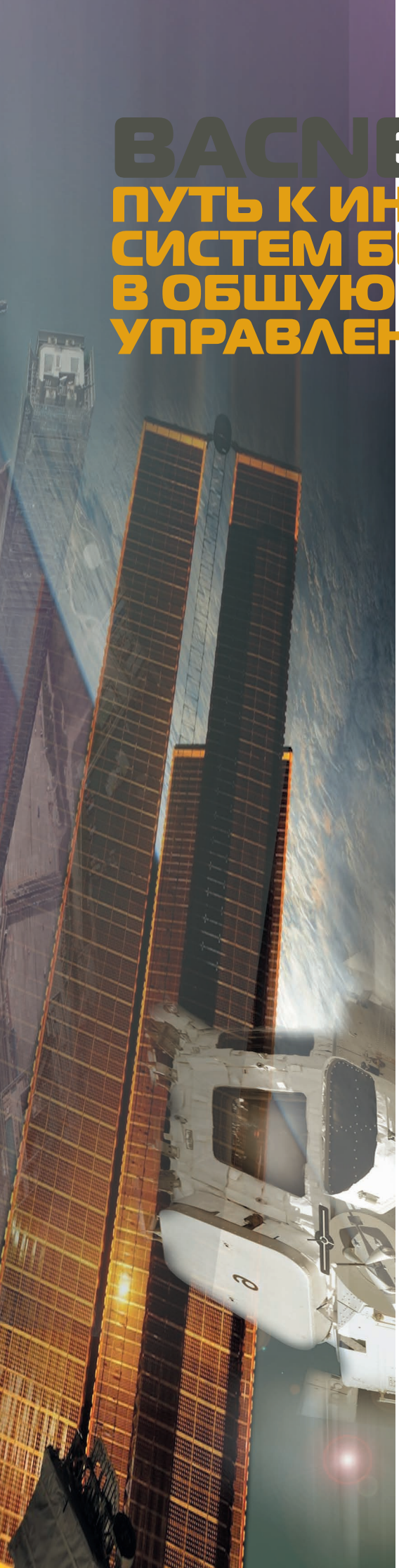


BACnet
ПУТЬ К ИНТЕГРАЦИИ СИСТЕМ БЕЗОПАСНОСТИ В ОБЩУЮ СИСТЕМУ УПРАВЛЕНИЯ ЗДАНИЕМ

ЧАСТЬ ВТОРАЯ

С. Лёвин
главный конструктор НПФ «Сигма-ИС»

ПРИКЛАДНОЙ УРОВЕНЬ

Прикладной процесс – это функциональность системы, производящая обработку информации, которая требуется для конкретного приложения. Все части Прикладного процесса вне Прикладного уровня (т.е. те, что не обеспечивают коммуникационные функции) находятся вне рассмотрения BACnet. Часть Прикладного процесса, которая находится внутри Прикладного уровня, называется Прикладная сущность. Другими словами, Прикладная сущность – это часть Прикладного процесса, связанная с коммуникационными функциями. Пользовательское приложение взаимодействует с Прикладной сущностью через API (Application Program Interface). API не определен в BACnet, но его функции всегда есть в конкретной реализации стека BACnet. Этот интерфейс не определен в BACnet, но эти функции и процедуры всегда есть в конкретной реализации стека BACnet.

Прикладная сущность состоит из двух частей: пользовательские элементы BACnetUser Element (UE) и служба элементов приложения BACnetApplication Service Element (ASE). BACnet UE несет несколько функций в дополнение к поддержке локального API. Они отвечают за обслуживание информации о контексте транзакции, включая генерацию ID для вызовов, с которым служба приложения запрашивает (отвечает) из (в) каждое устройство. Также эти функции отвечают за обслуживание счетчиков таймаутов, которые требуются для повтора передачи. BACnet UE управляет поведением устройств через BACnet объекты.

Информация, передаваемая между двумя приложениями, представлена в BACnet как обмен абстрактными сервисными примитивами, согласно соглашениям ISO, содержащимся в техническом отчете ISO о сервисных соглашениях ISO TR 8509. Эти примитивы используются для передачи сервисно ориентированных параметров. Определены 4 сервисных примитива: запрос, индикация, ответ и подтверждение. Информация, содержащаяся в примитивах, передается через набор Блоков Данных Протокола (Protocol Data Unit – PDU), определенных в стандарте BACnet.

