СИСТЕМЫ ПРОТИВОАВАРИЙНОЙ ЗАЩИТЫ ОТ SIEMENS

АЛЕКСАНДР ГУРЬЯНОВ
alexander.guryanov@siemens.com

В перерабатывающей промышленности часто встречаются сложные технологические процессы, в которых образуются или обрабатываются вредные для здоровья или взрывоопасные материалы и смеси. Выход из строя, неисправность оборудования или некомпетентное действие оператора могут иметь фатальные последствия. Чтобы минимизировать потенциальный вред для человека, оборудования и окружающей среды, необходима надежная система обеспечения безопасности (Safety Instrumented System, SIS), которая в критических обстоятельствах может автоматически перевести установку в безопасное состояние, при определенных условиях продолжить ее эксплуатацию, а также ограничить возможные отрицательные воздействия.

РИС. 1. Образцы технических компонентов систем автоматики безопасности

В настоящее время разработаны международные общепризнанные стандарты, позволяющие классифицировать и оценивать программно-технические комплексы и оборудование по различным уровням безопасности. Среди таких стандартов можно отметить, например:

- IEC 61508 — основной стандарт для спецификации, а также для разработки и эксплуатации систем обеспечения безопасности (классы безопасности SIL 1 — SIL4 (см. табл.));
- IEC 61511 — стандарт, ориентированный на приложения для перерабатывающей промышленности.

Системы обеспечения безопасности для автоматизации процессов фирмы Siemens полностью соответствуют стандартам безопасности вплоть до класса SIL3 (IEC/EN 61508, ГОСТ Р МЭК 61508) и обеспечивают безопасность на всех уровнях — от контрольно-измерительной аппаратуры для регистрации и преобразования сигналов до надежных отказоустойчивых устройств управления и исполнительных устройств, т. е., например, позиционных регуляторов, вентилей или насосов (рис. 1).

Традиционный подход к архитектуре системы безопасности отделяет управление и контроль функций безопасности от остальных приложений. Производители систем управления часто применяют контроллеры и шины безопасности параллельно с основной системой управления технологическими процессами (АСУ ТП). Необходимая информация может передаваться из контроллера безопасности в основную систему посредством шлюзов сетевой коммуникации, но две системы работают независимо. Технологические разработки сделали возможным использование одного контроллера для управления обеими задачами, что значительно сокращает стоимость разработки и эксплуатации системы.

Рассмотрим подробнее, как можно реализовать потенциал комплексной системы безопасности с АСУ ТП SIMATIC PCS7. Ее модульность и гибкость дает возможность индивидуально определить не только степень интеграции системы безопасности в АСУ ТП, но и степень резервирования контроллеров, полевой шины и периферии процесса (Flexible Modular Redundancy, FMR — гибкое модульное резервирование). Полная интеграция системы безопасности в SIMATIC PCS7 позволяет уменьшить занимаемую площадь, объем аппаратного обеспечения и проводки, а также сэкономить на монтаже, подключении и разработке проекта.

Система многозадачна, т. е. в одном CPU могут одновременно выполняться несколько программ — как приложения для управления основным процессом, так и приложения, направленные на обеспечение безопасности. Программы выполняются в разных циклах и областях памяти и не зависят друг от друга, но при необходимости могут обмениваться данными через системную шину Industrial Ethernet. Взаимодействуя с отказобезопасными сигнальными модулями станций децентрализованной периферии ET200M/S/iSP или подключенными непосредственно через полевую шину

ТАБЛИЦА. КРИТЕРИЙ ОЦЕНКИ SIS, ОПИСЫВАЮЩИЙ ВЕРОЯТНОСТЬ ВОЗНИКНОВЕНИЯ АВАРИЙНОЙ СИТУАЦИИ

Уровень безопасности	Вероятность возникновения ошибки (PFD) в течение года	Фактор снижения риска = 1/PFD
SIL 4	от >=10^{-5} до <10^{-4}	от 100000 до 10000
SIL 3	от >=10^{-4} до <10^{-3}	от 10000 до 1000
SIL 2	от >=10^{-3} до <10^{-2}	от 1000 до 100
SIL 1	от >=10^{-2} до <10^{-1}	от 100 до 10

