Using Software Mitigation Schemes to Improve the Availability of IoT Applications in harsh Radiation environment

Alessandro Zimmaro[1,2], Rudy Ferraro[1], Jérôme Boch[2], Frédéric Saigné[2], Alessandro Masi[1] and Salvatore Danzeca[1]

[1] CERN, Organisation européenne pour la recherche nucléaire,CH-1211 Genève.
[2] IES, Université de Montpellier, CNRS, Montpellier, France Switzerland.

Abstract

The integration of **IoT infrastructure in the context of particle accelerators promises numerous benefits** (reduced costs and maintenance time, increased deployment). However, the use of microcontroller units (MCUs), typical of IoT systems, may potentially compromise future accelerators availability performances. This paper presents **Software Mitigation Schemes (SMS)** designed to improve the availability performance of MCU-based systems under radiation. Their effectiveness is demonstrated through a radiation test on a CERN Wireless IoT Radiation Monitoring system, also called BatMon. **The results underline the IoT devices' feasibility as a viable solution for high-distribution systems in the future HL-LHC or Future Circular Collider (FCC).**

The Case Study

Needs of high mobility and versatility, and low cost drove CERN to develop the BatMon, the first Wireless IoT Radiation Monitoring system at CERN.

Battery Board

Features:
1. 4 Batteries
2. Max Vout: 7.2 V
3. Battery Capacity: 17 Ah

Main Board

Different Sub Systems (SSs) can be distinguished:
1. Controller SS: is the heart of the entire design and is based on an MCU
2. Transmission SS: is used for wireless communication and consists of a LoRa transceiver.
3. Storage SS: A non-volatile Flash Memory.
4. Recovery SS: an External Watchdog (Ext WTD) used to recover systems from Single Event Functional Interruptions (SEFIs).

Sensor Board

Radiation To electronics Effect monitoring through:
1. TID → FGDOS Sensor.
2. HEH and Th Fluences: two well-calibrated SRAMs sensitive to Thermal Neutron (Th) and High Energy Hadrons (HEH).

