ЗИ

АКАДЕМИЯ
СОВРЕМЕННЫХ
ИНФОКОММУНИКАЦИОННЫХ
ТЕХНОЛОГИЙ

**ЗИ Функциональная безопасность**

**ЗИ.15 Введение в функциональную безопасность**

**Курс лекций (Лекция 1, число стр. - 8)**

Москва, 2017

Академия Современных ИнфоКоммуникационных Технологий

Никто особенно не задумывается, что именно вкладывается в понятие «безопасность», и так все ясно: информационная безопасность (security). Однако, есть еще и другая сторона безопасности, safety, связанная с рисками для здоровья и жизни людей, а также окружающей среды. Поскольку информационные технологии сами по себе опасности не представляют, то обычно говорят о функциональной составляющей, то есть о безопасности, связанной с правильным функционированием компьютерной системы. Если информационная безопасность стала критична с появлением интернета, то функциональная безопасность рассматривалась и до появления цифрового управления, ведь аварии происходили всегда.

## Заслуживает ли внимания функциональная безопасность?

Важна ли функциональная безопасность на сегодняшний день? Ведь фокус внимания в основном направлен на информационную безопасность.

С одной стороны, функциональная безопасность напрямую связана с надежностью аппаратной составляющей, и здесь осталось немного нерешенных задач, электроника безотказно работает годами, а если и этого недостаточно, то всегда есть возможность резервирования. Но ведь есть еще программная составляющая, на которую как раз и возлагается управление функциями безопасности. Недавно была опубликована статья «Самые дорогие и судьбоносные ошибки в ИТ-индустрии». В ней дается описание нескольких кейсов, когда ошибка в софте систем управления космическими системами обходилась в миллионы долларов, и это далеко не все известные случаи. А еще есть системные проекты, включающие механическую, электронную и электрическую составляющие, и здесь, к сожалению, тоже есть место для ошибок.

В статье «Интернет вещей (IoT) – вызовы новой реальности» проведен анализ киберугроз и методов обеспечения информационной безопасности для интернета вещей (Internet of Things, IoT). Одним из потенциальных рисков является перехват управления на уровне физических устройств. Тогда злоумышленник может заставить систему управления выполнять

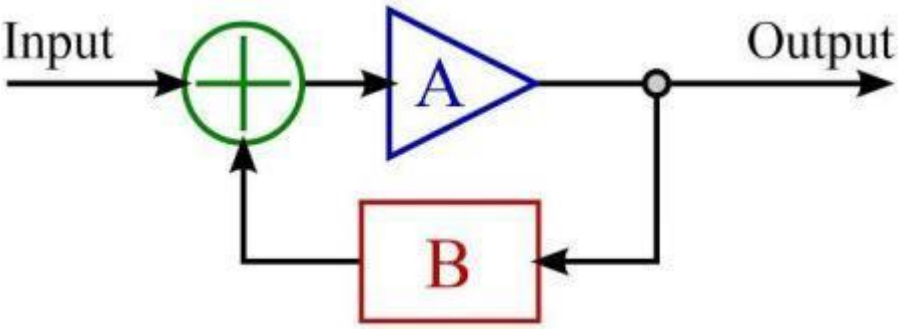
опасные функции. В этом случае информационная и функциональная безопасность являются двумя сторонами одного и того же явления. Свойство информационной безопасности должно обеспечить доступность, целостность и конфиденциальность данных системы управления. Свойство функциональной безопасности должно обеспечить корректное выполнение функций системы управления, а при возникновении отказов перевести объект управления в так называемое безопасное состояние.

Еще одним мотивом знакомства с функциональной безопасностью является понимание процесса сертификации и лицензирования. Объекты, которыми управляют компьютерные системы, зачастую создают риски для окружающей среды и людей (химическое производство, газовая и нефтяная промышленность, медицинские устройства, атомные и другие электростанции, железнодорожный, автомобильный, авиационный транспорт и т.д.). Компьютерные системы управления такими объектами должны выполнять функции безопасности и обладать определенными характеристиками (резервирование, отказоустойчивость, самодиагностика, устойчивость к внешним экстремальным воздействиям и т.п.). Контроль за разработкой, внедрением и эксплуатацией компьютерных систем управления, важных для безопасности, осуществляется государственными органами сертификации и лицензирования. Таким образом, разработчикам систем приходится знакомиться с требованиями к функциональной безопасности.

