РАСПРЕДЕЛЕННАЯ АРХИТЕКТУРА ПЕРСПЕКТИВНЫХ ВСТРОЕННЫХ СИСТЕМ УПРАВЛЕНИЯ

В.Федюкин, гл. констр. по САУ "НТЦ им.А.Люлька"
Л.Бондарев, зам. гл. констр. НПП "Темп им. Ф.Короткова"
В.Клепиков, к.т.н., нач. лаб.
ФГУП "ИТМиВТ им. С.А.Лебедева РАН"

Концепция архитектуры перспективной распределенной системы автоматического управления газотурбинными двигателями (САУ ГТД) базируется на архитектуре с временным распределением TTA (Time Triggered Architecture – архитектура с временным переключением). Она позволяет создавать системы высокой надежности и жесткого реального времени. Основа TTA-архитектуры – протокол TTP, обеспечивающий сетевой обмен по принципу временного разделения ресурсов. TTA-подход, кроме системных решений и элементной базы, включает в себя набор программных средств для проектирования, моделирования, разработки, интеграции и верификации системы. Основной компонент программного обеспечения – операционная система TTP-OS жесткого реального времени – разработана в соответствии с требованиями авиационного стандарта DO-178B.

Тенденции развития систем управления в авиационной и автомобильной отраслях основаны на концепции "сухого" или "электрического" управления (в англоязычной литературе используется термин "x-by-wire" (по проводам), например – flight-by-wire, brake-by-wire, steer-by-wire – управление полетом, тормозами, рулевым приводом по проводам). Сущность данного метода – в замене механических, гидравлических и пневматических приводов интеллектуальными электрическими приводами с локальными управляющими контроллерами, которые объединены в единую распределенную систему высокоскоростными цифровыми каналами информационного обмена. Основные требования к такой системе – высокая надежность в жестких условиях внешних возмущающих факторов и способность функционировать при появлении отказов в отдельных элементах и подсистемах.

Архитектура TTA разработана специально для удовлетворения приведенным требованиям. Кроме того, идеология TTA за 25 лет пополнилась методиками, инструментарием и аппаратно-программными компонентами, обеспечивающими интегрированный подход ко всем этапам проектирования, начиная с декомпозиции системы и заканчивая ее реализацией из специализированных и коммерчески доступных компонентов.

В настоящее время технологический и коммерческий успех платформы TTA определяется следующими основными факторами:

- **цена** – распределенная архитектура позволяет оптимальным образом разместить функции системы по процессорам сети, снижая тем самым общее количество процессоров и, соответственно, стоимость системы;
- **стабильность и надежность** – при отказах в аппаратуре и программном обеспечении, которые являются основными источниками нестабильности и ненадежности сложной распределенной системы, платформа TTA на архитектурном уровне обеспечивает устойчивость работы всей системы даже в случае ошибок и отказов отдельных ее компонентов, что существенно снижает сроки и стоимость разработки;
- **безопасность** – в сложной системе функции различного уровня критичности совместно используют системные ресурсы, поэтому при сертификации централизованной системы ко всем компонентам необходимо применять процедуры обеспечения качества, определяемые компонентом наивысшего уровня ответственности. Платформа TTA обеспечивает архитектурную безопасность и позволяет для каждой функции выполнять лишь необходимые для нее процессы обеспечения качества, тестирования и верификации;
- **резервирование датчиков** – возможность использования в различных подсистемах TTA системы информации сразу со всех доступных датчиков позволяет реализовать режим перекрестной проверки исправности датчиков, что повышает отказоустойчивость всей системы. Это свойство

также позволяет минимизировать общее количество однотипных датчиков.

Перечисленные свойства архитектуры TTA обусловливают ее широкое применение как в коммерческой, так и в специализированной аппаратуре. В коммерческих приложениях TTA-система наряду с хорошими стоимостными характеристиками обеспечивает простую интеграцию уже наработанных аппаратных и программных компонентов, позволяет проводить покомпонентный ремонт и модернизацию системы. Для критичных по надежности систем TTA-платформа, благодаря четкой стандартизации и документированности, предоставляет возможность выполнять проектирование в соответствии с самыми жесткими требованиями, такими как DO-178B уровня A. В настоящее время TTA-платформа активно задействуется в авиационной и автомобильной электронике, в частности при построении систем управлении ГТД с полной ответственностью (FADEC).

