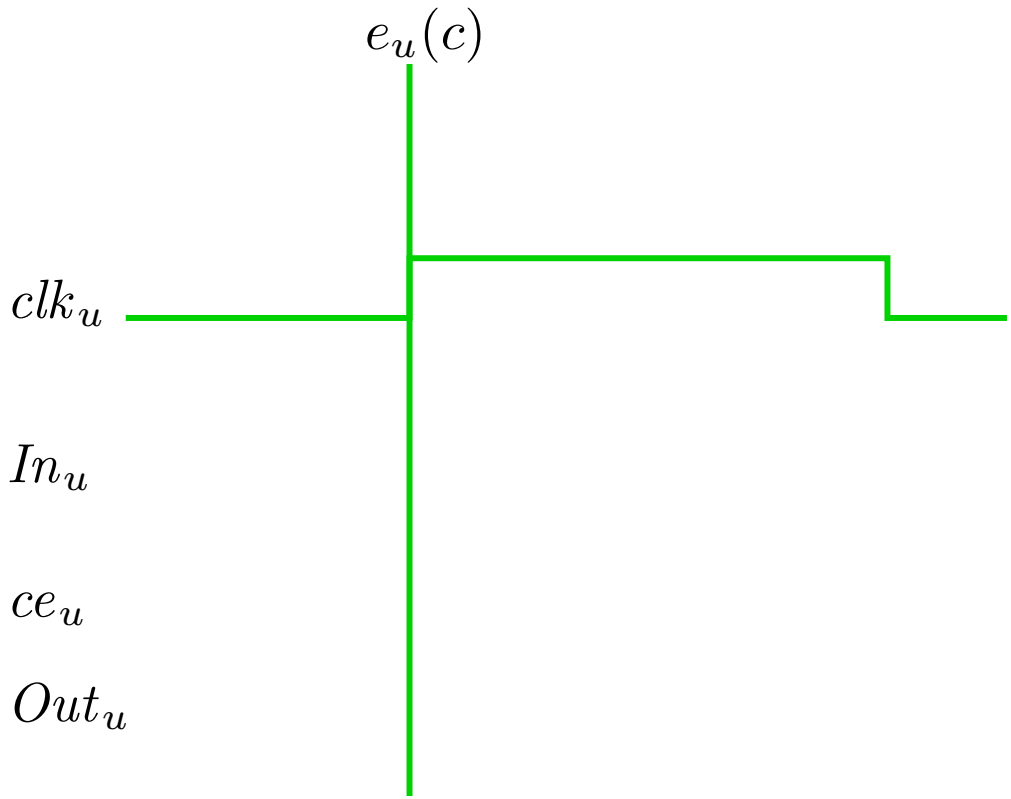
Outline

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

Modeling Principles

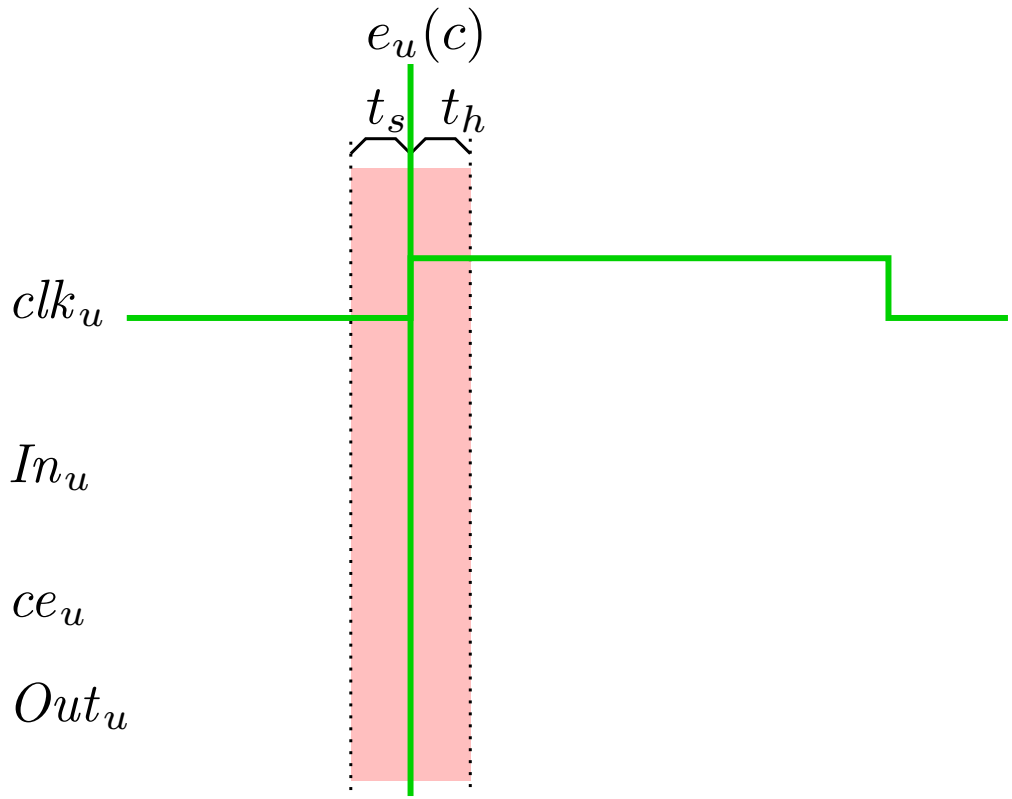
- 3-valued logic:
  - 0, 1 for “low” and “high” voltages
  - Ω for any other voltage
- Signals are functions from time to $\{0, 1, \Omega\}$
- Transition from low (high) to high (low) via Ω
- Clocks are offset/period pairs
  - Initial phase offset
  - Bounded drift of clock periods
  - We note $e_u(c)$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