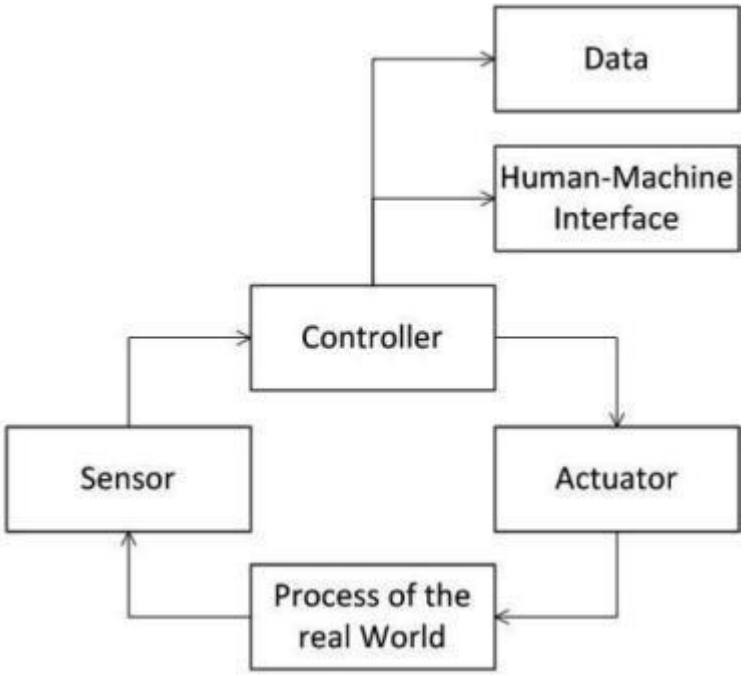
## Архитектура систем управления

К какому классу компьютерных систем может быть применено понятие функциональной безопасности? Очевидно, что это системы контроля и управления. Контроль или мониторинг может быть отнесен к частному случаю управления (сбор данных с выдачей управляющего воздействия только в случае обнаружения критического отказа), поэтому будем называть такие системы просто системами управления.

Для обобщения взглянем на очевидную структуру идеального контура управления.