СТРУКТУРА TTA-ПЛАТФОРМЫ

Основным блоком TTA-системы является узел. Узел состоит из процессора с памятью, подсистемы ввода-вывода, коммуникационного TTP-контроллера, операционной системы и соответствующего прикладного ПО. Узел реализуется в едином модуле, а в идеале – в едином кристалле. Дублированная TTP-шина объединяет узлы в кластер. TTP-шина вместе с коммуникационными контроллерами узлов образует в кластере коммуникационную систему, которая функционирует автономно в соответствии с определенным периодическим расписанием в режиме множественного доступа с разделением времени (TDMA – Time Division Multiple Access). Коммуникационная подсистема читает сообщения (пакеты данных) сетевого коммуникационного интерфейса (Communication Network Interface – CNI) узла в определенные расписанием моменты времени и отправляет их в CNI других узлов, обновляя записанную туда ранее информацию. Моменты времени чтения и записи сообщений содержатся в едином для всех узлов кластера расписании в виде описателя сообщений (Message Descriptor List – MEDL). Копии MEDL хранятся в каждом узле.

В настоящее время существуют две топологии TTA-архитектур: шинная (TTA-Bus) и звездная (TTA-Star) (рис.1). В шинной топологии каждый узел содержит локальный блок шинной защиты (bus guardian), предотвращающий отказ узла типа "забивание" шины (babbling idiot faults). В звездной топологии присутствуют центральные блоки шинной защиты, которыми пользуются все узлы кластера.

В основе построения TTA-архитектуры лежит протокол с временным разделением доступа – TTP (Time Triggered Protocol), который обеспечивает следующие основные функции:

- автономную отказоустойчивую передачу сообщений между CNI (Communication Network Interface – коммуникационный сетевой интерфейс) узлами кластера в строго определенные моменты времени и с минимальными флуктуациями (jitter) на основе дисциплины множественного доступа с разделением времени (TDMA) по дублированному коммуникационному каналу;
- отказоустойчивую синхронизацию часов всех узлов, что обеспечивает единое глобальное время кластера без привязки к центральному серверу;
- контроль целостности (membership) кластера путем сообщения всем исправным узлам о корректности передаваемых данных. Эта функция может рассматриваться как сервис распределенного подтверждения целостности, которая моментально информирует приложения о возникновении ошибки в коммуникационной системе;
- предупреждение группового распространения ошибок в случае невозможности их парирования на уровне протокола.

В протоколе TTP обмен данными организован в виде TDMA-раундов (рис.2). Раунд разделен на слоты. Каждый узел в коммуникационной системе имеет свой слот и должен в каждом раунде выполнять в данном слоте передачу пакетов (frames). Длина пакета определяется для каждого узла и может варьироваться в пределах от 2 до 240 байт, в пакете может содержаться несколько сообщений. Последовательность TDMA-раундов повторяется, образуя цикл кластера (cluster cycle). В пределах цикла каждый узел в своем раунде может передавать различные прикладные сообщения, но в течение цикла происходит повторяющийся обмен полным набором служебных сообщений. Данные защищаются 24-бит CRC-ко-

