

УДК 520.6.05

EDN: GVGHVE

© Д. В. Лисин, 2026

АЛГОРИТМЫ УПРАВЛЕНИЯ РЕЗЕРВИРОВАНИЕМ ЛИТИЙ-ИОННЫХ БАТАРЕЙ КОСМИЧЕСКИХ ЭКСПЕРИМЕНТАЛЬНЫХ КОМПЛЕКСОВ

Продолжено описание разработанной в ИЗМИРАН архитектуры построения высоконадежной системы электроснабжения на базе литий-ионных аккумуляторных батарей, предназначенной для проведения научных экспериментов на борту космических аппаратов. Рассмотрены вопросы построения алгоритмов управления двумя аккумуляторными батареями с учетом вопросов общей надежности системы в целом. Указанные алгоритмы предназначены для реализации в бортовом микропроцессорном блоке управления системой электроснабжения космического аппарата с двумя и более литий-ионными аккумуляторными батареями и в описываемом виде предназначены для реализации ручного управления перекоммутацией бортовых батарей в безопасном для аппарата режиме.

Ключевые слова: система электроснабжения, литий-ионная аккумуляторная батарея, космический эксперимент, управление резервированием, алгоритмы

ВВЕДЕНИЕ

Литий-ионные аккумуляторные батареи имеют весьма многообещающие возможности для применения в условиях проведения разного рода экспериментов на орбите Земли, касающиеся в основном их очень хороших массогабаритных характеристик [1, 2]. Наряду с этим данная технология обладает рядом принципиальных недостатков, к которым можно отнести: малый температурный диапазон применения, повышенная взрывоопасность и ускоренная деградация при отклонении режимов заряда/разряда от оптимальных, малый срок службы по сравнению с батареями других типов. Указанные недостатки могут быть во многом преодолены при условии применения интеллектуальных систем управления подобными батареями, в том числе встраиваемыми в саму батарею, а также применением особых подходов к организации систем электроснабжения и методов управления ими. В данной статье рассматриваются вопросы, связанные с алгоритмами управления двумя или более батареями с основной целью их взаимного резервирования в архитектуре системы управления, описанной в [3].

АРХИТЕКТУРА СИСТЕМЫ И ПОЛИТИКА РЕЗЕРВИРОВАНИЯ БАТАРЕЙ

Типичная архитектура организации системы электроснабжения экспериментального космиче-

ского аппарата, в которую с целью резервирования входят две литий-ионные аккумуляторные батареи, показана на рис. Вопросы, связанные с ее функционированием, достаточно подробно описаны в [3], однако приведенная на рис. схема имеет принципиальное отличие от рассматриваемой в [3] — с целью обеспечения возможности управления коммутацией основной и резервной батарей в нее введено два поляризованных реле отключения батареи. Применение поляризованных реле позволяет обеспечить энергонезависимость выбранной конфигурации, а само их наличие — возможность реализовывать различные политики управления резервированием, например:

1) обе батареи всегда соединены параллельно для увеличения общей емкости; однако при обнаружении в данных телеметрии признаков опасной деградации, в частности необратимой разбалансировки элементов [4], батарея может быть отключена от силовой шины как автоматически, так и по команде наземного центра управления (ЦУП);

2) одна из батарей находится "в холодном резерве", т.е. отключена от силовой шины изначально и подключается к ней только в случаях обнаружения критического разряда основной батареи — автоматически или по команде ЦУП;*

* Примечание. На рис. подразумевается, что цепи заряда всех батарей подключены к ним постоянно, управляются автоматически и на рисунке не показаны, т.к. не относятся к рассмотрению

