IAC-19-C3.4.3

A Control Framework for Autonomous Smart Grids for Space Power Applications

Jeffrey T. Csank[a]*, James F. Soeder[b], Marc A. Carbone[c], Matthew G. Granger[d], Brian J. Tomko[e], Matthew J. Muscatello[f], Jeffrey C. Follo[g]

[a] *Power Management and Distribution Branch, NASA Glenn Research Center, 21000 Brookpark Rd, Cleveland OH, 44135,* jeffrey.t.csank@nasa.gov
[b] *Power Division, NASA Glenn Research Center, 21000 Brookpark Rd, Cleveland OH, 44135,* james.f.soeder@nasa.gov
[c] *Power Management and Distribution Branch, NASA Glenn Research Center, 21000 Brookpark Rd, Cleveland OH, 44135,* marc.a.carbone@nasa.gov
[d] *Power Management and Distribution Branch, NASA Glenn Research Center, 21000 Brookpark Rd, Cleveland OH, 44135,* matthew.g.granger@nasa.gov
[e] *Information and Applications Office, NASA Glenn Research Center, 21000 Brookpark Rd, Cleveland OH, 44135,* brian.j.tomko@nasa.gov
f *Flight Software Branch, NASA Glenn Research Center, 21000 Brookpark Rd, Cleveland OH, 44135,* matthew.j.muscatello@nasa.gov
[g] *Flight Software Branch, NASA Glenn Research Center, 21000 Brookpark Rd, Cleveland OH, 44135,* jeffrey.c.follo@nasa.gov
* Corresponding Author

Abstract

With the National Aeronautics and Space Administration's (NASA) rising interest in lunar surface operations and deep space exploration, there is a growing need to move from traditional ground-based mission operations towards autonomous vehicle level operations. In lunar surface operations, there are periods of time where communications with ground-based mission control cannot occur, forcing vehicles and a lunar base to operate completely independent of the ground. For deep space exploration missions, communication latency times increase to greater than 15 minutes making real-time control of critical systems extremely difficult. These challenges are driving the need for an autonomous power control system that has the capability to manage power and energy. This will ensure that critical loads have the necessary power to support life systems and carry out critical mission objectives. This paper presents a flexible, hierarchical, distributed control methodology that enables autonomous operation of smart grids and can integrate into a higher level autonomous architecture.

1. Introduction

The National Aeronautics and Space Administration (NASA) is continuing its interest in deep space exploration and lunar operations by sending humans to the moon by 2024 through the Artemis program. Details of the program can be found in [1]. Both deep space exploration and lunar surface operations are increasing the need to move from the traditional ground-based mission control, which NASA currently utilizes, to control human rated spacecraft with increased autonomous capability. For deep space exploration missions, such as the Mission to Mars, communication latency times increase to greater than 15 minutes making real-time control of critical systems nearly impossible, as documented in [2,3]. For lunar surface operations, there are anticipated periods of time where communications with ground-based mission control cannot occur, forcing vehicles and a lunar base to operate entirely independent of the ground [3]. These communication challenges are driving the need for the vehicle and all of its subsystems to operate autonomously. Autonomous decision making implies that actions must be made without a human operator involved whether it be an astronaut or person on the ground. To meet this requirement, a vehicle control architecture has to be developed to allow an on-board computer to carry out functions typically performed by ground control personnel and coordinate with all of the vehicle subsystems. One of the challenges associated with autonomous control of these subsystems is how to accurately capture and incorporate system expertise gained with experience of operating these subsystems into flight rated software.

One of the vehicle subsystems that will have to operate autonomously is the electrical power system. The electrical power system must manage the power generation, energy storage assets, and distribution system to ensure critical loads have the necessary power to support life systems and carry out critical mission objectives.

Transitioning from traditional human controlled vehicles towards autonomous vehicle operations creates many implementation challenges. These challenges range from the sociological, for example, developing computer-based systems are capable of making intelligent decisions, to the technological, such as how to implement the software communication and controls to be both reliable and robust. Much of the automotive industry is favouring a heavily centralized control approach for autonomy [4,5,6].

