ESTCP

EXECUTIVE SUMMARY

Integrated Microgrid Control Platform

Gabor Karsai
Vanderbilt University

Srdjan Lukic
North Carolina State University

March 2024

ESTCP EW20-5139

EXECUTIVE SUMMARY
Project: EW20-5139

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS AND ABBREVIATIONS

ARPA-E	Advanced Research Projects Agency - Energy
DoD	Department of Defense
DER	distributed energy resource
DG	distributed generator
DOS	denial-of-service
ESTCP	Environmental Security Technology Certification Program
genset	diesel generator
HIL	hardware-in-the-loop
ICS	industrial control system
IEEE	Institute of Electrical and Electronics Engineers
IMCP	integrated microgrid control platform
LAN	local area network
POI	point of interconnection
RIAPS	resilient information architecture platform for smart grid
TCP/IP	transmission control protocol/internet protocol

ACKNOWLEDGEMENTS

This material is based upon work supported by the United States Army Corps of Engineers under Contract No. W912HQ20C0040 and the Department of Defense (DoD) Environmental Security Technology Certification Program (ESTCP). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Army Corps of Engineers or the DoD ESTCP.

1.0 INTRODUCTION

Microgrids are increasingly being used as energy systems for military installations and forward deployed units. Microgrids are small-scale energy networks, and they typically include several alternative, distributed energy resources (DER), like photovoltaic cells, battery energy systems, and diesel generators ('gensets') as energy sources, but they are also connected to the main utility grid, if needed. Energy is either supplied by the local DERs, or by the utility grid, but the microgrid could also supply power to the main grid.

Integration of heterogeneous generation sources and legacy devices into a DoD microgrid poses several hardware and software challenges: lack of advanced control algorithms; engineering processes for integrating various generation technologies; and the inherent complexities of system configuration and integration. Forming networked microgrids out of heterogeneous power sources adds more complexity due to the varying dynamics of the resources, potentially different communication protocols for each resource, and the required redesign of the protection systems. Further, the management of legacy loads presents another layer of complexity. A significant challenge here is to manage and control networks of microgrids, changing the system topology 'on the fly', i.e., while the system is operational.

A DoD Microgrid Control System is a mission- and safety-critical industrial control system (ICS), operating in a national security environment. But it is also a distributed system, implemented using computing and networking technologies that are potentially exposed to cyber threats. Hence, effort needs to be devoted to cyber-security to protect against various forms of cyber-attacks.

The integrated microgrid control platform (IMCP) project was designed and executed to address these issues. Subsequent sections summarize the objectives of this project, and the technology developed, assess the performance and estimated costs, and discuss implementation issues. The summary concludes with outlining implications for future research and benefits for DoD.

2.0 OBJECTIVES

The objective of the research was to demonstrate advanced technology for microgrid integration and control that provides a scalable and reusable solution, yielding a highly configurable IMCP, based on distributed computing techniques, advanced software engineering methods, cyber-security protections, and state-of-the-art control algorithms. This activity was directly related to the DoD Statement of Need for advanced, affordable, and resilient energy systems for military installations.

Here, the concept 'distributed' denotes an architecture where monitoring and control functions are implemented in a network of embedded computing nodes that are attached to key monitoring and control devices in a power network and communicate via a data network, collaborating in a peer-to-peer fashion. The solution developed by this project addressed the heterogeneity problem by encapsulating the specific details of protocols into reusable 'device components' with common interfaces, and the dynamic grid management and reconfiguration problem with advanced distributed algorithms that form the foundation for a decentralized and expandable microgrid controller.

The long-term vision of this project was that the distributed, open platform-based approach would not only enable technological advances, like intelligent energy management and networked microgrids, but would also reduce the engineering costs. Distributed systems also facilitate enhanced resilience through redundancy and provide opportunities for enhanced cyber protections. Arguably, distributed architectures could be made more resilient than centralized controllers, where the sole controller itself is a single point of failure.

However, these claims had to be validated in a hardware-in-the-loop (HIL) environment before fielding such systems. The goal of this project was to confirm these claims and to show how a resilient distributed microgrid control system could be built in a modular fashion, from pre-designed computational components, including advanced control algorithms and device protocol interfaces. This validation was performed through executing a suite of test scenarios in a high-fidelity, simulation-based HIL environment that showed the level of maturity of the technology and its readiness for use in the field.

