Архитектура безопасности.

Что означает «архитектура безопасности»?

Архитектура безопасности это структура цепей, применимая как к отдельным элементам системы управления, связанным с обеспечением безопасности, так и к комплексу таких элементов.

Стандарт EN ISO 13849-1:2006 рассматривает всем известные категории риска через архитектуры безопасности, проиллюстрированные ниже:

Рисунок 1. Категория 1 и B.

Рисунок 2. Категория 2.

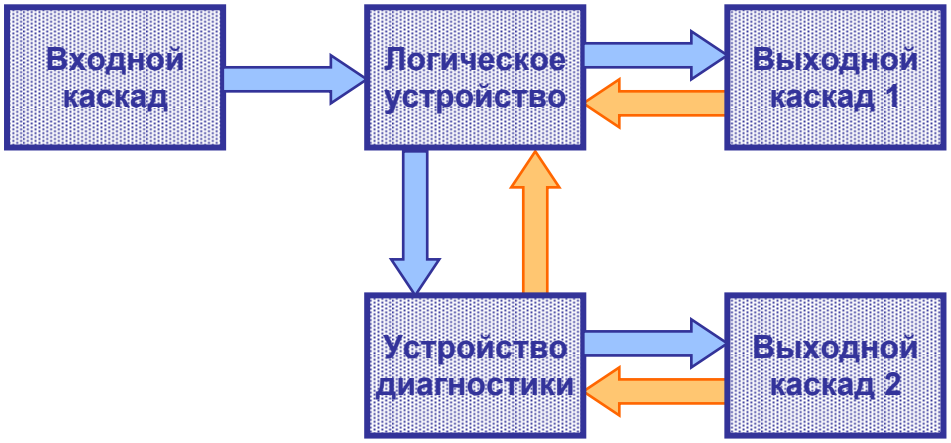
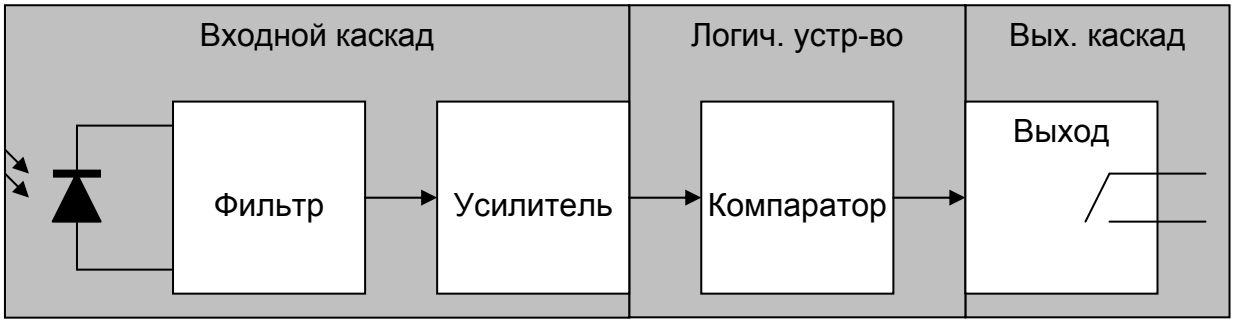


Рисунок 3. Категория 3 и 4.

Рассмотрим практическую реализацию архитектур безопасности на примере электронных датчиков.