Analog Register



Registers at rising clock edges

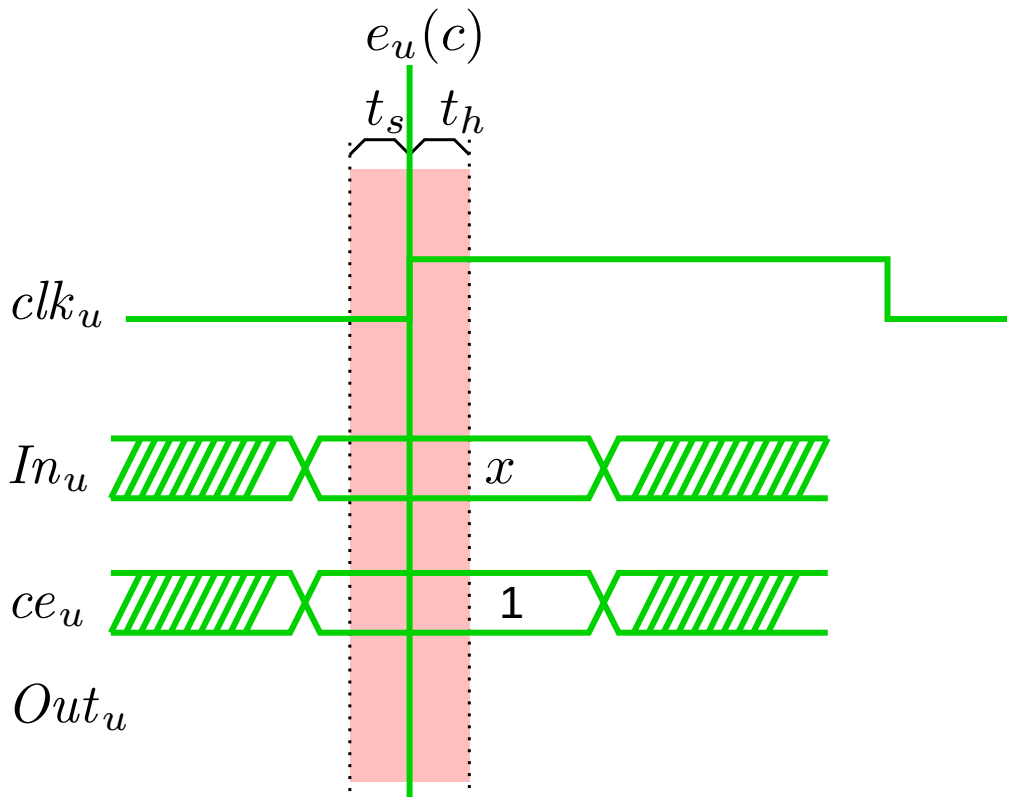
Analog Register



Setup and holding times determine a “metastability window”.

