DOI 10.5162/SMSI2021/D8.4

Precision Measurement of the Application dependent Current Consumption of a Wireless Transceiver Chip

Thomas R. Doebbert, Christoph Cammin, Gerd Scholl
Electrical Measurement Engineering,
Helmut-Schmidt-University, Hamburg, Germany
thomas.doebbert@hsu-hh.de

Summary:
Modern production concepts generate a demand for reliable, fast and secure wireless communication solutions. Therefore, the current consumption should not increase highly due to additional security operations. This paper shows a principle current measurement method exemplarily of a transceiver for IO-Link Wireless protocol. The results show that the current consumption increases by about 316 µA when using hardware-based encryption features, whereby an experimental standard deviation of the mean values of about 15 µA was determined.

Keywords: Wireless Security, Current Measurement, IO-Link Wireless, Current Consumption, Industry 4.0

Introduction

Reliable and secure radio-based communication systems are an important component for the enhancement of modern production concepts like Industry 4.0. An essential requirement, especially in an industrial production environment, is that fixed cycle times can be guaranteed even for secured transmissions, where security operations influence the power consumption and the timing of the data transmission of wireless transmission protocols.

Due to typical timing demands in the order of less than 1 ms and low power requirements of hardware modules, these investigations represent a demanding measurement task, because broadband measurements need to be realized with a high amplitude resolution.

In this paper, the current consumption of the data transfer in plaintext and in ciphertext using a Phytec module based on a CC2650 SoC radio transceiver chip [1] is investigated. The IO-Link Wireless protocol is used because it directly addresses the special requirements in the field of production automation in terms of latency, reliability and number of sensors [2].

Principle Measuring Method

In the first step of the measurement, the internal shunt resistor of the current measurement device is used to find an indentation of the measurement range. In the second step, an external exchangeable shunt resistor is used to achieve a better fitting measurement range for using the internal 18 bit ADC of the measurement device. In the third step, plaintext mode of operation is compared to cryptographic mode of operation. In the last step, a statistical evaluation is used to analysis the measurement accuracy.

To measure the influence of the cryptographic algorithms compared to the plaintext mode or unencrypted operation, only every other downlink, cryptographic operation is activated. In this way, within 10 ms three measurements with cryptographic operations and three with plaintext mode are recorded. Thermal effects are neglected, because the effects are subtracted with the operation without cryptographic algorithm.

Measurement Assessment

To achieve a more accurate measurement range compared to the setup with an internal shunt, a measurement setup with an external shunt is used [3], as shown in Fig. 1. The external debugger, which was connected to the Device under Test (DUT) is not shown here.

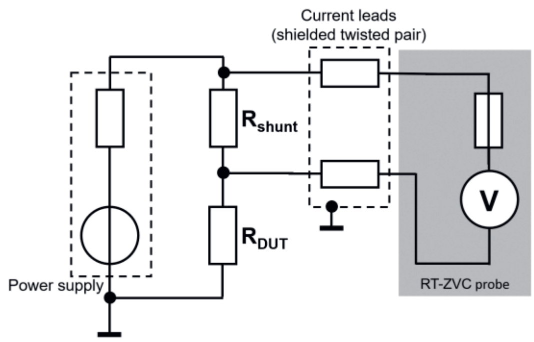

Fig. 1. Setup of measurement 3] with external shunt according to [4, p. 32].

A constant voltage source [5] provides a stable voltage supply for the DUT. The appropriate measurement range of 13.81 mA was chosen by selecting a shunt resistor, which was measured using a precision multimeter [6] to have a value of 3.259 Ω. The accuracy of the current measurement can be approximated by using the data sheet of the power probe [4]. The appropriate type of current (DC or AC) has to be selected according to the data sheet. Eq. (1) uses the AC version (10 Hz to 40 kHz) of the approximated measurement value, because the signal is characterized as a pulsed DC signal, as in Fig. 2. The abbreviated symbols in eq. (1) characterize the measured current ($I_{acc,ZVC}$), tolerance of the external resistor with additional connectors (R_{tol}), the measurement range (I_{range}) and the internal ADC tolerance of the ZVC probe (ADC_{tol}).

