МПСУвЭПиТК

ПЛК и безопасность

ПЛК может создавать потенциально опасные ситуации по разным причинам. Первая (и, по-видимому, самая распространенная) – это логические ошибки в программе. Они могут возникнуть из-за оплошности или неправильного понимания со стороны разработчика, который не учел, что *именно такая* последовательность действий может представлять опасность, или в результате последующих изменений, сделанных людьми, которые умышленно (или случайно) удалили некоторую защиту, позволяющую избежать отказов в ночное время. Особенно неприятным фактором является *ночное программирование*, поскольку обычно нарушителем выступает только один человек, который знает, как оно выполнялось, и опасность может возникнуть по прошествии значительного времени (дни, недели, месяцы, годы), когда для нее созреют соответствующие условия.

Вторая возможная причина – это неисправность входных и выходных модулей, особенно элементов, непосредственно связанных с объектом и подверженных влиянию высоковольтных помех (а возможно, напрямую соединенных с источниками высокого напряжения кабелем, который может быть поврежден). Выходные модули могут также пострадать от скачка тока при коротком замыкании цепи (что также вполне вероятно).

Типичными выходными элементами являются симисторы, тиристоры и транзисторы. Их отказ невозможно предсказать заранее; все они могут быть повреждены при обрыве или коротком замыкании цепи. В этих случаях ПЛК не сможет управлять выходными устройствами. Точно так же входной сигнал, имеющий два состояния (логические 1 и 0), может быть неправильно интерпретирован ПЛК в случае отказа элементов входной платы.

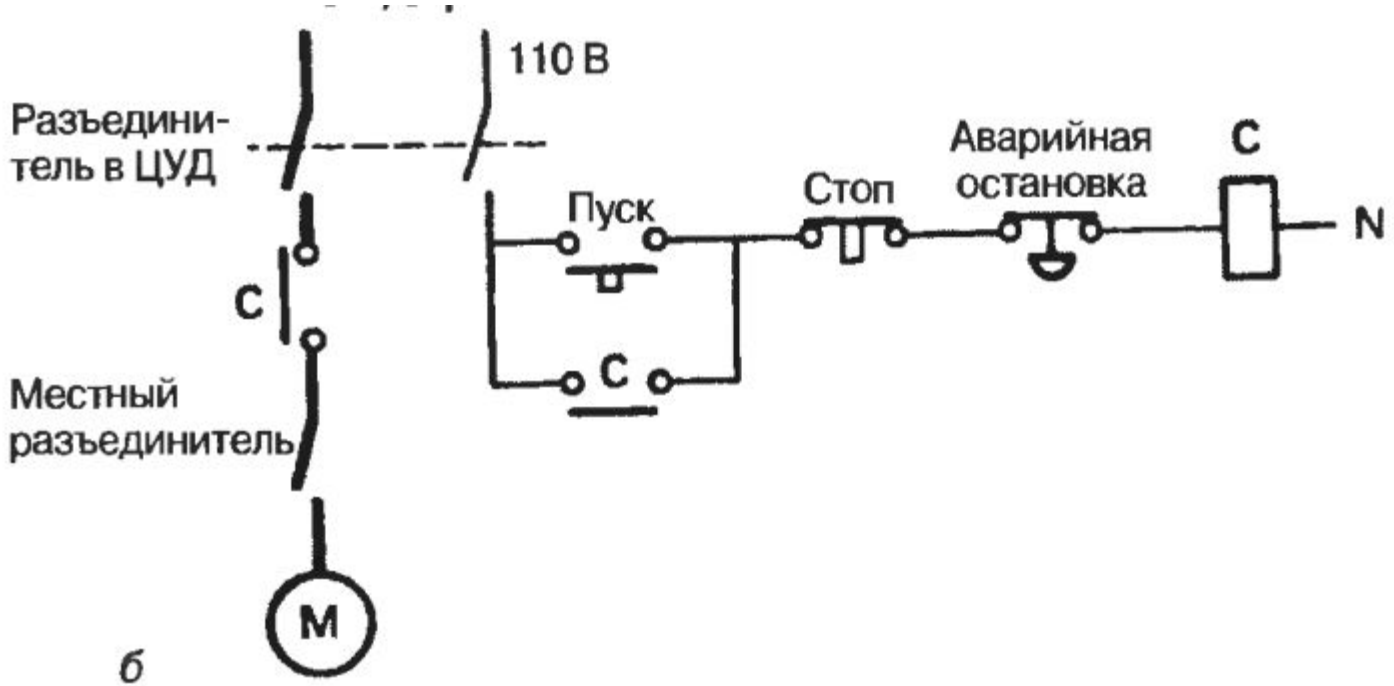
Следующий вид неисправностей связан собственно с ПЛК. Его можно подразделить на отказы аппаратуры, сбои в программах и эффекты, обусловленные влиянием окружающей среды. Отказ аппаратных средств происходит в самой машине – уязвимыми являются источник питания, процессор, память (которая содержит программы, предоставленные поставщиком с учетом особенностей ПЛК, пользовательские программы и хранилище данных). Некоторые из этих отказов имеют предсказуемые последствия; при отказе источника питания все выходы будут отключены, а поставщик ПЛК обязан предусмотреть средства тестирования памяти

