EUROPEAN SPACE AGENCY CONTRACT REPORT

The work described in this report was done under ESA contract. Responsibility for the contents resides in the author or organisation that prepared it.

E/0904-611 – GSTP Element 1 “Develop”
ESA Contract No. 4000139825/22/NL/AS

SoC-HEALTH^2 –Hierarchical Health Management in Heterogeneous Systems

Final Report

On-Chip Fault Management Framework for FPGA-Based Satellite Electronics

Document revision 1.4

Notices

This document is intended to fulfil the contractual obligations (ESA/ESTEC Contract No. 4000139825/22/NL/AS) and to inform interested stakeholders about the key achievements in SoC-HEALTH2 project with respect to Health Management demonstration framework development.

For more information, please contact Testonica Lab at email: info@testonica.com

About Testonica Lab. Established in 2005, Testonica has become a global technological leader in automated synthetic and virtual embedded instrumentation, specializing in advanced solutions for electronic test and diagnostics. The company is the creator of Quick Instruments (QI) – an FPGA-based platform that temporarily transforms existing on-board FPGAs into fully automated embedded testers, which streamlines debugging and improves first-pass yield by catching defects early in the production process. For 20 years, Testonica's tools have been used across industries such as telecommunications, automotive, aerospace, defense, industrial electronics, and consumer devices with proven deployment in over 20 countries. The company also provides deep technical capabilities in system health management, including the development of hierarchical embedded instrumentation networks for in-field error detection and diagnostics. Testonica focuses on technologies like embedded CPUs, microcontrollers, reconfigurable FPGAs, and SoC-FPGAs.

List of Abbreviations

ACAP – Adaptive Compute Acceleration Platform
AFPN – Automatic Fault Propagation Network
API – Application Programming Interface
APU – Application Processing Unit
AXI – Advanced eXtensible Interface (bus)
BIST - Built-in Self-test
BSP – Board Support Package
BTMR – Block TMR
CCSDS – Consultative Committee for Space Data Systems
COTS – Commercial-Off-The-Shelf (components)
CPU – Central Processing Unit
CRC – Cyclic Redundancy Code
DNN – Deep Neural Network
DTMR – Distributed TMR
EGSE – Electrical Ground Support Equipment
EI – Embedded Instrument
ESA – European Space Agency
ESIB – Enhanced SIB
FPGA – Field Programmable Gate Array
HAL – Hardware Abstraction Layer
HM – Health Manager
IJTAG – Internal JTAG
IM – Instrument Manager
IP – Intellectual Property
IPI – Inter-Process Interrupt
IRQ – Interrupt Request
ISR – Interrupt Service Routine
LAN – Local Area Network
LEO – Low Earth Orbit
MII – Media-independent Interface
NASA – National Aeronautics and Space Administration
NN – Neural Network
OCFM – On-Chip Fault Management
OCM – On-Chip Memory
OS – Operating System
PL – Programmable Logic
PMC – Platform Management Controller
PMU – Platform management Unit
PS – Processor System
PUS – Packet Utilization Standard
RAM – Random Access Memory
RTOS – Real-time Operating System
RPU – Real-time Processing Unit
RSN – Reconfigurable Scan Network

SDK – Software Development Kit
SEE – Single-Event Effects
SET – Single Event Transient
SEU – Single Event Upset
SGMII – Serial Gigabit MII
SIB – Segment Insertion Bit
SoC – System-on-Chip
ST – Service Type
SW – Software
SM – System Map
TC – Telecommand
TCM – Tightly Coupled Memory
TEMAC – Tri-Mode Ethernet Media Access Controller
TID – Total Ionizing Dose
TM – Telemetry
TRS – Technical Requirement Specification
UART – Universal Asynchronous Receiver Transmitter
VSEI – Vendor specific EI
XML – Extensible Markup Language

1 Overview

Ensuring the reliability and fault tolerance of satellite electronics is paramount for mission success in diverse space environments. Over the last decade, the space sector has seen significant diversification between traditional institutional missions led by agencies such as ESA and NASA and commercial New Space initiatives driven by private companies. Both domains have increasingly adopted high-performance commercial-off-the-shelf (COTS) components, such as FPGAs, accelerators, microprocessors, and memories, to meet growing demands for computational power and cost efficiency. COTS components usually offer orders of magnitude higher performance compared to radiation-hardened or radiation-tolerant alternatives. However, their susceptibility to radiation-induced Single-Event Effects (SEE) and Total Ionizing Dose (TID) radiation effects poses critical challenges.

For institutional missions, reliability and compliance with stringent standards remain important. These missions often use proven and qualified components, but efforts are underway to incorporate COTS devices alongside advanced fault mitigation strategies. Conversely, commercial New Space missions prioritize high performance and rapid deployment, leveraging COTS components with systematic testing and software-based fault mitigation to achieve cost and time efficiencies. CubeSat deployments and Low Earth Orbit (LEO) satellite constellations often operate with minimal qualification processes, relying on shorter mission lifetimes and operational flexibility to accommodate risks.

The **On-Chip Fault Management (OCFM)** framework provides a unified solution to address the needs of both institutional and commercial missions. The framework integrates real-time fault detection, isolation, and recovery capabilities into FPGA-based satellite electronics, including platforms like **Xilinx Versal ACAP**. By implementing fine-grained health monitoring and hierarchical cross-layer fault management, OCFM ensures autonomous and adaptive system operation even in a hostile environment.

OCFM's health management enables graceful degradation, leveraging remaining healthy resources to sustain mission-critical functions. Its modular design supports scalability, from single SoC implementations to complex multi-board systems, ensuring applicability across diverse mission architectures. The framework also maintains compliance with industry standards for institutional missions while offering the agility needed for New Space applications. This dual focus positions OCFM as an essential enabler of next-generation satellite systems, balancing performance, reliability, and cost efficiency.

A key advantage of this solution is its hierarchical cross-layer health management approach. Fault detection, data collection, and recovery mechanisms are distributed across the system's hardware, OS software, and application layers. This architecture enables fault-aware task scheduling and adaptive resource utilization, providing decent performance using remaining healthy resources. By leveraging the OCFM framework, satellite systems can achieve unparalleled resilience and operational efficiency, reducing downtime and mission risks while minimizing the reliance on full hardware redundancy. The ESA-funded GSTP project SoC-HEALTH2 expanded the OCFM framework to support advanced FPGA SoC platforms like Xilinx Versal ACAP (Adaptive Compute Acceleration Platform) to a significant extent.