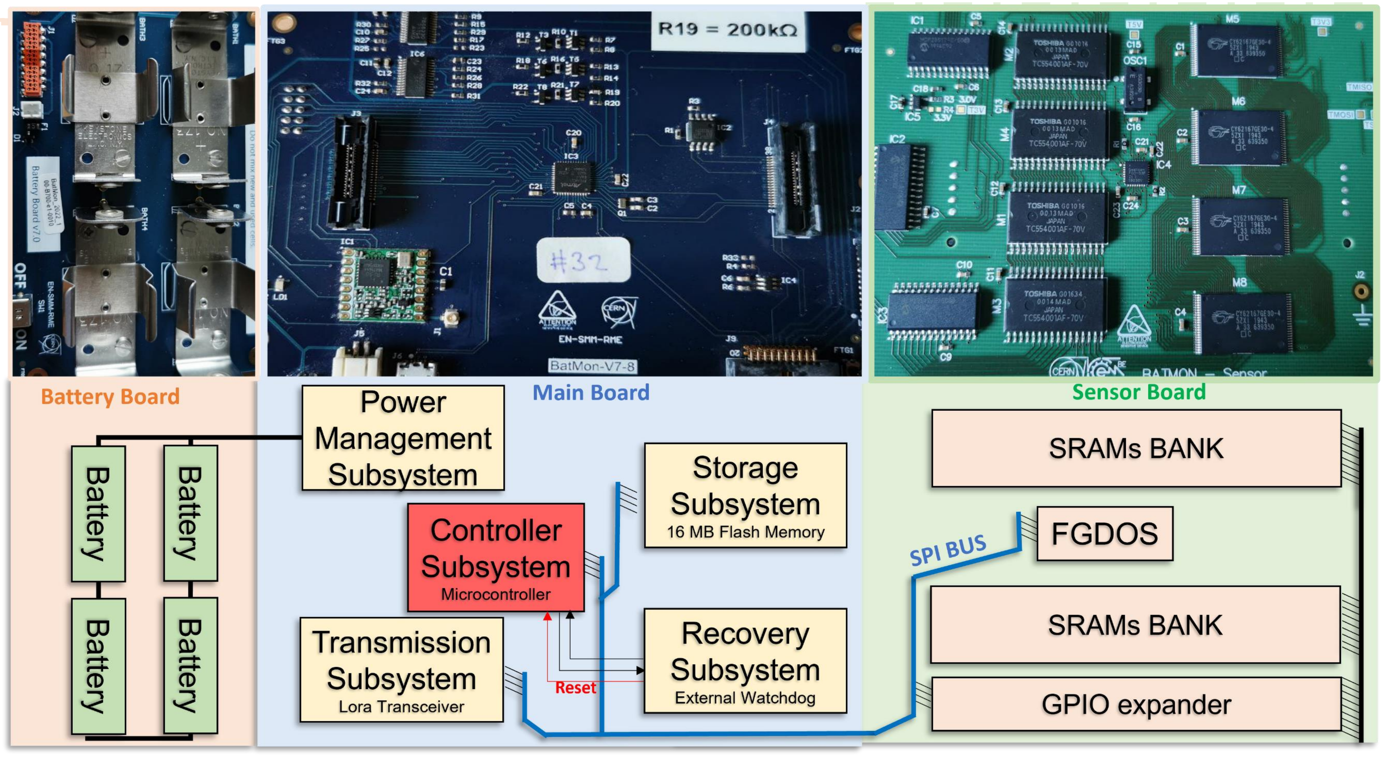

Fig. 1. BatMon boards and general hardware architecture.

Firmware

A Finite State Machine of three states is used to control the system:

- **App Init**: Initialization state where sensors are initialized, and network connection is established.
- **App Sleep**: Power safe state which is reached once a reading is taken from the sensor and transmitted or the device fails to connect to the network due to network unavailability.
- **App Meas**: Measurement state that is only reached if the end node has joined the network. Sensor reading, measurement storage, and transmission operations are performed during this phase.