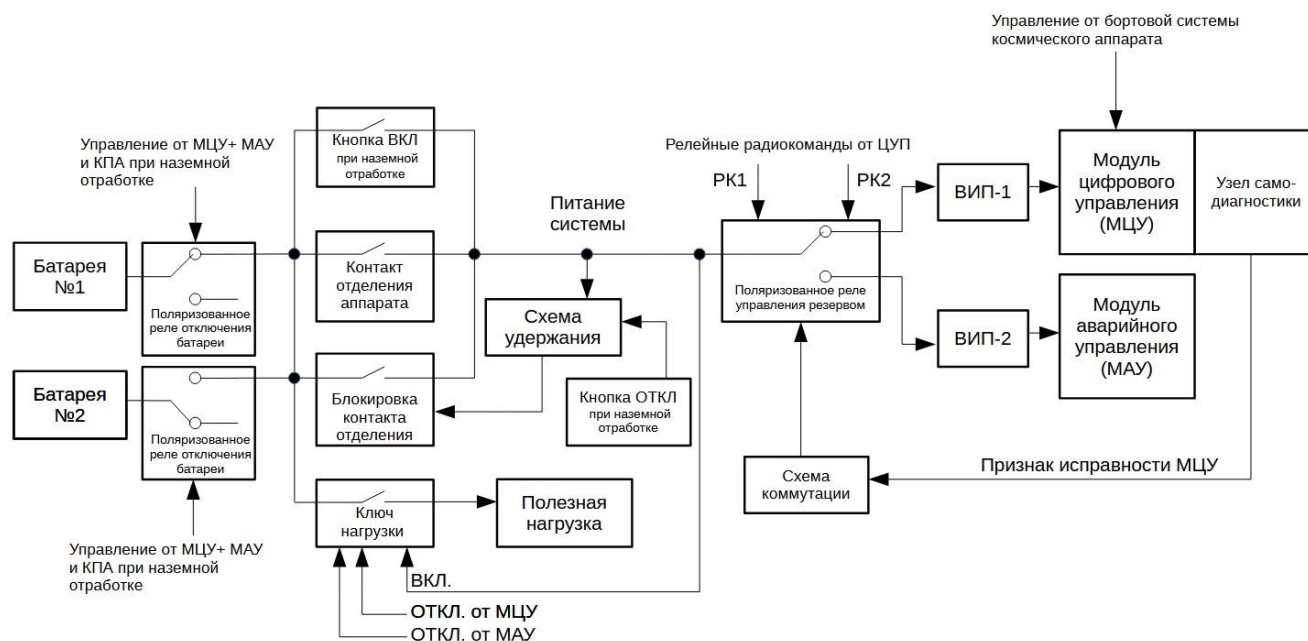


Рис. Архитектура системы электроснабжения космического аппарата.

ВИП — вторичный источник электропитания, РК — радиокоманда, КПА — наземная контрольно-поверочная аппаратура

3) в каждый момент времени питание нагрузки осуществляется только от одной батареи, выбор которой циклически меняется с некоторой периодичностью (также автоматически или по команде ЦУП).

Каждая из вышеперечисленных политик имеет свои достоинства и недостатки, обсуждение которых выходит за рамки настоящей статьи, призванной осветить лишь алгоритмы реализации столь ответственного действия, как коммутация силовых шин бортовых аккумуляторных батарей космического аппарата в процессе реализации вышеперечисленных или каких-либо иных политик управления их резервированием.

ДОСТОИНСТВА И НЕДОСТАТКИ ПРЕДЛАГАЕМОЙ АРХИТЕКТУРЫ

Применение управляемых ключей (поляризованных реле) в силовых цепях обеих резервируемых батарей открывает широкие возможности в реализации различных вариантов их взаимного резервирования, особенно с учетом достаточно специфических характеристик литий-ионных элементов [1], однако представляет собой чрезвычайно опасное решение с точки зрения управления подобной системой. Основ-

ная опасность — подать ошибочную последовательность команд, которая приведет к отключению обеих батарей, что равнозначно потере космического аппарата. Тем не менее возможность фактически заменить неисправную батарею во время орбитального полета, в том числе в автоматическом режиме, зачастую может дать весьма значительные результаты с учетом существенного продления времени работы сложного и дорогостоящего комплекса экспериментальной аппаратуры, который питается от нее.

В случае принятия достаточных системных мер для защиты от ошибочного необратимого отключения обеих батарей предлагаемая архитектура может быть использована с сохранением достаточного уровня надежности комплекса аппаратуры в целом. Такие меры можно классифицировать по трем основным группам: аппаратные, программные и программно-аппаратные защиты. В качестве аппаратных мер может быть предусмотрено, например, использование дополнительных контактных групп поляризованных реле, которые служили бы датчиками их состояния для аппаратной схемы блокирования подачи импульсных команд на отключение обоих реле одновременно. Возможны и иные варианты аппаратной организации схемы коммутации батарей, которая

исключала бы их одновременное отключение, однако их рассмотрение выходит за рамки настоящей статьи. При разработке предлагаемого подхода к решению описанной выше основной проблемы был выдвинут принцип минимизации использования аппаратных цепей в узле коммутации, т.к. надежность правильно спроектированного алгоритма всегда выше надежности контактов реле и других аппаратных компонентов.

ЛОГИКА УПРАВЛЕНИЯ КЛЮЧАМИ СИЛОВЫХ ШИН БАТАРЕЙ

Рассмотрим общую логику работы поляризованных реле отключения батарей на рис., которые для краткости будем называть ключами их силовых шин. Следует подчеркнуть, что эти ключи предназначены не для управления коммутацией нагрузок (служебные системы космического аппарата, приборы комплекса научной аппаратуры и т.д.), а исключительно для управления коммутацией бортовых аккумуляторных батарей. Эта коммутация может выполняться в двух основных состояниях космического аппарата: при наземной отработке и в ходе орбитального полета.

В первом случае выдача импульсных команд на переключение ключей выполняется в ручном режиме от контрольно-проверочной аппаратуры (КПА), которая обычно подключается к специально выделенным для нее соединителям. Как правило, это будут специально обозначенные кнопки с наименованиями типа "ВКЛ. АБ-1", "ОТКЛ. АБ-1" и т.п. с соответствующей индикацией либо соответствующие релейные выходы некоторой автоматизированной системы, применяемой при наземной отработке комплекса. В этом случае переключение контактных групп (реконфигурация аккумуляторных батарей аппарата) должно происходить при отсутствии тока нагрузки (контакт отделения, его имитаторы и схемы его блокировки на рис. должны быть разомкнуты). В этом случае практически не будет происходить износа контактов при любом объеме экспериментальной отработки. Это требование достаточно несложно обеспечить соответствующим построением программ наземной экспериментальной отработки (ПНЭО) комплекса.