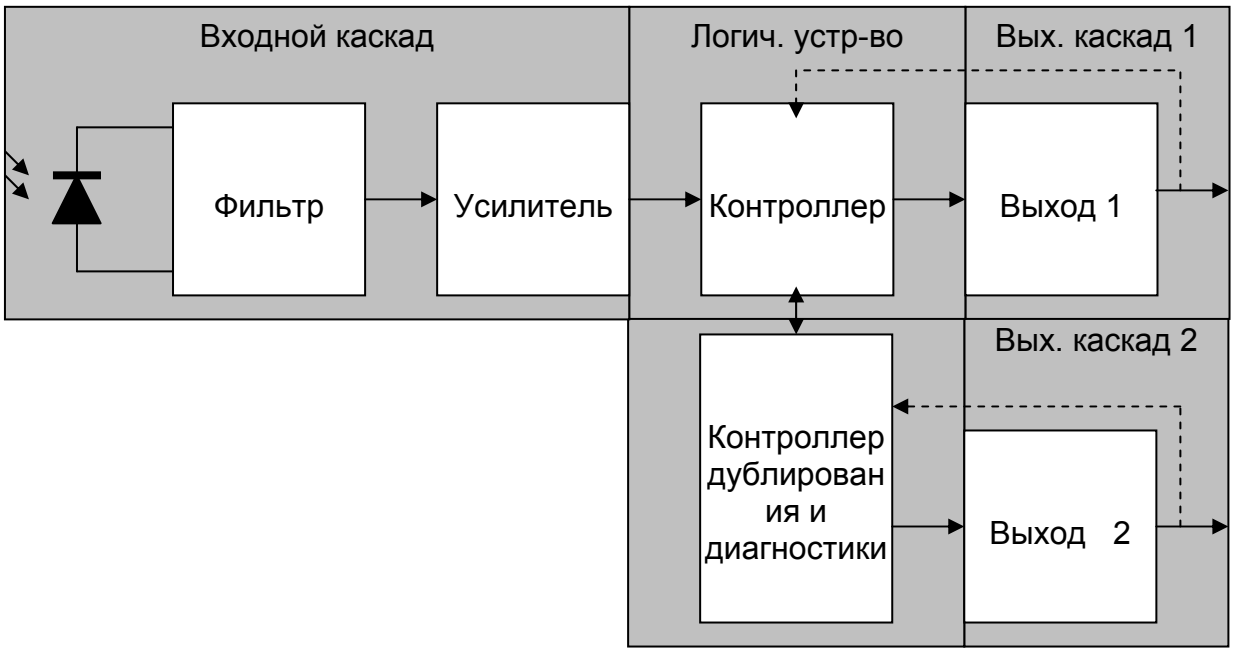
Категории 1, B соответствует схемотехника обычного дискретного оптического датчика (см. рисунок 4).

Рисунок 4.



Категория 2 предъявляет более строгие требования, согласно которым элементы безопасности должны быть оборудованы сдублированными выходными сигналами и устройством, осуществляющим диагностику выходов и внутренней схемы (Рисунок 5).

