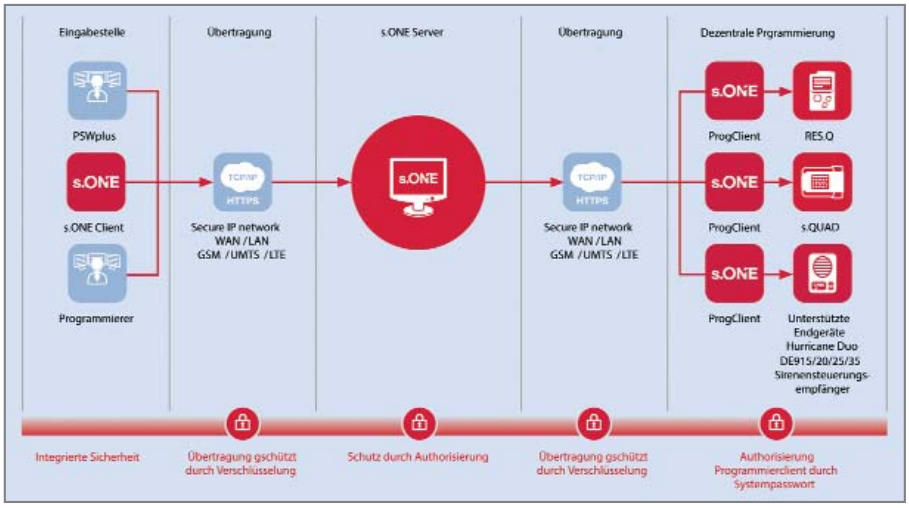
Zuverlässig und sicher muss es sein

Verschlüsselung von Alarmierungssystemen

Philipp Zimmermann

Dank der Integration von verschiedenen Verschlüsselungssystemen bietet Swissphone seit Beginn dieses Jahres seinen Kunden ein offenes Verschlüsselungskonzept: Sowohl die Netze als auch die Melder des Unternehmens sind im Stande, adressspezifisch die gewünschten Verschlüsselungsverfahren anzuwenden – jeweils im gleichen Netz und bei Bedarf auch im gleichen Melder. Somit haben Swissphone-Kunden die Wahl, das Verschlüsselungsverfahren frei auf die bestehenden Melder und Gegebenheiten ihrer internen Kunden anpassen. Warum eine Entscheidung gut durchdacht und die Frage nach der Praktikabilität geklärt sein muss, zeigt sich bei genauerer Betrachtung von Overhead, Rufbeschleunigungsverfahren, sicherem Schlüsselmanagement und Zeitauthentifizierung.



DiCal-IDEA ist Teil einer integrierten Sicherheitsarchitektur, die neben der Verschlüsselung der Meldungen die sichere und zuverlässige Verwaltung der Schlüssel sowie die verschlüsselte Übermittlung der Programmierdaten beinhaltet

Die Anforderungen an eine effiziente und zeitgerechte Alarmierung von Einsatzkräften sind vielfältig. Die Einsatzkraft verlangt qualitativ hochwertige Endgeräte, die Alarme in jeder Situation schnell und zuverlässig übermitteln. Organisationen möchten gezielt und dynamisch alarmieren, um die Einsatzkräfte möglichst schnell selektiv oder auch in Gruppen adressieren zu können. Für den Gesetzgeber ist es wichtig, dass Hilfsfristen eingehalten und schützenswerte Daten verschlüsselt übermittelt werden. Im Rahmen der Einführung der Datenschutzgrundverordnung (DSGVO) hat die Verschlüsselung von Nachrichten mit persönlichen Daten nochmals an Wichtigkeit gewonnen.

Als Hersteller hochwertiger integrierter Alarmierungslösungen mit aufeinander abgestimmten Komponenten hat Swissphone bereits vor Jahren mit DiCal-IDEA einen Verschlüsselungsstandard geschaffen, der nunmehr in weit über hundert Alarmierungsnet-