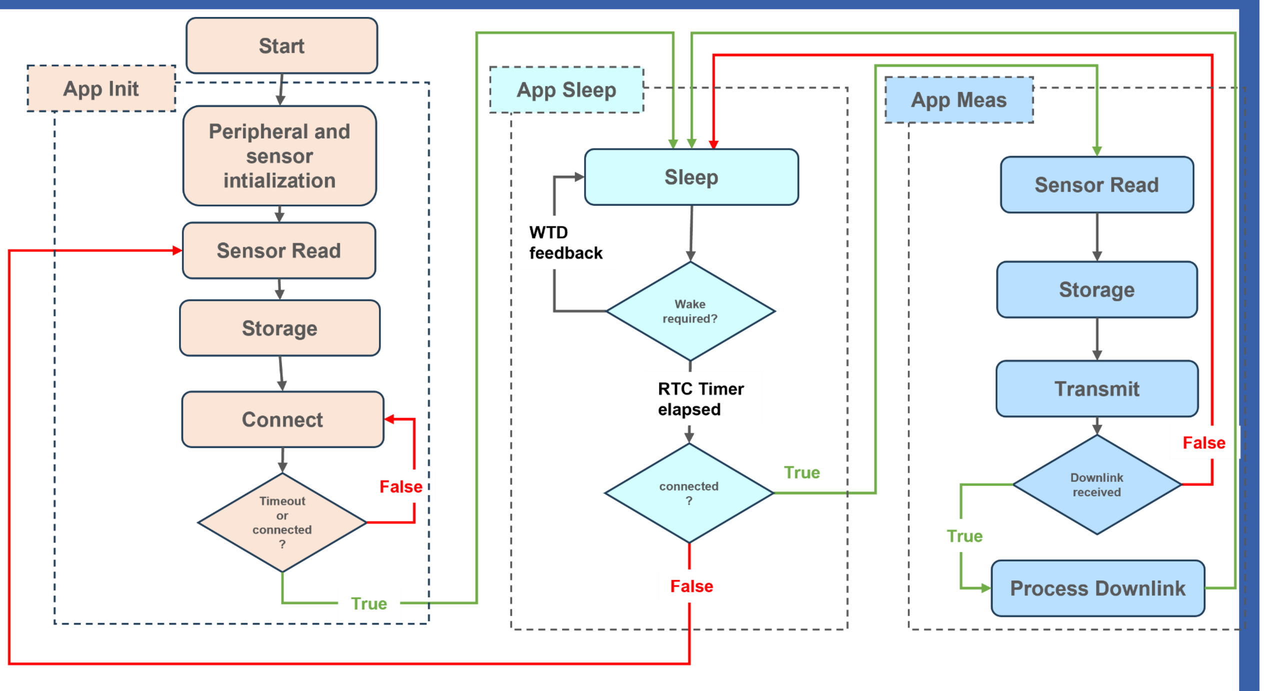

Fig. 2. BatMon Firmware flowchart description.

An internal Real Time Clock is used to schedule all the operations. During all phases, the MCU feeds the Ext WTD via an external interrupt. By changing the App sleep duration, it is possible to increase the system lifetime:

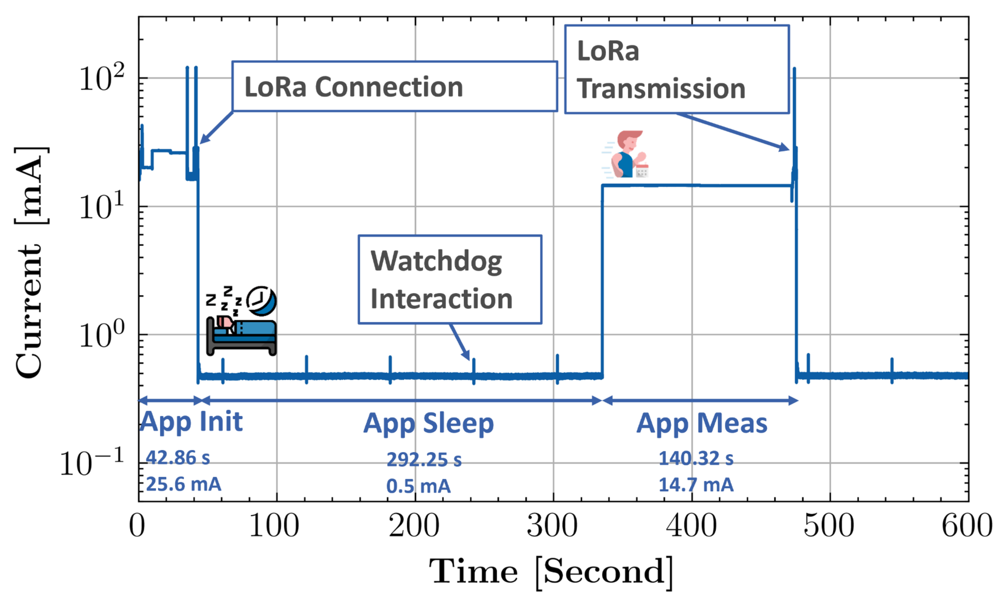

Fig. 3. BatMon current consumption over time.