надежными преобразователями, эти программы могут распознавать как ошибки процесса, так и собственные, внутренние ошибки и в случае сбоя автоматически переводят установку в безопасное состояние. Основным элементом таких систем противоаварийной защиты (ПАЗ) являются центральные процессоры (Failsafe CPU), принцип работы которых имеет ряд отличительных особенностей по сравнению со стандартными ЦПУ. Помимо обработки сигналов из модулей ввода/вывода, эти ЦПУ полностью контролируют корректность выполнения как отдельной программной операции, так и всей программы в целом, постоянно проверяя себя на предмет возникновения любой ошибки (включая работу микросхем) и при необходимости автоматически переводя компоненты в безопасное для технологического процесса состояние. Failsafe CPU подвергает проверке логику работы программы, преобразуя входные операнды на обратные и проводя над ними обратные операции (рис. 2). В случае несоответствия результатов прямой и обратной обработки выдается сигнал об ошибке и принимается решение о переводе системы в безопасное состояние. Можно сказать, что в одном аппаратном процессоре Failsafe (F) работают по принципу «И» два виртуальных процессора, результаты работы которых постоянно сравниваются.

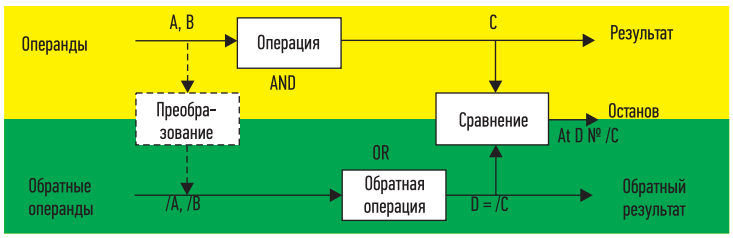


РИС. 2. ◀ Логика выполнения отказобезопасных программ

ОТКАЗОБЕЗОПАСНЫЕ И ОТКАЗОУСТОЙЧИВЫЕ СИСТЕМЫ

Отказобезопасная система может быть и отказоустойчивой (резервированной). Между этими двумя понятиями есть разница: задача отказобезопасности — перевести процесс в безопасное состояние в случае возникновения ошибки, вплоть до полной остановки процесса, а задача отказоустойчивости — поддержать работу системы в случае выхода из строя компонентов управления, не влияющих на безопасность процесса. В резервированных системах управления повышенной надежности каждый элемент, начиная со станции оператора до устройств полевого уровня, включая и саму шину, может быть зарезервирован посредством дублирования. Дублирующие ЦПУ синхронно выполняют одну и ту же программу и могут находиться как рядом, так и на значительном расстоянии друг от друга, например на противоположных концах цеха или завода. В зависимости от задачи автоматизации и вытекающих из нее требований по обеспечению безопасности степень резервирования может быть отдельно определена для контроллера, полевой шины и децентрализованной периферии. Таким образом, могут быть реализованы индивидуальные, точно адаптированные к конкретным задачам отказоустойчивые архитектуры, которые могут парировать несколько одновременно возникающих отказов. FMR предусматривает резервирование только там, где оно необходимо.

ОТКАЗОБЕЗОПАСНЫЕ СИСТЕМЫ С БИБЛИОТЕКОЙ F-БЛОКОВ

Еще один аспект отказобезопасных систем — это программирование. У SIEMENS такие системы программируются с помощью специальных дополнений стандартных инжиниринговых средств и сертифицированных TÜV[1] блоков из специальной библиотеки.