2 The Changing Paradigm of Space Missions

In the evolving landscape of satellite technology, ensuring reliability and fault tolerance has become a critical challenge. Institutional space agencies like ESA and NASA prioritize stringent reliability and compliance standards, ensuring mission success over extended lifetimes. Conversely, New Space ventures, driven by commercial entities, emphasize rapid deployment, cost efficiency, and high performance. This divergence underscores the need for scalable and adaptable fault handling solutions capable of addressing the unique challenges of both domains.

The adoption of high-performance commercial-off-the-shelf (COTS) components, such as FPGAs, accelerators, microprocessors, and memories, has revolutionized the space sector by providing superior computational capabilities. However, these components bring inherent vulnerabilities to radiation-induced effects, such as Single Event Upsets (SEUs) and Total Ionizing Dose (TID), making robust fault management indispensable.

COTS components are pivotal in bridging performance gaps, enabling advanced capabilities for Earth observation, telecommunications, and scientific research. However, their susceptibility to radiation-induced faults poses a significant barrier to their widespread adoption in critical missions. Satellites operating in Low Earth Orbit (LEO) and beyond encounter harsh environments where robust fault mitigation strategies are non-negotiable.

The **On-Chip Fault Management (OCFM)** framework emerges as a cutting-edge solution, addressing the diverse needs of institutional and commercial New Space missions alike.

2.1 Radiation Environment and Challenges in Space

The radiation environment that poses significant challenges to satellite electronics primarily consists of protons, electrons, cosmic rays, and solar particle events. High-energy protons are abundant in the Van Allen radiation belts surrounding Earth, particularly affecting satellites in LEO. Electrons with lower mass but significant energy levels also contribute to cumulative radiation exposure, causing degradation over time. Galactic cosmic rays are high-energy charged particles originating outside our solar system. They include protons, heavy ions, and nuclei, and are capable of penetrating satellite shielding, leading to ionization effects in sensitive components. During periods of heightened solar activity, solar flares and coronal mass ejections release bursts of high-energy protons and heavy ions. These events can cause sudden and severe radiation exposure to satellites.

Radiation exposure leads to various faults in satellite electronics, which can disrupt or degrade performance. Here are a few key examples. Single Event Upsets (SEUs) - bit flips in memory or logic circuits caused by a single charged particle striking a sensitive node. Single Event Latchups (SELs) - persistent high-current states in CMOS devices that may lead to component failure. Single Event Transients (SETs) - temporary voltage spikes in analog or digital circuits caused by ionizing particles. Total Ionizing Dose (TID) - accumulation of ionizing radiation over time can degrade the performance of semiconductor materials, leading to parameter shifts or permanent damage in components. Displacement Damage (DD) - non-ionizing energy

deposition displaces atoms in the crystal lattice of semiconductor materials, reducing performance in photodiodes, sensors, and transistors.

These faults necessitate robust fault mitigation strategies to ensure uninterrupted satellite operations and prevent mission-critical failures.

2.2 Typical Solutions and Their Limitations

Several fault mitigation solutions are typically employed in the space sector, primarily focusing on hardware redundancy, error correction codes (ECC), and Triple Modular Redundancy (TMR). While these methods have proven effective in mitigating faults, they exhibit several limitations:

- **Hardware Redundancy**:
  - Relies on duplicating or triplicating hardware components to ensure fault tolerance. This approach significantly increases weight, power consumption, and cost, making it impractical for many New Space missions.
  - Redundant hardware cannot dynamically adapt to evolving system degradation scenarios, leading to inefficient resource utilization.
- **Error Correction Codes (ECC)**:
  - While effective for memory integrity, ECC is limited to detecting and correcting single-bit or small-scale errors. Larger-scale radiation-induced faults may go undetected or require additional mechanisms for recovery.
- **Triple Modular Redundancy (TMR)**:
  - Ensures fault tolerance through majority voting but increases system complexity and resource requirements.
  - Vulnerable to common-mode failures caused by simultaneous faults in redundant modules, particularly in harsh radiation environments.
- **Software-Based Fault Management**:
  - Commonly used in New Space missions due to its cost efficiency and flexibility. However, software-only approaches are slower in fault detection and recovery, lacking the real-time responsiveness required for mission-critical operations.

2.3 Market Demand Study – Survey Results

We have carried out a survey to map potential users and partners as well as outline their expectations towards the OCFM/HM framework. In total, we have received 14 responses out of 90+ potential respondents from 55 various organizations to whom the questionnaire has been sent.

The majority of actual respondents belonged to space platforms vendors both HW and SW whereas the New Space and commercial segments prevail, being followed by the institutional and the scientific segments. Minimum contribution from start-ups and universities was received. According to the answers, the most active application segments today are The Earth observation and telecommunication. Another large group is formed by scientific missions like probes, instruments, and other experiments.

While some answers give encouraging insights, the modest overall number of active respondents prevents us from drawing general conclusions about the potential application of the developed technology. The most important conclusions are given hereby.

The average mission duration is expected to be 5-10 years, dominated by LEO ones, followed by MEO/GEO. The ECSS standard compliance is expected by majority of respondents both for mission-critical and non-mission-critical sub-system as well as for health management functions. Some respondents would accept military and industrial standards as a possible alternative.

The respondents are using the following hardware modules and operating systems in their satellites (see the table and the figure below).

