

Скрытая война микропроцессоров или фактор некомпетентности

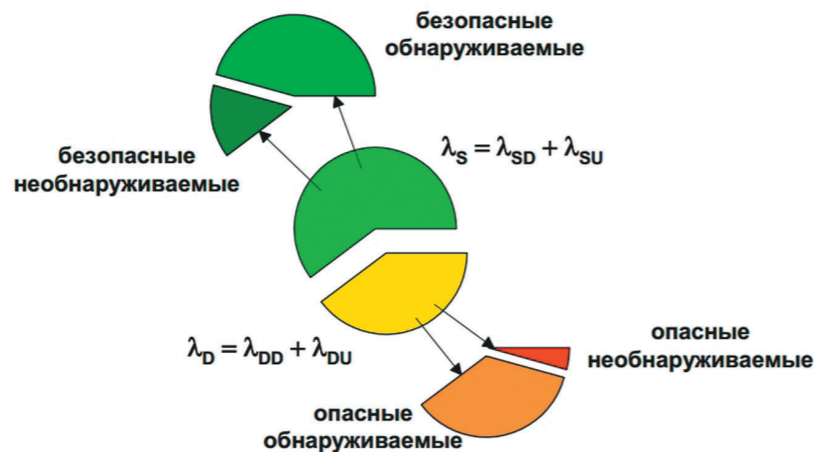
Функциональная безопасность электронных программируемых систем.



Валерий Потехин,
генеральный директор группы компаний
«Системы промышленной безопасности»
(ООО «СПБ-XXI»), ООО «СПБ-Экспертиза»)

Valery Potekhin,
General Director of Companies Group
«Industrial security systems»
(«SPB-XXI») LLC, «SPB-Expertiza» LLC)

Hidden microprocessors war or incompetence factor
Functional security of electronic programmable systems.



Структура распределения интенсивностей отказов по типам

Уважаемые читатели — главные инженеры предприятий, инженеры по автоматизации, специалисты в области промышленной безопасности, инженеры проектных институтов и разработчики электронных программируемых систем! В данной статье я хочу обратить ваше внимание на специфику применения микропроцессорных систем, называемых также «цифровыми» и «электронными, программируемыми» в проектах АСУ ТП, а также системах пожарной и газовой безопасности, которые применяются как на опасных производственных, так и на гражданских объектах для управления системами жизнеобеспечения, транспортными и подъемными механизмами.

Техногенные аварии в России последних лет, такие как разрушение ги-

дроагрегата с катастрофическими последствиями, пожар и полное уничтожение производства этилена, ложные срабатывания систем автоматического пожаротушения на телецентре и в отделении банка, повлекшие человеческие жертвы, а также многочисленные инциденты на ОПО, связанные с ложными срабатываниями систем противоаварийной защиты, отказами в системах управления и системах автоматического пожаротушения, объединяет один факт — применение на этих объектах систем на базе микропроцессорной техники и отсутствие анализа по их функциональной безопасности как на стадии проектирования, так и в отчетах по расследованию аварий и инцидентов.

С начала 1990-х гг. и до настоящего времени в нашей стране в области автоматизации происходит переход от релейных, аналоговых, тиристорно-транзисторных систем — к цифровым системам на базе микропроцессоров. При этом большинство российских производителей автоматизированных систем управления за основу концепции программно-логического контроллера на базе микропроцессора используют структуру вычислительных каналов и способ резервирования, разработанные первоначально для тиристорно-транзисторных систем. Проще выража-

Обозначение	Тип отказа
λ_s	безопасный отказ
λ_{sd}	безопасный обнаруживаемый отказ
λ_{su}	безопасный необнаруживаемый отказ
λ_d	опасный отказ
λ_{dd}	опасный обнаруживаемый отказ
λ_{du}	опасный необнаруживаемый отказ

Обозначение интенсивностей отказов и их типов

ясь, убрали тиристоры, транзисторы и вставили микропроцессор, получив систему с однокомпонентным вычислительным элементом и с традиционными принципами диагностики электрических цепей. Для надежности при этом оставили отработанный тип резервирования — замещением, то есть обычное переключение на резерв.

Европейские производители изначально пошли таким же путем, но уже в середине 1980-х — начале 1990-х гг. европейские и американские организации технического регулирования, анализируя первопричины и расследуя всю цепочку развития аварий, включая невыполнение функций автоматического срабатывания систем безопасности, что повлекло катастрофические последствия, ввели новые стандарты. Которые ограничивали и регламентировали применение различных структур микропроцессорных систем для опасных производств (DIN 19250 — 1984 г., EIC 61508 — 1998 г.).