$$I_{acc,ZVC} = I_{meas} \pm \left[\frac{\%R_{tol}}{100\%} \cdot I_{meas} + \frac{\%ADC_{tol}}{100\%} \cdot I_{range}\right] = 8.63\text{ mA} \pm \left[\frac{0.4\%}{100\%} \cdot 8.63\text{ mA} + \frac{0.02\%}{100\%} \cdot 13.81\text{ mA}\right] = 8.63\text{ mA} \pm 0.0373\text{ mA}\,. \quad (1)$$

Theoretically, the 18 bit ADC can resolve 105.35 nA steps over an input range of 13.81 mA. Practically, assuming that the two least significant bits cannot be used, an amplitude resolution due to amplitude quantization of 421.4 nA over the input range is feasible.

An example measurement of 16 bytes AES-ECB algorithm is shown in Fig. 2. A moving average filter smoothed the data over 125 samples.

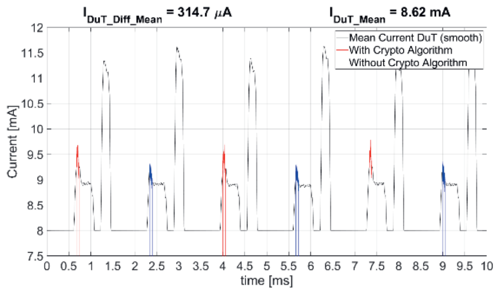

Fig. 2. AES-ECB encryption of 16 bytes using the on chip hardware accelerator.

Each measurement consists of 445 data sets with each 50 k samples (at 5 MSa/s) recorded (2.225 G samples) and used for further calculations, as in [3].

Table 1 shows the statistical parameter of 10 measurements each with 445 data sets.

Tab. 1: Measurement Results.

	Current Mean DUT	Current Difference of crypto to plaintext
Mean value	8.63 mA	316.2 µA
Experimental Standard Deviation	15.2 µA	25.0 µA

Results

The experimental standard deviation of the mean currents are factor 2.5 smaller than the accuracy according to the data sheet of the measurement equipment [4]. Furthermore, the experimental standard deviation of the mean value is about two orders of magnitude larger than the theoretical step size of the ADC, thus, the quantization effects like quantization noise have a negligible effect. The mean value of current difference is 316.2 µA (i.e. about 3.7 % of the mean value) and has therefore only a minor influence on potential battery life. The experimental standard deviation of the current difference of crypto to plaintext is 25.0 µA, which is significantly smaller than the mean current difference of crypto to plaintext.

In a future step, the frequency spectrum needs to be evaluated, because the pulsed DC signal is not considered in the datasheet [4]. The approximation of an AC current with 10 Hz to 40 kHz was used. However, the statistical parameter lead to a validation of the accuracy estimation given in the datasheet [4].

Acknowledgment

The authors would like to acknowledge Mr. Jockram and Dr. Heynicke for their support as well as the company Kunbus GmbH.

References

[1] PHYTEC Embedded Pvt. Ltd., phyWAVE-CC26xx Hardware Manual, Available: https://www.phytec.in/fileadmin/user_upload/images/content/1.Products/IoT/L-824e_1.pdf, August 2016.

[2] R. Heynicke, et al., IO-Link Wireless enhanced factory automation communication for Industry 4.0 applications, J. Sens. Sens. Syst., 7, 131–142, (2018); doi: 10.5194/jsss-7-131-2018.

[3] T. Doebbert, et al., IO-Link Wireless Device Cryptographic Performance and Energy Efficiency, submitted for publication

[4] Rohde & Schwarz, R&S RT-ZVC Multi-Channel Power Probe, User Manual, Available: https://scdn.rohdeschwarz.com/ur/pws/dl downloads/dl common library/dl manuals/gb1/r/rt zvc/RT-ZVC UserManual en 03.pdf, Version 03, 2020-10-23.

[5] Rohde & Schwarz, R&S NGM200 Power Supply Series, Data Sheet, Available: https://scdn.rohde-schwarz.com/ur/pws/dl_downloads/dl_common_library/dl_brochures_and_datasheets/pdf_1/NGM200_dat_en_3609-1685-32_v0200.pdf

[6] Keysight, Keysight 3458A Multimeter, User's Guide, Available: https://literature.cdn.keysight.com/litweb/pdf/03458-90014.pdf