Последней причиной являются электрические помехи (обычно называемые шумом). Внутренние схемы почти всех ПЛК работают с сигналами уровня 5 В, но они находятся в окружении высоковольтных, сильноточных устройств. Шум может привести к тому, что ПЛК будет воспринимать входные сигналы с искажениями, а в крайних случаях он даже может испортить внутреннюю память ПЛК. Обычно ПЛК снабжается защитой от повреждения памяти и помех, наводимых в линиях последовательной дистанционной связи с входными/выходными устройствами (опять-таки с помощью CRC и аналогичных идей), поэтому самым простым эффектом помехи будет выключение ПЛК (и перевод выходов в неактивное состояние). В этом, однако, нельзя быть полностью уверенным.

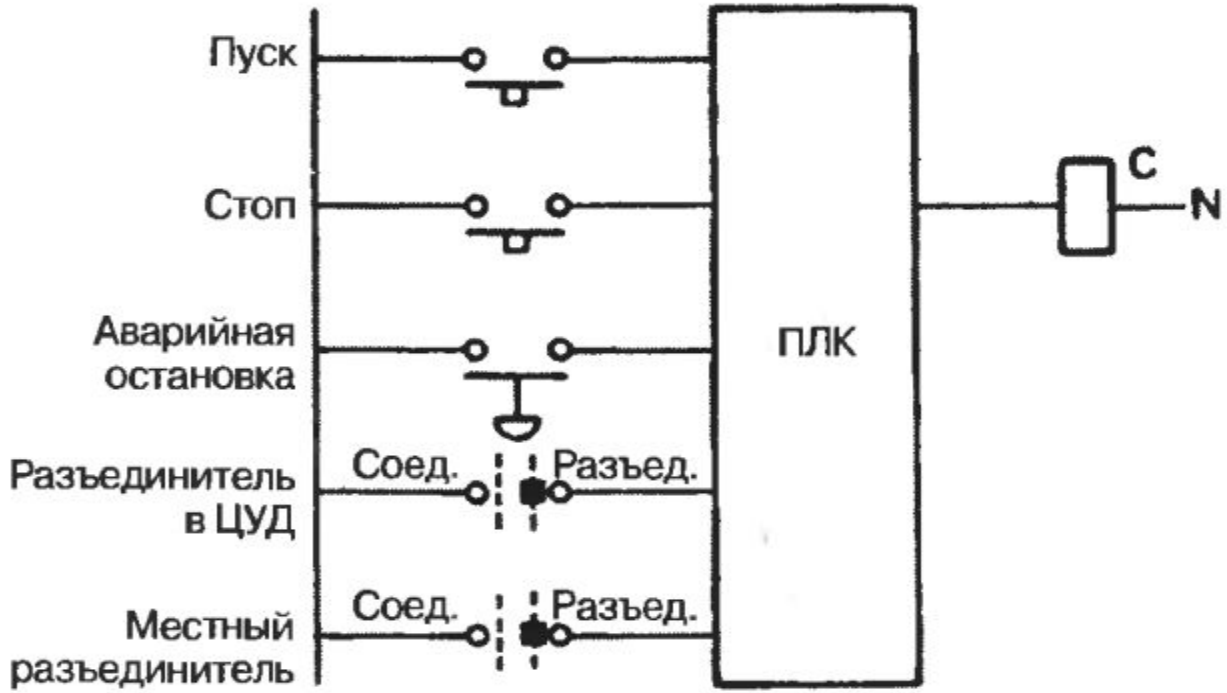
Не существует такого понятия, как абсолютно безопасный процесс; всегда можно найти потенциально возможные причины отказов, которые приводят к опасным последствиям. Но в качественно спроектированной системе такие режимы отказов практически маловероятны.

44% происшествий вызваны плохими или неточными техническими требованиями;
15% вызваны ошибками при проектировании;
6% появились в процессе монтажа и ввода в эксплуатацию;
14% выявлены в процессе работы и текущего обслуживания;
21% вызван плохо продуманными решениями при модернизации.