	OBC module	Payload module	Other	Total
Linux	3	7	3	13
Bare-metal	3	6	4	13
RTEMS	3	4	4	11
FreeRTOS	3	5	2	10
Hypervisor	2	3	2	7
Other OS	4	3	8	15

Table 1. Operating systems used in satellites according to respondents

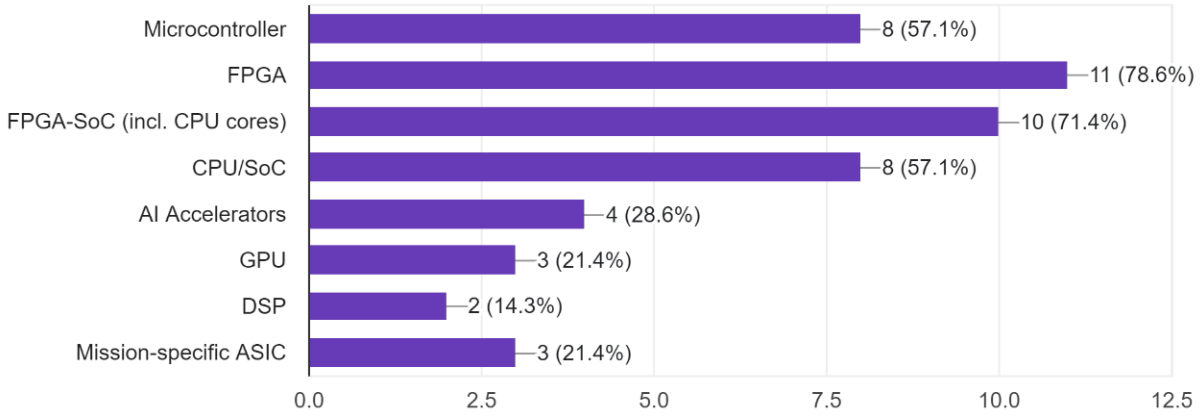

Figure 1. Satellite HW modules that respondents are responsible for

The survey has shown that FPGA SoC devices are expected to clearly win against all other computing/processing platforms (like MCUs, CPUs, GPUs, etc.), whereas the majority of companies plan to employ AMD/*Xilinx Kintex Ultrascale* and *Versal ACAP* as well as *Microsemi (Microchip) PolarFire SoC* devices in their upcoming missions. This confirms the choice of the primary target for the SoC-HEALTH2 activity being FPGA SoCs to be very well positioned.

Since the space industry is traditionally conservative, most of the companies are still not ready to employ off-the-shelf fault-tolerance products and instead rely on their own in-house

solutions, while being still personally curious about the SoC-HEALTH2 project results. Still, almost one third of respondents consider becoming future customers or partners in this activity!

In case of 3rd-party health management technology the users would prefer turn-key solutions taking care of the entire system, including the local FDIR and the fault-tolerance of the CPU/FPGA/SoC sub-system. The most important function of HM is fault detection followed by telemetry reporting as well as in-situ fault correction and fault statistics collection.

Most of the respondents foresee application of HM for both mission-critical (e.g., OBC) and non-mission-critical (e.g., payload) modules. Data-related functions (e.g., data storage, handling and streaming, image processing) are reported to be the most suitable for this type of protection. Command and control related functions (e.g., command and tracking, attitude control, etc) are less relevant.

Regarding the overhead (i.e., memory, storage, power, FPGA logic) of the HM, the responses were spread in a wide range of 1% to 50%. Except for power consumption, there is typically no shortage in HW resources in COTS components. Hence, some respondents did not impose any limits on the HW overhead allowed. All in all, we interpret the highly diversified answers so that sacrificing 10-15% of resources for HM-related functions would generally be tolerable. However, in terms of power budget, the average expectation for the overhead is 5-8%.

Two-thirds of the respondents consider the following techniques as promising for further improving fault tolerance (see the table below).

Fault tolerance technique	**Using now**	**Plan to use in future**	**HM applicability**
TMR in FPGA logic	36%	64%	Monitoring
Dynamic partial FPGA reconfiguration	7%	57%	FDIR
Rad-hard components	43%	50%	Monitoring
Latch-up protection	71%	43%	Monitoring
Global TMR	0%	43%	Monitoring
Fault-tolerant multi-core task scheduling	0%	43%	FDIR
FSM- or block-level TMR	14%	39%	Monitoring
Memory protection mechanisms	79%	35%	Monitoring
Watchdogs/timers	64%	35%	FDIR
Property checkers, embedded instruments	33%	21%	FDIR

Table 2. Fault tolerance techniques applicable to satellite electronics according to respondents

3 SoC-HEALTH2 OCFM Framework: A Unified Approach

The On-Chip Fault Management (OCFM) framework offers a holistic cross-layer fault management approach to fault detection, isolation, and recovery (FDIR) that spans from hardware (e.g., DSPs, NoC) to software (OS, application tasks), leveraging Versal's integration of ARM cores and programmable logic. In this manner, the OCFM ensures sustained operations for a diverse range of satellite architectures even in adverse conditions.

3.1 Key Features

- **Real-Time Fault Management**: Integration of fault monitors and sensors for detecting and isolating hardware faults across processing, memory, and interconnects, while the Automatic Fault Propagation Network (AFPN) ensures low-latency fault signaling.
- **Scalability**: Modular design for seamless integration with diverse satellite architectures, allowing for customization to meet specific mission requirements.
- **Allows predicting** potential hardware failures, enabling proactive fault mitigation and preemptive recovery strategies.

3.2 Architecture Enabling Resilience and Scalability

At the heart of the OCFM framework lies the **Instrument Manager (IM)** and the **Health Manager (HM)**, each serving distinct yet complementary roles in ensuring fault resilience and operational reliability:

- **Instrument Manager (IM)**:
    - Acts as the centralized hub for fault aggregation and diagnostics at the user hardware level. The IM interfaces with embedded sensors, fault monitors, and Reconfigurable Scan Networks (RSN) to collect and process real-time health data.
    - Employs redundancy mechanisms such as Triple Modular Redundancy (TMR) and Error Correction Codes (ECC) to ensure fault-free operation even under radiation-induced soft errors.
    - The IM ensures swift responses to urgent fault conditions using latency-optimized communication pathways via the Automatic Fault Propagation Network (AFPN).
    - Operates autonomously within the programmable hardware layer to isolate, analyze, and propagate fault data, ensuring the integrity of the system's physical components.