Во втором случае эти импульсные команды генерируются как автоматически действующими на базе модулей цифрового/аварийного управления (МЦУ/МАУ) алгоритмами, так и прямыми командами, получаемыми по бортовой радиолинии космического аппарата от ЦУП.

Например, типичный сценарий проведения наземных испытаний с последовательным использованием обеих батарей может выглядеть так:

- нажатиями кнопок "ВКЛ. АБ-1", "ОТКЛ. АБ-2" на пульте контрольно-проверочной аппаратуры (КПА) батарея № 1 подключается к силовой шине, а батарея № 2 отключается от нее;
- нажатием кнопки "ВКЛ" происходит шунтирование контакта отделения, питание подается на модуль цифрового управления (МЦУ), который начинает обработку штатной циклограммы включения и включает нагрузку;
- после отработки циклограммы проверок с питанием от батареи № 1 на пульте КПА нажимается кнопка "ОТКЛ", что воздействует на схему удержания и разрывает цепь шунтирования контакта отделения, отключая нагрузку;
- нажатиями кнопок "ОТКЛ. АБ-1", "ВКЛ. АБ-2" на пульте КПА батарея № 1 отключается, а батарея № 2 подключается к силовой шине, и циклограмма проверок повторяется с питанием от батареи № 2;
- нагрузка отключается кнопкой "ОТКЛ", поляризованные реле отключения батарей командами от КПА переводятся в исходное состояние, соответствующее избранной политике резервирования батарей.

В этом случае отключение обеих аккумуляторных батарей в процессе наземной отработки вполне возможно и может быть в ряде случаев даже желательным вариантом отладки комплекса. Рассматриваемая архитектура алгоритма управления включает в себя два независимых контура защиты, совместная работа которых представляется достаточной для применения в рассматриваемой области. При управлении по второму контуру (автоматическими алгоритмами или по командам ЦУП) возможность отключения обеих аккумуляторных батарей должна быть полностью исключена.

Следует отметить, что дальнейшее изложение предполагает управление модулем цифрового управления (МЦУ) системы электроснабжения от бортовой системы управления космического аппарата по стандартному мультиплексному каналу обмена (МКО), что, однако, не снижает общности изложения, т.к. управление по иным протоколам так или иначе будет использовать принцип пакетной передачи набора команд. При этом, безусловно, подразумевается и далее не оговаривается наличие высоконадежных средств проверки достоверности передаваемых командных пакетов на всех этапах — от форми-

рования их в ЦУП до передачи в МЦУ по бортовому каналу, обеспечиваемых применением хэш-сумм, корректирующих кодов и других способов обнаружения одиночных и групповых ошибок.

ПЕРВЫЙ КОНТУР АЛГОРИТМИЧЕСКОЙ ЗАЩИТЫ

Для отключения батареи с индексом i по команде наземного центра управления необходимо выполнить следующие действия:

1. Подать команду "Разрешить отключение АБ- i ". Эта команда разрешает прохождение дальнейшей команды отключения АБ- i в течение 5 с, после чего режим разрешения автоматически отменяется. Обязательное требование: эта команда должна быть единственной в командном пакете МКО, в противном случае она выполнена не будет.

2. Подать команду "Отключить АБ- i ". Если ни одна блокировка этому не препятствует, реле АБ- i будет отключено. Обязательное требование: эта команда должна быть единственной в командном пакете МКО, в противном случае она выполнена не будет.

Требование единственности критической команды в пакете обусловлено необходимостью подтверждения намерения центра управления осуществить потенциально опасное действие без организации полноценной обратной петли типа "запрос – ответ". В данном случае логика защиты простирается в том числе и на возможные варианты сбоев автоматизированных систем формирования командных последовательностей, широко применяемых в современных ЦУП, которые по каким-то гипотетическим причинам могут сформировать правильный формат критической команды.

Если подобная команда в результате программного, аппаратного сбоя или ошибочных действий оператора будет создана и вставлена в общую последовательность команд, то она будет проигнорирована в силу требования единственности в пакете.

Если по подобным причинам будет создан пакет, содержащий единственную одну из двух критических команд, то она также будет проигнорирована в силу требования их последовательной подачи в течение 5 с.

Во всех остальных случаях разнородных технических сбоев в каналах передачи, алгоритмах хеширования и т.п. этот уровень обеспечивает дополнительную страховку имеющихся средств обнаружения и коррекции ошибок.

При необходимости количество последовательных разрешений для снятия блокировки отключения может быть увеличено, однако предлагаемый вариант представляется вполне достаточным в практических применениях. Время действия команды снятия блокировки в 5 с также выбрано на компромиссной основе путем анализа опыта работы с различными каналами управления космическими аппаратами и может быть при необходимости изменено.

ВТОРОЙ КОНТУР АЛГОРИТМИЧЕСКОЙ ЗАЩИТЫ

Второй уровень защиты работает автоматически путем учета значений "Битов Блокировки Отключения" (ББО- i , $i = 1, 2$) для каждой батареи i . Состояние этих битов должно отображаться в телеметрии космического аппарата и имеет следующий смысл:

– если бит "ББО- i " установлен в "0", то прохождение команды отключения на реле i разрешено;

– если бит "ББО- i " установлен в "1", то прохождение команды отключения на реле i безусловно запрещено. В этом случае МЦУ в принципе не должен иметь возможность выдать команду на отключение соответствующего реле на аппаратном уровне, а соответствующий триггер должен иметь устойчивую к однократным сбоям аппаратную архитектуру (троирование с автокоррекцией).