Zugleich verschlüsselt und unverschlüsselt

Es kann erforderlich sein, dass ein Alarmsystem Meldungen abwechselnd verschlüsselt und unverschlüsselt versenden kann. Einerseits um eine einfachere Migration von alten zu neuen Funkmelderausstattungen zu ermöglichen, andererseits um einen Notbetrieb sicherzustellen, falls z.B. ein Verschlüsselungsserver ausfällt. Ebenso wie BOSKrypt unterstützt die neueste Version von DiCal-IDEA deshalb das Empfangen unverschlüsselter Nachrichten auf Adressen, die normalerweise eine verschlüsselte Nachricht empfangen. Das muss allerdings für die Erhöhung der Datenintegrität durch ein entsprechendes Schlüsselwort geschehen. Alle Swissphone-Melder mit DiCal-IDEA-Verschlüsselung, die über einen Firmwarestand verfügen, lassen diese Möglichkeit bei entsprechender Implementierung im Netz zu. In der neuesten Version von DiCal-IDEA wurde außerdem die automatische Meldungskorrektur im Melder verbessert, was die Empfangswahrscheinlichkeit der Nachricht zusätzlich erhöht.

Philipp Zimmermann ist Head of Marketing bei der Swissphone Wireless AG in Samstagern, Schweiz

zen mit mehreren hunderttausend Pocsag-Meldeempfängern erfolgreich verwendet wird. DiCal-IDEA fügt sich einerseits in die Gegebenheiten von digitalen Funkrufnetzen optimal ein. Andererseits erfüllt er die oben erwähnten Anforderungen der verschiedensten Gruppen. Aufgrund der Erfahrungen und aktueller Kundenwünsche erweiterte der Hersteller den Standard funktionell (siehe *Textkasten Zugleich verschlüsselt und unverschlüsselt*).

Offenes Verschlüsselungskonzept

In der Regel besteht bei den meisten Alarmierungsnetzen bisher keinerlei Notwendigkeit, von der DiCal-IDEA-Verschlüsselung abzuweichen. Sollten jedoch innerhalb einer Region Funkmeldeempfänger unterschiedlicher Hersteller mit Verschlüsselungswunsch eingesetzt werden, kann sich prinzipiell auch das mittlerweile mehreren Herstellern zugängliche Verfahren BOSKrypt anbieten. In Swissphone-Alarmierungsnetzen können beide Verschlüsselungsverfahren quasi parallel und adressspezifisch genutzt werden, z.B. für Swissphone-Funkmeldeempfänger DiCal-IDEA und für Funkmelder eines anderen Herstellers BOSKrypt.

Ab sofort bieten die Schweizer ihren Kunden auch die freie Wahl hinsichtlich der Verschlüsselungssysteme im Endgerät an: Sowohl Netze als auch Melder des Unternehmens können somit adressspezifisch die verschiedenen Verschlüsselungsverfahren anwenden – jeweils im gleichen Netz und bei Bedarf auch im gleichen Melder. Behörden und Leitstellen haben damit die Freiheit, das Verschlüsselungsverfahren auf die bestehenden Melder und Gegebenheiten ihrer Organisationen anzupassen. Vor der Wahl eines Verschlüsselungsverfahrens lohnt es sich jedoch, die Vor- und Nachteile der jeweiligen Technik sorgfältig abzuwägen.

Tauglichkeit für Pocsag-Funknetze

Das BOSKrypt-Verschlüsselungsverfahren ist hinsichtlich Datensicherheit und Integration gut gelöst:

- Die 256-bit-AES-Verschlüsselung bietet grundsätzlich ein Maximum an Zugriffsschutz durch Dritte.
- Der Initialisierungsvektor aus elf Zeichen, der fehlerfrei empfangen werden muss, bietet zusätzlich Dateninteгrität.
- Durch das Base-64-Encoding des verschlüsselten Produkts lässt sich das Verfahren einfach in Drittsysteme integrieren.

Zugleich ergeben sich im Rahmen eines Funksystems aber auch Nachteile:

- Die Tatsache, dass sieben Pocsag-Codeworte (elf Zeichen) fehlerfrei empfangen werden müssen, führt bei kleinsten Funkstörungen zum Nichtanzeigen der Meldung, weil

Express-Alarm

Angesichts der heutzutage knappen Ressourcen wird es immer wichtiger, die Zeit und Verfügbarkeit der Freiwilligen zu respektieren und nur die aktuell verfügbaren Ressourcen zu alarmieren. Das patentierte Express-Alarm-Verfahren von Swissphone ermöglicht es, Einsatzkräfte einzeln zu alarmieren, ohne die Alarmdauer zu erhöhen. Anstelle jeder RIC-Adresse (A1, A2, A3 bis An) einzeln die Nachricht mit dem gesamten Meldungstext zuzustellen,