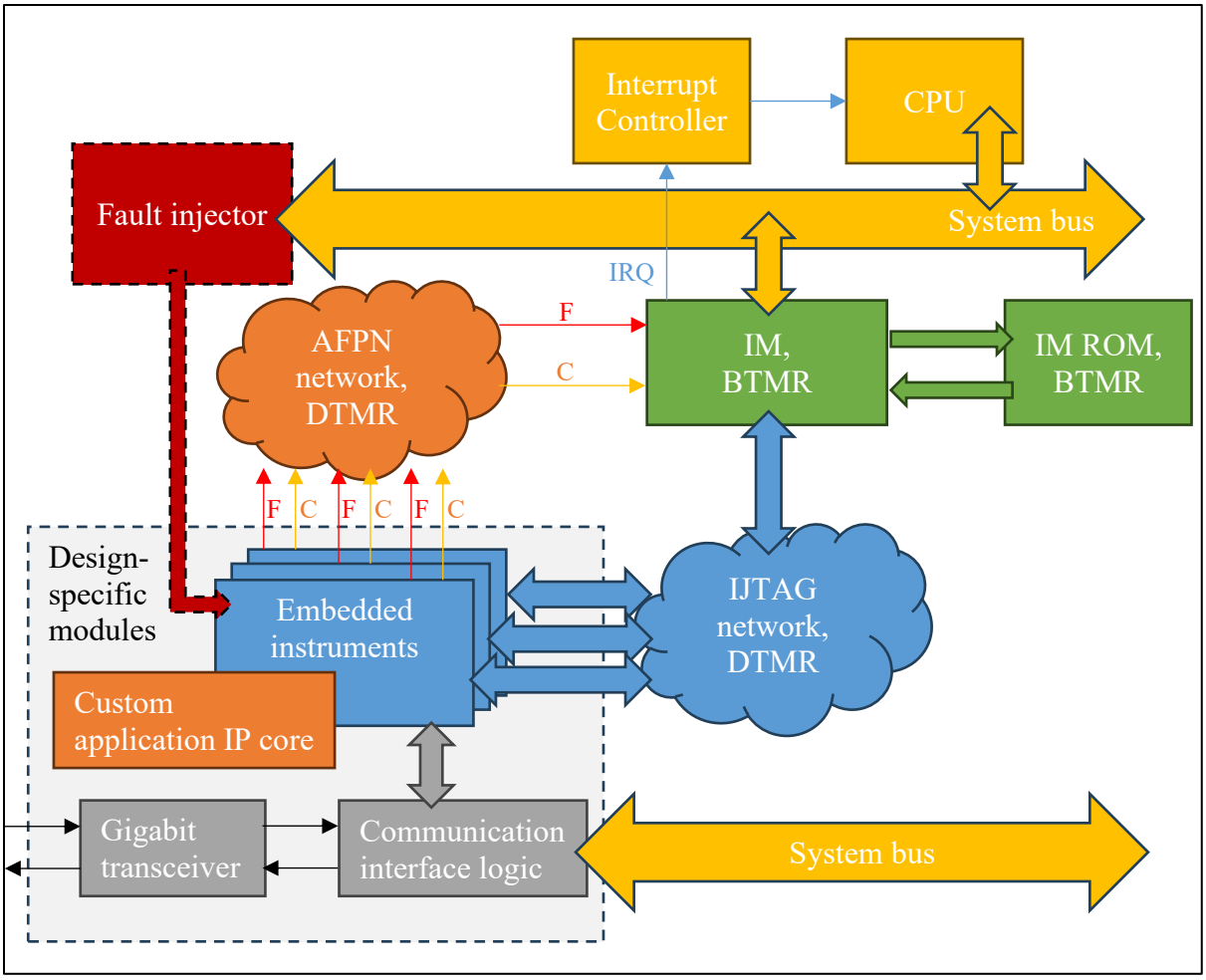

Figure 2. HM hardware block diagram

- **Health Manager (HM)**:
  - Operates at the software layer, leveraging the data provided by the IM to build dynamic health profiles of system components.
  - Maintains the **Health Map,** that provides real-time insights into system health and resource availability.
  - Implements recovery protocols for high-level system operations, coordinating with the IM to initiate hardware-level fault mitigation actions as required.

Together, the IM and HM form a hierarchical fault management mechanism, where the IM ensures low-level fault detection in programmable hardware and immediate response, while the HM oversees system-wide resource management and recovery planning. This collaboration ensures uninterrupted fault management even under severe radiation-induced disruptions, providing a robust foundation for satellite electronics. Other important OCFM framework components are:

- **Fault Monitors**:
  - Sensors embedded in FPGA pipelines, memory, and interconnects provide granular health data and fault detection capabilities.

    - Integration with IJTAG-based networks enables comprehensive fault coverage and efficient instrumentation control.
- **Automatic Fault Propagation Network (AFPN)**:
    - Enables low-latency fault signaling across the system, ensuring rapid detection and isolation of critical faults.
    - Designed for scalability to handle large multi-board systems, maintaining efficiency under high fault loads.
- **Health Map :**
    - HM dynamically updates the health status of system components in Health Map, enabling fault-aware decision-making.
    - HM uses Health Map to track the availability and utilization of system resources, facilitating adaptive scheduling and resource allocation.
- **Self-Protection Mechanisms**:
    - The OCFM framework itself is safeguarded against soft errors through redundancy in critical fault management paths, including the IM and AFPN subsystems. Error Correction Codes (ECC) are implemented in memory blocks to ensure the integrity of stored health data.
    - Periodic self-check routines monitor the integrity of the OCFM hardware and software layers, with a fallback mechanism to recover from transient faults.
    - Triple Modular Redundancy (TMR) is employed in critical components such as the IM, ensuring fault-free operation even under radiation-induced soft errors.

Additionally, the framework's integration of configuration memory protection mechanisms ensures system integrity. Periodic scrubbing corrects transient errors, while ECC and TMR enhance resilience against persistent faults. These features are particularly critical for FPGAs in space, where configuration memory integrity is paramount for mission success.

3.3 Health Management Software Stack

- **Real-Time Fault Management**:
    - Integrated into the operating system to handle fault detection, reporting, and recovery processes autonomously.
    - It applies pre-configured rules and adaptive algorithms to detect anomalies and trigger fault-handling mechanisms.
    - It is built with a hierarchical architecture to manage scalability across complex systems, including multi-board and heterogeneous configurations.
    - Supports multi-layer health monitoring across hardware, OS, and application levels.
- **APIs and Extensions**:
    - HealthMap API provides a standardized interface for historical health data collection and analysis to identify trends and predict potential HW failures.
    - Instrument Manager API enables custom configurations for system-specific fault monitoring needs.