При начальной загрузке вычислителя МЦУ (включение питания, перезагрузка по сторожевому таймеру и по аварийному снижению напряжения питания процессора) биты "ББО- i " устанавливаются в состояние "0", т.е. блокировка отключения батарей неактивна. Этому должна соответствовать ситуация, когда все батареи изначально подключены к силовым шинам питания в ходе наземной отработки перед запуском, что является критическим моментом и должно быть четко прописано в ПНЭО. Для упрощения далее приводится алгоритм для случая двух бортовых батарей.

После выполнения команды "Отключить АБ-1":

– бит "ББО-2" устанавливается в "1", безусловно запрещая в дальнейшем отключение реле АБ-2;

– работа алгоритма управления нивелиром поэлементных напряжений АБ-1 блокируется установкой соответствующего бита управления, отключается также сам нивелир [4];

– работа алгоритма поэлементного контроля АБ-1 [4] блокируется установкой соответствующего бита управления;

– МЦУ выдает импульсную команду на поляризованное реле отключения АБ-1, которая отключает ее от силовой шины питания нагрузки.

После выполнения команды "Отключить АБ-2":

– бит "ББО-1" устанавливается в "1", безусловно запрещая в дальнейшем отключение реле АБ-1;

– работа алгоритма управления нивелиром поэлементных напряжений АБ-2 блокируется установкой соответствующего бита управления, отключается также сам нивелир;

– работа алгоритма поэлементного контроля АБ-2 блокируется установкой соответствующего бита управления;

– МЦУ выдает импульсную команду на поляризованное реле отключения АБ-2, которая отключает ее от силовой шины питания нагрузки.

После выполнения команды "Включить АБ-1":

– бит "ББО-2" устанавливается в "0", делая возможным в дальнейшем отключение реле АБ-2;

– работа алгоритмов управления нивелиром и поэлементным контролем напряжений АБ-1 разрешается;

– МЦУ выдает импульсную команду на поляризованное реле отключения АБ-1, которая подключает ее к силовой шине питания нагрузки.

После выполнения команды "Включить АБ-2":

– бит "ББО-1" устанавливается в "0", делая возможным в дальнейшем отключение реле АБ-1;

– работа алгоритмов управления нивелиром и поэлементным контролем напряжений АБ-2 разрешается;

– МЦУ выдает импульсную команду на поляризованное реле отключения АБ-2, которая подключает ее к силовой шине питания нагрузки.

При выполнении условия, что перед запуском аппарата оба реле АБ-1 и АБ-2 будут находиться в замкнутом состоянии (обе АБ подключены к шине питания), состояние битов "ББО-1/2" будет правильно отражать текущее состояние блокировок и самих батарей:

– значения "ББО-2" = 0 и "ББО-1" = 0 ("00") будут показывать, что обе батареи подключены к силовой шине;

– значения "ББО-2" = 1 и "ББО-1" = 0 ("10") будут показывать, что АБ-1 отключена;

– значения "ББО-2" = 0 и "ББО-1" = 1 ("01") будут показывать, что АБ-2 отключена;

– комбинация "ББО-2" = 1 и "ББО-1" = 1 ("11") будет невозможной.

Однако следует иметь в виду, что в случае перезагрузки вычислителя МЦУ в процессе полета (воздействие тяжелой заряженной частицы, просадка питания, вызвавшие перезагрузку от встроенных средств парирования однократных сбоев) значения битов ББО будут установлены в исходные состояния (00) и перестанут правильно отображать фактическое состояние реле отключения АБ. При этом в случае, если одна из АБ отключена, функция блокировки одновременного отключения обеих АБ работать не будет — снимается второй уровень защиты. Этот факт может быть зафиксирован по телеметрии космического аппарата, т.к. биты ББО изменят свое значение, а в признаках срабатывания защит должна быть показана информация о факте перезагрузки вычислителя МЦУ. При этом первый уровень защиты будет работать при любых условиях.

Для восстановления второго уровня защиты от необратимого события (отключения обеих АБ) имеется возможность восстановить правильные значения битов ББО специальными командами типа "Установить ББО 01" и "Установить ББО 10":

– если зафиксирован факт перезагрузки бортового вычислителя МЦУ и известно, что АБ-1 отключена от шины, то следует подать команду "Установить ББО 10" и проконтролировать по последующей телеметрии факт правильной установки этих битов;

– если зафиксирован факт перезагрузки вычислителя и известно, что АБ-2 отключена от шины, то следует подать команду "Установить ББО 01" и также проконтролировать факт правильной установки этих битов;

– если зафиксирован факт перезагрузки вычислителя и известно, что обе АБ подключены к шине, то действий никаких не требуется, т.к. биты ББО будут установлены в правильные состояния 00.

Ввиду потенциальной опасности неправильной установки битов ББО командами типа "Установить ББО 01/10" на каждую из них целесообразно установить защиту предварительной подачей соответствующей разрешающей команды, аналогично первому контуру защиты от отключения обеих АБ.