Инструментальное средство разработки отказобезопасных систем S7 F Systems делает возможной параметризацию отказобезопасных контроллеров AS 4xxF/FH, а также отказобезопасных F-модулей из спектра ET 200M/S/iSP. Оно поддерживает проектирование систем посредством следующих функций:

- сравнение отказобезопасных F-программ;
- распознавание изменений F-программ через контрольную сумму;
- разделение функций обеспечения безопасности (F-функций) и стандартных функций.

Доступ к F-функциям защищен паролем. Встроенная в S7 F Systems библиотека F-блоков (рис. 3) содержит готовые к применению функцио-

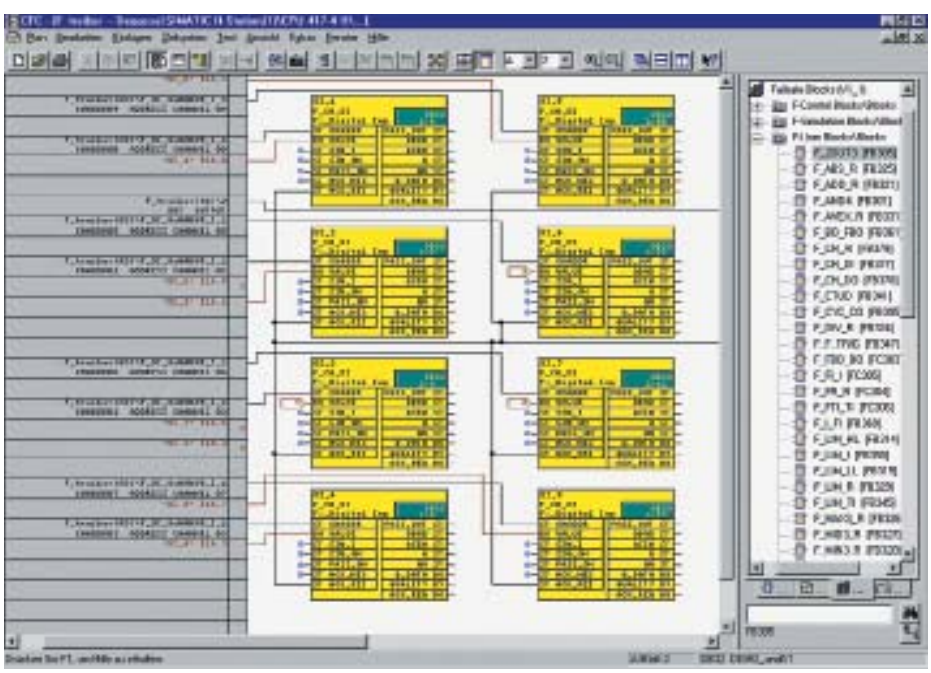


РИС. 3. ▼ Сертифицированные модули библиотеки S7 F Systems

[1] TÜV – немецкая сертификационная организация.