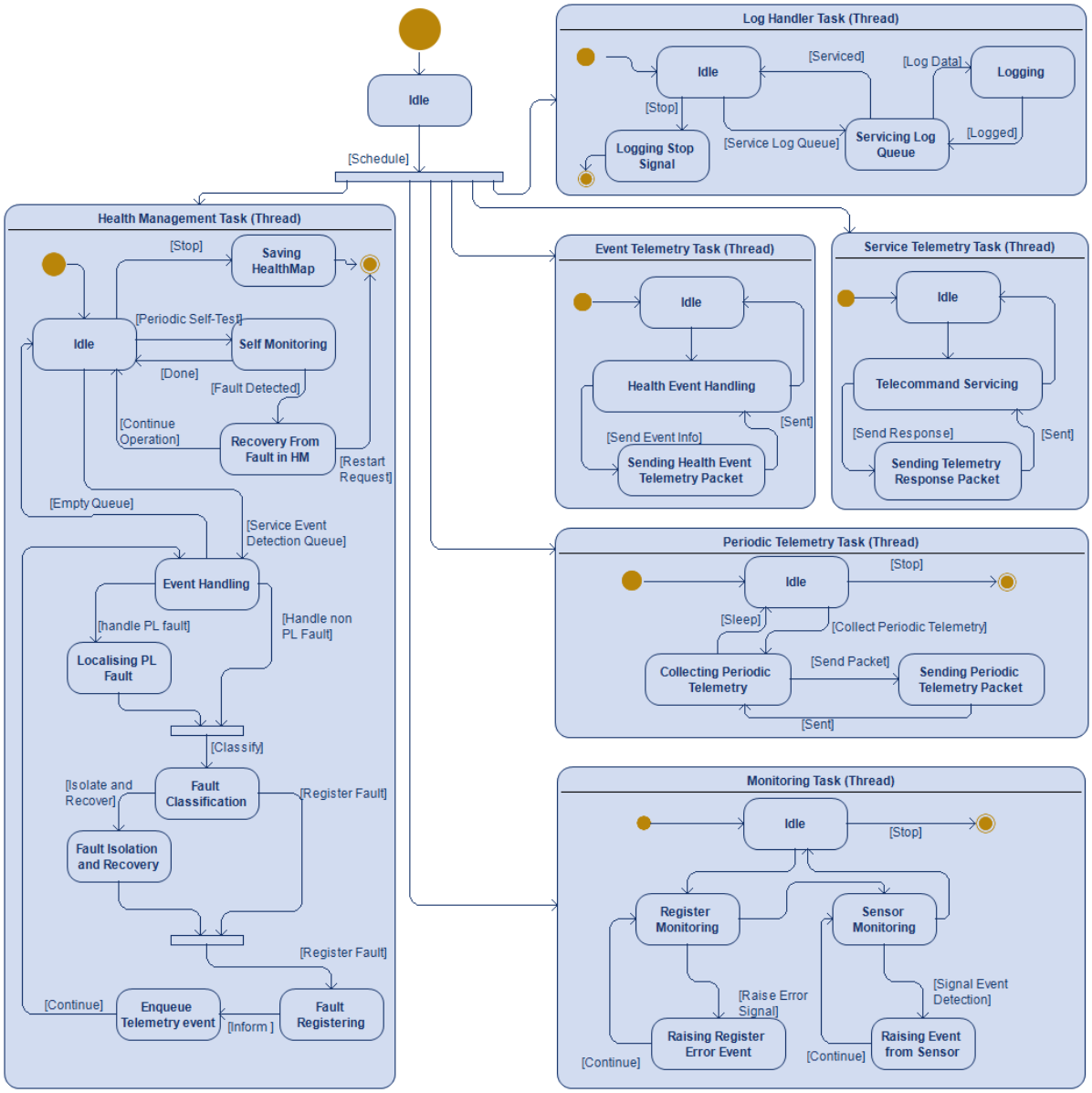

Figure 3. HM software state machine diagram

3.4 FPGA-Specific Enhancements

The ESA-funded GSTP project SoC-HEALTH2 expanded the OCFM framework to support advanced FPGA SoC platforms like **Xilinx Versal ACAP** (Adaptive Compute Acceleration Platform) to a significant extent. Versal ACAP introduces a heterogeneous and highly flexible architecture, including scalar engines (ARM CPUs), adaptable hardware (programmable logic), and intelligent engines (AI cores) as well as some integrated fault-tolerance infrastructure. These vendor-provided fault-tolerance mechanisms are, however, fragmented, leading to inefficiencies and unprotected areas. The OCFM extension to Versal ACAP aims at closing these gaps by offering advancements in several areas.