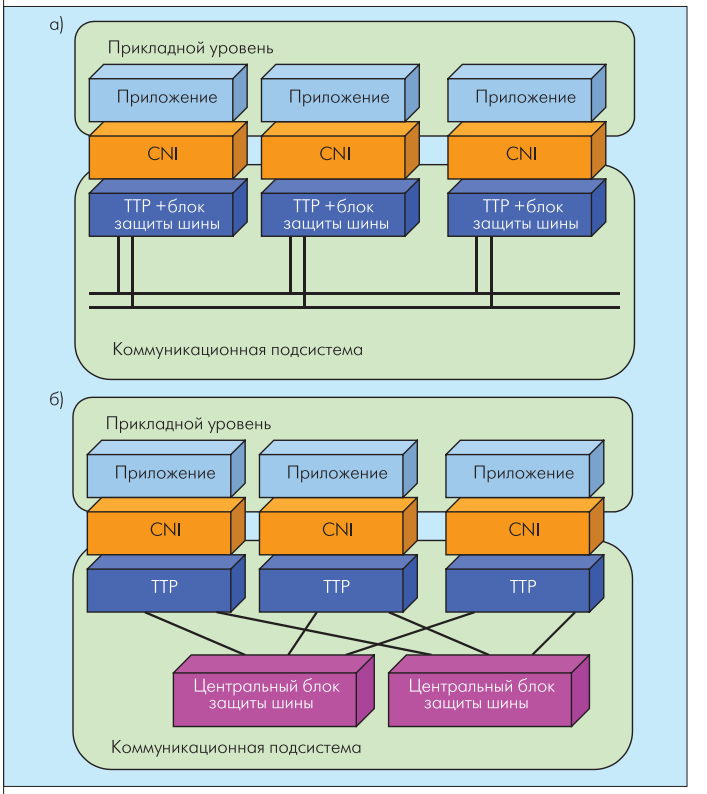

Рис.1. Шинная топология с локальными блоками защиты (а) и звездная топология с центральными блоками защиты (б)

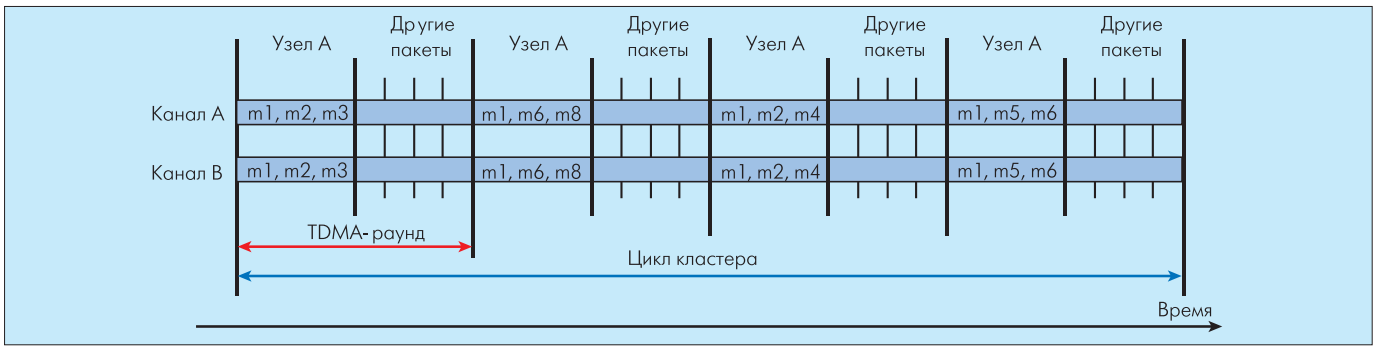

Рис.2. Пакеты, сообщения, слоты, TDMA-раунд, цикл кластера

дом (Cyclic Redundancy Check). Расписание обмена хранится в коммуникационных контроллерах узлов в виде описателя сообщений (MEDL).

Синхронизация часов необходима для обеспечения всех узлов единой временной базой, позволяющей всем узлам пользоваться единым расписанием обмена. Каждый узел на основе априорно известного ожидаемого времени прихода корректного сообщения и фактического времени его прихода вычисляет разницу хода часов передатчика и приемника. Отказоустойчивый усредняющий алгоритм вычисляет коррекцию локальных часов, чтобы они находились в синхронизации со всеми остальными часами кластера. Распределенный алгоритм контроля целостности кластера в случае отказа выясняет место его возникновения – выходная цепь передатчика или входная цепь приемника. Базовые алгоритмы TTP-протокола были формально верифицированы и успешно протестированы в условиях имитации миллионов отказов, при воздействии радиационного и электромагнитного излучений.

В TTP реализована **концепция парирования одиночных отказов,** основанная на том, что вероятность одновременного появления отказов в двух различных компонентах ничтожно мала. Для того чтобы исключить блокирование или "забивание" шины отказавшим узлом, TTP содержит блок защиты шины (bus guardian). Этот блок гарантирует, что узел может выполнять передачу только один раз в течение TDMA-раунда, тем самым исключая монополизацию шины отказавшим узлом. При появлении множественных отказов, которые не могут быть парированы самим протоколом, TTP информирует об этом прикладное приложение, которое, в свою очередь, может принять решение о прекращении своей работы или о переходе в "режим безопасного функционирования".