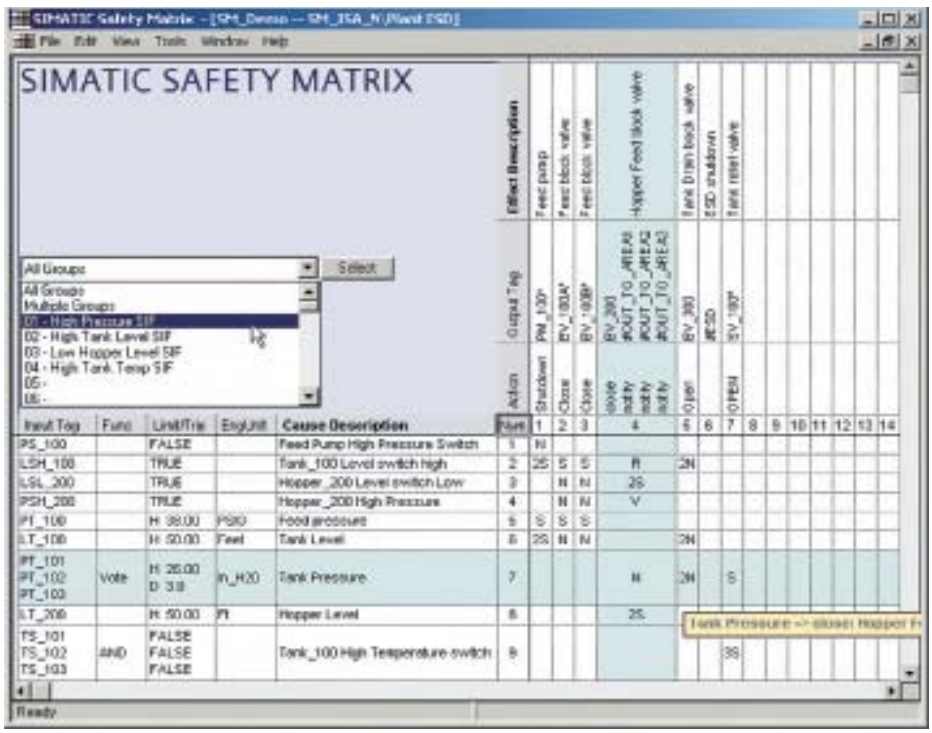


РИС. 4. ▲
Матрица безопасности

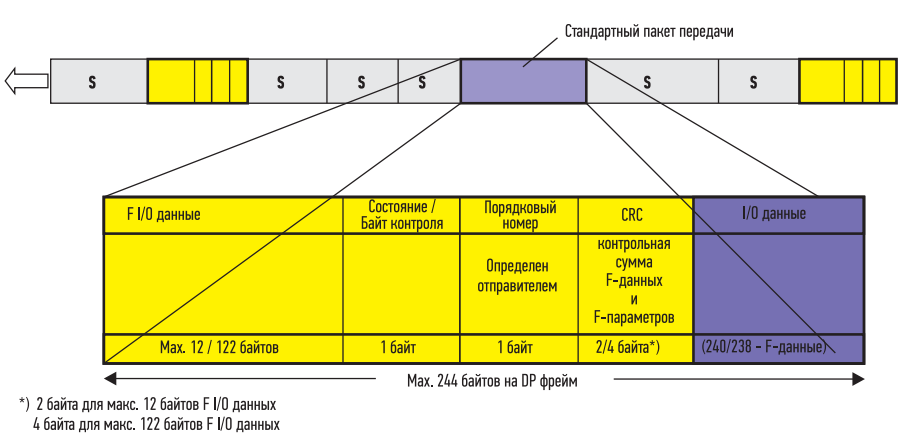
нальные блоки для создания отказобезопасных приложений с помощью CFC или основанной на CFC матрицы безопасности (Safety Matrix). Сертифицированные F-блоки перехватывают такие ошибки программирования, как деление на ноль или выход значений за допустимые пределы. Стандартное приложение может быть запрограммировано в F-ЦПУ обычным образом в CFC-редакторе без влияния на F-функциональность.

МАТРИЦА БЕЗОПАСНОСТИ SIMATIC SAFETY MATRIX

Матрица безопасности SIMATIC, которая может быть использована в дополнение к CFC, является инструментальным средством (Safety Lifecycle Tool), предназначенным для обеспечения безопасности на протяжении всего жизненного цикла установки. Ее можно использовать как для удобного проектирования отказобезопасных приложений, так и для их эксплуатации и обслуживания. Основанная на испытанном принципе матрицы «причина-следствие», она хорошо подходит для процессов, в которых заданные состояния требуют определенных реакций для обеспечения безопасности.