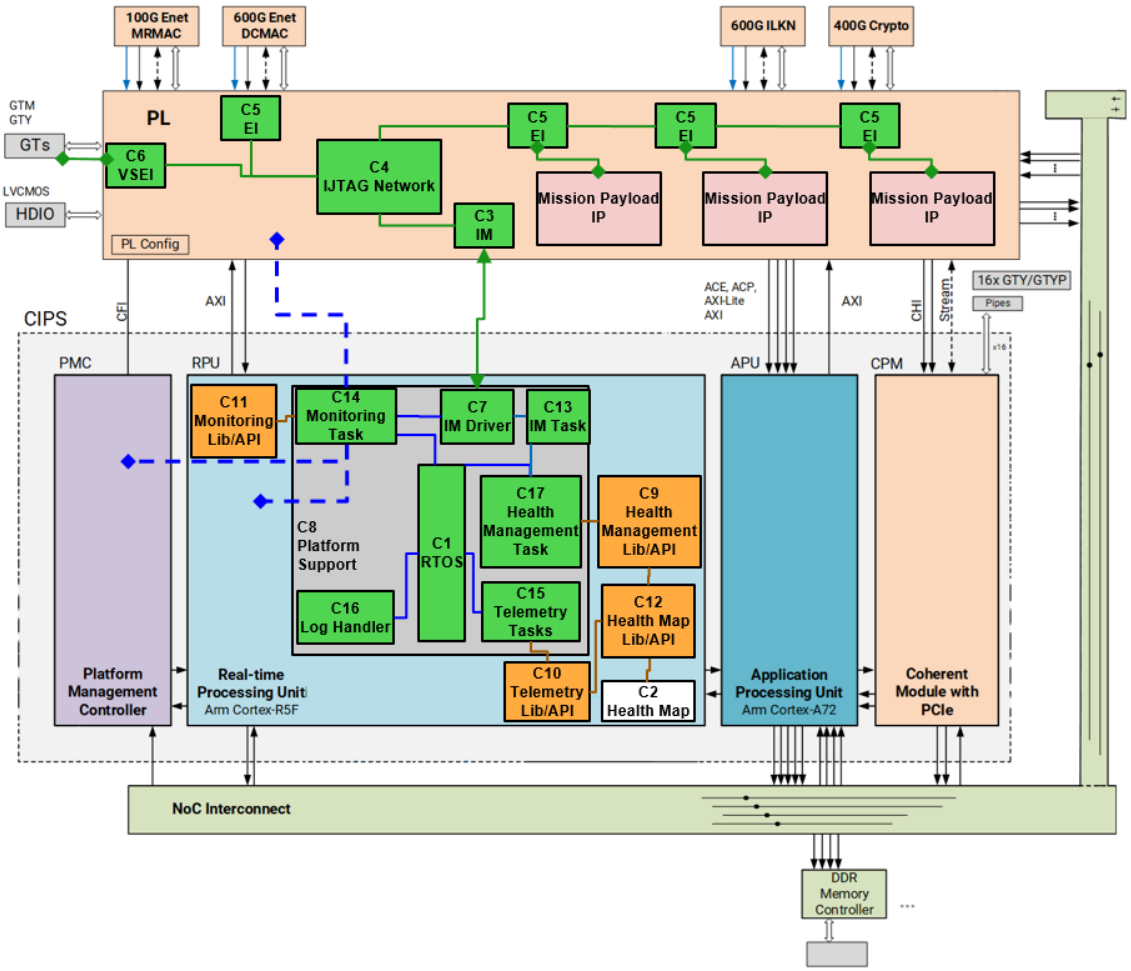

Figure 4. HM demo components location in Xilinx Versal ACAP platform

- **Embedded Instrumentation**:
  - Custom IP blocks deployed in FPGA fabric for monitoring buses, interfaces, and accelerators.
  - Leveraging programmable logic to implement fault-detection logic tailored to mission-specific requirements.
  - Monitoring Versal's AI matrix multipliers and DSP cores for faults in tensor and vector processing units within AI engines.
  - Monitoring Versal's HW component status and configuration (registers in PMC, NoC, LPD and FPD domains , etc.) to gather detailed health data.

- **Integration with Heterogeneous Components**:
  - The modularity of OCFM allows it to monitor scalar (CPU cores), adaptable (programmable logic), and intelligent (AI cores) components of Versal ACAP.
  - Flexible interfaces for external health monitoring modules to expand coverage beyond the SoC.
  - Health Map includes specialized components like DSPs, AI cores, and adaptable logic blocks, alongside CPUs and memory units.
  - Enhance fault classification algorithms support distinct fault models across these heterogeneous elements.

- **Dynamic Reconfiguration Support**:
    - The OCFM can benefit from Versal's ability to dynamically reconfigure hardware at runtime to isolate faulty components and redirect workloads to healthy ones.
    - Interface APIs to Versal's dynamic reconfiguration controllers

Incorporating a cross-layer reliability model integrating hardware health data with OS-level fault handling and recovery protocols based on a unified Health Map that correlates faults across hardware and software layers, the OCFM framework provides a strong foundation for fault handling and health monitoring, supporting a platform as complex as Versal ACAP.

4 SoC-HEALTH2 Framework Demo: Scenarios and Modes

The SoC-HEALTH2 demonstrator showcases hierarchical health management (HM) in FPGA-based systems, specifically implemented on two platforms:

- **VCK190** (Versal ACAP-based, full-featured)
- **ZCU104** (Zynq UltraScale+ MPSoC, reduced feature set)

Demonstration scenarios cover:

1. Fault handling in the **Neural Network (NN) accelerator**
2. Fault handling in the **communication module** (VCK190 only)

Both platforms include a health manager (HM), embedded instruments (IJTAG), EGSE software, and fault injection capabilities.

The demonstrator validates fault management in FPGA-based systems under realistic conditi-ons, demonstrating robust detection, reporting, and recovery mechanisms across processing and communication components. It highlights the value of autonomous fault handling for mission-critical embedded systems in space and other high-reliability applications.

4.1 System Behavior with Health Management Disabled

- Faults occur without detection or mitigation.
- In the NN accelerator, injected faults result in recognition errors in digit classification tasks.
- In the communication module (VCK190), faults interrupt Ethernet connectivity**:**
    - TEMAC faults inhibit the operation of the communication module and will stop data transfers. The physical link connection will be still in “up” state as GTY transceivers remain operational.
    - GTY transient faults disturb transceiver operation for a short period of time(~25 uS). After that period, the transceiver will restore its functions. Such fault will not be discovered at OS level, due to built-in TCP/IP error correction mechanisms.
    - GTY permanent fault causes GTY transceiver to permanently stop its operation. The link will be considered as “down” by Linux OS (i.e., link is completely not operational) causing full link loss, with no system recovery.

4.2 System Behavior with Health Management Enabled

The HM system constantly monitors system parameters, detects**,** localizes**,** classifies**,** and reacts to faults. Logs health events and communicates with the EGSE tool and applications.

- Faults in NN accelerator:
    - HM system detects the fault, localizes, classifies and informs user application running in Linux.

    - Informs the user application to reprocess the affected image recognition in NN accelerator.
    - Accuracy of image recognition task remains unaffected.
- Communication module faults (VCK190):
    - **TEMAC register fault** is detected and corrected (correct value will be restored in the corrupted register; the communication module will resume its operation after a short delay).
    - **GTY transient fault** is detected, registered with the extra diagnosis (GTY status signals state read-out via GTY monitor) and classified as a transient event.
    - **GTY permanent faults** is detected, registered with extra diagnosis, subsequently classified as requiring recovery action. The recovery action (re-programming PL/transceiver) is executed to restore the operation of GTY transceiver (and communication module).