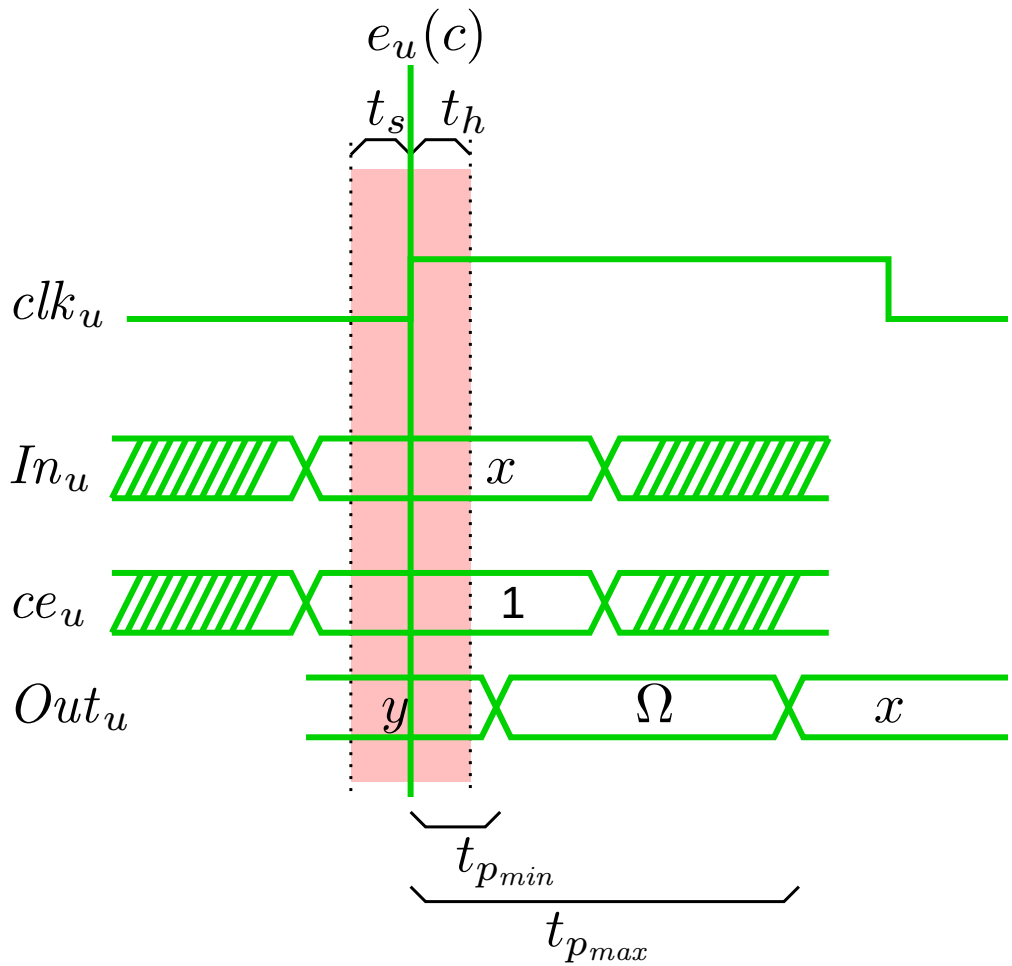
Metastable means output voltage is neither 0 nor 1.

Analog Register



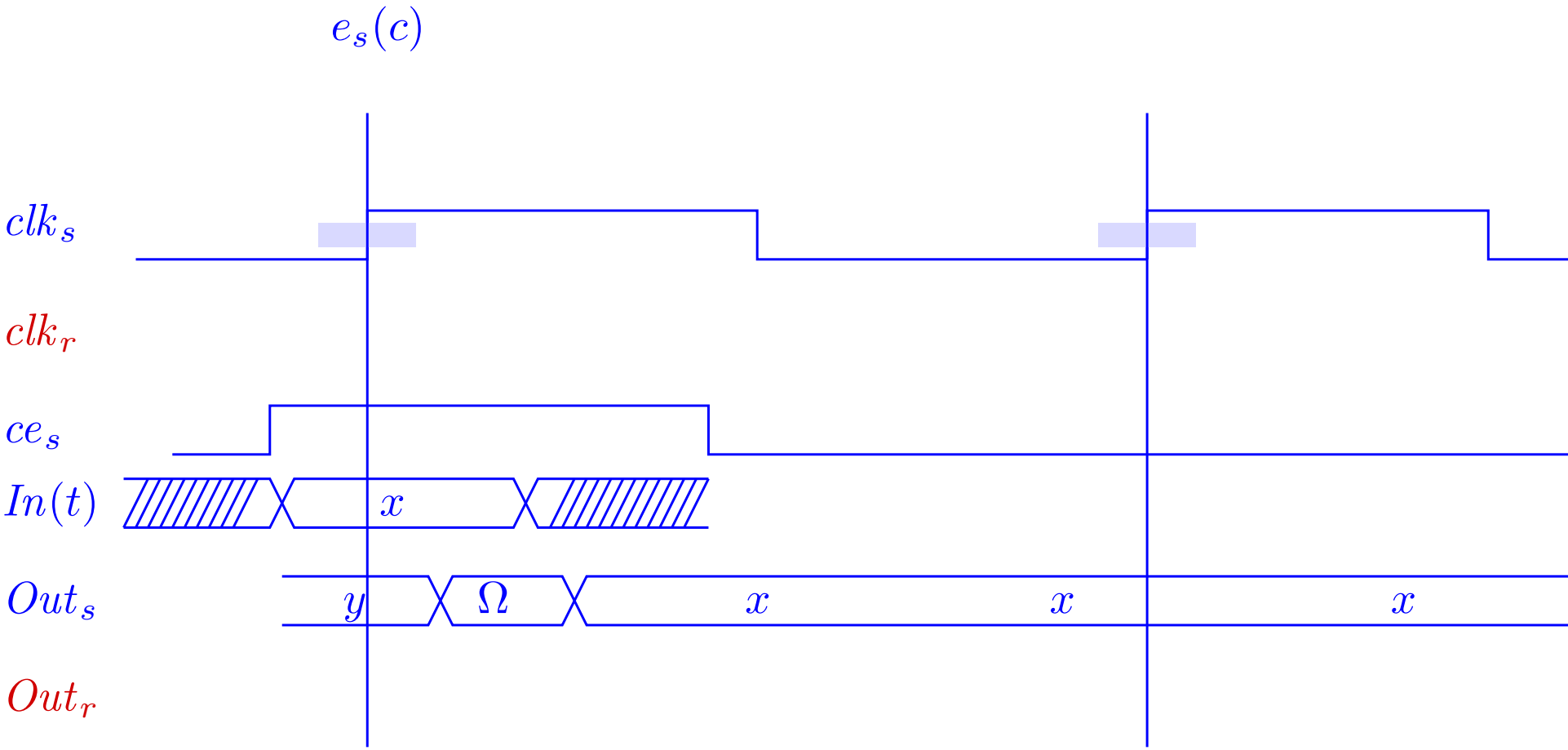
Input and control signals *defined* and *stable* in this window.

