Packet Sniffer for the Physical Layer of the Single Wire Protocol

Michael Roland, Christian Saminger, Josef Langer

Upper Austria University of Applied Sciences, Hagenberg, Austria

FH Science Day 2008

Embedded Systems Design
http://www.fh-hagenberg.at/esd

Outline

Outline

Secure Element

- Container for NFC applications
- Applications and data related to a certain user
- UICC already contains subscriber identity module (SIM)
- UICC can be used as the secure element
  - ⇒ independent of the mobile phone
  - ⇒ bound to a user identity

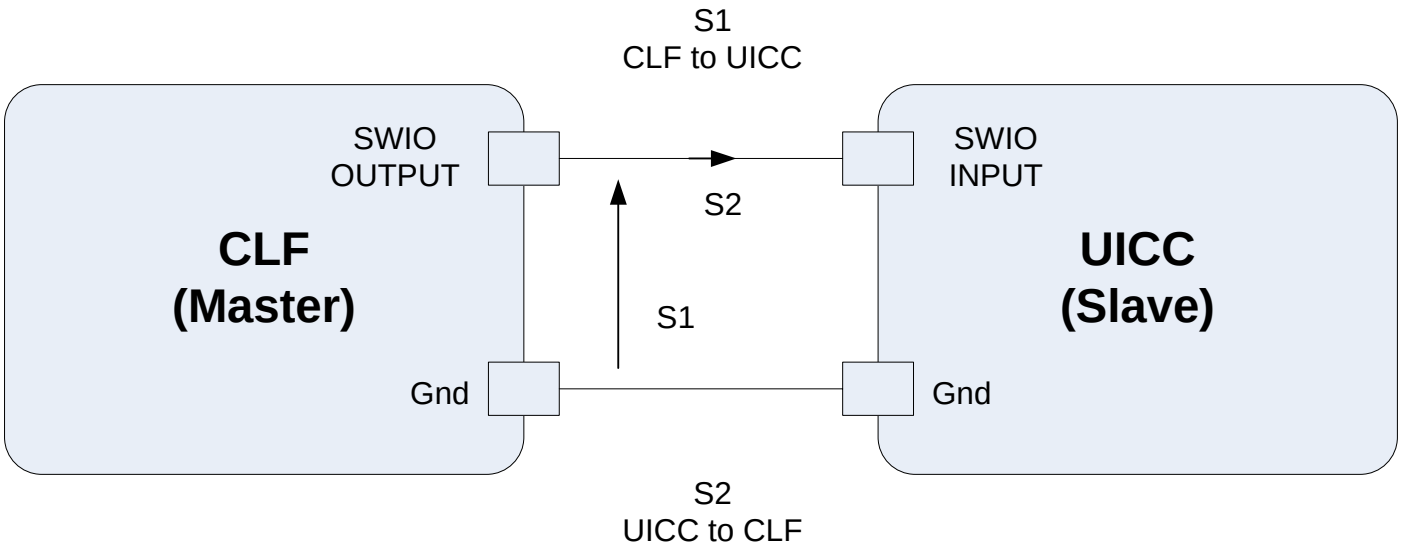
Outline

Why use the Single Wire Protocol?

- UICC used as the secure element
- Direct interface between the UICC and the CLF necessary
- UICC has only one unused IO pin left
- Major vendors agreed on the Single Wire Protocol
- First devices announced and in production

What is the Single Wire Protocol?

- Full-duplex serial communication protocol
- Uses only one IO wire
- Master-to-slave data (S1): voltage domain
- Slave-to-master data (S2): current domain