На уровне прикладных приложений устойчивость к отказам в TTA-системе достигается путем дублирования программного обеспечения на двух независимых узлах. Одиночный отказ узла может быть парирован с помощью механизма голосования "1 из 3" (Triple Modular Redundancy Voting). Обнаружение одиночного сбоя или отказа узла обеспечивают оба подхода. Для парирования отказов протокол TTP поддерживает механизм горячего резервирования узлов.

Перечисленные механизмы отказоустойчивости реализуются благодаря способности TTP-протокола поддерживать **согласованность (consistency) данных.** В однопроцессорной системе согласованность гарантируется возможностью для всех компонентов ПО пользоваться одной копией данных, записанных в ОЗУ. Такой тип согласования данных не работает в распределенной системе по следующим причинам. Во-первых, из-за задержек при передаче нет гарантии, что переданное сообщение будет принято всеми узлами-приемниками в одно и то же время. Во-вторых, некоторые узлы могут находиться в нерабочем состоянии или сообщение может быть потеряно из-за сбоя в коммуникационной системе. Поддержка согласованности данных в TTP-протоколе обеспечивается на уровне коммуникационного контроллера CNI путем реализации на аппаратном уровне функций контроля целостности кластера (membership), подтверждений (acknowledgment) и предотвращения сегментации (clique avoidance).

Контроль целостности кластера. Благодаря циклической (round-robin) схеме TDMA-раундов, каждый узел ожидает и проверяет список членов кластера для всех узлов данного раунда. Каждый передатчик, не соответствующий списку членов, определяется как неисправный. Это обеспечивает согласованное взаимодействие группы узлов, каждый из которых видит другие в своих списках членов кластера.

Подтверждения. Узел А после каждой своей передачи ожидает от других узлов подтверждения того, что его сообщение было принято на коммуникационном уровне. Это достигается проверкой в списке членов кластера узла А первого и, возможно, второго подтвердившего узла. Если эти узлы находят узел А в своих списках членов кластера, они подтверждают, что передача узла А была успешно принята. В противном случае узел А извещается о неудачной передаче. В силу принципа временного разделения повторная передача выполняется в следующем цикле.

Предотвращение сегментации кластера. Перед выполнением каждой операции посылки узел проверяет – является ли он членом наибольшего сегмента (majority clique) кластера. Если узел находится в наименьшем сегменте, это означает, что вероятность необнаруженной ошибки велика и может привести к несогласованности данных. Эта информация транслируется прикладному приложению, которое должно решить вопрос о переходе в состояние "останова" или в режим "безопасного функционирования".

Комбинация этих алгоритмов наряду с общей временной базой, поддерживаемой алгоритмом синхронизации часов, обеспечивает согласованность коммуникационного канала, т.е. все корректно работающие узлы получают одинаковую информацию в одинаковые моменты времени. TTA-платформа, таким образом, обеспечивает приложения мощной программной моделью, которая позволяет эффективно работать со сложными распределенными системами.

В дополнение к механизмам гарантированной и согласованной передачи данных TTA обеспечивает **механизм обмена событийной информацией,** для чего часть пакета может быть отдана для передачи событийных сообщений.

ОСОБЕННОСТИ ПРОЕКТИРОВАНИЯ TTA-СИСТЕМЫ

TTA-система создается в два этапа или на двух уровнях – кластерном и узловом. На кластерном уровне проектируются топология сети и интерфейсы узлов. Далее каждый узел проектируется на основе функциональных спецификаций и спецификаций сетевого интерфейса.

Двухуровневый подход к проектированию TTA-архитектуры позволяет реализовать важное свойство **компонуемости** (composability) системы. Систему, обладающую таким свойством, можно разделить на отдельные модули. Модули разрабатываются и тестируются независимо друг от друга и затем они могут быть проинтегрированы без учета их взаимного влияния. При интеграции в единый кластер модули не влияют на работу друг друга, так как каждый из них взаимодействует только со своим блоком CNI. Блоки CNI, в свою очередь, работают под управлением статически сформированного расписания, не зависящего от того, какие модули присутствуют в кластере.

Проектирование кластера TTA-системы вручную – достаточно трудоемкий процесс. Разработка сетевого протокола (циклического расписания) требует синхронизации сотен данных между десятками задач, выполняемых на разных узлах. Компания TTAutomotive поставляет набор инструментальных пакетов TTXTools, позволяющих автоматизировать все этапы проектирования как на кластером, так и на узловом уровнях. Моделирующий пакет TTXMatlink, реализованный в среде Matlab/Simulink, позволяет графическими средствами создать модель будущей TTA-системы, проверить ее функционирование и получить практически исполняемый код посредством пакета Real-Time Embedded Workshop.

