Gebäude-, Personen- und Datensicherheit in intelligenten Gebäudesystemen

Grinewitschus, V; Hildebrand, R.; Kemmerling, M.; vom Bögel, G.

Fraunhofer IMS und inHaus-Zentrum Duisburg

1. Motivation

Infrastrukturen für Intelligente Gebäudesysteme werden zurzeit vorwiegend durch die Kopplung mehrerer unterschiedlicher Teilsysteme realisiert. Die Vorgehensweise hat einige gute Gründe, weswegen sie vermutlich auch in Zukunft in ähnlicher Form beibehalten wird. So kann für unterschiedliche Anforderungen an Übertragungsbandbreite, Zuverlässigkeit, Datensicherheit, Quality of Service und Preis jeweils das optimale Subsystem gewählt werden, wenn nicht ohnehin bestehende Strukturen und vorhandene Produkte aus Kompatibilitätsgründen erschlossen und unterstützt werden müssen. Durch den Einsatz einzelner Gateways als Schlüsselkomponenten können mit geringem Aufwand bewährte Systeme um neue Funktionalitäten ergänzt und zu umfassenden Gesamtsystemen integriert werden. Dabei stehen zurzeit zwei Einsatzfelder im Vordergrund, nämlich die Anbindung bisher lokaler Systeme an externe Netze und die Kopplung von bisher proprietären Systemen an Standard-Bussysteme.

Beiden Einsatzfeldern ist gemein, dass sie die Kompatibilität zu bestehenden Lösungen bewahren müssen und dass die nun zusätzlich möglichen Anwendungen nicht bei der ursprünglichen Konzeption der Systeme vorgesehen waren.

2. Beispieltopologie

An dem nachfolgend präsentierten Beispiel, bei dem EIB-Komponenten sowohl untereinander als auch über externe Netze sicherheitsrelevante Daten austauschen, sollen die wesentlichen Sicherheitsaspekte diskutiert werden. Die hierbei auftretenden Lösungsansätze sind auch auf andere Bussysteme übertragbar.

Die Anbindung an externe Netze übernimmt wie in Abb. 1 dargestellt ein Residential Gateway. Dieses Gerät muss die erforderlichen Protokolle und Dienste sowohl für das externe Netz (z.B. ISDN, DSL oder Ethernet), als auch für den internen Hausbus (in diesem Beispiel EIB) bereitstellen. Zusätzlich stellt es dabei Funktionen zur Umwandlung von Diensten bereit. Über EIB ist das Residential Gateway mit mehreren EIB-Komponenten verbunden, bei denen es sich zum Teil um herkömmliche EIB-Komponenten handelt, zum Teil besitzen sie aber auch Protokoll-Erweiterungen, um gesicherte Dienste erfüllen zu können.

Das Residential Gateway stellt einen leistungsfähigen eingebetteten Rechner dar, der einerseits komplexe Protokolle zur Anbindung an externe Rechnersysteme bearbeiten kann, andererseits aber zuverlässiger, kleiner und vor allen Dingen energiesparender als ein PC ist.

Die EIB-Komponenten sind in der Regel ebenfalls Controller-basierte Produkte, allerdings mit erheblich geringerer Rechenleistung und Speicherausstattung. Daher muss bei der Auswahl der Verschlüsselungsmechanismen, mit denen üblicherweise die Sicherheitsanforderungen erfüllt werden, auf die Ressourcen dieser Teilnehmer besonders viel Rücksicht genommen werden.