A generalized centralized autonomous control architecture is shown in Figure 1. This approach is similar in nature to a Task Control Architecture in [7] which can be applied to distributed robots. In this type of control architecture, the majority of the autonomous operations and decision making occurs in a high level central controller, referred to here as the vehicle manager. These functions include mission management, such as planning (scheduling) and ensuring the vehicle meets the mission objectives, and fault management which includes fault detection, isolation, and recovery. The reactive layer connects the physical hardware to the central controller. These devices take commands from the vehicle manager and then execute them on the hardware. Within the reactive layer, monitoring and protection functions are implemented to maintain and safeguard the system in the event of a fault, failure, or malfunction. This level of control is not responsible for complex decision making. Examples of this include the ability to trip a circuit breaker after a hard fault in a power system distribution cable.

This paper presents a more flexible, hierarchical control methodology that enables autonomous operation of smart grids that is capable of integrating with a higher level of autonomous control. This upper level of control is responsible for coordinating vehicle subsystems that may include power, thermal, avionics, and life support controls.

2. Hierarchical Control Architecture

A generalized hierarchical control architecture is shown in Fig 2. In this architecture, many of the decision making functions on how each subsystem operates are distributed to the subsystem control layer. This middle layer of control includes functions such as fault management and state awareness. These functions are better suited for the subsystem layer since they will be processed at a higher rate; however, they only have knowledge of their own subsystem. The vehicle manager, which has a global perspective of the system, is now mainly responsible for ensuring the vehicle (or overall system) meets the mission objectives (includes scheduling loads) and dealing with faults that cross subsystem boundaries. In these situations, multiple subsystems may indicate that there was a fault within their respective subsystem. However, the actual source of the fault may have only occurred within a single subsystem, where the other subsystem indications are simply symptoms of the true fault. The vehicle manager control layer is responsible for making this determination. An autonomous architecture similar to this has been previously proposed in [8, 9]. In this architecture, the reactive layer remains as originally designed. The distributed architecture provides an additional benefit in that the vehicle manager could be replaced by ground control (or flight crew) and the subsystem controller can still provide useful data to the human operator. This allows for a transition period from fully human operated to fully autonomous by increasing just the automatic response of the subsystem.

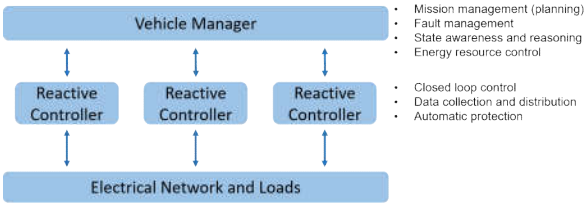
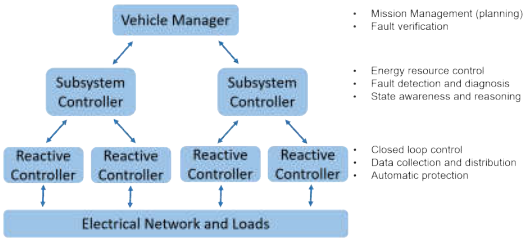


Fig 1. Generalized Centralized Autonomous Control Architecture

3. Space Power Control in an Autonomous Architecture

A power control system that integrates in a distributed autonomous control architecture for a spacecraft is proposed. The integrated autonomous power control system is responsible for managing the power system without human intervention, which



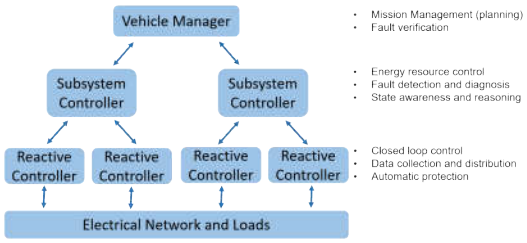


Fig 2. Generalized Hierarchical Autonomous Control Architecture

includes the ability to safely operate the power system within the component limits at all times, and provide power to as many high priority loads as possible. This is accomplished via energy management, fault management, and maintenance, mitigation, and recovery (MMR), or sometimes referred to as contingency management. These functions typically reside at the subsystem level with information from both the vehicle manager (commands), and telemetry from the reactive layer.

3.1 Fault Management

The ability to detect, isolate, and recover from a fault is a critical aspect for the power management system. The fault management strategy is employed at all layers of the hierarchical architecture.