3.0 TECHNOLOGY DESCRIPTION

IMCP included two technologies: (1) resilient information architecture platform for smart grid (RIAPS), a software platform, and (2) a microgrid control and integration technology based on advanced, distributed, and resilient control algorithms, running on RIAPS. RIAPS has been supported by an earlier Advanced Research Projects Agency – Energy project, and it has been improved for the purposes of this project. The ESTCP program has supported (1) the implementation of the IMCP control algorithms and (2) the extensions to RIAPS to support device connectivity for the microgrid controller.

3.1 RIAPS

RIAPS is a software platform: an ‘operating system’ for Smart Grid software, not unlike Android for smartphones that supports the construction and operation of distributed applications (‘apps’) that run on a network of field computing devices. It is based on a message-oriented software component model, where the applications are constructed from a network of interacting components (similar to ‘agents’, but more tuned for real-time performance) that exchange messages, but also communicate with local power system devices (e.g., phase measurement units, inverters, breakers, relays, etc.). RIAPS runs on small, inexpensive, embedded computing devices, and provides several services for messaging, dynamic application composition, resource management, distributed coordination among dispersed components, and fault tolerance. It also provides a foundation for strong cyber security, including encryption and mandatory access control for applications. RIAPS has a software development kit, including tools for application deployment and management, and is available under an open-source license. Figure ES-1 shows the software platform’s architecture.

RIAPS consists of two sets of software modules: (1) the component framework that includes support libraries to build distributed apps, and (2) the platform managers that includes service programs that assist with the remote installation, operation, security, and management of the apps.

RIAPS is a software layer above an underlying operating system (real-time enabled Linux), and can support a variety of applications that implement various functions, like power management,

secondary level microgrid control, etc. What RIAPS offers to developers is a set of services that help with building resilient, secure distributed applications. Each computing host ('RIAPS node') in a RIAPS network runs a copy of the platform, as shown on Figure ES-1.

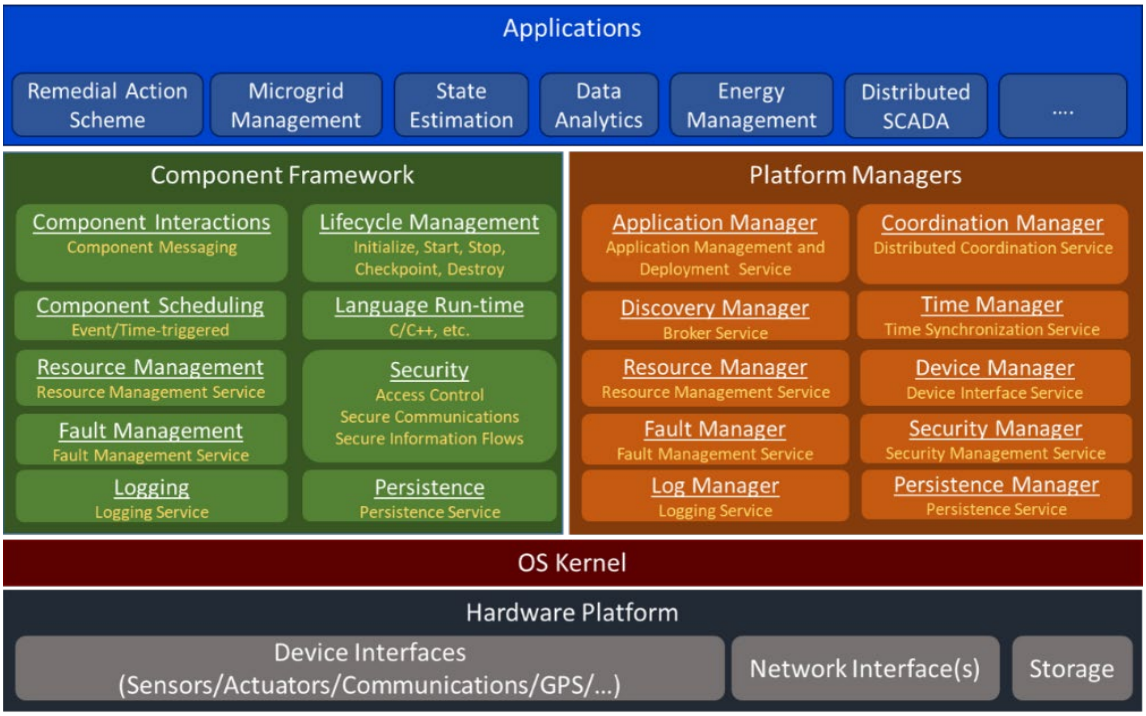

Figure ES-1. RIAPS Architecture.