Эффективность использования TTA-архитектуры значительно повышается с применением **операционной системы жесткого реального времени,** такой как QNX или TTP-OS, специально предназначенной для приложений, основанных на использовании TTP-протокола. Данные операционные сис-

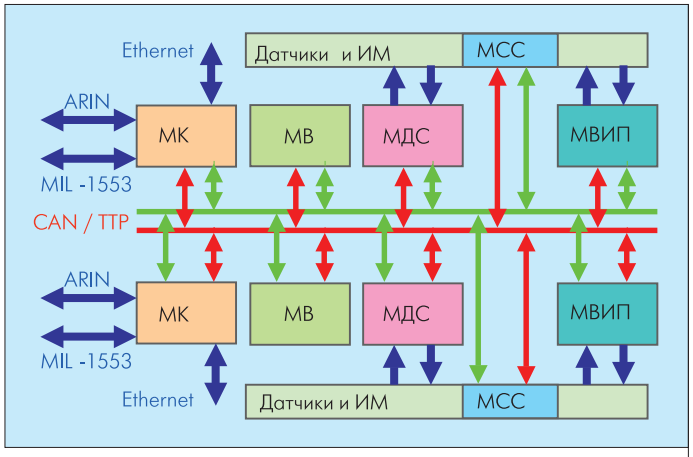

Рис.3. Пример архитектуры распределенной системы

темы занимают исключительно малые вычислительные ресурсы и обеспечивают быстрое переключение задач. TTP-OS разработана в соответствии с требованиями стандарта сертификации авиационных систем DO-178B Level A.

ОБЛАСТИ ПРИМЕНЕНИЯ TTA-АРХИТЕКТУРЫ

Архитектуру TTA широко применяют в авиационных системах управления и, в частности, в системах управления газотурбинными двигателями. Фирма Honeywell использует TTA в системе FADEC двигателя F124-GA-200 самолета Aermacchi"s M-346. Как единая платформа TTP применяется в самолетах: GROB Ranger G 160, EXTRA EA-500, IBIS Ae270 и др.

Фирма General Electric применяет TTP-протокол в FADEC F110 истребителя Lockheed Martin F-16. В лайнере A380 используются решения фирмы Nord-Micro на основе TTP-протокола в системах контроля давления в кабине пилота и в пассажирских отсеках, а также для контроля состояния клапанов утечек, что является критически важной функцией. Фирма Hamilton Sundstrand Corporation использует TTP-протокол в системах электропитания и контроля внешней среды самолета Boeing 787 Dreamliner.

TTA-подход принят за основу при построении распределенной **аппаратно-программной платформы САУ перспективных двигателей** авиационного и наземного применения. Для реализации проекта создания перспективной платформы под руководством НПО "Сатурн" и ОАО "НПП "ЭГА" на базе Института точной механики и вычислительной техники им. С.А. Лебедева РАН создан **Отраслевой координационный совет,** в который также вошли представители ведущих предприятий отрасли – ОКБ "Сухой", ФГУП ЦИАМ, АО "Завод им. Климова" и др.

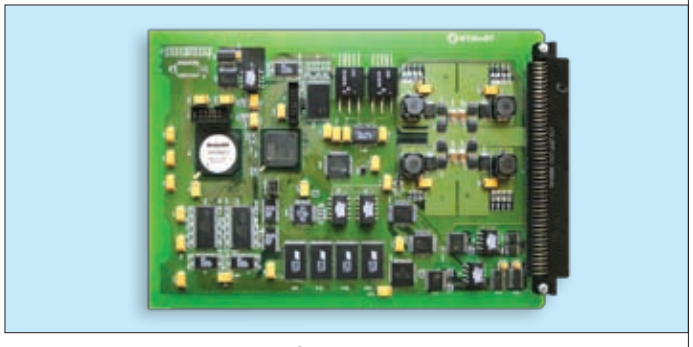

Рис.4. Процессорный модуль САУ ГТД

Применение платформенного подхода предполагает тесную взаимную увязку элементной базы, функциональных модулей, архитектурных решений, системного и прикладного программного обеспечения, инструментальных средств проектирования аппаратного и программного обеспечения, технологической и производственной подготовки, сопровождения САУ в эксплуатации.