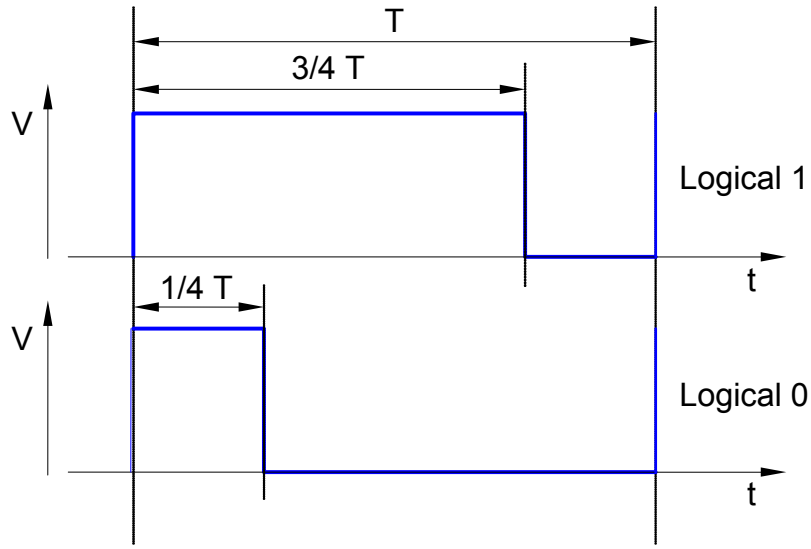


Embedded Systems Design
http://www.fh-hagenberg.at/esd

FH OBERÖSTERREICH

Master-to-slave (S1) Signaling

- Voltage domain



- *Disabled:* S1 is constantly low
- *Enabled:* S1 is constantly high
- *Data:* S1 is modulated
  - Pulse width modulation bit coding
  - Logical 1: 75% high, 25% low
  - Logical 0: 25% high, 75% low
  - Variable bit-duration on each transmitted bit

Embedded Systems Design
http://www.fh-hagenberg.at/esd

FH OBERÖSTERREICH

Slave-to-master (S2) Signaling

- Current domain

- *No data:* S2 is constantly low
- *Data:* S2 is modulated
  - Non-return-to-zero-level bit coding
  - Current signal is only valid during high-pulses of S1
  - Logical 1: current between 600 and 1000 μA
  - Logical 0: current between 0 and 20 μA

Outline

Wiretapping and Packet Sniffing

- Tap into wired data link
- Intercept electrical signal
- Analyze the state of the communication
- Receive the data frames

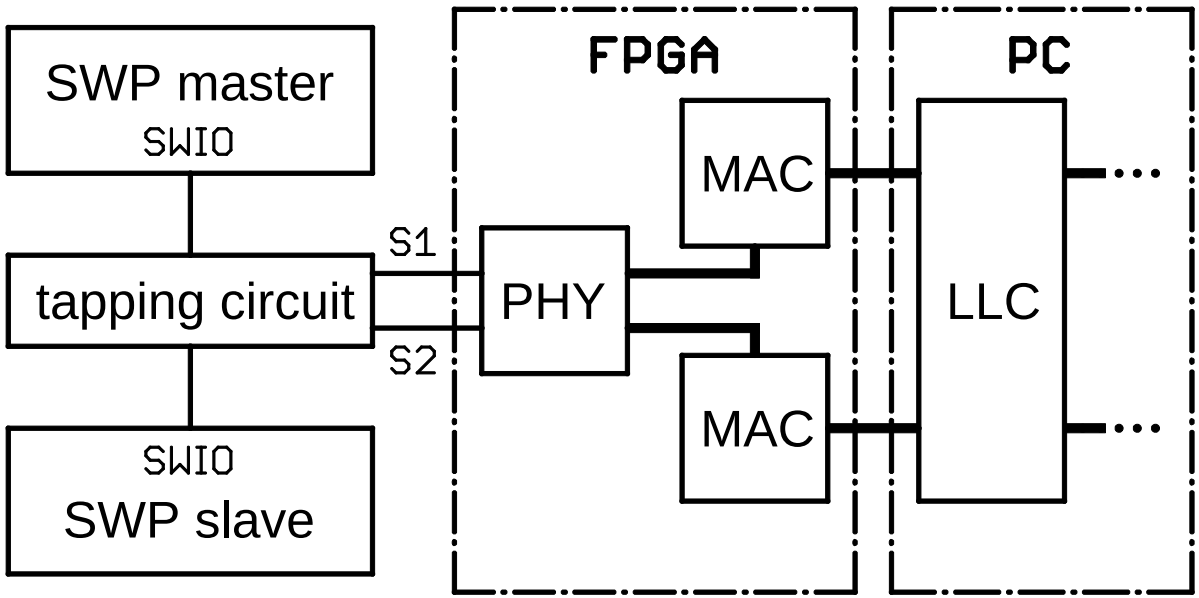
Why is Packet Sniffing useful?