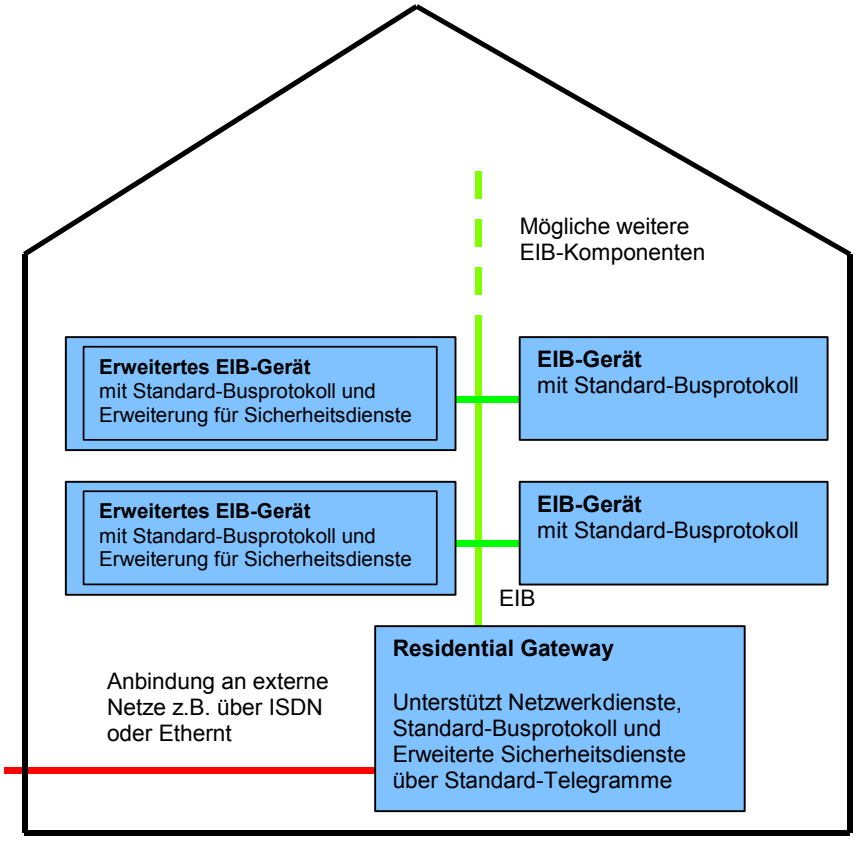

Abbildung 1: „Referenzarchitektur für die Applikationsbeispiele“

3. Typische Anforderungen

Die nachfolgend dargestellten typischen Anforderungen an intelligente Haussysteme sollen helfen, die Grenzen bestehender Lösungen aufzuzeigen. Die Auswahl ist natürlich nicht vollständig; es ergeben sich hieraus aber Ansprüche an verschiedene Komponenten, mit denen fast alle Anwendungsfälle abgedeckt werden können.

3.1 Alarmmeldung

Die Funktionalität der klassischen Alarmanlage zur Meldung von Einbruch oder Feuer stellt sehr hohe Ansprüche, denen deshalb oft mit spezialisierten Systemen begegnet wurde. Sowohl eine ausbleibende Meldung als auch Fehlalarme können große Schäden nach sich ziehen. Daher müssen diese Systeme hohe Zulassungshürden bestehen, von qualifizierten Fachleuten geplant und installiert, sowie ggf. regelmäßig gewartet werden. Dadurch fallen entsprechend hohe Kosten an. Bei der Meldung von technischen Alarmen wie z.B. dem Ausfall der Heizung oder dem Unterschreiten des Füllstands eines Heizöltanks sind die hohen Kosten oft nicht gerechtfertigt, so dass hier auch auf Systeme mit niedrigeren Sicherheitsansprüchen zurückgegriffen wird.

Das Absetzen von Alarmmeldungen oder Benachrichtigungen ist eine Funktion, die typischerweise durch Residential Gateways bearbeitet wird. Je nach Einsatzgebiet kommen hier unterschiedliche Protokolle zu Einsatz, z.B. zur Meldung an VdS-konforme Sicherheitsdienste, Versenden von Email bzw. SMS oder Sprachausgaben. Das Residential Gateway wandelt die über den Hausbus entgegengenommenen Daten in vorkonfigurierte

Nachrichten um, wobei je nach Freiheitsgrad der Konfiguration wieder Fehlverhalten erzeugt werden können.