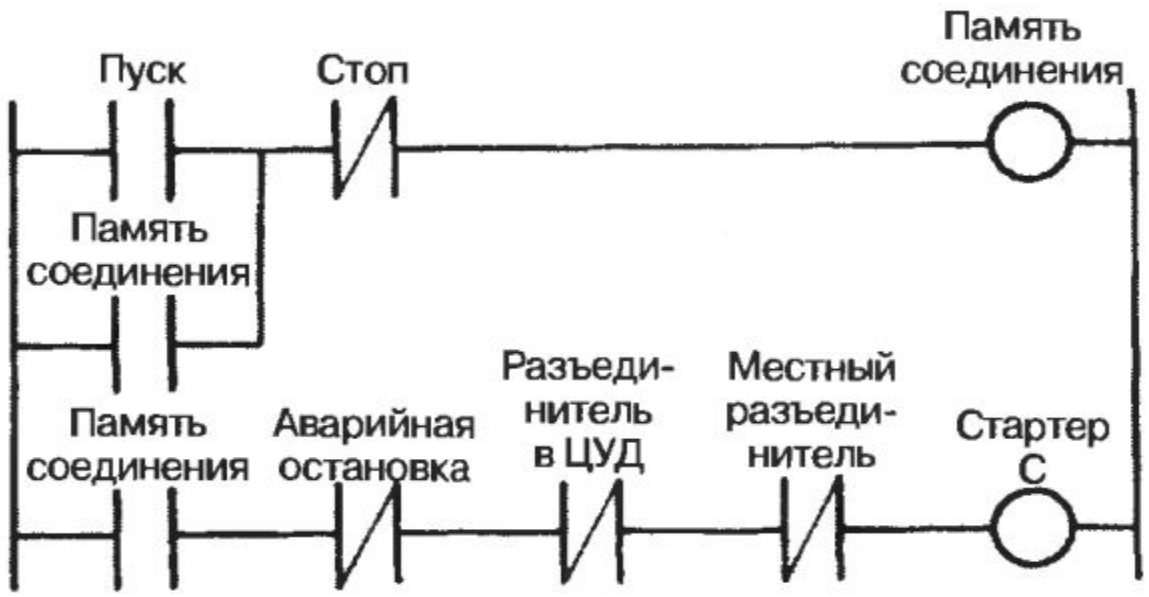
Иными словами, наиболее распространенными причинами происшествий были упущения при составлении исходных технических



Обычное пусковое устройство двигателя:


Пуск
Стоп
Аварийная остановка
Разъединитель в ЦУД
Соед.
Разъед.
Местный разъединитель
Соед.
Разъед.
ПЛК
C
N

а


Пуск
Стоп
Память соединения
Память соединения
Память соединения
Аварийная остановка
Разъеди-нитель в ЦУД
Местный разъеди-нитель
Стартер C

б

Различия (и опасности) проявляются в типе неисправностей или необычных условиях. В частности:

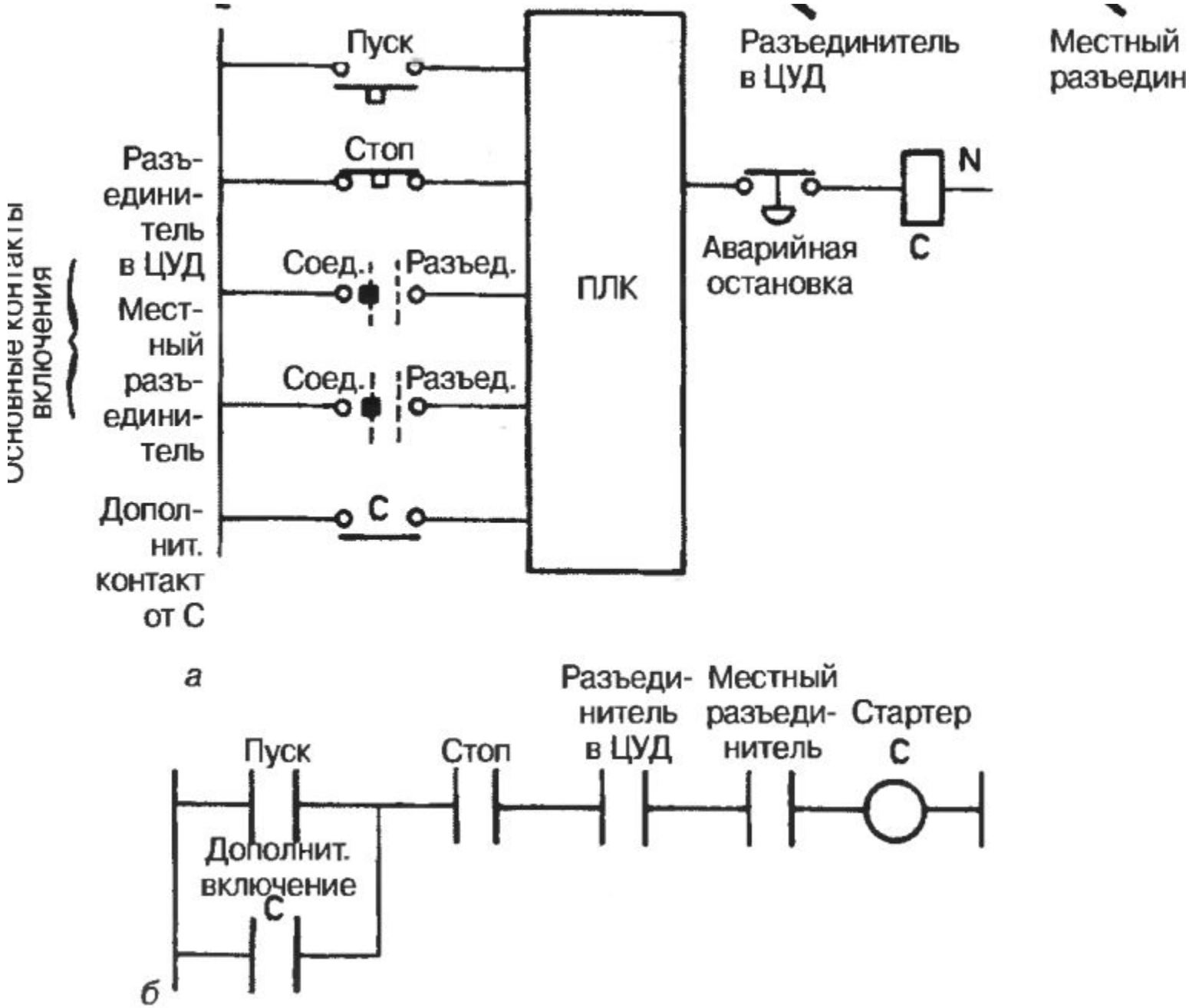
А. Человек, использующий терминал для программирования, может принудительно изменить входные или выходные сигналы, проигнорировав разъединение. Хотя вряд ли кто-то будет делать это умышленно, но очень легко можно перепутать похожие адреса и переставить биты (например, вместо О:32/01 указав О:23/01).

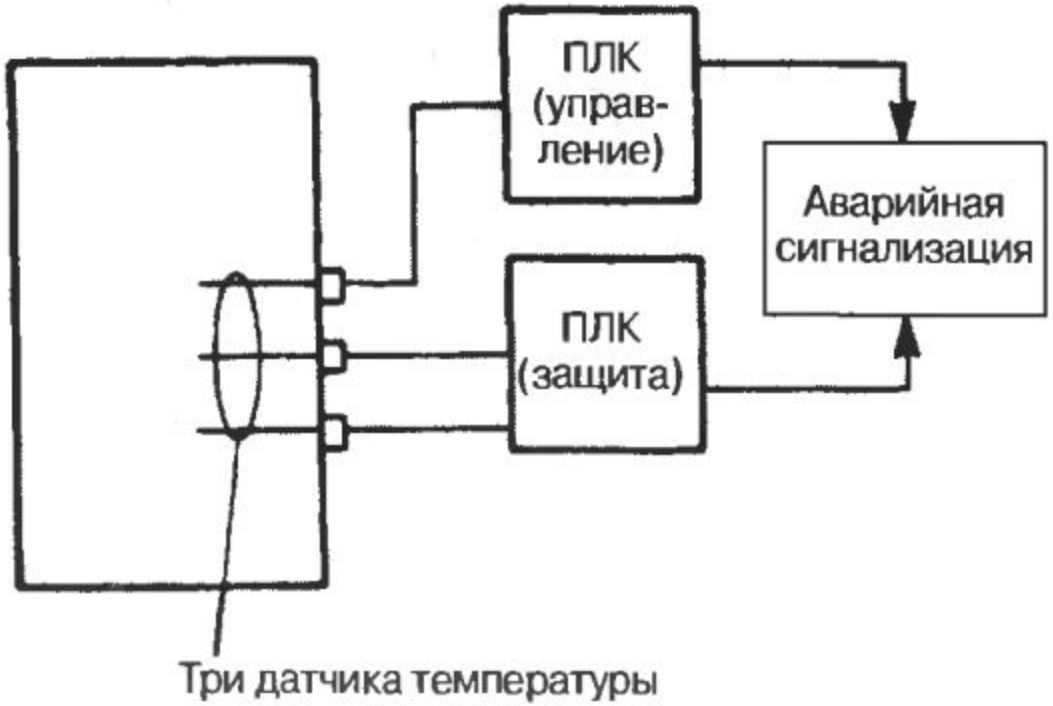
Б. Пропажа питания устройств управления вводом при работающем двигателе будет означать, что его нельзя будет остано-

В. Если нажать и отпустить кнопку аварийной остановки, то двигатель вновь будет запущен.