3.1.1. Reactive Layer Fault Management

The reactive layer components are designed to operate at a high update rate, on the order of kHz to MHz. At this level, the main objective of the fault management approach is to protect the power system equipment and all the vehicle loads by detecting and isolating major faults, capable of damaging the electric power system equipment. These power distribution faults include hard short to ground or neutral, overloading, thermal overload, etc. These hard power faults can be detected by trip curves (to detect overcurrent) and limit checks (over/under voltage). Trip curves are a special case of limit checks which measure the change in current over time, which may result in a protective action such as breaking the circuit. For a small overcurrent, it may take several seconds until the switch responds while a very large current (10x max) would take less than a second depending on the device. These algorithms are critical to ensuring the protection of the electrical power system equipment, which can damaged or destroyed from the thermal impacts of a fault.

The reactive layer can play an important role in the overall fault management scheme. For instance, the trip settings can be adjusted based on their location for fault coordination and zonal protection as discussed in ref [10]. The reactive layer is also used to help identify communication failures. For example, a heartbeat is sent from the subsystem controller to the central controller. If heartbeats are lost, or subsystem control data becomes out of sync, the central controller can respond by entering a safe state or continue operating without communication under purely distributed control.

3.1.2. Subsystem Control Layer Fault Management

The subsystem control level is where the several of the power system fault management functions occur. This level deals with system level issues and failures that require additional data to detect. This includes, sensor failures (sensor bias or excessive noise faults), soft or small magnitude shorts (soft faults), and stuck switch (command mismatch fault). To detect these faults, the subsystem controller employs a model-based state estimation of the system to validate the behaviour of the physical hardware. Using the analytical redundancy of the state estimator, faulty or missing data can be identified and replaced with estimates. The synthesized data points can then be sent to other autonomous power control algorithms to be used for fault analysis or generation-side control.

The subsystem control layer is also where machine learning, big data, and other artificial intelligence is implemented. These functions allow the controller to detect anomalies, degradation, and predict failures. Additional system level strategies are discussed in [10, 11].

3.1.3 Vehicle Manager Layer Fault Management

The vehicle manager mainly is responsible for validating faults identified by the subsystems, accepting or modifying the subsystem responses to the faults, and coordinating responses for faults that crosses subsystem boundaries. A simple example would be a stalled rotor within a motor load subsystem. In this case, the power system and the load subsystem may both respond by indicating a fault/failure occurred in their respective subsystems. The power system may diagnose the fault as an overcurrent on a line, while the load subsystem may accurately determine that the rotor has stalled. The vehicle manager would then have to vet the true cause of the fault (the stalled rotor) only log the motor subsystem failure. At this level expert systems, statistical analysis, and model-based techniques are used.

3.2 Energy Management

Spacecraft power systems, such as the International Space Station, often have more total electrical load than it can supply. To prevent overloading of the power generation devices (solar arrays and batteries), loads must be carefully scheduled. Each load is given a time frame when the load is permitted to consume power. The power controller sets a limit on the maximum power each load can draw. The role of the scheduler is to create a plan that (1) allows the loads to consume the power required to meet their objectives (2) ensure the load objectives meets the overall vehicle and mission objectives, (3) ensure power generation, energy storage, and power distribution constraints are not violated, and (4) minimize unused power from power generation devices. For the scheduler or planner to accomplish this, the power system must accurately capture the constraints of the power system, which is done via a power profile. The power profile describes the nominal and maximum power constraints for a group of loads

within a section of the power system. The power profile defines these parameters over a period of time for the mission.

The main energy management objective is to clearly define the power and energy constraints for a system scheduler or planner. These constraints are dependent on the orbital parameters of the vehicle, health and availability of the power system generation components, and current state of the power distribution system. The schedule can be broken down into time units that would represent some notional amount of time, for instance 5 minutes. In addition, the power constraints can be characterized for an independent channel and by module or some physical separation. Since the scheduler is mainly concerned about the power to the loads, the scheduler needs to know the:

- Maximum power (by element, channel, for each time unit)
- Nominal power (by channel and time unit)
- Energy available (by channel)

The maximum power available to a group of loads ensures that the power distribution lines and equipment are not overloaded. This value is often impacted by the loss of power distribution equipment and/or thermal constraints. If the temperature is too high, maximum power might be reduced.