Analog Register



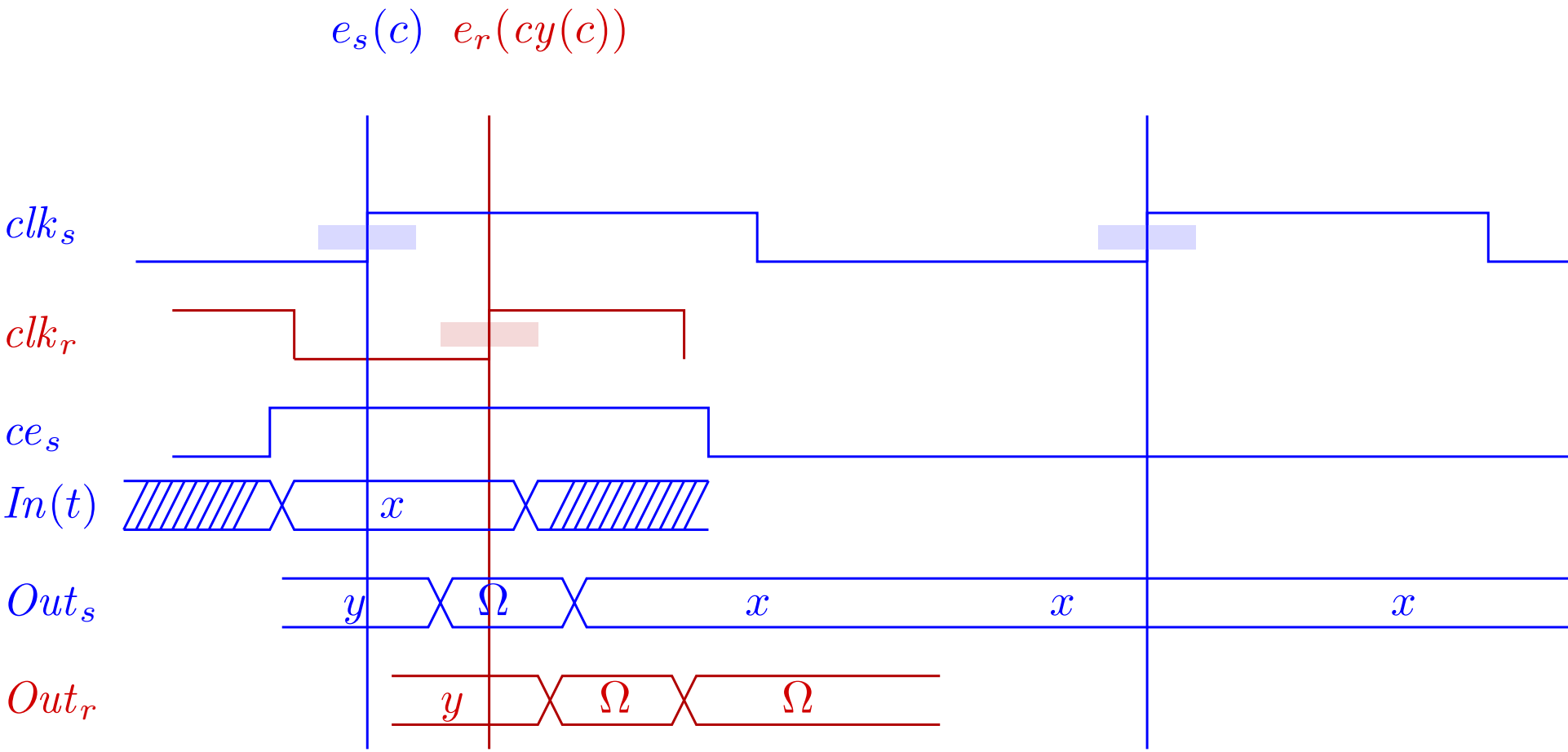
Transition after $t_{p_{min}}$. Final value after $t_{p_{max}}$