The functions of distributed applications arise from the interactions among computing nodes. Interactions are implemented as message exchanges, through which the application components share data and salient events. Each node is responsible for its own control actions, but it works with the other nodes to achieve overall control objectives.

There are several features in RIAPS to facilitate this paradigm, including support for fault detection, isolation, and recovery, high-precision clock synchronization across the network, real-time scheduling, and encrypted and authenticated communications.

3.2 DISTRIBUTED MICROGRID CONTROLLER

The microgrid controller algorithm manages: (1) islanded operation, including energy management functions and emergency dispatch order functions based on the energy management goals defined by the use case; (2) grid connected operation, including demand response, and methodologies to reduce demand charges, based on the information provided about the site; (3) transition functions that ensure planned and unplanned seamless transition from grid connected to islanded operation and back to grid connected mode; and (4) black start functionality. Thus, the microgrid controller design provides for all the functional requirements that ensure a technically sound operation of the microgrid, per the Institute of Electrical and Electronics Engineers (IEEE) 2030.7 standard. The standard defines the microgrid operating modes and transitions among them, as shown on Figure ES-2.

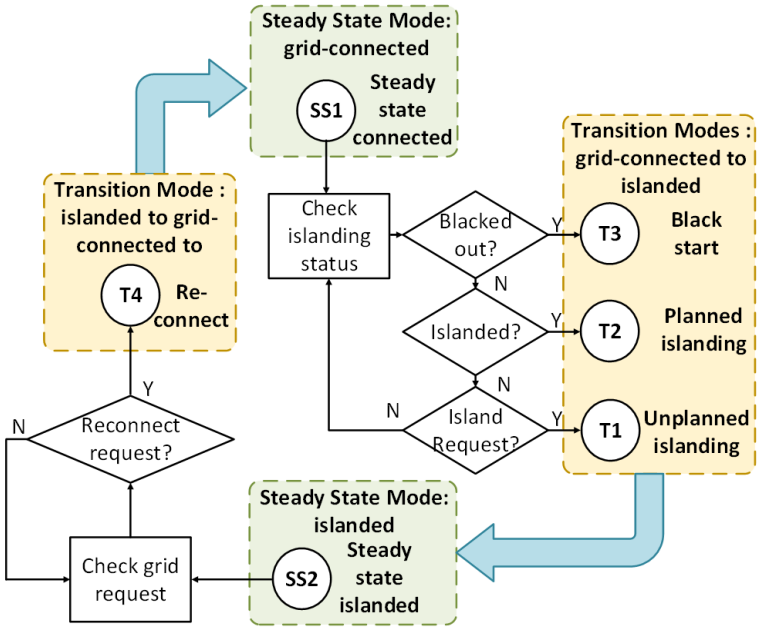

Figure ES-2. Microgrid Operation Modes per IEEE Std. 2030.7.

Conventional microgrid controllers implement these functions using a centralized architecture, where each distributed generator (DG) can be individually monitored and controlled, but the actual control function is implemented in a single, central controlling computer. This solution leads to potential problems with fault-tolerance: the centralized controller is a single point of failure. Furthermore, the network round-trip time between the DG and the centralized controller can be unacceptable. Another disadvantage of a centralized controller is the rigidity of the boundaries between microgrids, where combining microgrids with separate microgrid controllers becomes a control challenge as does changing the boundaries of the existing microgrid as the system gets reconfigured. In a distributed paradigm, changing microgrid boundaries, adding resources to a microgrid controller, and commanding microgrids is seamlessly managed by a membership function that defines the communication links, without the necessity to change the underlying management algorithms.

To address these shortcomings, IMCP implemented these functions in a fully distributed architectures as illustrated on Figure ES-3. In this architecture, each DG had its own local controller, which exchanged data with other controllers connected to the same network. Each local controller was capable of operating independently, although with degraded performance, even if connectivity to the network were lost. This provided resilience for the overall system. If the local controller was connected to its peers, coordination was possible, and the system operated with high performance. The distributed microgrid controller IMCP has been implemented as a RIAPS ‘application’.