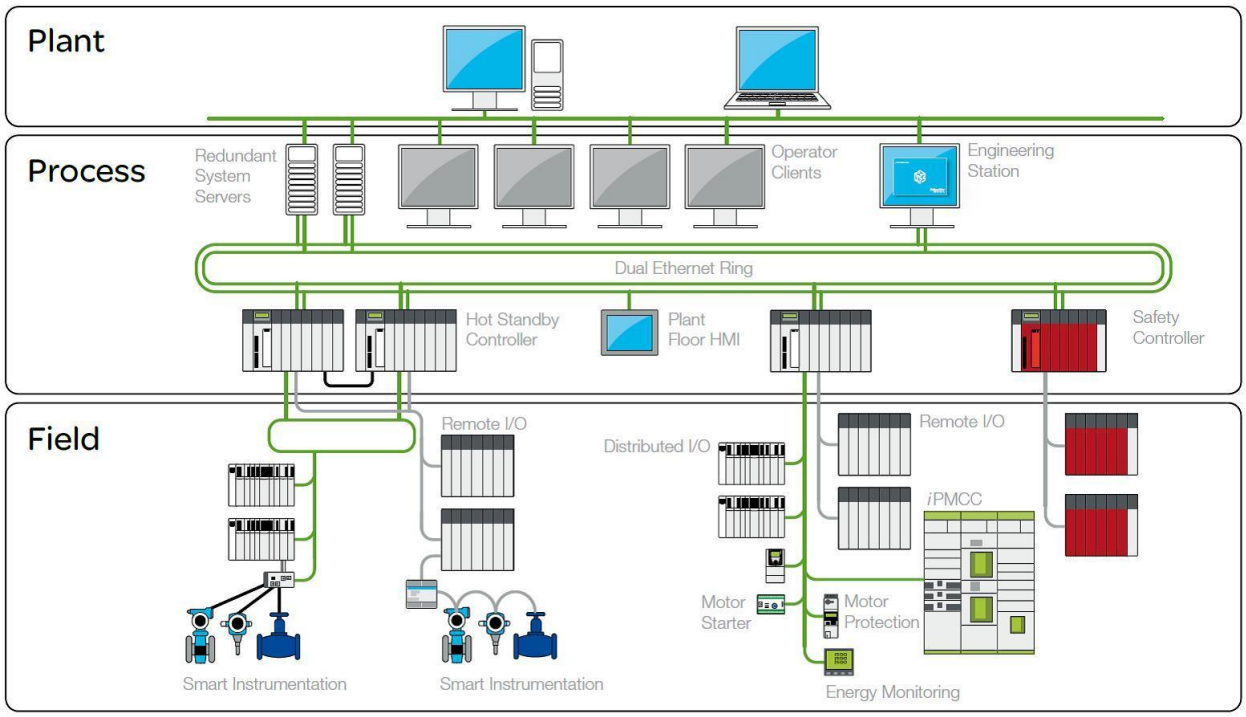



В реальном мире в этом контуре имеем: управляемый процесс, датчик, контроллер и исполнительный механизм. Необязательной с точки зрения управления, но, тем не менее, неотъемлемой частью сегодняшних систем управления являются человеко-машинный интерфейс и обработчики данных, полученных в результате мониторинга.



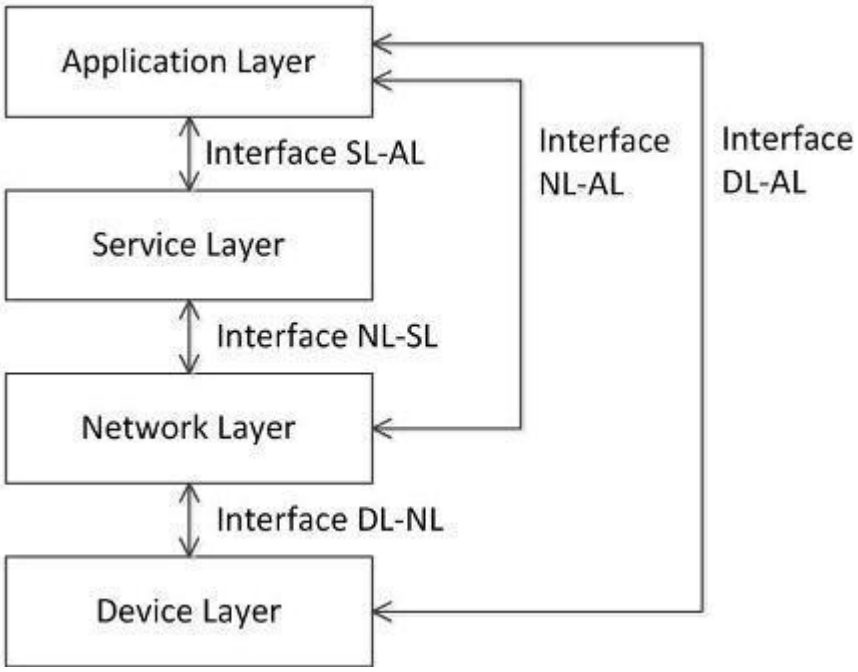

Подобная архитектура реализуется для встроенных систем (Embedded Systems), широко применяемых в промышленной автоматизации, бытовых устройствах, автомобильных системах, медицинских устройствах, коммуникационных сетях, роботах, дронах и т.п.

В АСУ ТП (Industrial Control Systems) применяется более разветвленная архитектура, включающая объединенные в сеть датчики, программируемые логические контроллеры (ПЛК), исполнительные механизмы, хранилища данных, сервера и рабочие станции.




Schneider Electric – Modicon Quantum PLC

Наиболее сложной является типовая архитектура IoT.




Управляющая система реализуется на уровне Device Layer. Ее программно-аппаратная реализация может быть аналогична встроенной системе. С точки зрения информационной безопасности критическими являются интерфейсы DL-NL & DL-AL доступа к уровню Device Layer.