Register-Register Bit Transfer



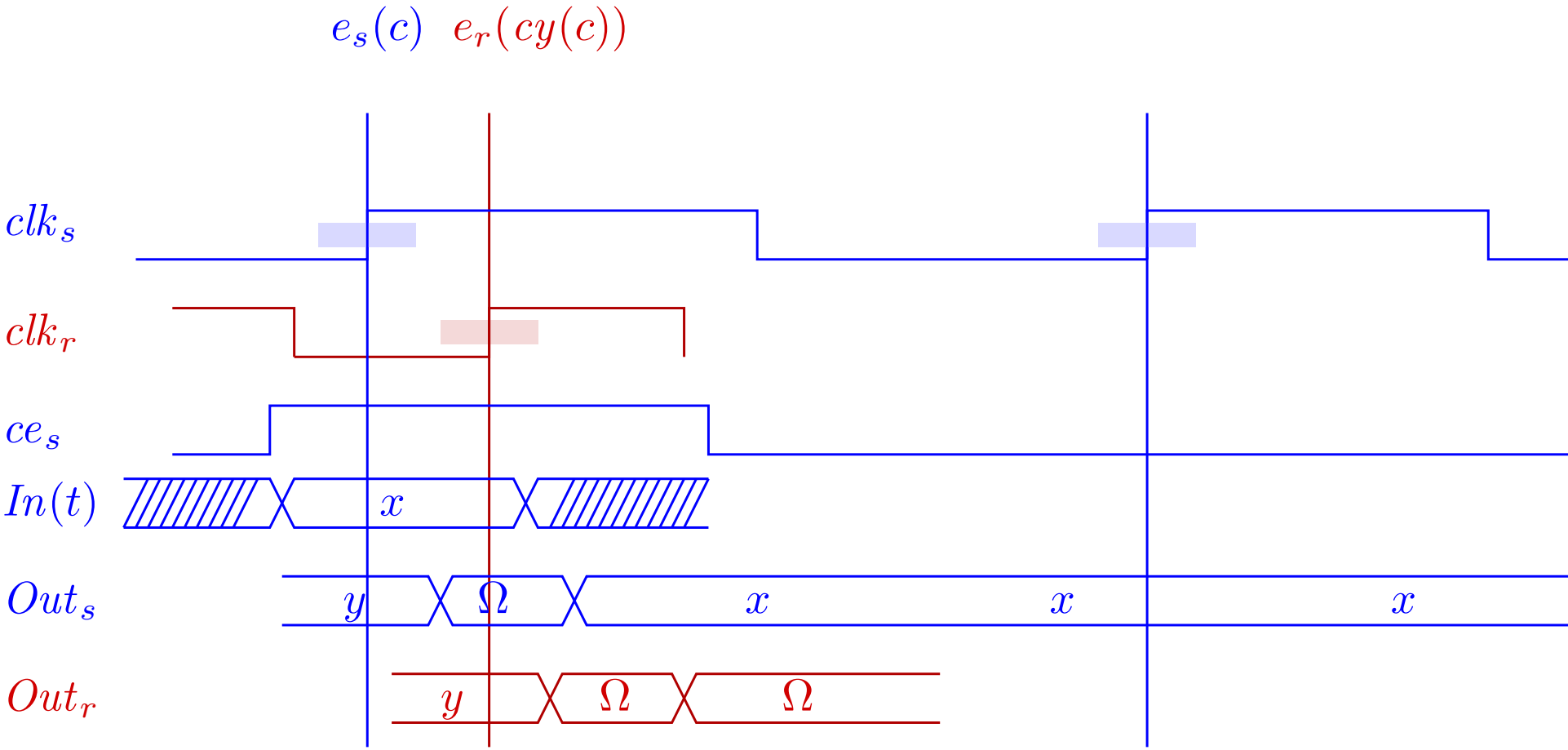
Sender creates a “safe sampling window”.