Для подключения батареи с индексом i по команде наземного центра управления необходимо выполнить следующие действия также в соответствии с первым контуром защиты:

1. Подать команду "Разрешить включение АБ- i ". Эта команда разрешает прохождение дальнейшей команды включения АБ- i в течение 5 с, после чего режим разрешения автоматически отменяется. Эта команда должна быть единственной в командном пакете МКО, в противном случае она выполнена не будет.

2. Подать команду "Включить АБ- i ". Если блокировка по предыдущей команде разрешения этому не препятствует, реле АБ- i будет включено. Эта команда также должна быть единственной в командном пакете МКО, в противном случае она выполнена не будет.

Описанная выше логика защиты по понятным причинам будет иметь смысл исключительно при условии ручного режима управления перекоммутацией бортовых батарей со стороны ЦУП. С учетом новизны предлагаемой архитектуры системы электроснабжения это представляется вполне достаточным на первых этапах ее внедрения и возможной доработки. Для реализации потенциально заложенных в нее возможностей безопасной автоматической перекоммутации в аварийных случаях, по-видимому, единственным вариантом ее реализации следует признать введение в систему дополнительных датчиков состояния поляризованных реле отключения батарей в процессе начальной загрузки вычислителя МЦУ в случае разнородных сбоев при эксплуатации, приводящих к его перезагрузке.

ВЫВОДЫ

Описанные алгоритмы управления резервированием литий-ионных аккумуляторных батарей открывают возможность рассмотрения этих специфических элементов систем электроснабжения космических экспериментальных комплексов как объектов применения классических методов резервирования. Это позволяет снять некоторые ограничения, препятствующие применению батарей этого типа в условиях космического пространства, как уже отмечалось ранее в работе [3].

Следует подчеркнуть, что предлагаемые алгоритмы имеют основным предназначением

защиту от необратимого отключения батарей в режиме ручного управления со стороны ЦУП исключительно в результате разнородных *непреднамеренных* ошибок и сбоев, включая такие, вероятность которых зачастую невозможно достоверно установить в численном выражении аналитически или по различного рода нормативной документации. В основном это касается ошибок, обусловленных человеческим фактором, который, как показывает практика различного рода аварий и техногенных катастроф, никогда нельзя исключать из рассмотрения.

СПИСОК ИСТОЧНИКОВ

1. Lithium Batteries: Science and Technology / ed. by G.-A. Nazri, G. Pistoia. New York, Springer, 2009. 708 p. DOI: 10.1007/978-0-387-92675-9
2. Хромов А.В. Литий-ионные аккумуляторные батареи низкоорбитальных космических аппаратов // Вопросы электромеханики. Труды ВНИИЭМ. 2016. Т. 152, № 3. С. 20–28. URL: <https://elibrary.ru/item.asp?id=28394136>
3. Лисин Д.В. Архитектура системы электроснабжения космических экспериментальных комплексов на базе литий-ионных аккумуляторных батарей // Научное приборостроение. 2025. Т. 35, № 2. С. 67–77. URL: <http://iairas.ru/mag/2025/abst2.php#abst5>
4. Лисин Д.В. Реализация метода поэлементного контроля литий-ионных аккумуляторных батарей при работе на борту космических аппаратов научного назначения // Научное приборостроение. 2018. Т. 28, № 2. С. 69–74. URL: <http://iairas.ru/mag/2018/abst2.php#abst10>

Институт земного магнетизма, ионосферы и распространения радиоволн им. Н.В. Пушкова Российской академии наук (ИЗМИРАН), г. Москва, Троицк

Контакты: Лисин Дмитрий Валерьевич,
lisindv@izmiran.ru

Материал поступил в редакцию 27.01.2026

BACKUP MANAGING ALGORITHMS FOR LITHIUM-ION BATTERIES OF SPACE EXPERIMENTAL COMPLEXES

D. V. Lisin

*Pushkov Institute of Terrestrial Magnetism, Ionosphere and Radio Wave Propagation (IZMIRAN),
Troitsk, Moscow, Russia*

The article continues the description of the architecture developed at IZMIRAN for building a highly reliable power supply system based on lithium-ion batteries designed for conducting scientific experiments on board spacecraft. The issues of constructing algorithms for controlling two batteries are considered, taking into account the issues of overall reliability of the system as a whole. These algorithms are designed to be implemented in an on-board microprocessor control unit for the power supply system of a spacecraft with two or more lithium-ion batteries.

Keywords: power supply system, lithium-ion battery, space experiment, redundancy management, backup algorithms

REFERENCES

1. Nazri G.-A., Pistoia G., eds. *Lithium Batteries: Science and Technology*. New York, Springer, 2009. DOI:10.1007/978-0-387-92675-9
2. Khromov A.V. [Lithium-ion accumulator batteries for low-orbit spacecraft]. *Voprosy elektromekhaniki. Trudy VNIEM* [Electromechanical matters. VNIEM proceedings], 2016, vol. 3, iss. 152, pp. 20–28. URL: <https://jurnal.vniem.ru/text/152/20-28.pdf> (In Russ.).
3. Lisin D.V. [Architecture of the power supply system for space experimental complexes based on lithium-ion batteries]. *Nauchnoe priborostroenie* [Scientific instrumentation], 2025, vol. 35, no. 2, pp. 67–77. URL: <https://iairas.ru/mag/2025/full2/Art5.pdf> (In Russ.).
4. Lisin D.V. [Implementation of a single element control method for lithium-ion batteries when operating on board scientific spacecraft]. *Nauchnoe priborostroenie* [Scientific instrumentation], 2018, vol. 28, no. 2, pp. 69–74. DOI: 10.18358/np-28-2-i6974 (In Russ.).