3.2 Fernzugriff

Der Fernzugriff auf Gebäudesysteme stellt einen hohen Nutzen für den Anwender dar. Im Gegensatz zu Alarmmeldungen, mit denen er vorwiegend bei Defekten oder Notfällen konfrontiert wird, gibt ihm der Fernzugriff eine Zugriffsmöglichkeit auf normale Steuer- oder Abfragefunktionen. Auch hier ist wieder das Residential Gateway als Schlüsselkomponente für die Bearbeitung des Fernzugriffs zuständig, da es die Schnittstelle zwischen externem Netzwerk und internem Bussystem darstellt. Die wichtigste Aufgabe ist zunächst die Überprüfung der Zugriffsberechtigung, z.B. anhand von Passwörtern, Absenderinformationen o.ä. Kriterien. Eine weitere Aufgabe ist die Verhinderung von Fehleingaben, bzw. die Überprüfung von gültigen Wertebereichen. Für beide Aufgaben ist wiederum die Möglichkeit zur Konfiguration durch den Benutzer erforderlich.

Allerdings hat langfristig die Möglichkeit zum Fernzugriff auch Auswirkungen auf das Verhalten von Systemkomponenten. So sind z.B. bei manueller Bedienung eines Tasters Umschaltbefehle an eine Lampe unproblematisch, da der Benutzer die Lampe ja im Allgemeinen sehen kann. Beim Fernzugriff sind dagegen eher absolute Befehle (beim Beispiel Lampe konkrete Ein- oder Ausschaltbefehle) erforderlich, da die Rückmeldung nicht automatisch gegeben ist. Zusätzlich kann es erforderlich werden, dass die ferngesteuerten Geräte sich sehr viel stärker selbst überwachen, als dies zur Zeit üblich ist.

Um z.B. eine Badewanne ferngesteuert zu befüllen, könnte man busfähigen Ventile verwenden, die über Steuerbefehle von einem Handy ein- und ausgeschaltet werden. Die sich so einstellende Füllhöhe und die resultierende Wassertemperatur wären allerdings höchst unsicher, schlimmstenfalls könnten eventuell aufgrund technischer Probleme (Funkempfang, Akkukapazität, ...) sogar die Abschaltbefehle verloren gehen. Daher muss für solche Aktionen die Überwachung durch die Endgeräte selber erfolgen, so dass die Aktionen durch den Fernzugriff zwar noch gestartet, eingestellt und ggf. vorzeitig beendet werden können, der eigentliche Ablauf (Temperaturregelung, Überwachung des Füllstandes, Verbrühschutz) aber lokal bearbeitet und überwacht wird.

3.3 Überwachung von Komponenten

Wenn einzelne Komponenten in einem System kritische Aufgaben wahrnehmen, ist es oft erforderlich, dass ihre korrekte Funktion überwacht wird. In EIB-Systemen werden dazu üblicherweise zyklische Telegramme verwendet, deren Ausbleiben detektiert wird. Auf diese Weise können z.B. Sabotageversuche durch Auftrennen von Busleitungen oder sonstige Beschädigungen erkannt werden. Viele EIB-Komponenten können zyklische Telegramme senden, zusätzlich kann ein Residential Gateway bei Bedarf gezielt einzelne Komponenten abfragen.

Durch die Anbindung an externe Netze muss man zusätzlich den Fall berücksichtigen, dass gezielt falsche Daten in das System eingespeist werden könnten. Auf diese Weise könnte z.B. ein Schlüsselschalter zum Öffnen einer Tür übergangen werden, indem einfach das erforderliche Telegramm in das System eingespielt wird. Daher ist es für viele Anwendungen wichtig, die Identität des Absenders sicher zu erkennen. In EIB-Telegrammen ist zwar eine Absenderkennung enthalten (physikalische Adresse), sie kann jedoch leicht gefälscht werden und stellt daher keine verlässliche Information dar.