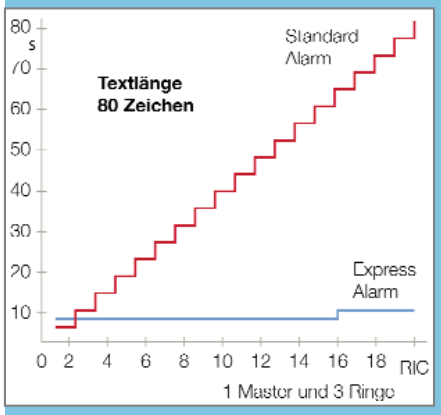
A1	Alarmtext	A2	Alarmtext	A3	Alarmtext	....	An	Alarmtext

werden zu Beginn einer Übertragung nur die Einzeltonrufe (RICs der Empfänger: A1, A2, A3 bis An) übermittelt. Anschließend wird eine gemeinsame alphanumerische Adresse Aα mit anschließendem Alarmtext gleichzeitig an alle erforderlichen Benutzer gesendet.

A1	A2	A3	....	An	Aα	Alarmtext

Abhängig von seinem RIC zeigt das Terminal die Meldung an – oder nicht. Dieses Verfahren reduziert das Volumen der zu sendenden Daten, was die Zeit der Alarmübertragung erheblich verkürzt. Beispielsweise können bis zu 32 Alarmadressen in 1 s gesendet werden (Pocsag bei 1.200 bit/s).

Folgender Vergleich illustriert die Alarmzeiten beider Verfahren unter Berücksichtigung unterschiedlicher Zeichenlängen (Berechnung auf Basis von Pocsag 1.200 bit/s):



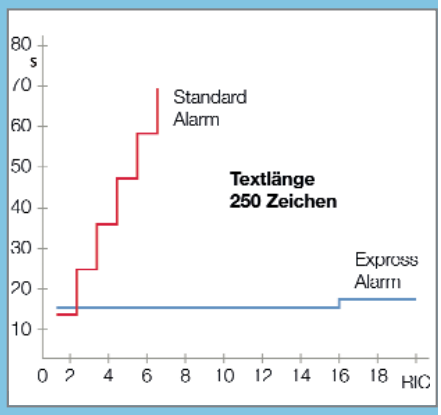


Bild links: Ein Alarm mit bis zu 15 Adressen und ca. 80 Zeichen Text in einem Netz bestehend aus einem Master und drei Ringen dauert nur 8 s. Ohne Express-Alarm endet die Übertragung erst nach 60 s

Bild rechts: Alarmmeldungen mit einer Länge von 250 Zeichen benötigen auch bei 15 Alarmadressen nur 16 s

Das patentierte Rufbeschleunigungsverfahren Express-Alarm ist insbesondere nützlich, wenn die selektive Alarmierung mit einer Verschlüsselung kombiniert wird, die die Nachricht zusätzlich verlängert.

ansonsten die Datenintegrität nicht mehr gewährleistet ist.
- AES 256 und das Base-64-Encoding haben den Nachteil, dass die zu übertragenden Daten um bis zu 40 % größer werden. Der sog. Overhead führt zu einer längeren Übertragungsdauer (siehe *Textkasten* unten).

DiCal-IDEA arbeitet mit einer Schlüssellänge von 128 bit. Auch angesichts der heute verfügbaren enormen Rechenleistungen reicht diese Verschlüsselung gegen einen Brute-Force-Angriff aus. Um einen Schlüssel mit 2^{128} Zeichen mittels des Bitcoin-Netzes mit einer aktuellen Hash Rate von 60 Mio. TH/s (2^{65}) zu knacken, bräuchte ein Angreifer statistisch 2^{63} s, was 13 Mal dem Weltalter entspricht.

Beim IDEA-Verfahren ist der Initialvektor lediglich zwei Codeworte lang. Er muss fehlerfrei empfangen werden, damit die Nachricht korrekt angezeigt werden kann. Um das Verfahren robuster zu machen, wurde die automatische Meldungskorrektur im Melder verbessert. Dies verringert Fehler und erhöht die Empfangswahrscheinlichkeit der Nachricht zusätzlich.