The microgrid controller application coordinated a set of low-capacity DGs to achieve a system-level goal. As a power system, this was different from many state-of-the art microgrid implementations where one large energy storage unit had sufficient capacity to smooth out the system dynamics and act as the “grid forming” unit in islanded mode. In islanded operating mode and for microgrid synchronization to the main grid, the DG assets coordinated to proportionally share the real and reactive power system load while restoring the microgrid voltage and frequency

and eliminating the amplitude and phase differences between the voltages on either side of the relay at the point of interconnection (POI). This approach used pinning-based consensus algorithms to coordinate among the DG assets. Other applications used a similar approach to coordinate assets in neighboring microgrids to achieve seamless connection and islanded operation of adjacent microgrids and thus supply critical loads when facing system contingencies or fault conditions. Note that these algorithms could manage networked microgrid as well. These distributed applications made use of the consensus-based algorithms implemented on the RIAPS platform, the platform group formation and time synchronization functionalities.

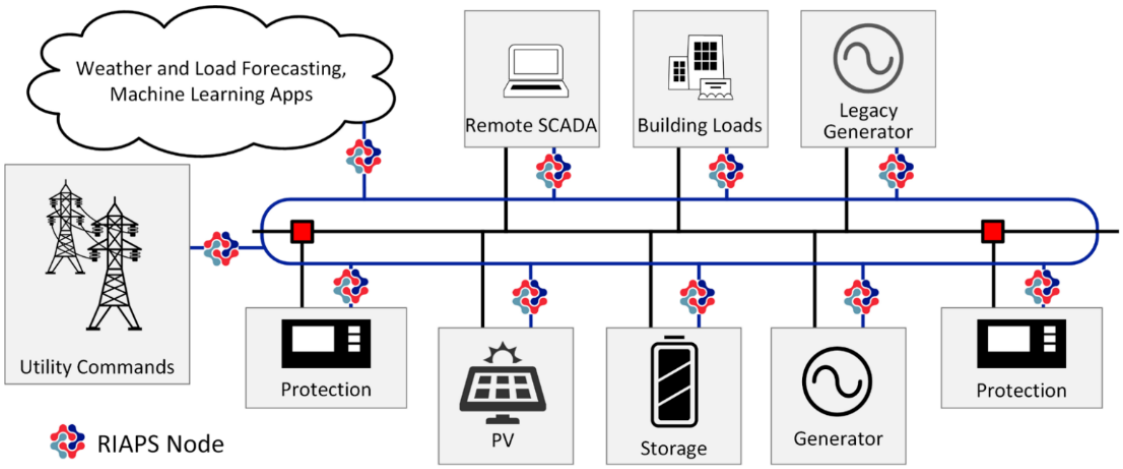

Figure ES-3. Distributed Microgrid Control Application: IMCP built with RIAPS.

The IMCP was designed to be a highly configurable software system. Each device interface that connected the controller software to actual physical inverters, relays, gensets, etc., was customizable to specific device addresses accessible via the Modbus protocol. The controller algorithms coefficients, i.e., the controller gains were also customizable for specific functions. Furthermore, the IMCP was extended with a simple graphical user interface that allows the visualization of the one-line diagram of the microgrid's circuits, and these user interfaces could also be customized to specific data points, sensed or controlled, available in the actual instance of the IMCP application, for a given microgrid.

The benefit of this approach was in the reusability of the algorithms and the interfaces across many DoD installations and microgrid use cases though the development of highly configurable and reusable software components. The project team envisioned that controllers for new microgrid configurations could be inexpensively constructed by composing ('wiring') and parameterizing existing software components. This approach built on an open-source platform that allowed for easy integration of state of the art and legacy equipment into a microgrid management system. Different from other commercial offerings, the developed solution was: (1) fully open source—allowing for applications, component interfaces, energy management and power management algorithms to be used across any number of installations and use cases; (2) the approach was distributed—allowing for simple system scaling, and reconfiguration, as the microgrid grew, or as the boundaries of the microgrid and its critical loads moved—while existing state of the art solutions were designed to be closed to the user and were typically designed to be centralized. The life cycle cost advantage came from the reusability of the interfaces and algorithms.