- Analyze communication
- Debug communication problems
  - Framing errors
  - Bit-stuffing errors
  - Checksum errors
  - Problems with the interface state
- Log data traffic

Outline

System Design

- Discrete tapping circuit
- FPGA-based processing of PHY and MAC layers
- PC-based processing of higher layers



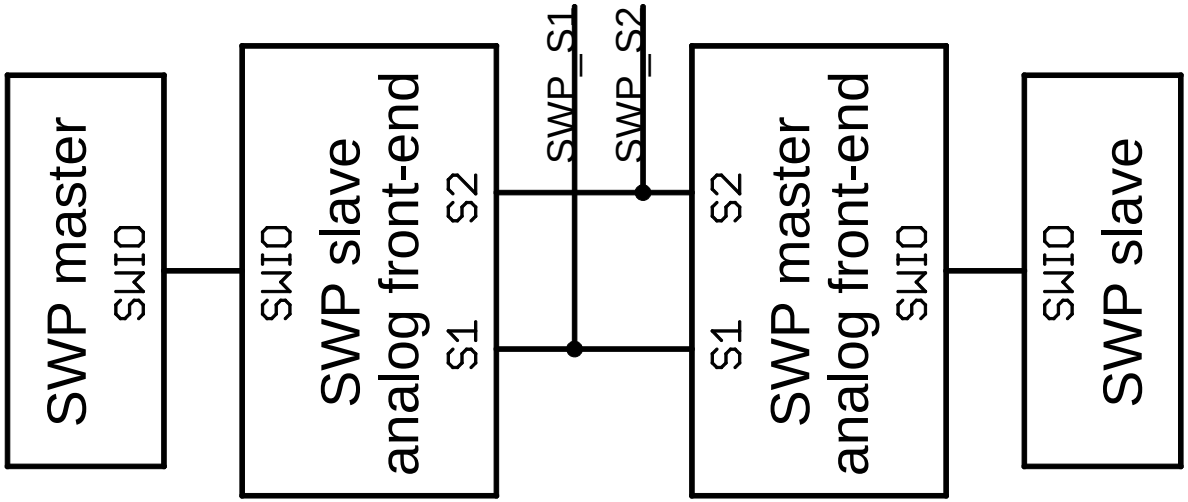
Embedded Systems Design
http://www.fh-hagenberg.at/esd

FH OBERÖSTERREICH

Outline

Using an Analog SWP Front-end

- Master connected to a slave's analog front-end
- Slave connected to a master's analog front-end
- Intermediate digital signals can be easily tapped