Rufbeschleunigungsverfahren

In Deutschland hat sich die selektive Alarmierung mit unterschiedlichen Alarmadressen (RICs) pro Einsatz weitgehend durchgesetzt. Sendet eine Leitstelle für einen Einsatz aber mehrere Alarme bestehend jeweils aus RIC und Einsatztext, wird die Alarmierung aufgrund der großen Zahl der zu versendenden Nachrichten langsam. Erfolgt noch die Verschlüsselung der Einsatztexte, ist BOSKrypt aufgrund der deutlich größeren Datenmenge im Vergleich zu DiCal-IDEA überproportional langsamer. Zusammen mit der Funktionsweise von Funkrufnetzen ist dieses Verhalten besonders schwerwiegend, da jede Nachricht in mehreren Aussendungen zwischen den Basisstationen weitergesendet werden muss; die Dauer der Aussendungen addiert sich. In beiden Fällen, insbesondere bei BOSKrypt, lohnt es sich deshalb, ein Rufbeschleunigungsverfahren einzusetzen. Swissphone bietet hier das patentierte Express-Alarmverfahren an (siehe *Textkasten Express-Alarm*). Durch das Zusammenfassen der Nachrichten zu einer Aussendung unterstützt dieses die dynamische Alarmierung optimal. In diesem Zusammenspiel ermöglichen DiCal-IDEA und Express-Alarm eine Alarmierung mit minimalen Alarmierungszeiten und mit zuverlässiger, sicherer Nachrichtenübermittlung.

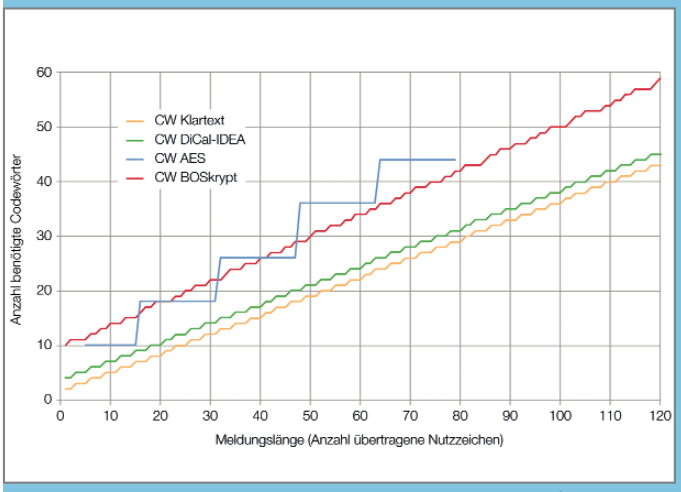
Ende-zu-Ende-Verschlüsselung

Es gibt symmetrische und asymmetrische Verschlüsselungsverfahren. Bei Systemen, die wie Funkrufnetze nur in eine Richtung kommunizieren, werden die Nachrichten in derselben Länge wie die Klartextmeldung angezeigt werden. Der verschlüsselten Nachricht werden bloß 40 bit vorangestellt, beispielsweise mit Informationen zur Zeitauthentifizierung. Dadurch ist der DiCal-IDEA-Verschlüsselungs-Overhead vernachlässigbar gegenüber einer Klartextmeldung (*Bild links*).

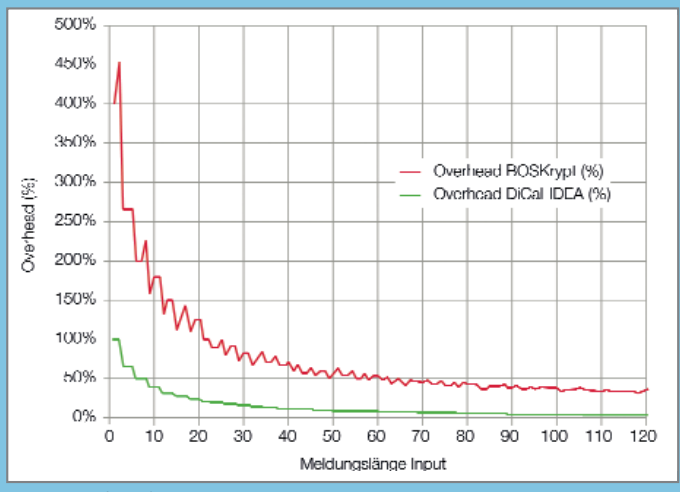
Bei BOS-Krypt ist diese vorangestellte Information länger als bei DiCal-IDEA (*Bild rechts*). Außerdem verwendet das Verfahren einen anderen Zeichensatz für die Codierung der verschlüsselten Meldung (Base64). Dieser hat den Vorteil, dass mit BOSKrypt verschlüsselte Nachrichten herstellerübergreifend gelesen werden können, allerdings verlängert sich die Nachricht dadurch um 40 % gegenüber dem Klartext. Dadurch wird die Übertragungszeit länger und die Netz-Performance sinkt, was sich insbesondere bei selektiven Alarmierungsverfahren negativ auswirkt. Die Übertragungszeit kann durch das Express-Alarm-Rufbeschleunigungsverfahren verkürzt werden.