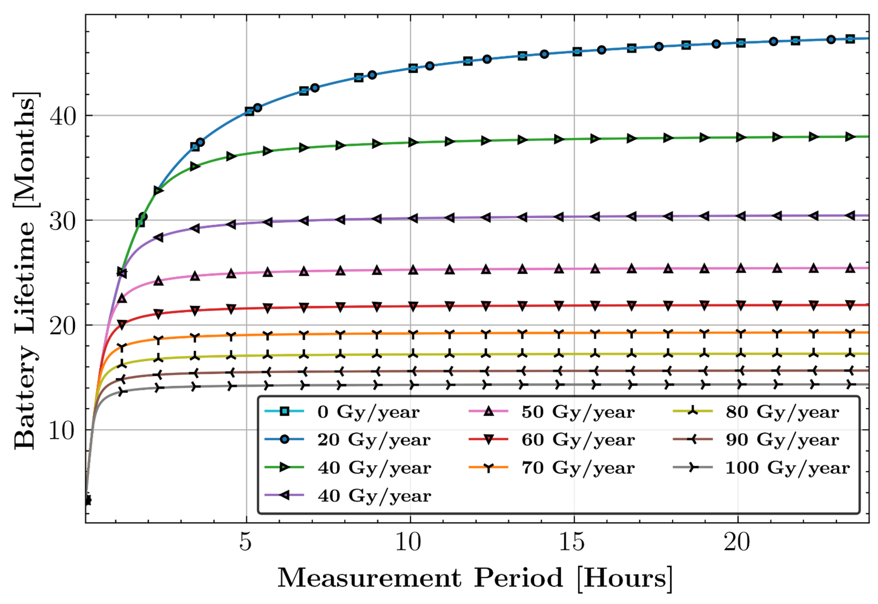

Fig. 4. Expected BatMon Lifetime for different yearly dose rates and Measurement Period.

Mitigation Schemes

(1) Ext WTD

- The Ext WTD is the classic hardware mitigation used to restore MCU functionality.

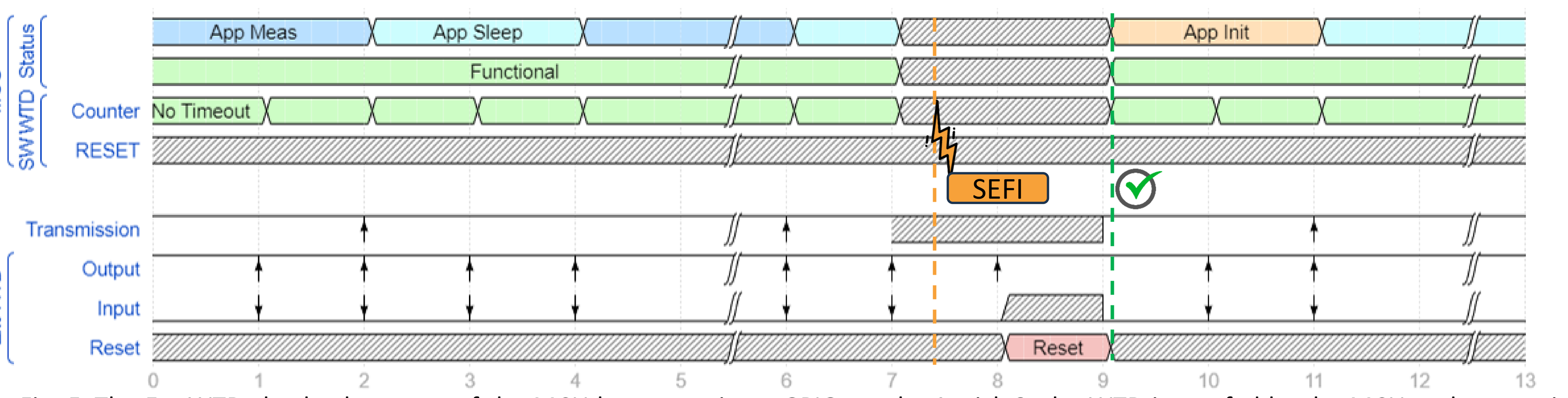

Fig. 5. The Ext WTD checks the status of the MCU by requesting a GPIO toggle. At tick 8, the WTD is not fed by the MCU and a reset is performed by the external component. MCU functionality is restored.