4.3 Demo Scenario Example: Faults in Neural Network Accelerator

```
HM event received: id=1363226913, param=114, ts_sec=1745942246, ts_nsec=0, data=0x10000005A
>>>>>>>>>>>>>>>>>>>> FAULT DETECTED <<<<<<<<<<<<<<<<<<<<
Reported by instrument with ID: 114, (detections count: 1)
Setting health event detection flag!
Processing image 7/7 with Lenet NN IP (enter 'q' to stop):
    :
   %*    ?;
  ,#    :S
  S;   .#.
  %@%?%@%
   ,+:,@,
     +?
     #,
    :#
    ;#%,
     :
Recognized digit: 0  (INCORRECT! should be: 4)
INFO: Health event detected, processing result (recognized digit: 0) may be affected by fault.
INFO: Image 7/7  will be processed again.

Processing image 7/7 with Lenet NN IP (enter 'q' to stop):
    :
   %*    ?;
  ,#    :S
  S;   .#.
  %@%?%@%
   ,+:,@,
     +?
     #,
    :#
    ;#%,
     :
Recognized digit: 4 (correct)
Statistics correct/total: 7/7 (100.00 %), reprocessed due to faults 1
```

Prerequisite: The sh2demo Linux app is running and performs handwritten digit classification on a preloaded set of digits using a LeNet NN IP core. Application sends data and status for every digit processing to Linux console.

- **Fault injection**

  Open Linux console on the target system and run script: dnn_fault_inject.sh. Script executes commands to perform fault injection into NN IP. Injected fault leads to recognition errors seen in the sh2demo Linux app output.

- **Fault injection with enabled HM**

  HM detects a fault in NN IP and sends a IPI message to the sh2demo Linux app. The application receives a fault notification and displays a "Fault detected " message to Linux console. Potentially erroneous recognition is *automatically reiterated,* improving accuracy.

Verify by observing the Linux console output that the fault is being detected by HM, reported to user-application which restarts the recognition process to get the correct results.

In addition, registered fault events and system health status can also be observed in EGSE emulation application.

4.4 User Interaction

The following user interaction means with the target system are provided:

- Linux access via UART or SSH (only for VCK190).
- Fault injection via pre-installed scripts in /home/root/fi.
- Health status and response verification via EGSE GUI and Linux logs. In EGSE, press "*Report health map*" button to update the health map. Notice, the recorded faults inside the GTY IP module:

Health Map update 19:28:48

	Id	Name	Status	Faults/Detections	Fault Pers
40	0x1040001	PL	Propagated Fault	0	Permanen
41	0x21a0001	PL.CRAM	Healthy	0	-
42	0x21b0001	PL.VSEI	Healthy	0	-
43	0x3040001	PL.VSEI.FPGA_PLL	Healthy	0	-
44	0x21c0001	PL.DSP-engines	Healthy	0	-
45	0x21d0001	PL.CommModule	Propagated Fault	0	Permanen
46	0x3050001	PL.CommModule.GTY	Own Fault	4	Permanen
47	0x3060001	PL.CommModule.TEMAC	Healthy	0	-

Figure 6. Heals Map status report

4.5 EGSE Software

HM system is designed to run autonomously and unsupervised. The telemetry component of HM system is optional and can be included at compile time. HM Telemetry is compliant to CCSDS space packet structure defined in ECSS-E-ST-70-41C.

To display the HM system operation, the application emulating EGSE equipment by sending and receiving CCSDS/PUS packets to HM system is provided as part of the demonstrator.

EGSE software is provided as Python GUI application with multiple panels (Control, Status, Console, Health Map).

EGSE Software application control panel provides instruments to send receive CCSDS/PUS packets to:

- Enable/disable health management operation
- Enable/disable monitoring of system status and various parameters (e.g. voltage and temperature)
- Download HM log data
- Request system health status (health map)