The continuous nominal power for each phase of the orbit is used to determine how much power can be consumed during a specific power-related event such as insolation, eclipse, and electric propulsion thrusting. For example, during a 30 minute eclipse the power controller must define the power that could be consumed by all the loads of a channel for the entire 30 minutes without violating the energy storage constraints. If one of the batteries was below the desired state of charge (due to degradation or other damage), then the nominal power would be reduced in the upcoming eclipse period. For a period spanning multiple eclipse cycles, the nominal power may fluctuate according to the forecasted available power.

The energy available is the total energy that can be used for the particular phase, for example for a single eclipse period or insolation period. This value does take into account the current health and status of the batteries and is used to determine the nominal power. With this information, the scheduler may find a period in which it satisfies the maximum power constraint for each grouping of loads, may exceed the nominal power for two time units and is blow the nominal power for three time units, and satisfies the energy availability for the phase, which is acceptable. The nominal power gives a baseline in the amount of power to schedule each time unit.

3.3 Maintenance, Mitigation and Recovery (MMR)

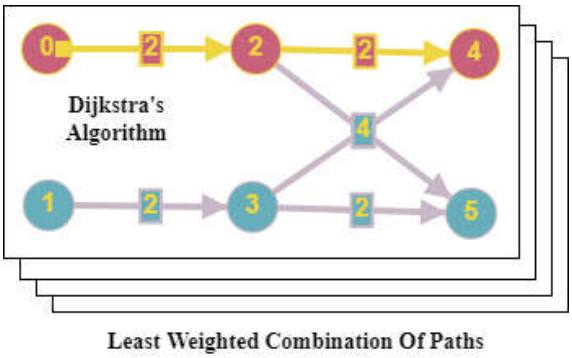


Fig 3. Visualization of the MMR optimal topology search algorithm.

Maintenance, mitigation, and recovery (MMR) system coordinates the power distribution system configuration and plays a major role in power availability. With all power distribution equipment available, the MMR system will set the power distribution to its nominal or desired configuration. As equipment becomes unavailable due to faults or failures, the fault manager will inform MMR of the unavailable equipment and MMR will determine a new configuration to maximize power availability to the loads. If a module needs to be serviced (replaced or repaired), this can be identified and MMR will create a new configuration to allow for this maintenance. Future versions of the power controller (MMR) and the vehicle manager will allow for MMR and the vehicle manager to determine the optimal time to remove equipment from service for maintenance based on the vehicle subsystem's performance.

One of the main objectives of MMR is to reconfigure the electrical network to maximize power availability. This is accomplished using Dijkstra's algorithm. Dijkstra's algorithm is used to find an optimal path from multiple power sources to as many power distribution units as possible using a directed weighted graph [12]. MMR also takes into account any faulted component in the power system to generate the least weighted path from every power source to every power distribution unit. Each combination of paths has a calculated overall weight based on its combination of individual paths. If a line is used to connect a source to multiple loads, the weight of this overall configuration is increased. MMR searches all of the possible network topologies, and selects the configuration with the minimum total weight as shown in Figure 3.

4. Communication Framework

In order to achieve autonomous or semi-autonomous power system control, a design framework that is highly robust, adaptable and reliable will be needed [13]. A distributed control scheme is implemented to achieve

the desired plug-and-play operation as well as peer-to-peer communication. To enable this type of control, the electric power system controller relies on a service oriented architecture. Each service provides a unique function to the electrical power system. These services operate collectively achieve the control functions necessary to operate and maintain the electric power system.

Services communicate to each other using a combination of synchronous and asynchronous messages. The backbone of the messaging system is an open source messaging broker, which allows for agile development and well documented support. The message broker allows services to create and subscribe to queues, enabling data to be published and received by the necessary services. The flexibility of the messaging system allows for more sophisticated message structures between the services, allowing services to interact through cooperation and competition. Asynchronous messaging increases the level of intelligent decision making capability within the services, allowing them to behave proactively.