Receiver Starting Point



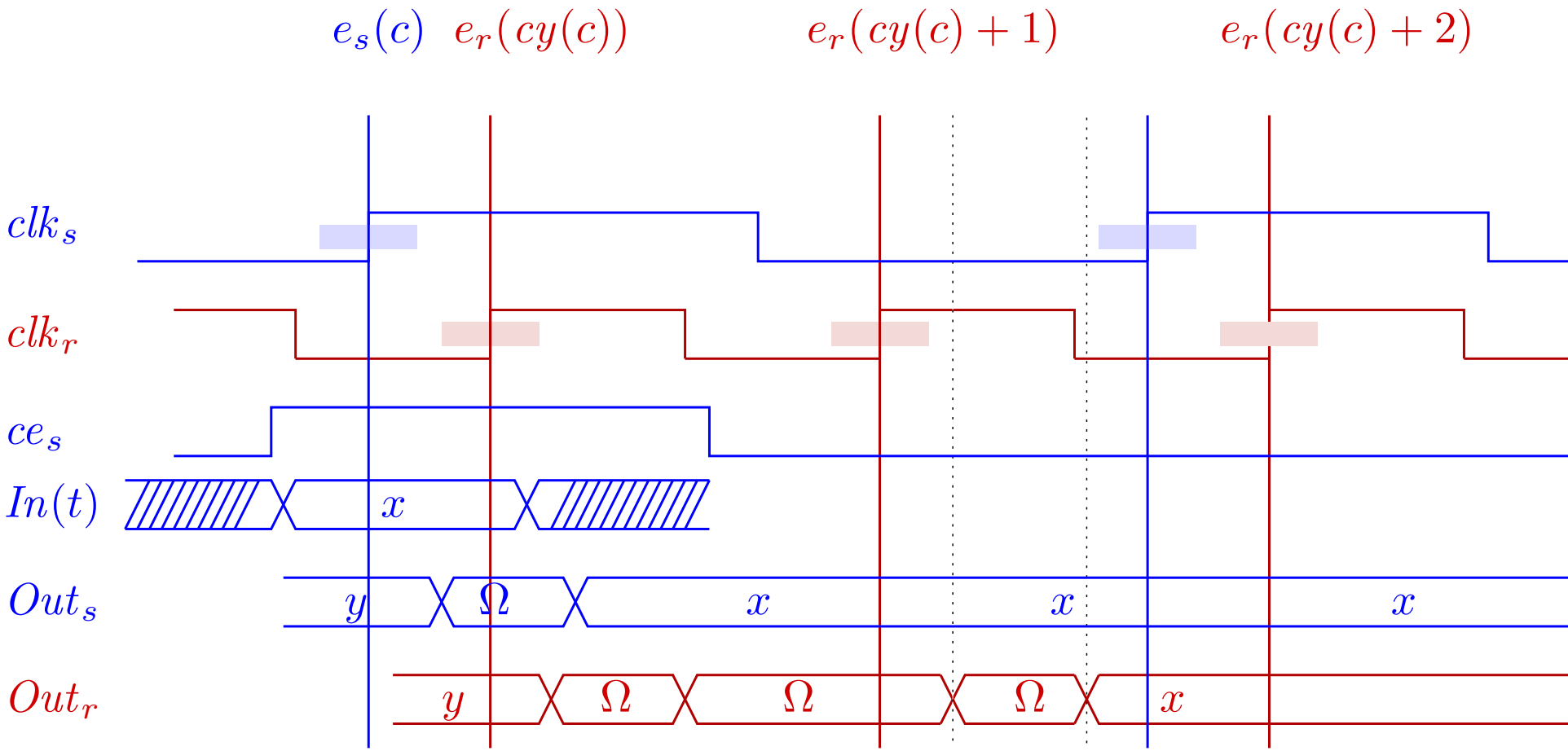
Receiver starting point is the first edge to be “affected”.

Receiver Starting Point



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

Good Sampling



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
  - Ω if ce and In violate setup or holding times constraints
  - $_tR_u^{c-1}(e_u(c))$ during $t_{p_{min}}$, Ω and $In_u(e_u(c))$ at $t_{p_{max}}$
- See previous diagram !

BigEnough S.S.W.

- Safe sampling window large enough to entail n receiver cycles

$$BigEnough(k,n) \equiv \tau_s \cdot (k+1) \geq \tau_r \cdot (n+2)$$

- $n+1$ cycles because of our weak hypothesis
- $n+2$ cycles because of metastability
- $BigEnough$ = 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**.