(2) Software (SW) WTD

- Some failures may be invisible to the Ext WTD (longer sleep time, stack in while loop) Hardware internal watchdog is not an option due to lifetime limitation (< 100 Gy).

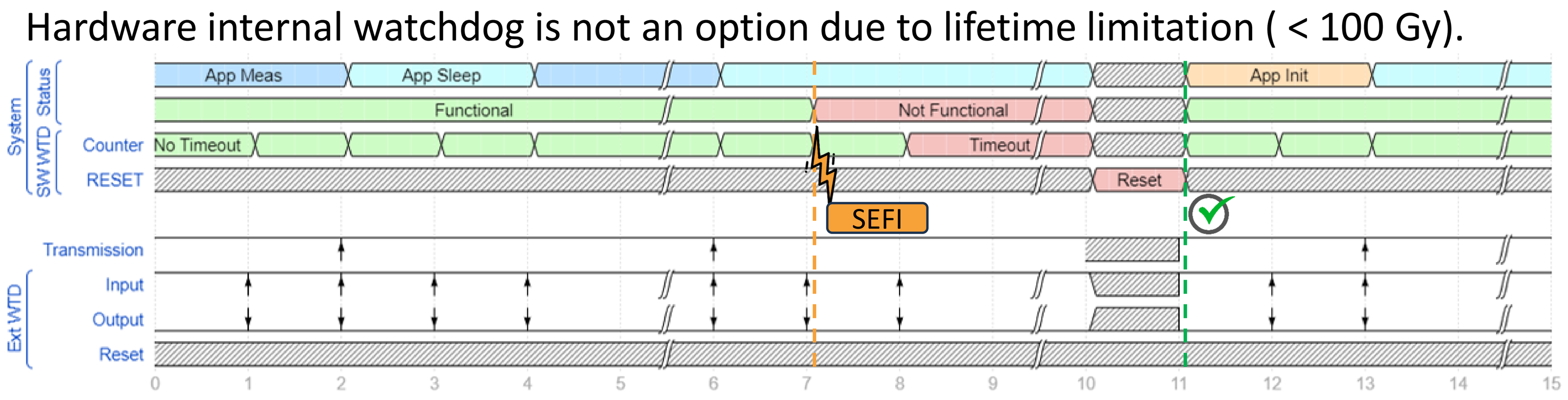

Fig. 6. At tick 7 a failure occurs which the watchdog cannot detect because the MCU continues to reply. Due to the failure, the MCU is locked in App Sleep. At tick 10, the timeout has been reached, the SW WTD recognizes that the system is not functional and self-resets.

(3) Network Link Check

- A link check mechanism based on the use of LoRa Confirmed Uplink (CU) is employed to check for network unavailability or transceiver failure.