Contacts: *Lisin Dmitrij Valer'evich*,
lisindv@izmiran.ru

Article received by the editorial office on 27.01.2026

INTRODUCTION

Lithium-ion batteries hold great promise for use in various types of experiments in Earth orbit, primarily due to their excellent weight-to-size characteristics [1, 2]. However, this technology has a number of fundamental drawbacks, including a narrow operating temperature range, increased explosion hazard, accelerated degradation when charge/discharge conditions deviate from optimal values, and a short service life compared to other types of batteries. These drawbacks can be largely overcome by using intelligent battery management systems, including those built into the battery itself, as well as by employing special approaches to organizing power supply systems and control methods. This article examines issues related to control algorithms for two or more batteries, primarily for their mutual redundancy, within the control system architecture described in [3].

SYSTEM ARCHITECTURE AND BATTERY REDUNDANCY POLICY

A typical architecture for the experimental spacecraft's power supply system, which includes two lithium-ion batteries for redundancy, is shown in Fig. The operating aspects of this system are described in detail in [3], but the circuit shown in Fig. differs fundamentally from that discussed in [3]: to control the switching of the primary and backup batteries, it incorporates two polarized battery disconnect relays. The use of polarized relays ensures the energy independence of the selected configuration, and their presence allows for the implementation of various redundancy management policies, for example:

- 1) both batteries are always connected in parallel to increase the total capacity; however, if signs of dangerous degradation are detected in the telemetry data, in particular irreversible imbalance of the elements [4], the battery can be disconnected from the power bus either automatically or by command from the ground control center (GCC);

- 2) one of the batteries is in "cold reserve", i.e., initially disconnected from the power bus and is connected to it only in cases where a critical discharge of the main battery is detected — automatically or by command from the GCC;*

- 3) at any given time, the load is powered by only one battery, the selection of which changes cyclically at regular intervals (either automatically or by command from the GCC).

* Note: The figure assumes that the charging circuits of all batteries are connected to them constantly, are controlled automatically and are not shown in the figure, since they are not relevant to the consideration

Fig. Spacecraft power supply system architecture.
ВПП — secondary power source, РК — radio command, КПА — ground test equipment

Each of the above policies has its own advantages and disadvantages, a discussion of which is beyond the scope of this article, which is intended only to highlight the algorithms for implementing such a critical action as switching the power buses of the spacecraft's onboard batteries during the implementation of the above or any other redundancy management policies.

ADVANTAGES AND DISADVANTAGES OF THE PROPOSED ARCHITECTURE

The use of controlled switches (polarized relays) in the power circuits of both redundant batteries opens up wide possibilities for implementing various options for their mutual redundancy, especially given the rather specific characteristics of lithium-ion cells [1]. However, it represents an extremely dangerous solution in terms of controlling such a system. The main danger is sending an erroneous sequence of commands, which would lead to the shutdown of both batteries, which would be tantamount to the loss of the spacecraft. Nevertheless, the ability to effectively replace a faulty battery during orbital flight, including in automatic mode, can often yield very significant results, considering the significant extension of the operating time of the complex and expensive experimental equipment powered by it.

If sufficient systemic measures are taken to protect against erroneous irreversible disconnection of both batteries, the proposed architecture can be used while maintaining a sufficient level of reliability of the equipment complex as a whole. Such measures can be classified into three main groups: hardware, software, and software-hardware protection. Hardware measures can include, for example, the use of additional contact groups of polarized relays, which would serve as state sensors for the hardware circuit blocking the sending of pulse commands to disconnect both relays simultaneously. Other hardware options for organizing the battery switching circuit, which would exclude their simultaneous disconnection, are also possible; however, their consideration is beyond the scope of this article. In developing the proposed approach to solving the main problem described above, the principle of minimizing the use of hardware circuits in the switching node was put forward, since the reliability of a properly designed algorithm is always higher than the reliability of relay contacts and other hardware components.

CONTROL LOGIC FOR BATTERY BUS KEYS

Let's consider the general operating logic of the polarized battery disconnect relays shown in the figure, which for brevity we will refer to as their power bus keys. It should be emphasized that these keys are not intended to control load switching (spacecraft service systems, scientific equipment, etc.), but exclusively to control onboard battery switching. This switching can be performed in two main spacecraft states: during ground testing and during orbital flight.

In the first case, pulse commands for switching the keys are issued manually from the test equipment, which is usually connected to dedicated connectors. Typically, these will be specially designated buttons with names such as "AB-1 ON," "AB-1 OFF," etc., with corresponding indication, or corresponding relay outputs of some automated system used during ground testing of the complex. In this case, switching of contact groups (reconfiguration of the apparatus's batteries) should occur in the absence of load current (the compartment contact, its simulators, and its blocking circuits in the figure should be open). In this case, there will be virtually no contact wear during any amount of experimental testing. This requirement is quite easily met by appropriately designing the ground experimental testing (GET) programs for the complex.