BigEnough Safe Sampling Window

$\wedge$ Correct Analog Control Signals

$$ce_s(e_s(c)) = 1 \wedge \forall l \in [1:k], ce_s(e_s(c+l))$$

$\wedge$ Analog Connection

$$\forall c, In_r = {}_tR_s(c, clk_s, ce_s, In_s, Out_s^0)$$

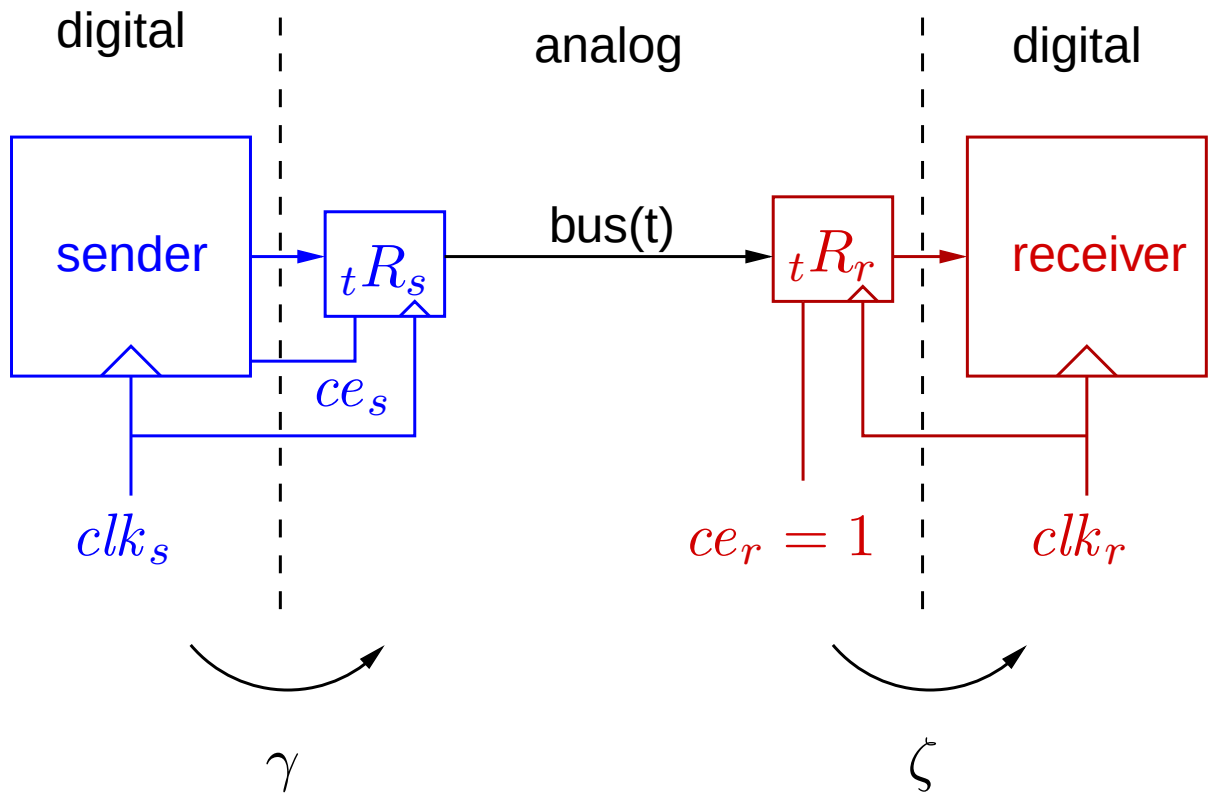
$\rightarrow$ $n+1$ good samples

$$\forall l \in [0:n], {}_tR_r^{cy(c)+1+l} = In_s(e_s(c))$$

Outline

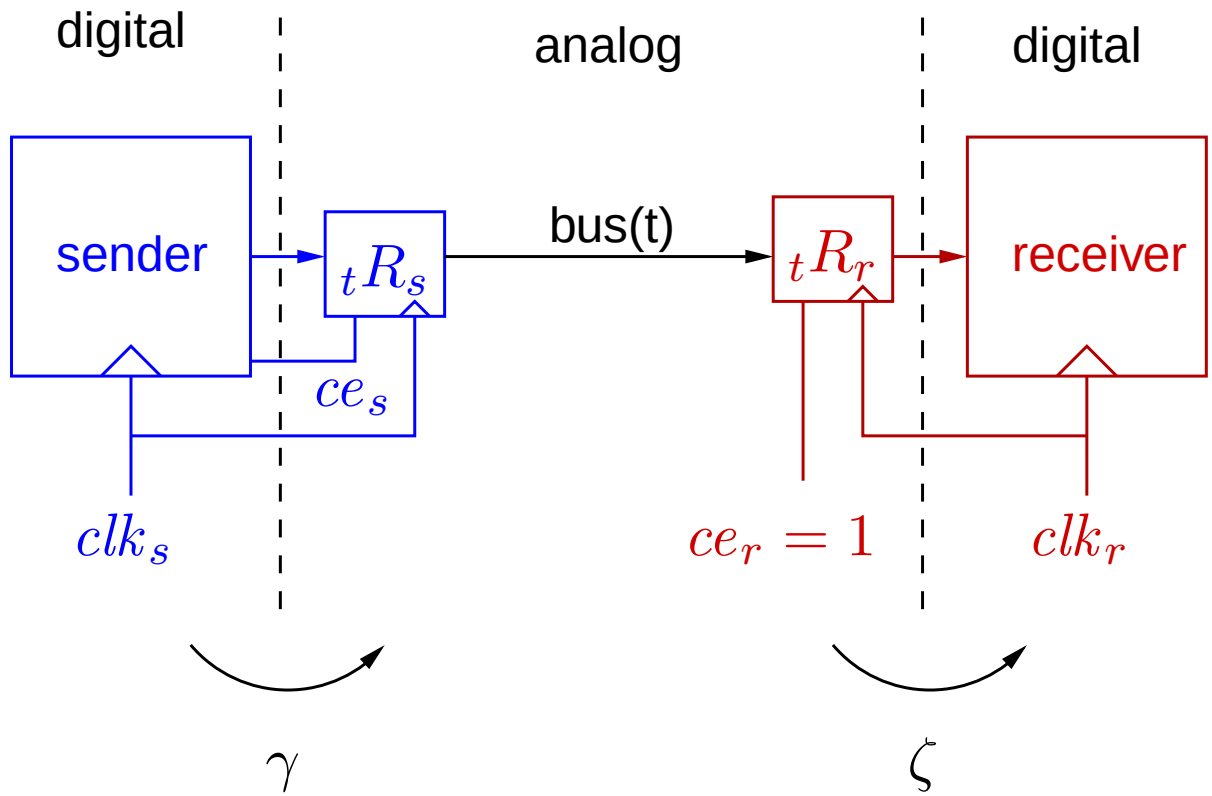
- Asynchronous communications
- Analog bit transfer correctness
- Connection with a fully digital world