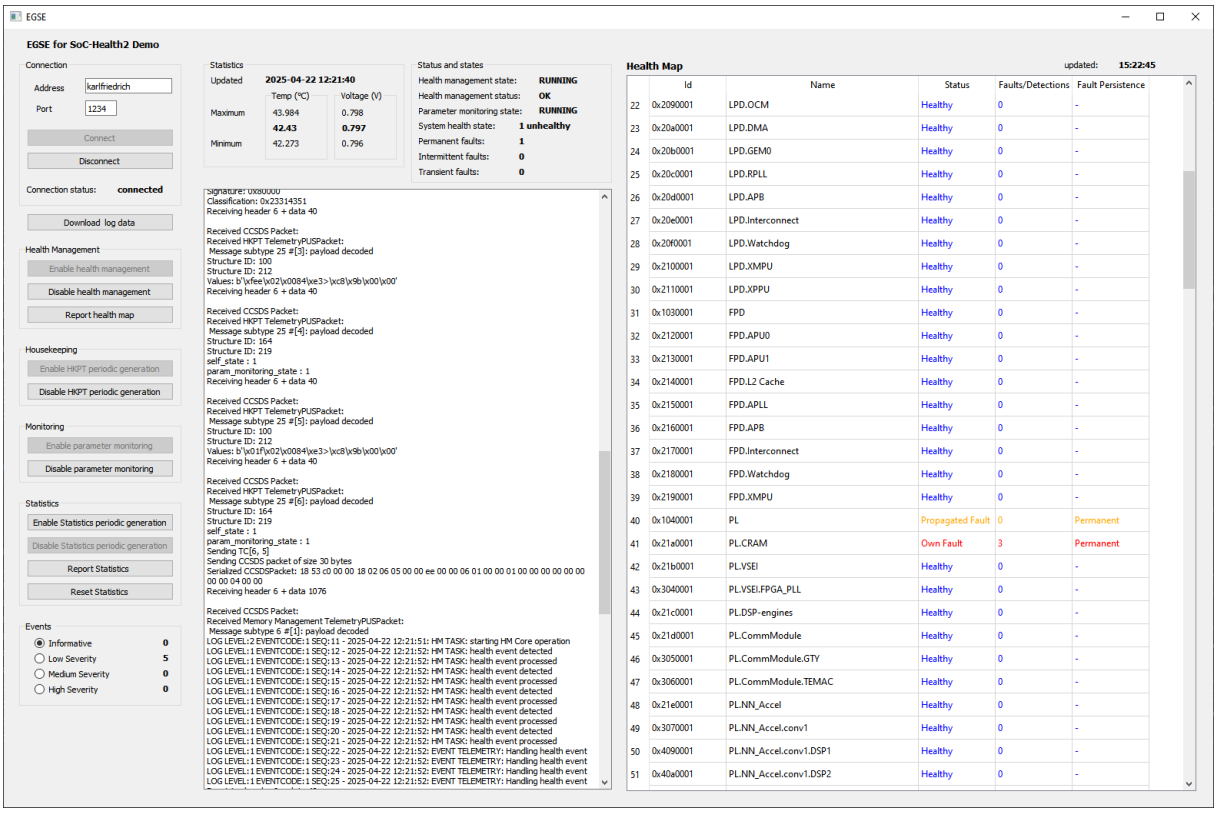

Figure 6. EGSE emulation software GUI

5 Benefits and Differentiators

Adapting the OCFM framework to Versal ACAP allows to leverage its complexity, reconfigurability, and heterogeneity towards advancements in dynamic reconfiguration, intelligent fault prediction, and cross-layer integration. OCFM maximizes the reliability and efficiency of Versal-based systems in the following ways.

- **Increased Reliability**: Continuous operation of critical systems under adverse conditions ensures mission success and operational stability.
- **Reduced Costs**: Minimization of hardware redundancy requirements and associated weight and launch costs provides significant financial and payload efficiency.
- **Extended Mission Lifespan**: Fault prediction, coupled with graceful degradation mechanisms, extends system longevity and reduces the need for frequent interventions.
- **Operational Flexibility**: Adaptable to heterogeneous FPGA-based systems and future mission needs, ensuring compatibility with a variety of satellite platforms and payload configurations.
- **Standards Compliance**: Fully aligned with ECSS requirements for space electronics, ensuring rigorous quality and reliability.
- **Improved Sustainability**: Proactive fault management reduces system downtime, enabling more efficient utilization of satellite resources throughout the mission lifecycle.

5.1 Applicability to payload and OBC subsystems

The OCFM framework is arguably better suited for the on-board computer (OBC), given its centralized role in satellite operations and the need for system-wide fault resilience. However, implementing OCFM in payload subsystems provides a value for missions where payload data is the mission's primary output. For maximum mission reliability, a hybrid approach could integrate OCFM into both subsystems, leveraging its adaptability to address the specific needs of each.

5.1.1 Applicability to payload subsystems:

- The payload often contains highly specialized instruments and sensors critical to the mission's primary objectives (e.g., imaging, communications, scientific experiments).
- OCFM's fine-grained health monitoring and fault-tolerant mechanisms ensure sustained operation of these sensitive components.
- Health-aware scheduling can prioritize mission-critical tasks during degraded states, ensuring payload functionality is maintained even when resources are constrained.
- Configuration memory protection and partial reconfiguration mechanisms safeguard the payload's programmable logic and FPGA subsystems against radiation-induced faults.
- While ensuring payload resilience is vital, the complexity of implementing OCFM across diverse and specialized payload designs may require additional customization.

5.1.2 Applicability to OBC subsystems:

- The OBC is the brain of the satellite, responsible for managing mission operations, processing data, and maintaining communication with ground stations.
- OCFM is inherently well-suited for the OBC, as its hierarchical fault management integrates seamlessly with the processing cores, memory units, and interconnects typically found in OBC architectures.
- AI-driven fault prediction can enhance the OBC's ability to preemptively address potential failures, ensuring uninterrupted command and data handling (C&DH) operations.
- The framework's ability to dynamically reallocate resources ensures continued operation of critical OBC functions, even in partially degraded states.
- The OBC's centralized role in mission success means fault management here is non-negotiable, and OCFM's robust design can maximize reliability in this subsystem.

5.2 Added Value for Users

While traditional approaches depend heavily on full hardware redundancy, increasing cost and power consumption, the OCFM approach balances the workload only being activated for detecting and mitigating faults where it’s needed, thus reducing redundancy needs while maintaining high reliability. Designed for FPGA-based platforms, including Xilinx Versal ACAP, enabling scalability across diverse satellite architectures and use cases. AI-driven fault prediction ensures adaptability to evolving mission requirements and emerging technologies, making the system robust against unforeseen challenges.

- **Mission Success Assurance**: Real-time fault management and predictive maintenance ensure uninterrupted satellite operations and maximize uptime.
- **Cost Efficiency**: Reduced dependency on hardware redundancy translates to lighter payloads, lower launch costs, and better utilization of mission budgets.
- **Enhanced Reliability**: Comprehensive fault coverage mitigates the risks of radiation-induced faults and other environmental challenges, ensuring long-term operational stability.
- **Long-Term Support**: Post-deployment services, including updates, optimizations, and technical support, safeguard mission longevity and adaptability.
- **Future Adaptability**: Modular and AI-driven design ensures readiness for future technologies and mission requirements, offering flexibility for evolving operational needs.

6 Conclusions

While traditional approaches depend heavily on full hardware redundancy, increasing cost and power consumption, the OCFM approach balances the workload only being activated for detecting and mitigating faults where it's needed, thus reducing redundancy needs while maintaining high reliability. Designed for FPGA-based platforms, including Xilinx Versal ACAP, enabling scalability across diverse satellite architectures and use cases.

The proposed OCFM implementation for FPGA-based satellite electronics offers a cross-layer solution for improving system reliability, fault tolerance, and cost efficiency. The ESA-funded GSTP project SoC-HEALTH2 expanded the OCFM framework to support advanced FPGA SoC platforms like Xilinx Versal ACAP to a significant extent.

The SoC-HEALTH2 demonstrator proves robust detection, reporting, & recovery mechanisms under realistic conditions and across processing and communication components highlighting the value of autonomous fault handling for mission-critical systems and applications.

According to our user survey study most of the companies still support a conservative approach relying on their own in-house solutions. However, almost one third of respondents considered becoming future customers or partners in this activity

Our team is committed to delivering a customized and scalable solution tailored to target satellite mission needs. With a focus on long-term support, adaptability, and mission-critical reliability, the OCFM framework is the ideal choice for next-generation satellite electronics.

For any inquiries, please contact us at info@testonica.com.