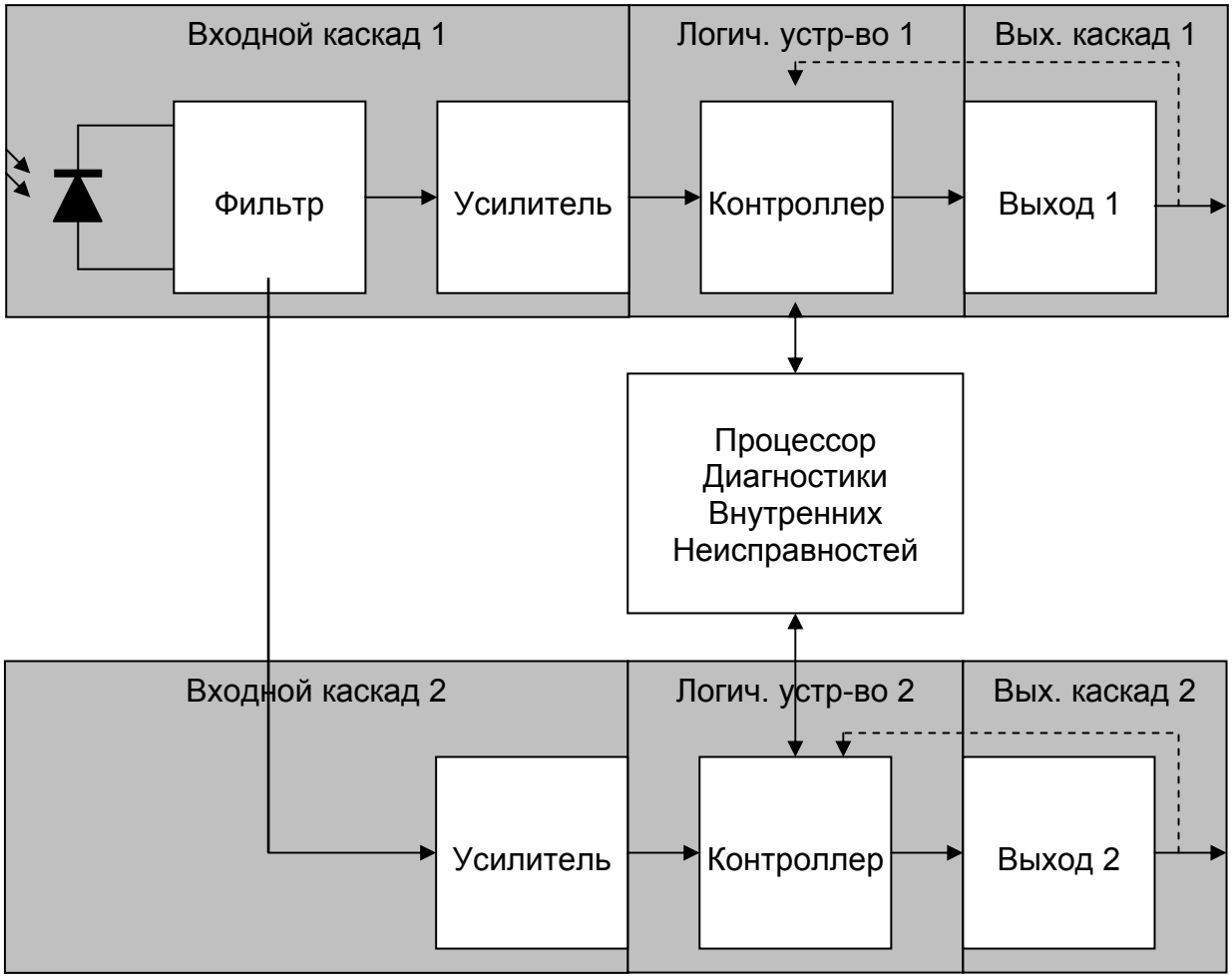
Рисунок 5.



В Категории 2 диагностика выходов и внутренней схемы происходит периодически. В периоды диагностики контроллер не реагирует на изменение сигнала, поступающего из входного каскада. Это означает, что в данные периоды датчик безопасности не обнаруживает вторжения в опасную зону. Тем не менее, согласно современным требованиям, быстродействие самодиагностики не менее, чем в 100 раз должно превышать потребности функциональной безопасности оборудования.

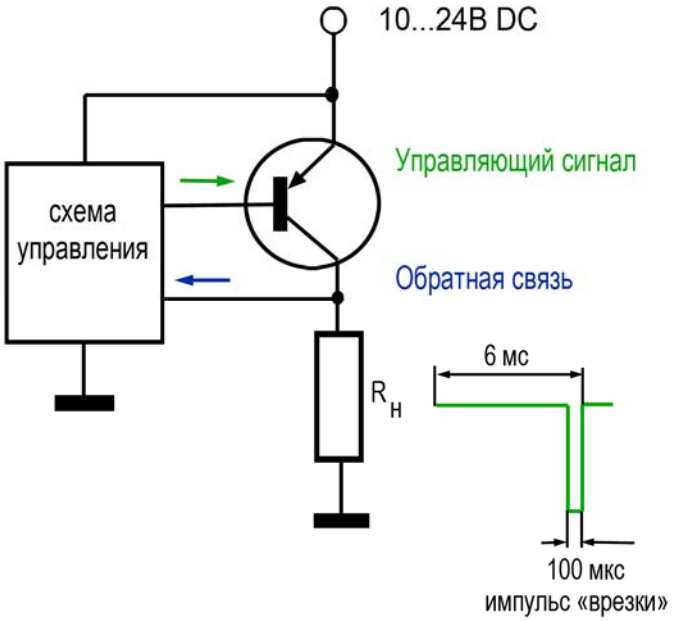
В Категориях 3 и 4 действует беспрерывное обнаружение с одновременной самодиагностикой за счет применения полного дублирования внутренних схем и действия т.н. процессора диагностики внутренних неисправностей, осуществляющего кросс-диагностику между обоими каналами (Рисунок 6.).