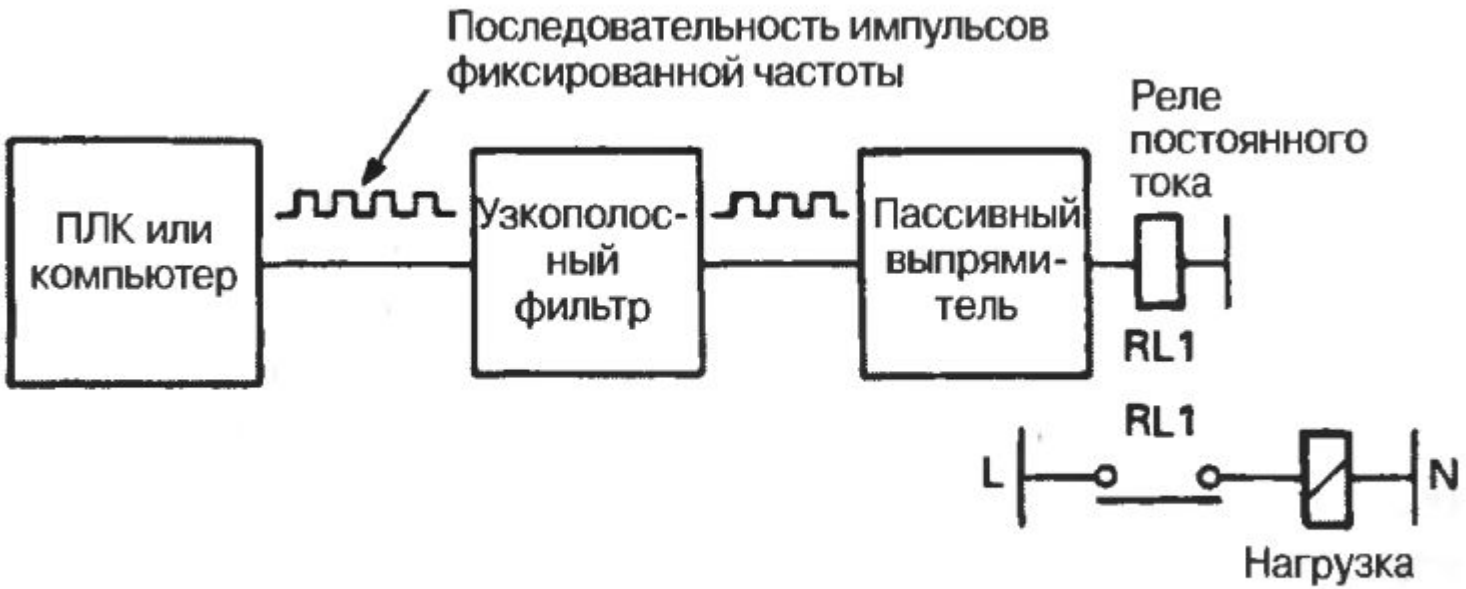
Ни одно из этих условий не является очевидным для пользователя до тех пор, пока о них не придется вспомнить в случае аварии.

Таким образом, при использовании в системе управления ПЛК или компьютеров первое правило таково: «Система должна быть по меньшей мере столь же безопасной, как и обычная система».


Пуск
Стоп
Разъединитель в ЦУД
Местный разъедин
Разъ-единитель в ЦУД
Соед.
Разъед.
Мест-ный разъ-единитель
Соед.
Разъед.
Основные контакты включения
Дополнит. контакт от С
С
ПЛК
Аварийная остановка
С
N
а
Пуск
Стоп
Разъеди-нитель в ЦУД
Местный разъеди-нитель
Стартер С
Дополнит. включение С
б



Если полагаться на дублирование систем управления, то они должны быть совершенно различными – различные машины с разными входными/выходными устройствами, различные программы, написанные разными людьми, разные источники питания для каждой машины и различные типы датчиков, подключаемых с помощью разных кабельных соединений. Вот это и будет означать настоящее резервирование.



Динамическая «отказобезопасная» схема