При анализе рисков установки проектировщик может соотнести события (причины), возникающие в ходе процесса, с определенными реакциями (следствиями). В горизонтальных строках матрицы, которую можно сравнить с программой обработки электронных таблиц, он вводит возможные события (входы), конфигурирует их вид и количество, логические операции над ними, возможные задержки и блокировки, а также, в случае необходимости, допустимые ошибки. Затем он определяет в вертикальных столбцах реакции (выходы) на созданные события. Связывание событий и реакций осуществляется простым щелчком на ячейке, находящейся на пересечении строки и столбца (рис. 4). На основе этих данных матрица безопасности автоматически генерирует сложные CFC-программы.

РИС. 5. ▼
Пакеты PROFIsafe профиля



*) 2 байта для макс. 12 байтов F I/O данных
4 байта для макс. 122 байтов F I/O данных

PROFIBUS С PROFIsafe

Для обмена данными между компонентами распределенной F-системы или несколькими F-системами используются сети PROFIBUS и PROFINET. В стандартном виде эти сети не могут обеспечить адекватную отказоустойчивость для достижения необходимого уровня надежности. Фреймы сообщений могут теряться, портиться или доставляться в неправильной последовательности. Для обеспечения целостности данных, удовлетворяющей требованиям безопасности, можно использовать специальный профиль PROFIsafe (рис. 5), который осуществляет контроль времени, контроль нумерации кодовых посылок, контроль подписи сообщений и дополнительный контроль целостности данных. PROFIsafe реализуется как дополнительный слой программного обеспечения внутри устройств системы автоматизации без изменения стандартных коммуникационных механизмов PROFIBUS и PROFINET. С помощью PROFIsafe передаваемые сообщения расширяются дополнительными данными, на основе которых партнеры по обмену информацией могут распознавать и компенсировать такие ошибки, как задержка, неправильная последовательность, потеря, ошибочная адресация или искажение данных. Стандартные компоненты (например, коммуникационные и интерфейсные модули), участвующие в обмене данными абонентов PROFIsafe, могут использоваться

без дополнительных модификаций. Профиль не требует дополнительных настроек и настраивается автоматически при конфигурировании аппаратного обеспечения F-систем.

ОТКАЗОБЕЗОПАСНЫЕ МОДУЛИ/СУБМОДУЛИ

Резервируемые отказобезопасные сигнальные F-модули/субмодули ET 200M/S/iSP (DI/DO/AI) согласованы с функциями обеспечения безопасности F/FH-систем и могут диагностировать как внутренние, так и внешние ошибки. Стандартные модули ввода/вывода можно использовать в одной системе с F-модулями, однако в F-программе допускается использовать информацию только от F-модулей. Модули ввода/вывода имеют дополнительные контрольные цепи для каждого канала, что дает возможность проводить проверку достоверности сигнала и выявлять ошибки (рис. 6). Сигнал с датчика логически раздваивается в канале и проходит дополнительную обработку с последующим сравнением, что гарантирует его правильную оценку и интерпретацию.

Для F-модулей ввода/вывода, в зависимости от уровня безопасности, который необходимо обеспечить, предусмотрена возможность разных схем подключения датчиков и исполнительных элементов. Например, если при менее жестком уровне безопасности SIL 2 подключение производится по схеме датчик-канал, то при SIL 3 датчик разводится сразу на два аппаратных канала или используется специальный двухканальный датчик, т. е. сигнал проходит удвоенную проверку в контрольных цепях каждого из каналов. Они не дублируют друг друга, хотя это возможно, а проводят дополнительный контроль сигнала на предмет выявления ошибки. Между каналами могут устанавливаться логические связи с принципами обработки сигналов 1oo1, 1oo2, 2oo2 и 2oo3.

F-ДАТЧИКИ

Для построения завершенной системы ПАЗ необходимо использовать специальные F-датчики. Особенно большая серия этих датчиков под названием SIGUARD предназначена для машиностроения и тяжелой промышленности, где преобладают дискретные сигналы защиты в виде зон безопасности и безопасных концевых положений. Наиболее продвинутыми датчиками из этой серии являются световые барьеры и сканеры для контроля зон безопасности. Они незаменимы для использования на предприятиях, где есть прессы, обрабатывающие центры, роботы и манипуляторы всевозможного назначения и другое машиностроительное оборудование. Эти устройства сертифицированы вплоть до SIL 3 и их можно настраивать на определенные условия эксплуатации, такие как число нарушений зоны до срабатывания, настройка зон нечувствительности, время прохождения сигнала и т. д.