Рисунок 6.



Согласно стандартам, выходные каскады или выходы, оборудованные средствами самодиагностики, носят название OSSD – Output Signal Switching Device или Устройство Переключения Выходного Сигнала. Соответственно для сдублированных каналов: OSSD1 и OSSD2.
В электронных, оптоэлектронных и программируемых приборах безопасности выходной ключ должен быть непременно полупроводниковым: транзистор, оптрон, твердотельное реле.
Средством самодиагностики выхода, как правило, является т.н. импульс «врезки», как показано на рисунке 7.

Рисунок 7.



Диагностический импульс «врезки» позволяет выявить короткое замыкание и неисправность выходного ключа.

«Тип» и «Категория» - в чем заключается разница?

Электрические, электронные и программируемые системы по-прежнему сертифицируются на соответствие категориям.
Тип (безопасности) характеризует оптоэлектронные защитные устройства, которые, в отличие от других систем, должны удовлетворять специфическим «оптическим» требованиям, вкл. угол расхождения луча, длина волны излучения и др.. По принципу построения электрических цепей, Типы полностью соответствуют Категориям.

Поэтому, когда средством защиты оборудования, риски которого классифицируются по Категории 4, является оптоэлектронное защитное устройство, например, фотобарьер, оно должно соответствовать Типу 4.

Отдельные элементы и комплексные системы, связанные с обеспечением безопасности.

Архитектуры безопасности распространяются как на отдельно взятые приборы, так и на системы, обеспечивающие безопасность.

Например, в цепи обеспечивающей безопасность механического пресса (Категория риска 4) участвует фотобарьер (Тип 4), реле безопасности (Категория 4) и 3-линейный 2-канальный пневмораспределитель с электро-пневматическим управлением. Данная система (Рисунок 8.), состоящая из элементов, воплощающих архитектуру безопасности по Категории 4, в целом претендует на соответствие данной Категории. Дублирование каналов управления поддерживается вплоть до конечного элемента безопасной цепи.

Рисунок 8.

Не являются ли требования Категорий избыточными?

Чем выше Категория, тем лучше способность защитных приборов обнаруживать неисправность внутри себя и тем меньше (до ничтожных величин) вероятность НЕ ОСТАНОВА оборудования по причине сбоя в цепи безопасности.

Главной задачей систем безопасности является немедленный останов оборудования в случае обнаружения тела или частей тела человека в опасной зоне, а также, в случае возникновения внутренних сбоев, которые чаще всего вызваны внешними факторами, такими как чрезмерная пульсация напряжения питания, коммутационные и пиковые электромагнитные помехи, обрыв проводов и др..

Коммутация устройств в безопасной цепи строится по принципу принудительно-замкнутых контактов. Этот принцип, проецируемый на электромеханические и механические системы, справедлив и для упомянутого выше пневмораспределителя и для муфты-тормоза механического пресса. Пропадание в системе энергии – будь то электрический ток или сжатый воздух должно вызвать останов оборудования.

Вновь обратившись к способности самодиагностики, заметим, что при отсутствии таковой, неисправность ключа на выходе обычного датчика (Категория 1 и B) будет восприниматься как разрешающий сигнал и оборудование не будет остановлено в момент вторжения человека в опасную зону. Вероятность получения травмы в этом случае очень велика.