Фрагмент архитектуры системы показан на рис.3. Система состоит из набора типовых модулей, связанных по дублированному каналу TTP, поддерживается также дублированный CAN-протокол. Типовые модули размещаются в корпусе системы или непосредственно на датчиках и исполнительных механизмах. В набор типовых модулей входят модуль вычислителя (МВ), коммуникационный модуль (МК), модуль дискретных сигналов (МДС), модуль следящей системы (МСС), модуль вторичного источника питания (МВИП) и еще около 30 модулей.

В соответствии с существующими требованиями перспективная платформа должна строиться на отечественной элементной базе, для чего будут разработаны ряд универсальных и специализированных микросхем, удовлетворяющих требованиям повышенной температурной, вибрационной и специальной стойкости. Планируется разработка микросхем микроконтроллера, межмодульного обмена, коммуникационного контроллера (MIL-1553, ARINC, Ethernet), следящей системы, силовой ИМС системы зажигания и ряда других.

ПРЕИМУЩЕСТВА TTA-ПОДХОДА

Использование платформенного подхода позволит:

- сократить сроки и трудозатраты на проектирование и освоение производства;
- обеспечить комплексное выполнение требований стандартов DO-254 и DO-178B на архитектурном, аппаратном и программном уровнях;
- унифицировать элементную базу и отказаться от импортной комплектации;
- повысить надежность САУ за счет применения типовых модулей;
- унифицировать состав бортовой и наземной аппаратуры (включая стендовую) и ПО;
- унифицировать системные решения на уровне смежных конструкторских бюро;
- выполнять модернизацию САУ, максимально используя предшествующие наработки;
- обеспечить длительные сроки сопровождения САУ в эксплуатации и ее модернизацию;
- унифицировать аппаратуру испытаний, диагностики и ремонта САУ.

Применение единого подхода построения бортовой и наземной аппаратуры позволяет решить сразу две задачи – повысить качество и надежность наземных систем до уровня бортовых и снизить стоимость бортовых систем за счет большого числа наземных установок.

Первым в семействе унифицированных модулей перспективной распределенной архитектуры бортовых систем управления является **процессорный модуль** (рис.4), разработанный в ИТМиВТ по заказу ОАО "НПП "ЭГА". Модуль содержит:

- центральный процессор 1892ВМ2Я (МС-24), работающий на частоте 80 МГц и имеющий двухъядерную архитектуру с универсальным и сигнальным процессором на одном кристалле (производство компании "ЭЛВИС");
- flash-память для программ (8 Мбайт) и параметров (8 Мбайт);
- ОЗУ 8 Мбайт;
- последовательные интерфейсы устройств ввода/вывода: ARINC-429, CAN, MIL-STD-1553RS-232, QSPI (5 МГц);
- ПЛИС, реализующую развитую логику ввода/вывода дискретных и частотных сигналов, сторожевой таймер, контроллер прерываний и буферные каскады коммуникационных каналов.

Управляется модуль операционной системой QNX 6.3 либо собственным диспетчером реального времени.

Архитектура TTA и ее протокол TTP благодаря таким свойствам, как контроль целостности, защита шины, предотвращение фрагментации, резервирование на архитектурном уровне и синхронизация часов, обеспечивают создание сложных распределенных систем. TTA – перспективная платформа для распределенных систем управления нового поколения, которые отвечают требованиям критических авиационных приложений. Работы по созданию отечественной распределенной платформы перспективных САУ ГТД авиационного и наземного применения целесообразно выполнять в рамках Отраслевого координационного совета.

ЛИТЕРАТУРА

Kopetz H.:A Platform for Safety-Critical Applications http://www.ttagroup.org.

TTP/C Specification. http://www.ttagroup.org.

Kopetz H.: The Time-Triggered Architecture http://www.ttagroup.org.

MAC Based FADEC Uses Time Triggered Protocol That Eliminates Complex Channel Change Logic// http://www.ttagroup.org/news/doc/PR-Honeywell_2005-04-11-First_Flight_Aermacchi_M-346.pdf

Fault Handling in the Time-Triggered Architecture// http://www.tttech.com/technology/docs/fault_handling/TTTech-Fault-Handling-TTA.pdf