***

В настоящее время расширение стандартов безопасности позволяет интегрировать электронные и программируемые системы безопасности непосредственно в частотные преобразователи и сервоприводы, давая возможность производителям оборудования создать такую систему безопасности, при которой перемещение осей или исполнительных механизмов происходит на безопасной скорости, если оператор находится в рабочей зоне. К функциям безопасности для частотных преобразователей и сервоприводов относятся функции безопасного состояния покоя, безопасного процесса остановки, безопасной рампы торможения, безопасной пониженной скорости, наличие входных/выходных сигналов с F-функциональностью и т. д. Использование подобного рода устройств с интегрированными функциями безопасности (например, станций ET200S и ET200pro) позволяет не только создать менее сложное решение ПАЗ, уменьшить стоимость оборудования и время запуска, но и обеспечить большую производительность установки за счет сокращения времени простоя при проверках, чистках, сменах инструмента и т. п. ●

Создание системы ПАЗ на базе стандартных элементов безопасности с интеграцией в АСУ ТП PCS7 имеет следующие преимущества:

- реализация функций управления основным процессом и функций обеспечения безопасности в одном контроллере;
- стандартный и отказобезопасный обмен данными между контроллером и периферийными устройствами ввода/вывода через общие полевые шины PROFIBUS и PROFINET с PROFIsafe (т. е. отсутствие необходимости в отдельной шине для обеспечения безопасности);
- совместная работа стандартных и отказобезопасных F-модулей в станциях ET 200M/S/iSP;
- унифицированная конфигурация и управление данными для основного и отказобезопасного процессов, включая визуализацию и диагностику процессов;
- проектирование функций обеспечения безопасности S7 F Systems, CFC и SIMATIC Safety Matrix в единой среде разработки проектов PCS7 Engineering System;
- автоматический учет сообщений о неисправностях системы безопасности в системе визуализации процесса с отметкой времени периферийных устройств (time stamp);
- унифицированные диагностика и обслуживание от датчиков и исполнительных устройств до системы автоматизации и операторской системы;
- встраивание отказобезопасной технологии в диагностику и обслуживание с помощью системы управления ресурсами PCS7 Asset Management (минимизация эксплуатационных затрат в течение жизненного цикла производства);
- сокращение расходов на аппаратное обеспечение, монтаж, подключение, установку, разработку и ввод в эксплуатацию проектов по мере увеличения степени интеграции.

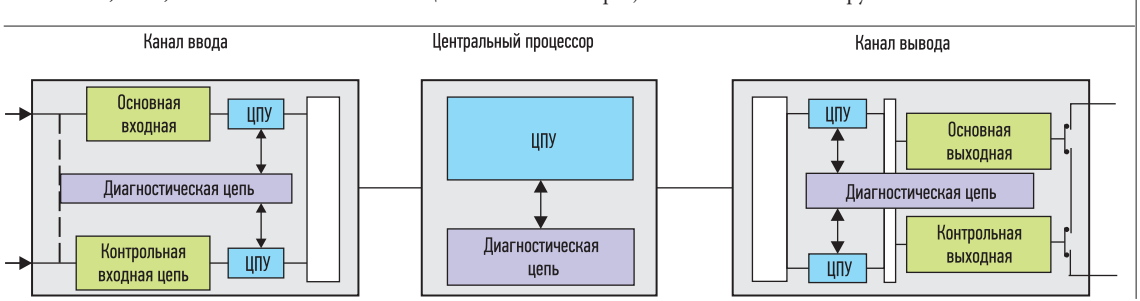


РИС. 6. ◄
Контроль каналов