Прикладная программа, которой необходимо связаться с удаленным прикладным процессом, получает доступ к локальному BACnet UE через API. Некоторые параметры вызовов API, такие как адрес устройства, передаются непосредственно в сетевой уровень через сетевую службу доступа (Network Service Access Point NSAP). В дополнение к сервисным примитивам и сервисно ориентированным параметрам имеются также управляющие параметры (Interface Control Information – ICI). Ниже приведены некоторые ICI-параметры:

- Destination address (DA) – адрес назначения;
- Source address (SA) – адрес источника;
- Network priority (NP) – 4-уровневый параметр приоритетности.

ПЕРЕДАЧА СООБЩЕНИЙ

В прикладном уровне BACnet используются два основных типа сообщений: с подтверждением и без подтверждения. Сообщения с подтверждением базируются на клиент-серверной коммуникационной модели. Соответственно, обеспечивается контроль передачи данных, в отличие от использования сообщений без подтверждения. Для передачи данных, длина которых превосходит максимальный размер, поддерживаемый коммуникационной сетью, приемным или передающим устройством BACnet, имеется возможность сегментирования данных. Причем сегментироваться могут только сообщения с подтверждением.

СЕТЕВОЙ УРОВЕНЬ

Назначение сетевого уровня BACnet – предоставление средства, с помощью которого сообщения могут передаваться из одной сети BACnet в другую независимо от коммуникационной технологии, используемой в каждой сети. В то время как нижестоящие уровни предоставляют возможности адресовать сообщения конкретному устройству или организовать широковещательную передачу только в локальной сети, сетевой уровень позволяет передавать сообщения всем устройствам во всех сетях. BACnet устройство однозначно определяется номером сети и MAC-адресом.

Устройства, которые объединяют две различные BACnet локальные сети, например Ethernet и ZigBee, называются BACnet маршрутизаторами. Маршрутизаторы создают и обслуживают таблицы маршрутизации автоматически, используя специальные сообщения сетевого уровня. Маршрутизатором может быть отдельное устройство, выполняющие только функции маршрутизации, иногда также могут выполняться и прикладные задачи по управлению и автоматизации здания.

Некоторые функции, определенные для сетевого уровня OSI, не требуются в BACnet. Например, функции выбора оптимального маршрута между передающим и приемным устройствами. Этого не требуется, потому что BACnet межсети разрабатываются и инсталлируются в большинстве случаев с простой топологией организации канала между двумя устройствами, и это существенно снижает сложность сетевого уровня. Другая важная функция сетевого уровня заключается в сегментировании и последующей сборке сегментированных сообщений. В общем случае сетевой уровень BACnet предоставляет сервис передачи данных для прикладного уровня без подтверждения и без установки соединения.

BACnet поддерживает передачу сообщений для многих получателей, используя мультиадресную (мультикастинг) и широковещательную (броадкастинг) адресацию. Мультикастинг используется для передачи сообщения группе получателей. Броадкастинг применяется для передачи сообщения всем устройством в локальной сети, удаленной сети или во всех сетях. И те и другие сообщения могут быть только без подтверждения.

КОЛЛЕКЦИИ ОБЪЕКТОВ

Структуры данных, используемых в устройствах для хранения информации, локальны по отношению к устройству. Для обмена информацией с другим устройством используя протокол BACnet, необходимо обеспечить соответствующее представление данных. Как уже говорилось ранее, в BACnet для этого используются объекты. Определен набор стандартных типов объектов, данные которых доступны на прикладном уровне. Службы прикладного уровня, в частности, используются для доступа и изменения свойств стандартных типов объектов. Все объекты имеют свойство Object Identifier. Каждый объект внутри устройства имеет уникальное значение этого свойства. Для адресации объекта в рамках всей BACnet сети это свойство объекта объединяется с аналогичным свойством Object Identifier устройства, в котором создан данный объект. Свойства могут быть обязательными и опциональными. Кроме того, имеется различие по правам доступа к данным свойств. Описание свойства в общем случае содержит идентификатор свойства, тип данных и тип самого свойства. Свойства бывают трех типов:

- O – опциональное;
- R – данные могут только считываться из свойства;
- W – данные могут как считываться, так и записываться в свойство.