3.3 IMPLEMENTATION AND TESTING

The IMCP has been implemented and tested for a modified version of the Banshee microgrid system. The implementation software architecture is shown on Figure ES-4. The modified one-line diagram of the microgrid is shown on Figure ES-5.

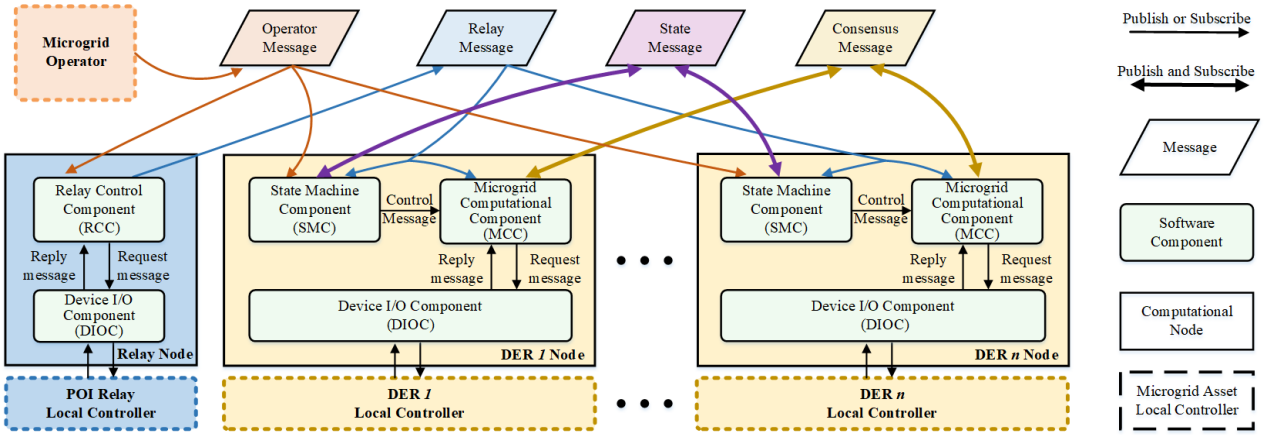

Figure ES-4. Implementation Architecture.

The testing involved HIL testing against a high-fidelity real-time simulation model of the microgrid that was running on an OPAL-RT simulator. The tests included microgrid functionality tests and cyber-security tests, summarized on Table ES-1.

Table ES-1. Summary of Tests.

Mode	Tests	Result – Demonstrated IMCP capability
Grid-connected	HIL.1: Power Dispatch at POI	Dispatching real and reactive power from the microgrid DERs proportionally to their ratings.
	HIL.2: Grid support at POI	Frequency/Watt mode dynamic reactive power support.
	HIL.3: Power Factor Control at POI	Power factor control to support the main grid.
	HIL.4: Loss of bus (load pickup)	Dispatching power to compensate for loss of bus.
Islanding	HIL.5: Disconnect command (Planned Islanding)	Maintain control of the microgrid in case of planned islanding.
	HIL.6: Unplanned disconnect (Unplanned Island)	Maintain control of the microgrid in case of unplanned, abrupt islanding.
Islanded	HIL.7: Connect two adjacent microgrids (Reconfiguration)	Maintaining control while feeders are connected/disconnected.
	HIL.8: Loss of bus (Load pickup)	Dispatching power to compensate for loss of bus.
Islanded to grid-connected	HIL.9: Reconnect to the main grid	Facilitating seamless transition to grid-connected mode by controlling voltage/frequency/phase angel to achieve zero power transfer at POI.
Cybersecurity	CS.1: Confidentiality	Strong encryption of all network messages of application.
	CS.2: Integrity	Modified network messages are automatically rejected.
	CS.3: Authenticity	Network packets of invalid source are rejected.
	CS.4: Availability	Controller remains functional under network overload (DOS) conditions.

