

## **Exp.007/Blofeld**

### **Hintergrund**

Die Absicherung von Sensordaten in Raumfahrzeugen und Lebenserhaltungssystemen nimmt eine immer größere Rolle bei dessen Betrieb und der Überwachung von Umwelt- und Vitalparametern ein. Die Steuerung eines Lebenserhaltungssystems erfordert die ununterbrochene Aufnahme und Übermittlung von Sensordaten aller Subsysteme sowie der Habinauten, um Systemzustände und Schwankungen zu vermessen und gegebenenfalls Änderungen in den Steuer-Parametern vornehmen zu können. Dabei ist nicht nur eine abhörsichere Verbindung zu den Sensoren, sondern auch die Validität der Daten von oberster Priorität. Im Experiment Exp.007/Blofeld soll zum ersten Mal das *Secure Element* NXP SE051 zur Beweiswerterhaltung per elektronischer Signatur und Verschlüsselung von wissenschaftlichen Sensordaten unter Weltraumbedingungen getestet werden.

Ein Nebeneffekt ist dabei der Einsatz sicherer Authentisierung von berechtigten Nutzern und Systemen beim Zugriff auf die Payload und wissenschaftlicher Daten. Dies lässt sich erweitern, so dass mit einer generischen „SpaceID“ Zugriffsberechtigungen und sichere Kommunikation realisiert werden könnten.

### **Experimentbeschreibung**

Im Experiment Exp.007/Blofeld werden Temperaturdaten von der isolierten und unisolierten Modulkappeninnenseite mittels berührungsfreien Thermosensoren (TMP007) aufgenommen und aufgezeichnet. Diese Daten tragen dazu bei, das thermale Verhalten der Experimentstruktur besser zu verstehen. Dabei wird der Datenstrom eines Thermosensors durch ein *Secure Element* geleitet, das SE051, welches mit dem Mikroprozessor (Teensy 4.1, NXP i.MX RT 1062 *edge computing platform*) eine verschlüsselte Kommunikation aufbaut.

Die Messwerte des zweiten Thermosensors werden zur Kontrolle unverschlüsselt vom Mikroprozessor aufgenommen.

Während der Aufnahme soll ein zweiter Mikroprozessor (Blofeld/RP2040) den verschlüsselten Datenstrom abgreifen, welcher dann als Grundlage zur Analyse und Visualisierung möglicher Angriffsszenarien auf das Verfahren am Boden dient.

Die Experimenthardware fliegt als Huckepack-Platine auf der Steuerplatine des Graviplax Experiments und wurde ohne das SE051 bereits auf Mapheus 9 mit erfolgreicher Datenaufnahme getestet.

Das Experiment Exp.007/Blofeld ist bis auf die Stromversorgung autark.

Gewicht	60 g
Größe LxBxH	70 mm x 50 mm x 25 mm
Strombedarf	Ø 220 mA bei 5 V (max. 248 mA)
007 CPU	Cortex M7F, 32 Bit, 816 MHz; 2MB int. on-chip RAM, 8MB SPI PSRAM
007 Flash	8MB on-board, 16MB QSPI, 32GB SD
Blofeld CPU	Cortex M0+, 32 Bit, 2x133 MHz; 264kB int. on-chip RAM
Blofeld Flash	8MB on-board

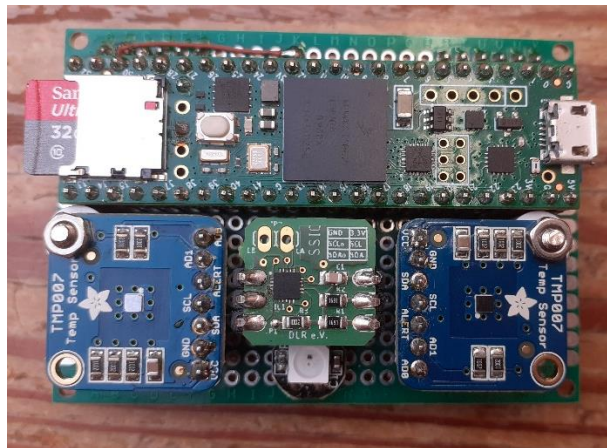


Figure 1: Exp.007/Blofeld Das Experiment ist aus folgenden Komponenten aufgebaut: Ein Teensy 4.1 mit Speichererweiterung (oben) übernimmt die Kommunikation mit den beiden TMP007 Thermosensoren (unten, rechts und links), Ein TMP007 Modul (links) überträgt seine Messwerte über das Secure Element SE051 (Mitte, unten). Am unteren Rand der Platine befindet sich zur Statusanzeige des Experiments eine RGB LED.

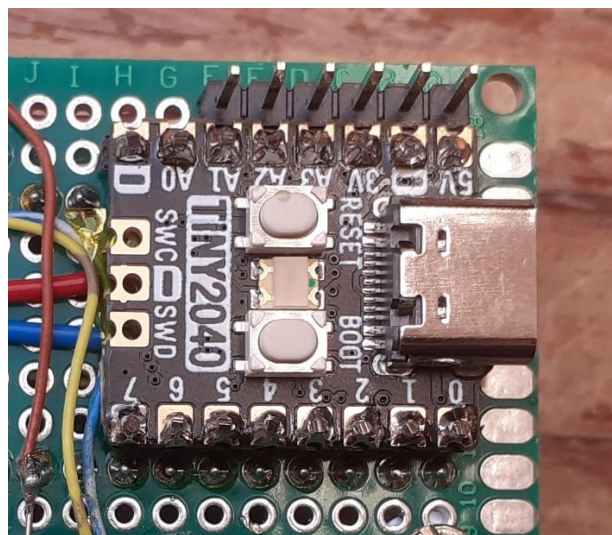


Figure 2: Auf der Rückseite ist der zweite Mikrokontroller, ein Tiny RP 2040 zu sehen, der im Experimentbetrieb den Datenstrom zwischen SE051 und dem Teensy 4.1 mitschneidet und aufzeichnet.