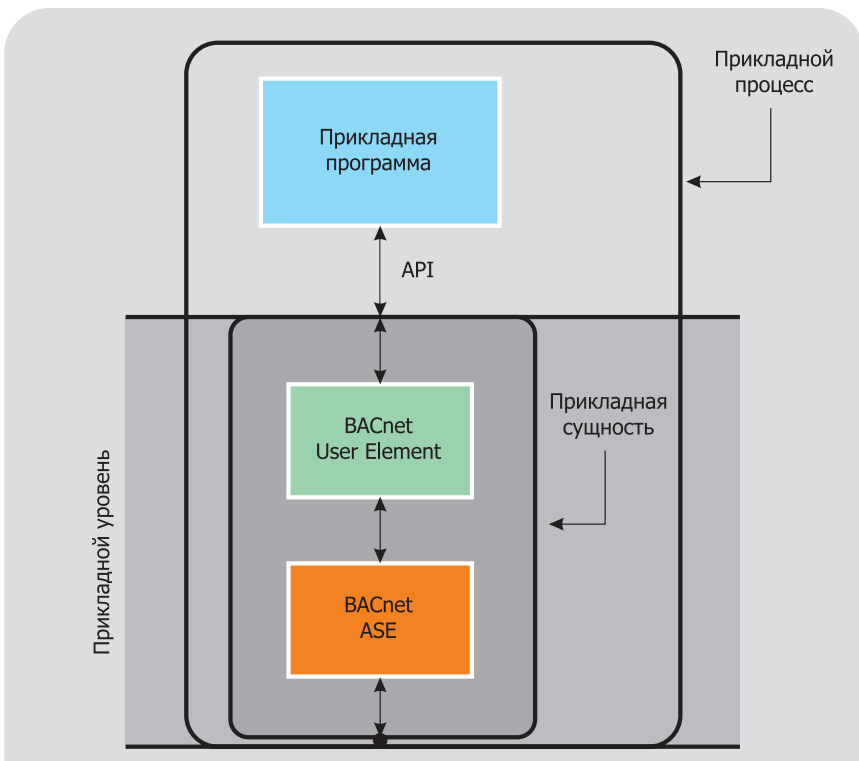
ОБЪЕКТ ТОЧКА ДОСТУПА

Для того, чтобы оценить, насколько полно объект BACnet и его свойства описывают реальную прикладную область со всей ее спецификой, давайте рассмотрим в качестве примера точку доступа. Тип объекта Точка доступа (AccessPointObjectType) определяет стандартный объект BACnet, чьи свойства представляют внешне видимые характеристики, ассоциируемые с процессом аутентификации и авторизации в системе контроля и управления доступом (дверь, турникет, ворота). Проход через точку доступа возможен только в одном направлении. Дверь, которая контролирует проход в обоих направлениях, представляется двумя раздельными объектами Точка доступа.

Аутентификация – это процесс проверки идентичности пользователя, запрашивающего проход через контролируемую дверь. Это может быть простая политика аутентификации по одному признаку (проксимити-карта, пинкод, биометрический признак пользователя). Либо при использовании политики аутентификации по нескольким признакам может использоваться их комбинация (карта + пинкод, биометрический признак + пинкод). Объект Точка доступа поддерживает оба способа. В случае ошибки при попытке аутентификации точка доступа может быть заблокирована на неопределенное или специально обозначенное время.

Авторизация – это процесс определения, имеет ли пользователь право на доступ в данную зону. После успешной аутентификации пользователя производится проверка критериев авторизации, дающих право на доступ. Если один или несколько критериев не выполняются, пользователю отказывается в доступе.