Таким образом, к системам управления, для которых важно рассматривать свойство функциональной безопасности, относятся АСУ ТП, встроенные системы и IoT.

## Стандарты, относящиеся к функциональной безопасности

В области стандартизации существует такое понятие, как “umbrella standard”, т.е. основополагающий «вертикальный» стандарт верхнего уровня. Для функциональной безопасности таковым является МЭК 61508 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью» (IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems), включающий семь частей. Данный стандарт переведен на русский язык и внедрен в Российской Федерации в виде ГОСТа.

Дальше кратко интерпретированы основные положения МЭК 61508. Они, скажем так, неидеальны, однако, здравый смысл в них имеется. Ниже следует авторская обработка с учетом личного опыта в сфере функциональной безопасности.

Согласно положениям МЭК 61508, под функциональной безопасностью (functional safety) подразумевается корректное функционирование, как системы управления, так и управляемого ею оборудования. Таким образом, для обеспечения функциональной безопасности необходимо сначала определить функции безопасности (safety functions), необходимые для снижения риска управляемого оборудования, а также для достижения и сохранения этим оборудованием безопасного состояния (например, функции противоаварийной защиты). Далее, система управления должна обладать свойством так называемой полноты безопасности (safety integrity), под которым МЭК 61508 подразумевает вероятность того, что система будет корректно выполнять функции безопасности при всех заданных условиях в течение заданного интервала времени.

При обеспечении полноты безопасности (safety integrity) учитываются два типа отказов: случайные (random failures) и систематические (systematic failures).

Случайные отказы вызваны выходом из строя аппаратных компонентов и парируются такими методами, как резервирование, самодиагностика, физическое и электрическое разделение компонентов, повышение устойчивости к внешним воздействиям и т.п.

Систематические отказы вызваны ошибками проектирования, в том числе, и ошибками программного обеспечения. Устранение систематических отказов возможно путем совершенствования процессов проектирования и разработки, тестирования, управления конфигурацией, проектного менеджмента и т.п. Кроме того, поскольку классическое резервирование не позволяет избежать систематических отказов, применяется так называемое диверсное (diversity) резервирование, когда резервные каналы разработаны с применением различного программного и аппаратного обеспечения. Дорого, неудобно, но иногда помогает.

Положения МЭК 61508 детализированы для потенциально опасных областей. Существуют, например, следующие стандарты:
— IEC 61511, Functional safety – Safety instrumented systems for the process industry sector;
— IEC 62061, Safety of machinery – Functional safety of electrical, electronic and programmable electronic control systems;
— IEC 61513, Nuclear power plants – Instrumentation and control for systems important to safety;
— ISO 26262, Road vehicles – Functional safety;
— EN 50129, Railway Industry Specific – System Safety in Electronic Systems;
— IEC 62304, Medical Device Software.

В аэрокосмической отрасли на МЭК 61508 не ссылаются, тем не менее, подход похожий:
— для авионики разработан стандарт RTCA DO-178C, Software Considerations in Airborne Systems and Equipment Certification;
— в космической отрасли стандарты разрабатываются космическими агентствами, например NASA использует стандарт STD 8719.13, Software Safety Standard.

## Выводы

В дружной, но непредсказуемой семье «безопасность», борющейся за свободу информационных технологий от

неприемлемых рисков, живут себе две сестры: старшая, функциональная безопасность (safety), и младшая, информационная безопасность (security).

Для управляющих систем, к которым относятся такие архитектуры, как АСУ ТП, встроенные системы и интернет вещей (Device Layer), основополагающим свойством является функциональная безопасность.

Под функциональной безопасностью подразумевается корректное функционирование, как системы управления, так и управляемого ею оборудования.

Информационная безопасность в таких системах носит дополнительный характер и должна предотвращать доступ злоумышленников к контролю над системой управления и управляемым оборудованием.

Автор: Владимир Скляр (Национальный аэрокосмический университет «Харьковский авиационный институт»), Project Manager, Functional Safety Expert, R&D

Материал взят с сайта Хабрахабр