## **DLR Institute for Aerospace Medicine** **adesso SE**

### **Exp.007/Bluffed**

#### **Background**

The safeguarding of sensor data in spacecraft and life support systems is assuming an increasingly important role in its operation and the monitoring of environmental and vital parameters. The control of a life support system requires the uninterrupted recording and transmission of sensor data from all subsystems as well as the habinauts in order to measure system states and fluctuations and, if necessary, to make changes in the control parameters. Not only a tap-proof connection to the sensors, but also the validity of the data is of highest priority. The Exp.007/Blofeld experiment will be the first to test the NXP SE051 Secure Element for preserving the value of evidence by electronic signature and encryption of scientific sensor data under space conditions.

A side benefit of this is the use of secure authentication of authorized users and systems when accessing the payload and scientific data. This can be extended so that a generic "SpaceID" could be used to implement access permissions and secure communications.

#### **Experiment description**

In the Exp.007/Blofeld experiment, temperature data from the insulated and uninsulated module flap interior are taken and recorded using non-contact thermal sensors (TMP007). These data help to better understand the thermal behavior of the experiment structure. In this process, the data stream from one thermal sensor is routed through a secure element, the SE051, which establishes encrypted communication with the microprocessor (Teensy 4.1, NXP i.MX RT 1062 edge computing platform).

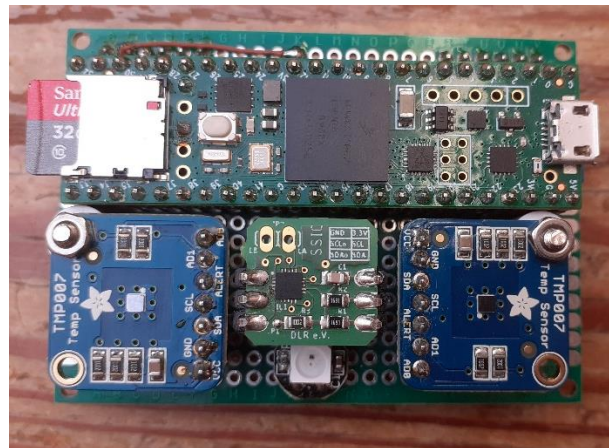
The readings from the second thermo sensor shall be recorded unencrypted by the microprocessor for control.

During recording, a second microprocessor (Blofeld/RP2040) will tap the encrypted data stream, which will then serve as the basis for analyzing and visualizing possible attack scenarios on the procedure on the ground.

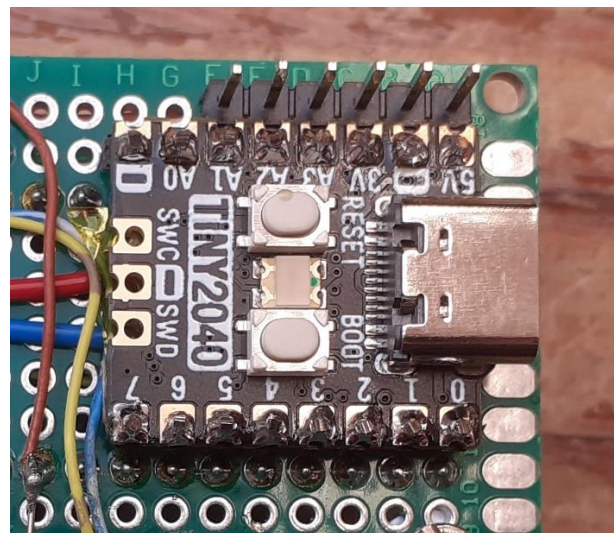
The experiment hardware flies as a piggyback board on the control board of the Graviplax experiment and has already been tested without the SE051 on Mapheus 9 with successful data acquisition.

The experiment Exp.007/Blofeld is self-sufficient except for the power supply

Weight	60 g
Size	70 mm x 50 mm x 25 mm
Power	Ø 220mA @ 5V (max. 248mA)
007 CPU	Cortex M7F, 32 Bit, 816 MHz; 2MB int. on-chip RAM, 8MB SPI PSRAM
007 Flash	8MB on-board, 16MB QSPI, 32GB SD
Blofeld CPU	Cortex M0+, 32 Bit, 2x133 MHz; 264kB int. on-chip RAM
Blofeld Flash	8MB on-board



**Figure 3: Exp.007/Blofeld** The experiment is constructed from the following components: A Teensy 4.1 with memory expansion (top) handles communication with the two TMP007 thermal sensors (bottom, right and left), A TMP007 module (left) transmits its readings via the Secure Element SE051 (middle, bottom). At the bottom of the board there is an RGB LED to indicate the status of the experiment.



**Figure 4:** On the backside you can see the second microcontroller, a Tiny RP 2040, which is recording the data stream between SE051 and the Teensy 4.1.