Точка доступа, которая авторизует вход в контролируемую зону, называется входной точкой для этой зоны. Точка доступа, которая авторизует выход из контролируемой зоны, называется выходной точкой. В типичном случае точка доступа может быть точкой выхода их одной зоны и в то же самое время являться точкой входа в смежную зону. Если точка доступа ведет из зоны доступа в неопределенную зону, такая точка будет являться только выходной, если наоборот – только входной. В конце концов, точка доступа может вообще являться ни



Модель прикладного процесса BACnet

Табл. 1. Свойства объекта Точка доступа

Свойство	Тип данных	Тип	Описание
Object Identifier	BACnetObjectIdentifier	R	Числовой код, используемый для идентификации объекта
Object Name	CharacterString	R	Произвольное текстовое название объекта
Object Type	BACnetObjectType	R	Тип объекта, для точки доступа это ACCESS POINT
Description	CharacterString	O	Опциональное текстовое описание объекта
Status Flags	BACnetStatusFlags	R	Набор флагов, описывающих состояния точки доступа. Например, флаг IN ALARM – наличие тревог, FAULT – неисправности
Event State	BACnetEventState	R	Интегрированное состояние объекта
Reliability	BACnetReliability	R	Техническое состояние объекта, показывающее возможна ли аутентификация и идентификация
Out Of Service	BOOLEAN	R	Флаг, показывающий, работает ли точка доступа или отключена
Verification Time	Unsigned	O	Время верификации
Threat Level	BACnetAccessThreatLevel	O	Уровень опасности, используется как дополнительный параметр при авторизации
Access Event	BACnetAccessEvent	R	Хранит последнее событие о доступе по этому объекту. Всего поддерживается более 50 различных событий о работе точки доступа
Zone To	BACnetDeviceObjectReference	O	Идентификатор входной зоны
Zone From	BACnetDeviceObjectReference	O	Идентификатор выходной зоны

Табл. 2. События объекта Точка доступа

Событие	Описание
GRANTED	Доступ предоставлен
MUSTER	Если точка доступа является терминалом сбора данных, при предъявления идентификатора генерируется данное событие
PASSBACK DETECTED	Нарушение правил прохода (например, попытка повторного входа)
DURESS	Проход под принуждением
LOCKOUT MAX ATTEMTPTS	Блокировка точки доступа после превышения количества ошибочных попыток доступа
DENIED UNKNOWN CREDENTIAL	Неизвестный идентификатор пользователя
DENIED NO ACCESS RIGHT	У пользователя нет прав на доступ
DENIED UPPER OCCUPANCY LIMIT	Превышение максимально возможного количества людей в зоне доступа
DENIED AUTHENTICATION FACTOR LOST	Попытка прохода с предъявлением утерянного ранее идентификатора
<Proprietary Enum Values>	Производитель оборудования может не ограничиваться набором событий, определенным в стандарте. Имеется возможность добавлять свои проприетарные события в дополнение к стандартным

Табл. 3. Свойства объекта Пользователь доступа

Свойство	Тип данных	Тип	Описание
Object Identifier	BACnetObjectIdentifier	R	Числовой код, используемый для идентификации объекта
Object Type	BACnetObjectType	R	Тип объекта, для точки доступа – это ACCESS USER
Description	CharacterString	O	Опциональное текстовое описание объекта
Global Identifier	Unsigned32	W	Уникальный идентификатор, который используется для глобальной идентификации пользователя в нескольких устройствах в рамках всей сети BACnet
User Type	BACnetAccessUserType	R	Тип объекта: ASSET – материальная ценность, GROUP – группа объектов, PERSON – физическое лицо
User Name	CharacterString	O	Имя пользователя
Members	List of BACnetDeviceObjectReference	O	Указатель на список, в котором указываются ассоциированные пользователи. Используется для группировки
Credentials	List of BACnetDeviceObjectReference	R	Указатель на список мандатов доступа для данного пользователя

входной, ни выходной, в том случае, если она используется как просто терминал аутентификации.

В объекте Точка доступа насчитывается более 40 свойств, которые достаточно полно описывают все возможные параметры, которые могли бы пригодиться в реальной жизни. В *таблице 1* приводятся некоторые из них.

В свойстве Access Event хранится последнее событие, связанное с точкой доступа. В *таблице 2* приводится список некоторых событий.