3.4 Verschlüsselung der Datenübertragung

Wenn eine vorhandene EIB-Infrastruktur verwendet werden soll, um sicherheitsrelevante Dienste zu realisieren, müssen die zu übertragenden Daten verschlüsselt werden können. Nur auf diese Weise können Anwendung wie z.B. Zeiterfassungssysteme personenbezogene Daten übertragen, ohne dass man mit einem Busmonitor diese Daten ausspähen oder manipulieren kann. Die verschlüsselte Datenübertragung sollte sinnvollerweise mit der normalen Datenübertragung gemischt werden können, um die Kompatibilität mit bestehenden Produkten und Diensten zu gewährleisten; alle Teilnehmer am verschlüsselten Datenverkehr müssen jedoch zusätzliche Funktionen erhalten. Das Residential Gateway nimmt in diesem Zusammenhang streng genommen keine Sonderrolle ein; da es aber im Vergleich zu den übrigen Komponenten aufgrund der hohen Anforderungen an Rechenleistung und Speicherbedarf meistens mit den größten Ressourcen ausgestattet ist und über erweiterte Konfigurationsmöglichkeiten verfügt, kann es zusätzliche zentrale Managementaufgaben übernehmen, die im Zusammenhang mit der Schlüsselverwaltung auftreten.

4. Erweiterung des EIB-Protokolls

Bei der EIB-Datenübertragung werden vorwiegend Datenobjekte durch Gruppentelegramme versendet, deren stark vereinfachter Aufbau in Abbildung 2 dargestellt ist. Es handelt sich dabei um einen Broadcast-Mechanismus, bei dem die physikalische Adresse den Absender identifiziert und die Gruppenadresse angibt, um welches Datenobjekt es sich handelt. Mögliche Datenlängen liegen zwischen 1 Bit und 14 Byte.

Physikalische Adresse	**Gruppenadresse**	**Länge**	**Daten (1 Bit bis 14 Byte)**

Abbildung 2: Vereinfachter Aufbau eines EIB-Gruppentelegramms

Bei der Konfiguration wird den Komponenten mitgeteilt, welche Gruppenadressen sie zu verwenden haben. Beim Empfang der Telegramme prüft jeder Teilnehmer, ob er Objekte mit dieser Gruppenadresse bearbeiten soll. Wenn nicht, ignoriert er dieses Telegramm.

Ein Mischbetrieb von normalen und verschlüsselten Telegrammen ist daher leicht zu realisieren, sofern hierfür getrennte Gruppenadressen verwendet werden, was aber, wie eben beschrieben, ohnehin eine Grundeigenschaft der EIB-Datenübertragung darstellt. Die Verschlüsselung darf sich dabei nur auf den Datenbereich beziehen, da sonst die übrigen EIB-Teilnehmer gestört werden könnten.

4.1 Anforderungen an den Verschlüsselungsalgorithmus

Der Entwurf eines neuen Verschlüsselungsalgorithmus ist eine aufwändige Angelegenheit, bei der sich leicht Sicherheitslücken einschleichen können. Gleichzeitig existiert eine große Anzahl bewährter Algorithmen, deren Eigenschaften bereits gründlich untersucht wurden. Bei der Auswahl eines geeigneten Verfahrens standen folgende Kriterien im Vordergrund:

1. Ver- und Entschlüsselung muss in Echtzeit erfolgen können
2. Symmetrischer Algorithmus
3. Blockgröße von 8 Byte
4. Implementierbarkeit auf 8-bit-Mikrocontrollern mit geringem Speicher