Verschlüsselungs-Overhead

Der Overhead bezeichnet die durch die Verschlüsselung entstehende zusätzliche Nachrichtenlänge. DiCal-IDEA verwendet den numerischen Zeichensatz gemäß Pocsag-Standard, der aus 16 druckbaren Zeichen besteht. Damit kann die verschlüsselte



Vergleich des Overhead der erhältlichen Verschlüsselungsverfahren



Overhead (in %) der Meldungslänge: DiCal-IDEA/BOSKrypt

den symmetrische Verfahren angewandt. Diese bedingen, dass Sender und Empfänger einen gemeinsamen Schlüssel für die zu übertragende Nachricht haben. Bei einer Vielzahl von Empfängern respektive Adressen haben Organisationen heute folgende zwei Optionen, Schlüssel einzusetzen:

- Alle Empfänger verfügen über einen gemeinsamen Schlüsselsatz, wovon jeweils einer den einzelnen Organisationen als aktiver Schlüssel zugeteilt ist. Hierbei kann weiterhin die Alarmierung von Gruppen durchgeführt werden. Dies vereinfacht das Handling der Schlüssel wesentlich, bedingt aber, dass der jeweils aktive Schlüssel in allen Endgeräten gewechselt werden muss, wenn dieser bekannt würde. Er wird dann mit einem neuen Schlüssel aus dem gemeinsamen Schlüsselsatz ersetzt. Der Tausch geschieht über einen OAP-Befehl (On Air Programming) über das Funknetz. Die Funkmelder müssen also nicht von Hand neu konfiguriert werden. Bei Bedarf können auch diese Schlüsselsätze ausgetauscht werden, was aber eine neue manuelle Programmierung oder eine Fernprogrammierung aller betroffenen Melder erfordert. Somit bleibt die Sicherheit jederzeit gewährleistet.
- Jede Adresse im Melder besitzt einen eigenen Schlüssel. Dies bedingt, dass jeder Melder den für seine Adresse gültigen Schlüssel speichern muss. Der Vorteil: Bei Verlust eines Pagers bzw. bei Diebstahl des Schlüssels ist nur eine Adresse kompromittiert. Ein neuer Schlüssel muss zu dieser Adresse generiert werden, der Verschlüsselungsserver muss aufdatiert und der Melder neu programmiert werden. Falls Gruppenrufe oder Expressalarme eingesetzt werden, entfällt dieser Vorteil jedoch, da dann dennoch auf allen betroffenen Pagern dieselbe Adresse programmiert ist. Ein Nachteil dieser Lösung ist, dass das Schüsselmanagement deutlich aufwendiger ist, um sicherzustellen, welcher Adresse welcher Schlüssel zugeordnet wird.

Um den jeweiligen Kundenanforderungen gerecht zu werden, bietet Swissphone mit DiCal-IDEA beide Optionen für die Schlüsseladressierung an. Sowohl DiCal-IDEA als auch BOSKrypt lassen zu, dass jeder Adresse ein eigener Schlüssel zugewiesen werden kann. Hier bleibt es dem Anwender überlassen, wie er die großen logistischen Hürden meistert, die Sicherheit der Schlüssel zu gewährleisten.

Sicheres Schlüsselmanagement

Das Schüsselmanagement an sich ist eine der größten Herausforderungen, wenn es um sichere Datenübertragung bei der Alarmierung geht. Es birgt einerseits das Risiko von Fehlern, andererseits von Sicherheitslücken. Swissphone bietet mit seiner Gesamtlösung aufeinander abgestimmte Produkte, die ein sicheres und zuverlässiges Verwalten der Schlüssel ermöglichen. Die Fernprogrammierungslösung ist ein Teil dieser Gesamtlösung, die sowohl das Schlüsselmanagement als auch die Fernkonfiguration der Melder fehlerfrei und sicher ermög-

licht. Durch die Zuordnung von Rechten und Rollen der Funkwarte gewährleistet die Leitstelle jederzeit, dass die Adressen mit den zugehörigen Schlüsseln programmiert und auch entsprechend im DAG hinterlegt werden. Zudem sind die Adressen und Schlüssel für niemanden ersichtlich. Die Übermittlung der Programmierdaten selbst geschieht Ende zu Ende verschlüsselt – von der Plattform bis zum Melder. Der Melder selbst ist durch ein Passwort geschützt, das nur das Fernprogrammiersystem kennt.