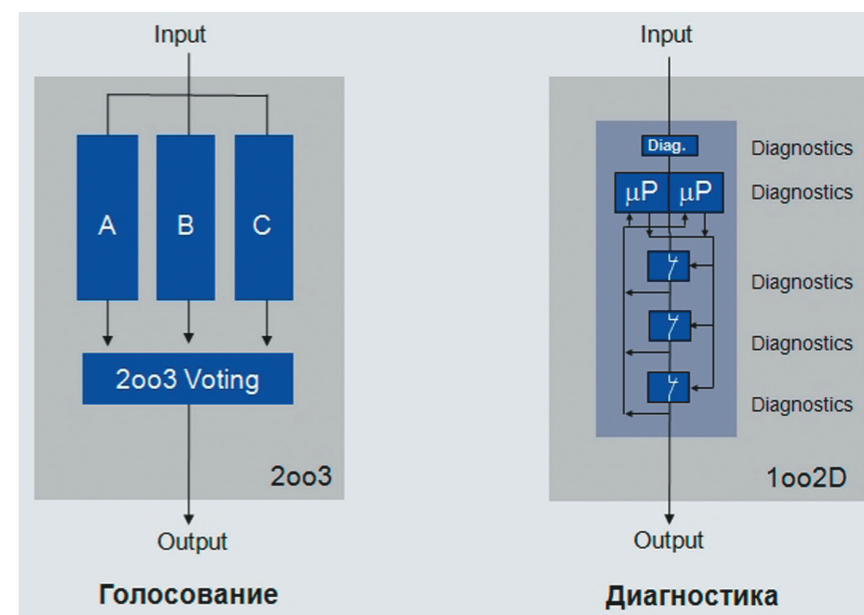
В 2008 г. в России был введен в действие стандарт по функциональной безопасности ГОСТ Р МЭК 61508, а в 2012 г. — ГОСТ Р МЭК 61511, которые классифицируют типы отказов микропроцессорных систем.

Как известно, опасный отказ может привести к отказу в выполнении функции безопасности.

Безопасный отказ не приводит к отказу в выполнении функции безопасности.

Для систем ПАЗ опасный отказ — это несрабатывание в момент развития аварии.

Наиболее критичны опасные необнаруживаемые отказы, не приводящие к остановке вычислительных функций процессора, но которые, тем не менее, могут полностью или частично заблокировать выполнение алгоритма безопасности. Такие отказы накапливаются



« Ложные срабатывания также могут являться опасным фактором. Например, при подаче газа в закрытые помещения, где находятся люди, или при несрабатывании в момент пожара



в системе в течение длительного времени и, как правило, являются следствием воздействия электромагнитных полей, радиочастотного излучения и других факторов. Устранение таких отказов происходит при обесточивании контроллера и полной его перезагрузке, что возможно сделать только при остановке производства.

Безопасные отказы для систем ПАЗ могут приводить к внеплановым остановкам. В случае безопасного и необнаруживаемого отказа мы можем по-

лучить ситуацию, когда все параметры производства как бы в норме, никаких отклонений не зафиксировано, аппаратная диагностика контроллера также в норме, но система отработала команду на остановку.

В случае применения микропроцессора для систем автоматического пожаротушения ложные срабатывания также могут являться опасным фактором. Например, при подаче газа в закрытые помещения, где находятся люди, или при несрабатывании в момент пожара.

Традиционные методы диагностики по контролю целостности электрических цепей, точности вычислительных преобразований по опорным напряжениям, сторожевые таймеры и др. определяют только обнаруживаемые отказы. А разработка систем с выполнением самых жестких требований стандартов по электромагнитной совместимости существенно снижает риск возникновения как опасных, так и безопасных отказов, но не гарантирует возникновение необнаруживаемых отказов в микропроцессорной системе.

На сегодняшний день отработанными методами косвенного определения статических математических ошибок процессоров являются методы сравнения или мажорирования (голосования) между значениями АЦП, контрольными вычислительными суммами вычислительных процессоров в дублированных или трированных архитектурах контроллеров или их комбинации.

Стандарты ГОСТ Р МЭК 61508/61511 определяют соответствие электронных программируемых систем для обеспечения требуемого снижения риска на ОПО.

Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств (ПБ 09-540-03, редакция 2013 г.) определяют требования по проверке функциональной безопасности и проведению анализа опасности и работоспособности (HAZOP) для систем, связанных с безопасностью.

Незнание и неприменение стандартов безопасности проектными организациями и специалистами по автоматизации является не только фактором некомпетентности, но и вопиющей ответственностью. 154