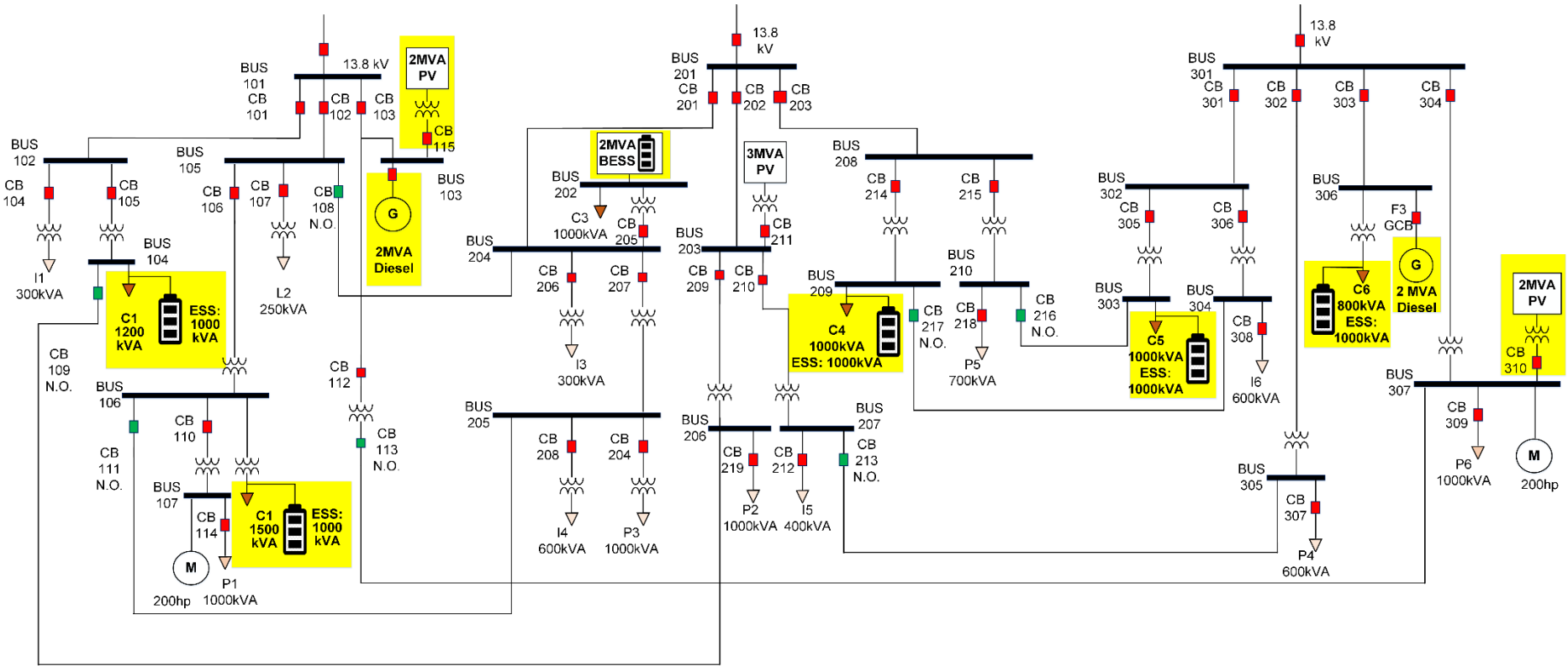

Figure ES-5. Test example: Modified Banshee Microgrid.

The microgrid controller software was running on a network of small, embedded computing devices: Beaglebone Black boards, that were connected to an ethernet-based local area network (LAN) on one side and to the real-time simulator on the other side. While both connections were done via the ethernet connectors and via the transmission control protocol/internet protocol (TCP/IP), the connection to the simulator was using Modbus/TCP-IP—an industry standard for communicating with power system devices.

The testing results showed that the IMCP met the functional and performance requirements. As outlined in Table ES-1, the proposed and adopted test plan considered various scenarios of system operation in grid connected and islanded mode and considered various transition scenarios from the two steady-state operating modes. The team implemented this test procedure on the testbed described earlier and found that the developed microgrid controller successfully met the performance metrics defined in the test plan.

The cyber-security tests were executed by monitoring the network packets (CS.1), monitoring the behavior of the application (CS.2 and CS.3), and observing the performance of the controller under adversary conditions (CS.4). The tests verified that only encrypted messages were sent through the network (CS.1), that tampered and invalid messages were rejected before reaching the application code, and that the controller remained functional even if node became isolated due to a denial-of-service (DOS) attack. As expected, the controller remained functional, although with lower performance, due to the lost messages. Once the attack ceased, the controller recovered.