⇒ Induces additional signal delays

⇒ Leads to invalid relation between S1 and S2

Embedded Systems Design
http://www.fh-hagenberg.at/esd

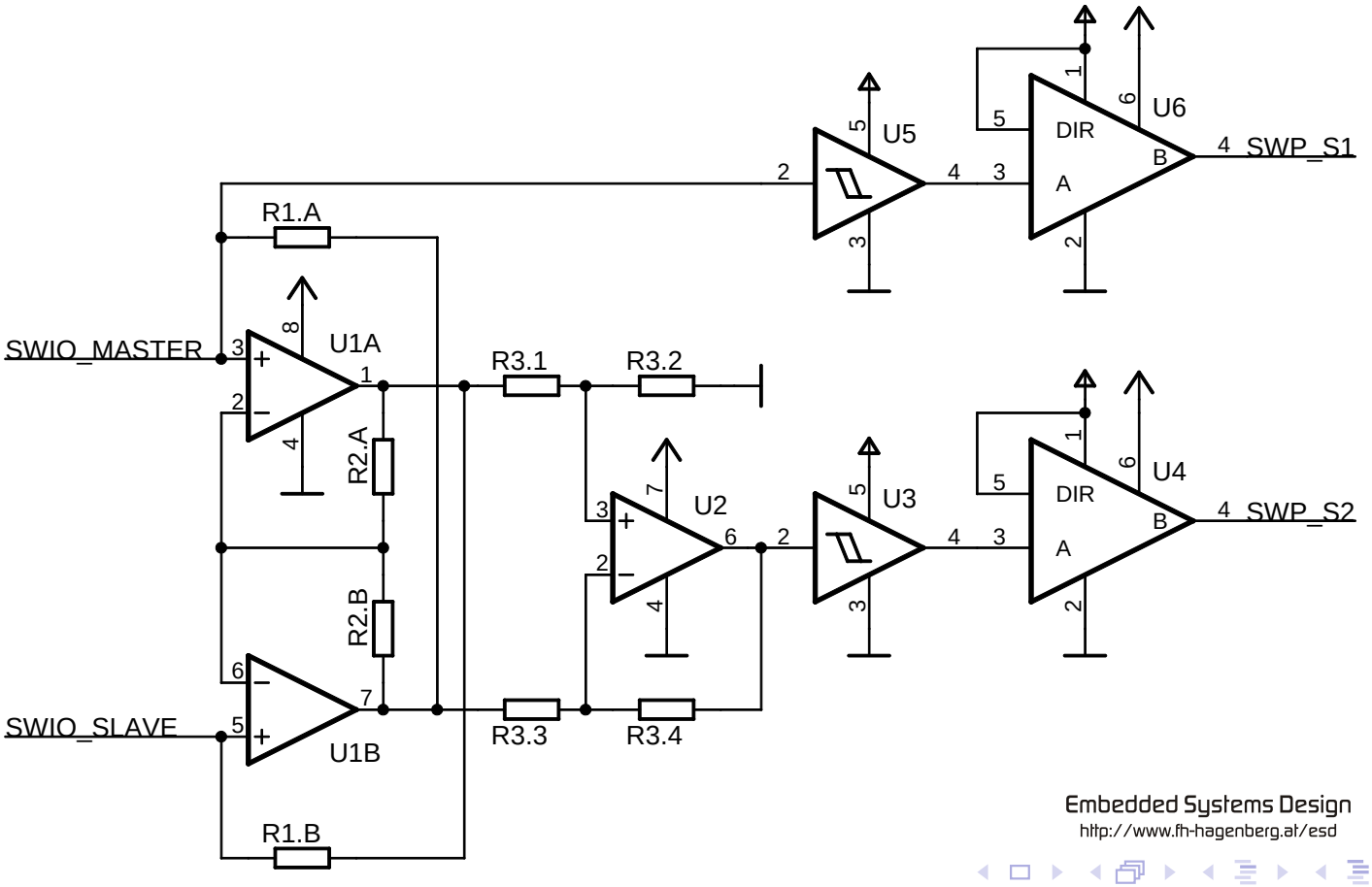
FH OBERÖSTERREICH

Measuring Current and Voltage on SWIO

- Voltage signal S1
  - Directly usable
- Current signal S2
  - Current signal has only between 0.6 and 1 mA
  - Current signal must be transformed into voltage signal
  - Current measurement must not influence the signaling
  - Very low voltage drop required

Measuring Current and Voltage on SWIO

- Ampere meter with low voltage drop transforms current signal into voltage signal
- Analog voltage signals converted to binary digital signals



Embedded Systems Design
http://www.fh-hagenberg.at/esd

Outline

Recovering the State of the SWP Interface

- FPGA-based processing of the digital versions of S1 and S2
- Decoded into bit-streams based on the interface state (i.e. when S1 is active)
  - *S1:* high and low phases compared to calculate logical ones and zeros
  - *S2:* sampled during the high phases of S1
- Bit-streams are then scanned for SWP frames
  - Packet sniffer should be used to debug communication problems

  $\Rightarrow$ Fault-tolerance required

Outline

Transmitting LLC Layer Packets to the PC

- SWP's minimum bit-duration is 590 ns

⇒ Each signal has a maximum data throughput of about 1.7 Mbps

- Full-duplex communication is possible

⇒ Data and status information requires up to 4 Mbps

Summary and Outlook

- Packet sniffing supports the debugging of SWP applications.
- A promising measurement circuit has been found.

- Outlook
  - The evaluated circuit has to be tested with bit-durations up to 590 ns.
  - The system has to be tested with real SWP devices outside the test environment.