Die Begründung für diese Kriterien liegt darin, dass dem flächendeckenden Einsatz verschlüsselter Telegramme möglichst keine Hürden in den Weg gelegt werden. Um bestehende Lösungen sicherer zu gestalten, dürfen (Kriterium 1) keine zusätzlichen Wartezeiten entstehen, da diese von den aktuell bestehenden Applikationen voraussichtlich nicht akzeptiert würden. Kriterium 2 folgt ebenfalls aus den zeitlichen Anforderungen, da symmetrische Algorithmen sehr schnell sind und daher in fast allen Verschlüsselungs-Anwendungen bei der eigentlichen Datenübertragung eingesetzt werden. Diese symmetrischen Algorithmen arbeiten im Allgemeinen blockorientiert mit typischen Blockgrößen von 8 Byte oder (besonders neuere Algorithmen) 16 Byte. Je umfangreicher die Blockgröße, desto effektiver kann die Bearbeitung größerer Datenmengen parallelisiert werden, weswegen eine Blockgröße von mindestens 16 Byte auch Teilnahmevoraussetzung für Algorithmen bei dem Wettbewerb um den neuen AES-Algorithmus darstellt. Leider können 16 Byte Blöcke aber nicht innerhalb eines einzelnen EIB-Telegramms transportiert werden (maximale Datenlänge 14 Byte), so dass eine Blockgröße von 8 Byte zum Einsatz kommt. Die Implementierung der Verschlüsselung auf einem 8-bit-Mikrocontroller ist wünschenswert, da diese in typischen EIB-Komponenten zum Einsatz kommen. Der Speicher in diesen Systemen ist aus Kostengründen typischerweise sehr knapp bemessen, wobei meistens mehr Programmspeicher als Datenspeicher vorhanden ist.

Der Algorithmus „Blowfish“ erfüllt diese Anforderungen sehr gut, bei einer Implementierung auf einem 8-bit-Controllersystem zeigte sich, dass beim Datenaustausch über EIB kontinuierlich ver- und entschlüsselt werden kann, ohne den Controller zu sehr zu belasten. Ein angenehmer Nebeneffekt von „Blowfish“ ist, dass die Bearbeitungszeit nicht von der Schlüssellänge abhängt. Hier muss also keine Entscheidung zwischen Sicherheit und Rechenleistung getroffen werden. Da „Blowfish“ mit schlüsselspezifischen Tabellen von ca. 5 kByte pro Schlüssel arbeitet, ist allerdings die Anzahl der gleichzeitig verwendbaren Schlüssel durch den zur Verfügung stehenden Speicher begrenzt.

4.2 Sicherheitsgewinn durch Zusatzinformationen in den Telegrammen

Die reine Verschlüsselung von Nutzdaten reicht für den praktischen Einsatz jedoch nicht aus, da diese Telegramme abgehört und später erneut gesendet werden könnten. Daher ist die Verwendung eines Zählers erforderlich, der von Sender und Empfänger gleichzeitig erhöht wird, um alte Telegramme zu erkennen und ggf. zu ignorieren. Für weitere Aufgaben z.B. im Zusammenhang mit der Schlüsselverwaltung wurde noch eine Service-ID hinzugefügt, um unterschiedliche Nachrichtenarten unterscheiden zu können.

Byte	Bezeichnung	
1	Service-ID	Counter
2	Counter	
3-8	Parameter / Füllbyte	
9-14	Füllbyte	

Abbildung 3: Aufbau des Datenteils einer verschlüsselten Nachricht

Die Nachrichtenarten können dabei unterschiedlich viele Parameter besitzen, maximal jedoch 6 Byte, da dann zusammen mit der 4 Bit-Service-ID und einem 12 Bit-Counter die Blockgröße von 8 Byte erreicht wird. Die restlichen 6 Byte sind ohne Bedeutung und werden als Füllbytes eingesetzt, da es im EIB zwar Nachrichten mit 14 Bytes, aber standardmäßig keine mit 8 Datenbytes gibt.

4.3 Schlüsselverwaltung

Grundeigenschaft symmetrischer Verschlüsselung ist es, dass alle Teilnehmer identische Schlüssel verwenden müssen. Dieser Schlüssel kann fest in den Komponenten hinterlegt bzw. bei der Konfiguration eingestellt worden sein. Diese Lösung ist allerdings nicht zu empfehlen, da die Möglichkeit, einen Code zu brechen mit der Menge der verfügbaren Daten steigt. Besser ist es daher, die Schlüssel über einen sicheren Kanal bei Bedarf zu ändern, wenn z.B. Komponenten neu hinzukommen oder der Verdacht besteht, dass ein Schlüssel bekannt geworden ist. Zu diesem Zweck kommen üblicherweise asymmetrische Verfahren zum Einsatz (z.B. RSA oder Diffie-Hellmann). Diese Verfahren benötigen allerdings erheblich mehr Ressourcen. Während eine erhöhte Rechenzeit noch zu ertragen ist, da die Schlüssel aufgrund der niedrigen Datenübertragungsrate nicht so oft gewechselt werden müssen, ist der höhere Speicherbedarf oft kritisch, da er unmittelbar die Systemkosten beeinflusst. Ein Ausweg bietet sich z.B. in der Verwendung mehrer symmetrischer Schlüssel pro Teilnehmer, wobei ein (teilnehmerspezifischer) „Masterschlüssel“ zur Zuteilung eines „Arbeitsschlüssels“ verwendet wird. Da auf diese Weise nur geringe Datenmengen durch den „Masterschlüssel“ verschlüsselt werden, kann dieser dauerhaft beibehalten werden oder sich selbst rechtzeitig gegen eine neue Version ersetzen.