Analog and Digital



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

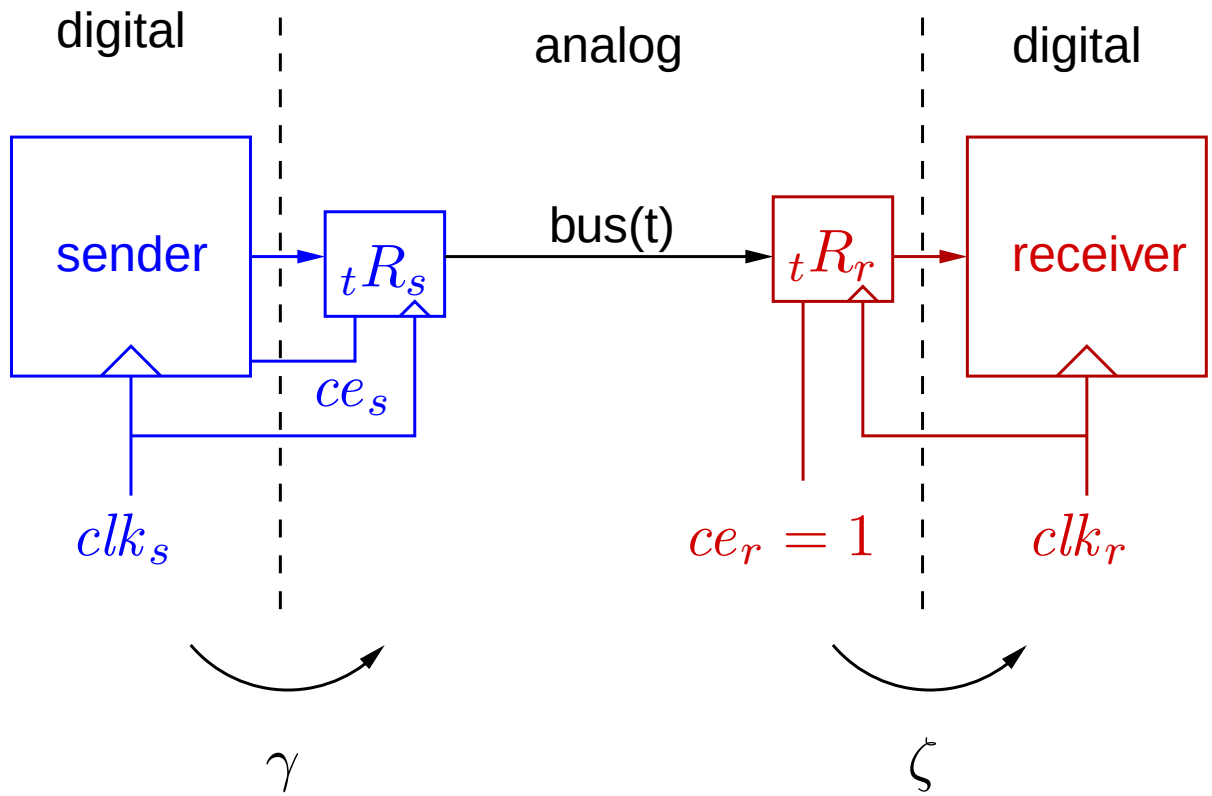
Analog and Digital



- γ converts bit lists to signals

$bv2sp(\gamma, l, clk) \equiv \gamma$ do not generate metastability

Analog and Digital



- ζ represents a synchronizer

  $\zeta(s,t) \triangleq$

  $\textbf{if}\ \ s(t) \in \{0,1\}\ \ \textbf{then}\ \ s(t)\ \ \textbf{else}\ \ \epsilon x, x \in \{0,1\}$

Analog/Digital Theorem

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

$$
\begin{array}{ll}
\wedge & \text{Analog Connection} \\
 & \forall c, In_r = {}_tR(c, clk_s, \gamma(\underline{ce_s}), \gamma(\underline{In_s}), Out_s^0) \\
\wedge & \text{Modeling Hypotheses}(bv2sp, BigEnough) \\
\wedge & \text{Digital Sender Behavior} \\
 & \underline{ce_s}[c] = 1 \wedge \forall l \in [1:k], \underline{ce_s}[c+k] = 0 \\
\rightarrow & n+1 \text{ good digital samples} \\
 & \forall l \in [0:n], \zeta({}_tR_r^{cy(c)+l+1}) = \underline{In_s}[c]
\end{array}
$$

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
- Verifi cation of a FlexRay-like Interface
  - Clock drift
  - Sample full messages

THANK YOU !!