In addition, this framework allows for new devices to be added or removed from the controller, without breaking the messaging structure. This feature is useful with modular components within the control system. Services can simply subscribe/publish to the proper message queues and begin communicating with the controller without interruption of service, and without the need to retro-fit the control scheme to the new structure.

Another benefit of the service oriented architecture is the reduction in computational burden from the central controller by delegating tasks to the distributed subsystem controllers. For complex systems such as electrical power systems, some of the control problems would be too "large" to solve at a centralized scale. Deploying smaller pieces of these algorithms in the distributed architecture relieves the computational complexity of the central controller. In addition, it reduces the total data transfer to the central controller by solving problems locally when possible.

From an engineering perspective it is important to limit the scope and flexibility of the services. For purposes of verification and validation, the services should be designed to have a single goal or objective at a given time. Competing objectives may lead to unpredictable/unwanted behaviour.

5. Future Work / Conclusions

Work is ongoing to improve the fault detection and reconfiguration capabilities of the electrical power controller. Future work includes the implementation of a machine learning based transient fault detection algorithm. This system augments the ability of the fault management system, enabling the detection of faults in the kHz time scale from any component in the electrical system. A highly configurable, high-fidelity transient simulation has been created to train the system, although experimental data may be used as it becomes available. In addition, the algorithm is capable of online classifier updates based on new information measured as the system operates.

Another area of research is controlled battery current sharing. This capability is critical for highly distributed power systems to maximize energy availability. Work has already been completed on the testing of a tertiary closed-loop current sharing and state-of-charge balancing algorithm. Future work includes updating this algorithm for robustness against communication failures and topology reconfiguration. Additionally, parameter estimation from transient and steady-state data can be leveraged to inform algorithm gain tuning, ensuring robustness and optimizing performance.

List of references

[1] A. Mann, NASA'S Artemis Program, July 3, 2019, https://www.space.com/artemis-program.html (accessed 7/12/2019).

[2] F. Jeremy, et.al., "Autonomous Mission Operations," 10.1109/AERO.2013.6496927, IEEE Aerospace Conference 2013.

[3] J. Badger, et.al., "Spacecraft Dormancy Autonomy Analysis for a Crewed Martian Mission," NASA TM 2018-219965, July 2018.

[4] K. Berntrop, T. Hoang, R. Quirynen, S. Di Cairano, "Control Architecture Design for Autonomous Vehicles," Mitsubishi Electric Research Laboratories (MERL), Conference on Control Technology and Applications (CCTA), 2018. https://www.merl.com/publications/docs/TR2018-125.pdf

[5] S. Behere and M. Torngren, "A Functional Architecture for Autonomous Driving," ACM, Proceedings of the First International Workshop on Automotive Software Architecture, Montreal, QC, Canada, May 04, 2015.

[6] R.D. May, et.al., "An Architecture to Enable Autonomous Control of Spacecraft," AIAA 2014-3834, 12th International Energy Conversion Engineering Conference (IECEC), Cleveland, OH, July 28-30, 2014.

[7] A. A.D. Medeiros, "A survey of control architectures for autonomous mobile robots," Journal of the Brazilian Computer Society, March 1998.

[8] P.J. Antsaklis, K.M. Passino, and S.J. Wang, "Towards Intelligent Autonomous Control Systems: Architecture and Fundamental Issues," Journal of Intelligent and Robotic Systems, Vol. 1 Issue 4, pp315-342, December 1989.

[9] P.J. Antsaklis, K.M. Passino, and S.J. Wang, "An introduction to autonomous control systems," IEEE

Control Systems Magazine, Vol 11, Issue 4, pg 5-13 June 1991.
[10] C.R. Mason, The Art & Science of Protective Relaying, John Wiley & Sons, Sixth Printing Edition, 1967.
[11] R. Apel, C. Jaborowicz, R. Kussel, "Fault Management in Electrical Distribution Networks," IEE, CIRED2001, June 18-21, 2001.
[12] E.W. Dijkstra, "A note on two problems in connexion with graphs," Numerische mathmatik, 1959
[13] R.D. May, K.A. Loparo, "The Use of Software Agents for Autonomous Control of a DC Space Power System," 12th International Energy Conversion Engineering Conference (IECEC), Cleveland, OH, July 28-30, 2014