4.0 PERFORMANCE ASSESSMENT

This project implemented the test procedure on a HIL setup that allows for the monitoring of the system voltage and frequency throughout the test. The relevant voltage and frequency measurement were taken at all buses of the microgrids, and the results show that the system met the performance requirements throughout the test. The key metric of interest was that the voltage and frequency of the system remained within the allowable IEEE 1547 range in all conditions.

Grid-connected mode test scenarios

Functionality tested	**Criteria met**
HIL.1: PQ dispatch	Value within 5% of rating within 30 seconds (IEEE 1547-2018 clauses 4.4).
HIL.2: Frequency Watt Mode; Dynamic Reactive Power Support	Value within 5% within 30 seconds (IEEE 1547-2018 clauses 4.4).
HIL.3: PF command	Value within 5% of rating within 30 seconds (IEEE 1547-2018 clauses 4.4).
HIL.4: Loss of bus (Load Pickup)	Downstream loads picked up within 30 seconds.

Islanded mode and grid to island transition test scenarios

Functionality tested	Criteria met
HIL.5: Disconnect command (Planned Island)	Seamless transition from grid connected to islanded mode at prescribed time. V,f within allowable bands throughout.
HIL.6: Unplanned disconnect (Planned Island)	Seamless transition from grid connected to islanded mode at prescribed time. V,f within allowable bands throughout.
HIL.7: Connect two adjacent microgrids (reconfiguration)	Seamless connection of two islanded microgrids. V,f within allowable bands throughout.
HIL.8: Loss of bus (Load pickup)	Downstream loads picked up within 30 seconds.

Island to grid transition test scenario

Functionality tested	Criteria met
HIL.9: Reconnect to the main grid	Seamless transition from islanded to grid connected mode within prescribed time. V,f within allowable bands throughout.

Cyber-security test scenarios

Concern tested	Attacker action	Criteria met
CS.1: Confidentiality	Snoop on network packets	Attacker is unable to decode content.
CS.2: Integrity	Modify and retransmit modified network packets	Modified packet is rejected by recipient.
CS.3: Authenticity	Spoof network packets	Modified packet is rejected by recipient.
CS.4: Availability	Flood network with packets	Controller app detects the problem and acts accordingly.

5.0 COST ASSESSMENT

The developed IMCP implementation is a fully functional prototype, and it is available under an open-source license. Open-source license applies to the entire software stack: the operating system (Linux), several software packages (e.g., Python, and others), the RIAPS platform, and the IMCP itself. RIAPS and IMCP use the Apache 2.0 license. All these licenses permit the use of the software as is, as well as its modification and distribution. To summarize, the software itself, in its current form, is available for use, with no cost.

However, if the software is used for another microgrid than the Banshee example (with Modbus/ TCP/IP interfaces), it needs to be configured, possibly customized and extended for a new microgrid.

The costs of using IMCP in a microgrid therefore includes customizing it to the specific microgrid, developing and configuring new software interfaces (if needed), and testing, installing, and maintaining it.

The software needs computing and network hardware. The actual controller software runs on small, networked embedded computers, while an additional computer is used to load and install the controller on the networked machines. For field installations, it is recommended to use industrial grade embedded computers, as well as an industrial quality LAN.

6.0 IMPLEMENTATION ISSUES

This development project did not encounter any significant implementation issues. The implementation and its testing were performed in a laboratory environment, using simulated power systems. The simulator was a high-performance, high-fidelity, real-time simulator (OPAL-RT), that also implemented the real-time hardware/software interfaces (specifically: the Modbus protocol) that is expected in a field environment. The IMCP software was running on a network of Beaglebone Black devices: small form factor, embedded computing devices, connected to an isolated LAN in the lab.

However, for fielding the results of this project, control algorithm implementations with state-of-the-art embedded, industrial-grade computing devices are needed, that have: (1) local area network interfaces with support for IEEE 1588 - Precision Time Protocol; and (2) interfaces to local DERs (e.g. Modbus of serial ports). The industrial embedded computers need to be housed in field-grade enclosures, must have uninterruptible power supplies, and need to connect to a local area network. The interfaces to the power devices need to be designed according to the requirements of the field environment. The developed software code base, which comprises the microgrid controller and the software platform, is open source, and as such can be used by developers of microgrids. However, it is necessary to customize it to a specific microgrid configuration and power system device.