Die Schlüsselverwaltung erfordert einen Teilnehmer im System, der über die momentan gültigen Schlüssel informiert ist und bei Bedarf neue Schlüssel oder neue Zählerstände für die übrigen Teilnehmer zuweisen kann. Hierfür bietet sich das Residential Gateway an, da es mit den resultieren Datenmengen leichter umgehen kann als die übrigen ressourcenbegrenzten Teilnehmer.

5. Zusammenfassung

Bei der Kopplung unterschiedlicher Bussysteme oder der Anbindung von Geräten an externe Netzwerke (z.B. an das Internet) stellt sich oft heraus, dass für diesen Anwendungszweck grundlegende Sicherheitsmechanismen fehlen. Durch intelligente Zusatzkomponenten, z.B. Residential Gateways, können bestehende Netzwerke erfolgreich miteinander gekoppelt werden, auch wenn sie sehr unterschiedliche Eigenschaften aufweisen. Die erforderlichen Anpassungen, Dienstekonversionen und Protokollumsetzungen können in die Gateways integriert werden, so dass gewohnte Betriebsarten, besonders bei der Konfiguration oder der Diagnose, beibehalten werden können.

Bei der Nutzung vorhandener Hausbus-Infrastrukturen für sicherheitsrelevante Zusatzfunktionen wie Zugangskontrollen, Zeiterfassungen oder Alarmanlagen hingegen stellt dieser Ansatz keine Lösung dar, da hier die Sicherheit innerhalb des Systems erhöht werden muss. Daher wird für solche sicherheitsrelevanten Anwendungen oft eine separate Kommunikationsinfrastruktur verwendet, obwohl ein Gebäudebus, z.B. ein EIB-System, zur Verfügung steht. Eine praktikable Lösung stellt hierbei die Verwendung der Standard-Übertragungsmechanismen des EIB dar, bei denen jedoch die eigentlichen Nettodaten verschlüsselt werden. Auf diese Weise kann normaler Datenverkehr mit gesichertem Datenverkehr gemischt werden, wobei natürlich die sicherheitsrelevanten Teilnehmer erweiterte Funktionalitäten wie Ver- und Entschlüsselung aufweisen müssen. Dem Residential Gateway kommt in solchen Systemen neben der Kopplung der internen Netzwerke und deren Anbindung an ein externes Netzwerk auch das intelligente Management der Schlüssel zu.

Im IMS wurde eine Beispielanwendung aus Transponder-Kartenleser und Display realisiert, die untereinander und zu einer PC-Applikation verschlüsselte Daten austauschen. Es konnte gezeigt werden, dass mit 8-Bit-Mikrocontrollern und sehr wenig Systemressourcen (Rechenleistung, Speicher) sicherheitsrelevante Anwendungen mit Hausbussystemen (am Beispiel des EIB) umgesetzt werden können und gemeinsam mit den Standard-EIB-Anwendungen in einem System zuverlässig betrieben werden können.

Damit sind sicherheitsrelevante Applikationen auch mit kostengünstiger Technologie in einfachen Hausbusinfrastrukturen realisierbar.

Literatur

„Secure EIB/KNX data transmission for security critical applications“; Olaf Russak, IPAS GmbH (Duisburg)