In the second case, these pulse commands are generated both by algorithms automatically operating within the digital/emergency control modules (DCM/EMC) and by direct commands received via the spacecraft's onboard radio link from the GCC.

For example, a typical scenario for conducting ground tests with sequential use of both batteries might look like this:

- by pressing the "AB-1 ON" and "AB-2 OFF" buttons on the test equipment console, battery No. 1 is connected to the power bus, and battery No. 2 is disconnected from it;
- by pressing the "ON" button, the compartment contact is bypassed, power is supplied to the digital control module (DCM), which begins processing the standard power-up sequence and turns on the load;
- after completing the test sequence with power from battery No. 1, the "OFF" button is pressed on the test equipment console, which activates the holdover circuit and breaks the bypass circuit of the compartment contact, disconnecting the load;
- by pressing the "OFF AB-1" and "ON AB-2" buttons on the control panel, battery No. 1 is disconnected and battery No. 2 is connected to the power bus, and the test sequence is repeated with power from battery No. 2;
- the load is disconnected using the "OFF" button, and the polarized battery disconnect relays are reset by commands from the control panel to their initial

state, corresponding to the selected battery backup policy.

In this case, disconnecting both batteries during ground testing is entirely possible and may even be a desirable option for debugging the system in some cases. The control algorithm architecture under consideration includes two independent protection loops, the combined operation of which appears sufficient for application in the area under consideration. When controlled by the second loop (either by automatic algorithms or by GCC commands), the possibility of disconnecting both batteries should be completely eliminated.

It should be noted that the following discussion assumes control of the digital control module (DCM) of the power supply system from the spacecraft's onboard control system via a standard multiplex communication channel (SMC). This, however, does not reduce the generality of the presentation, as control using other protocols will, in one way or another, utilize the principle of packet transmission of a set of commands. In this case, it is certainly implied and is not further specified that there are highly reliable means of checking the authenticity of command packets at all stages transmitted from their formation in the GCC to their transmission to the DCM via the onboard channel, and ensured by the use of hash sums, correcting codes and other methods of detecting single and group errors.

FIRST ALGORITHMIC PROTECTION CIRCUIT

To disconnect battery with index i upon command from the ground control center, the following steps must be performed:

1. Issue the "Allow AB- i Shutdown" command. This command allows further AB- i shutdown commands to proceed for 5 s, after which the permission mode is automatically canceled. Mandatory requirement: this command must be the only one in the SMC command package; otherwise, it will not be executed.
2. Issue the "Disable AB- i " command. If no interlocks prevent this, the AB- i relay will be deactivated. Mandatory requirement: this command must be the only one in the MKO command packet; otherwise, it will not be executed.

The requirement for a single critical command in the packet is due to the need to confirm the control center's intention to perform a potentially dangerous action without establishing a full-fledged request-response feedback loop. In this case, the protection logic also covers possible failures of automated command sequence generation systems, widely used in modern GCC, which, for some hypothetical reason, could fail to generate the correct format for a critical command.

If such a command is created and inserted into the general command sequence as a result of a software or hardware failure or operator error, it will be ignored due to the requirement for uniqueness in a package.

If, for similar reasons, a packet is created containing only one of two critical commands, the latter will also be ignored due to the requirement for their sequential transmission within 5 s.

In all other cases of heterogeneous technical failures in transmission channels, hashing algorithms, etc., this level will provide additional insurance for existing error detection and correction tools.

If necessary, the number of consecutive permissions for unlocking the shutdown lock can be increased; however, the proposed option appears to be sufficient for practical applications. The lock/unlock command duration of 5 s was also chosen as a compromise based on an analysis of experience with various spacecraft control channels and can be changed if necessary.

SECOND LOOP OF ALGORITHMIC PROTECTION

The second level of protection operates automatically by taking into account the values of the "Shutdown Lockout Bits" (SLI- i , $i = 1, 2$) for each battery i . The state of these bits must be reflected in the spacecraft telemetry and has the following meaning:

- if bit "SLI- i " is set to "0", then the shutdown command to relay i is permitted;
- if bit "SLI- i " is set to "1", then the shutdown command to relay i is unconditionally prohibited. In this case, the DCM should not be able to issue a command to disable the corresponding relay at the hardware level, and the corresponding trigger should have a hardware architecture that is resilient to single-shot failures (tripled with autocorrection).

During the initial bootup of the DCM calculator (power-up, reset by the watchdog timer, and by an emergency reduction in the processor supply voltage), the "SLI- i " bits are set to "0," i.e., the battery disconnect interlock is inactive. This should correspond to the situation when all batteries are initially connected to the power buses during ground testing before launch, which is a critical point and should be clearly specified in the GET. For simplicity, the algorithm for the case of two onboard batteries is provided below.