ОБЪЕКТ ПОЛЬЗОВАТЕЛЬ

Тип объекта Пользователь доступа (AccessUserObjectType) определяет стандартный объект BACnet, чьи свойства представляют внешние, т.е. доступные для прикладного уровня характеристики, ассоциируемые с пользователем системы контроля и управления доступом. Объект Пользователь доступа используется для представления физического лица, группы пользователей или объекта материальной ценности. Связи среди пользователей поддерживаются для представления иерархической организации (например, компании, департаменты, и группы и др.) или для представления принадлежности материальных ценностей.

Объект Пользователь доступа не участвует непосредственно в процессе аутентификации и авторизации. В основном он используется для информационных целей и может содержать имя пользователя, табельный номер и ссылку на внешнюю систему, предоставляющую детальную информацию о пользователях. Объект Пользователь доступа может иметь связку с объектом Мандат доступа (Access Credential) или, как это чаще называют, идентификатор пользователя. Идентификатором пользователя может быть проксимити-карта, пинкод, биометрический признак и т.п. Один пользователей может иметь несколько мандатов.

Когда один пользователь присутствует в нескольких устройствах, соответствующие объекты Пользователь доступа будут иметь разные значения Object Identifier в каждом устройстве. Тем не менее, они могут быть идентифицированы как один пользователь через свойство Global Identifier, которое используется для синхронизации объектов.

ОБЪЕКТ ПРАВА ДОСТУПА

Кроме описания точек доступа и пользователей для нормальной работы СКУД необходимо задавать права пользователей на проходы через точки доступа. Вполне естественно, что в BACnet имеется стандартный объект и для этой задачи. Тип объекта Права доступа (AccessRightsObjectType) определяет стандартный объект BACnet, чьи свойства представляют внешние, т.е. доступные для прикладного уровня характеристики, ассоциируемые с правами в СКУД.

Табл. 4. Свойства объекта Права доступа

Свойство	Тип данных	Тип	Описание
Object Identifier	BACnetObjectIdentifier	R	Числовой код, используемый для идентификации объекта
Object Type	BACnetObjectType	R	Тип объекта, для точки доступа – это ACCESS RIGHTS
Description	CharacterString	O	Опциональное текстовое описание объекта
Global Identifier	Unsigned32	W	Уникальный идентификатор, который используется для глобальной идентификации прав доступа в нескольких устройствах в рамках всей сети BACnet
Negative Access Rules	BACnetARRAY[N] of BACnetAccessRule	R	Список запретительных правил
Positive Access Rules	BACnetARRAY[N] of BACnetAccessRule	R	Список разрешительных правил
Accompaniment	BACnetDeviceObjectReference	O	Указатель на дополнительный мандат доступа. Используется для аутентификации по нескольким признакам. Правило будет работать, если указанный дополнительный мандат доступа был перед этим аутентифицирован в этой точке доступа

Объект Права доступа – это список правил, которые определяют привилегии для входа или выхода из зон доступа, а также доступ к другим ресурсам или функциям.

Объект Права доступа содержит набор правил, описывающих разрешения и запреты. Запретительные правила описывают, куда и когда доступ запрещен. Разрешительные правила описывают, куда и когда доступ может быть предоставлен. Запретительные правила имеют приоритет над разрешительными. Таким образом, политику прав доступа в BACnet можно назвать запретно ориентированной. Объект Права доступа связывается с объектом Мандат доступа.

Каждое правило доступа, разрешительное или запретительное, обозначает точку или зону доступа, условия которых определяют, будет ли данное правило применяться в данное время, и флаг, который показывает, что правило активно.

Так же, как и в случае с пользователями, когда один набор прав доступа присутствует в нескольких устройствах, соответствующие объекты Права доступа будут иметь разные значения Object Identifier в каждом устройстве. Тем не менее, они могут быть идентифицированы как одно и то же право доступа через свойство Global Identifier, которое используется для синхронизации объектов.

Как можно увидеть из вышеизложенного, протокол BACnet предоставляет чрезвычайно богатые возможности для организации полноценной поддержки системы контроля и управления доступа. Еще раз отмечу, что все это – стандартные объекты, поэтому весь функционал СКУД автоматически должен поддерживаться для построения совместных алгоритмов работы с любыми другими системами автоматизации здания, построенными на основе BACnet.

Продолжение следует...