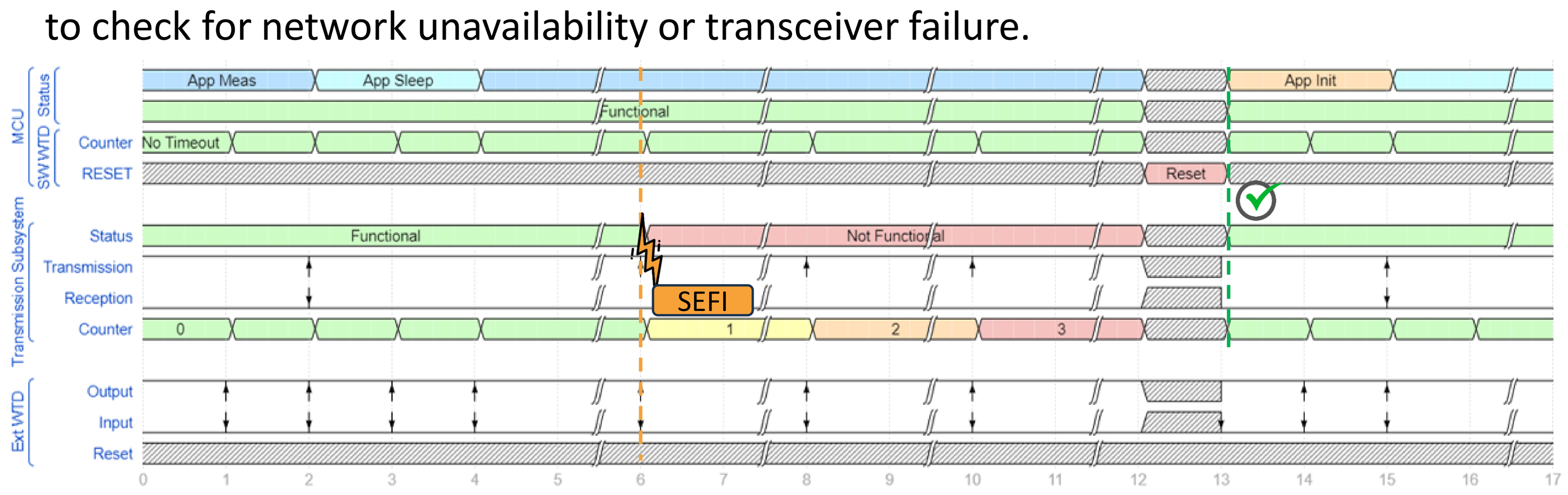

Fig. 7. The failure of the transceiver is invisible both to the Ext and SW WTDs. Every 3 transmissions, the MCU requests a CU and updates a counter. If the confirmation is received (Tick 2), the transceiver is considered operational. If the confirmation is not received (Tick 6), a counter is updated and a confirmation is requested at the next uplink. If it is not received 3 times in a row, the system restarts.

Other protection mechanisms:

- A management function via attribute instruction is assigned to all handler function definitions in the code and provides protection against incorrect configurations that could result from SEEs (4).
- TMR applied to critical counters used in the firmware functionalities (5) .

Proof Of Concept

To verify the impact on system operation in terms of availability, it was decided to test two BatMons at CHARM: one using SMS and one using only Ext WTD as mitigation. The LoRa Frame Counters (FCNT) (Transmission Counter) of the two devices, recorded during the tests:

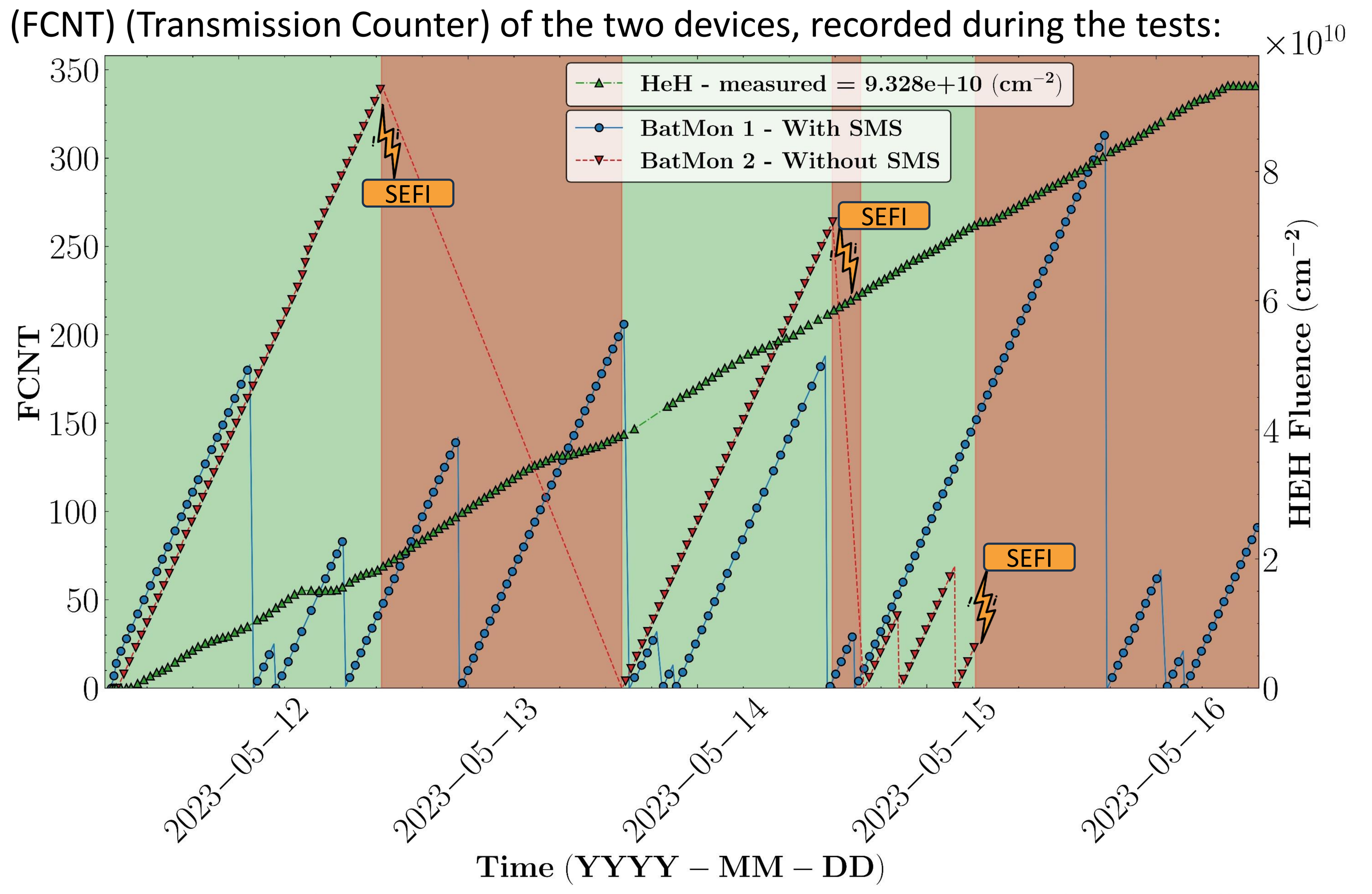

Fig. 8. The LoRa FCNT is depicted for the two BatMons tested in CHARM. The BatMon without the SMS (in red), was affected by SEFIs not detected by the only Ext WTD. During these malfunctioning periods (in Brown), the device was not able to transmit or was stacked in a while loop or sleep mode. On the other hand, when the SMS was implemented (BatMon 1 in blue), the device ran without interruption throughout the test, with only a few intervals without any data due to error detection and recovery times.

Device	Downtime Period [Minute]	Downtime/Uptime [%]	Mitigation Used
BatMon 1	187	2.58	All
BatMon 2	3517	48.82	(1), (4)

Conclusions

- In this paper, **Software Mitigation Schemes** for MCU-based designs going through different operating states, typical of IoT devices, have been presented and their impact on system availability under radiation was validated in CHARM → **downtime reduced by a factor 19.**
- The fluence cumulated corresponds to 1.87 years of operation Dispersion Suppressor (DS). Taking into account the downtime observed in CHARM and the time to cumulate such a level of radiation **in the DS, the expected unavailability per year is 0.01%.**
- Considering CERN's annual availability requirements for critical systems **(99.54%)**, an IoT application with BatMon-like performance can foresee 45 systems in this area while respecting the LHC constraints.
- As application **availability** depends on the annual fluence, it **will be higher in low radiation areas** (i.e. LHC alcoves), allowing more systems to be used. → **Most of equipment are installed in these areas.**
- These results demonstrate that **IoT devices can be a viable solution for critical high-distribution systems** in the future accelerators (FCC). In addition, the modularity and versatility of **BatMon** allow it to be **used** for **more critical applications such as system control.**