After executing the "Disable AB-1" command:

- the "SLI-2" bit is set to "1," unconditionally prohibiting further disabling of the AB-2 relay;
- the operation of the AB-1 element-by-element voltage level control algorithm is blocked by setting the corresponding control bit, and the level itself is also disabled [4];

- the operation of the AB-1 element-by-element monitoring algorithm [4] is blocked by setting the corresponding control bit;

- the DCM issues a pulse command to the AB-1 polarized shutdown relay, which disconnects it from the load power bus.

After executing the "Disable AB-2" command:

- the "SLI-1" bit is set to "1", unconditionally prohibiting further disabling of the AB-1 relay;

- the operation of the AB-2 element-by-element voltage level control algorithm is blocked by setting the corresponding control bit, the level itself is also disabled;

- the operation of the AB-2 element-by-element monitoring algorithm is blocked by setting the corresponding control bit;

- the DCM issues a pulse command to the AB-2 polarized shutdown relay, which disconnects it from the load power bus.

After executing the "Enable AB-1" command:

- the "SLI-2" bit is set to "0", allowing further disabling of the AB-2 relay;

- the operation of the level control algorithms and the AB-1 element-by-element voltage monitoring algorithm are enabled;

- the DCM issues a pulse command to the polarized trip relay AB-1, which connects it to the load power bus.

After executing the "Enable AB-2" command:

- the "SLI-1" bit is set to "0", enabling further tripping of the AB-1 relay;

- operation of the leveling and element-by-element voltage monitoring algorithms for AB-2 is enabled;

- the DCM issues a pulse command to the polarized trip relay AB-2, which connects it to the load power bus.

Provided that both relays AB-1 and AB-2 are closed before the device starts (both AB are connected to the power bus), the state of the "BBO-1/2" bits will correctly reflect the current state of the interlocks and the batteries themselves:

- values "SLI-2" = 0 and "SLI-1" = 0 ("00") will indicate that both batteries are connected to the power bus;

- values "SLI-2" = 1 and "SLI-1" = 0 ("10") will indicate that AB-1 is disconnected;

- values "SLI-2" = 0 and "SLI-1" = 1 ("01") will indicate that AB-2 is disconnected;

- the combination "SLI-2" = 1 and "SLI-1" = 1 ("11") will be impossible.

However, it should be kept in mind that if the DCM calculator is rebooted during flight (due to the impact of a heavy charged particle, a power failure, or a reboot caused by the built-in single-shot fault mitigation system), the SLI bit values will be reset to their

initial values (00) and will no longer correctly reflect the actual state of the AB shutdown relay. Furthermore, if one AB is disconnected, the function that blocks simultaneous shutdown of both AB will not function—the second level of protection is disabled. This can be recorded via spacecraft telemetry, as the SLI bits will change their values, and the protection activation indicators should record a reboot of the MCC computer. However, the first level of protection will operate under any conditions.

To restore the second level of protection against an irreversible event (disconnection of both AB), it is possible to restore the correct values of the onboard computer bits using special commands such as "Set SLI 01" and "Set SLI 10":

- If a reboot of the DCM onboard calculator is detected and it is known that AB-1 is disconnected from the bus, then the "Set SLI 10" command should be issued and the correct setting of these bits should be verified using subsequent telemetry;

- If a reboot of the calculator is detected and it is known that AB-2 is disconnected from the bus, then the "Set SLI 01" command should be issued and the correct setting of these bits should be verified;

- If a reboot of the calculator is detected and it is known that both AB are connected to the bus, then no action is required, since the SLI bits will be set to the correct values of 00.

Due to the potential danger of incorrectly setting the SLI bits with commands like "Set SLI 01/10," it is advisable to set protection for each of them by first sending the appropriate enabling command, similar to the primary protection circuit against disconnection of both AB.

To connect the battery with index i , following a command from the ground control center, the next steps must be performed, also in accordance with the primary protection circuit:

1. Send the "Allow AB- i to turn on" command. This command allows further AB- i turn-on commands for 5 seconds, after which the enable mode is automatically canceled. This command must be the only one

in the SMC command packet; otherwise, it will not be executed.

2. Send the "Turn on AB- i " command. If the previous enable command does not prevent this, the AB- i relay will be activated. This command must also be the only one in the SMC command packet; otherwise, it will not be executed.

The protection logic described above, for obvious reasons, will only make sense if the onboard battery switching mode is manually controlled by the GCC. Given the novelty of the proposed power supply system architecture, this seems entirely sufficient for the initial stages of its implementation and possible refinement. To realize the potential for safe automatic reconnection in emergency situations, the only implementation option seems to be the introduction of additional polarized battery disconnect relay state sensors during the initial boot process of the DCM computer in the event of various operational failures leading to its reboot.

CONCLUSIONS

The described algorithms for managing the redundancy of lithium-ion batteries open the possibility of considering these specific elements of the power supply systems of space experimental complexes as objects for the application of classical redundancy methods. This makes it possible to remove some of the limitations that hinder the use of batteries of this type in space conditions, as previously noted in [3].

It should be emphasized that the proposed algorithms are primarily designed to protect against irreversible battery shutdowns under manual control by the GCC solely as a result of various unintentional errors and failures, including those whose probability is often impossible to reliably quantify analytically or using various regulatory documentation. This primarily concerns errors caused by human error, which, as experience with various types of accidents and man-made disasters shows, can never be ruled out.