Zeitauthentifizierung

Auch wenn damit die Verschlüsselung möglichst sicher ist, muss immer noch sichergestellt werden, dass Sicherheitsmaßnahmen nicht übergangen werden können, z.B. durch das Aufnehmen und Wiedereinspielen von verschlüsselten Nachrichten zu einem späteren Zeitpunkt, das zur Auslösung von Falschalarmen führt.
Ein Vermeiden des Wiedereinspielens von Nachrichten bietet die Zeitauthentifizierung. Mit jeder verschlüsselten Nachricht wird gleichzeitig ein Zeitstempel mitgeschickt; die Nachricht wird nur dann dargestellt, wenn der Zeitstempel mit der Zeit auf dem Funkempfänger übereinstimmt. So wird ein Wiedereinspielen von Nachrichten verhindert.
Damit die Zeitauthentifizierung funktioniert, muss dem Melder regelmäßig über einen OAP-Befehl (OAP) ein Zeitstempel übermittelt werden. BOSKrypt sieht keine Spezifizierung des Setzens der Uhrzeit vor und überlässt dies stattdessen den Herstellern. Dabei ist es entscheidend, dass die Zeitsetzung verschlüsselt geschieht, weil sonst der Zeitstempel abgefangen und damit die Zeit auf allen Pagern falsch gestellt werden kann. In diesem Fall würde bei der Aktivierung der Zeitauthentifizierung gar kein Melder Nachrichten empfangen; das Netz wäre komplett sabotiert.

Klare Verantwortlichkeit

Diese voneinander abhängigen Elemente einer Verschlüsselung wirken sich auf die Zuverlässigkeit, Schnelligkeit und Sicherheit der Alarmierung aus. Sie sollten von Organisationen bei der Wahl einer Verschlüsselungsoption berücksichtigt werden. Bis heute gibt es in Alarmierungsnetzen keinen Mischbetrieb beider Verfahren. BOSKrypt wird seit kurzem nur in wenigen Netzen eingesetzt, daher fehlt eine Langzeiterfahrung. Als Systemanbieter übernimmt Swissphone die Verantwortung für die einwandfreie Funktion seiner Lösungen und im Markt erprobter Techniken und Verfahren.
Institutionen, die die Einführung einer Verschlüsselung planen, sollten aus Sicht von Swissphone ihre Alarmierungslösung ganzheitlich betrachten. Nicht die Wahl eines bestimmten Verfahrens entscheidet über ein sorgenfreies Verschlüsselungssystem, sondern vielmehr der sinnvolle Einbezug aller Komponenten der Alarmierungskette. Aus Sicht des Herstellers empfiehlt sich deshalb die Wahl eines Generalunternehmers, der das gesamte System, also Alarmierungsrechner (DAG), Funknetz (DAU) und Endgeräte (DME) sowie Verwaltungssoftware aus einer Hand liefert. Damit kann einerseits die Kompatibilität aller Netzkomponenten im Hinblick auf eine reibungslose Umsetzung vorausgesetzt und sichergestellt werden. Andererseits steht dem Betreiber ein einzelner Ansprechpartner zur Verfügung, sollte es tatsächlich einmal zu Fehlern oder Nichtalarmierungen kommen. *(bk)*

PMR-News

+++ Gemeinsam mit seinen Partnern hat **Airbus** das französische **Projekt LTE4PMR** (Long Term Evolution for Professional Mobile Radio) erfolgreich abgeschlossen. Das Entwicklungsergebnis des Projektes hat gezeigt, dass Polizeibeamte mit der von Airbus entwickelten Applikation für Gruppenkommunikation Tactilon Agnet über das neue LTE-System verschlüsselte Videos, Fotos und Daten übertragen können.
+++ SPIE baute im Landkreis Leipzig im zweiten Halbjahr 2018 das **digitale Alarmierungsnetz** aus. Durch die Erschließung sechs neuer Standorte in Naunhof, Borna, Deditzhöhe, Kühnitzsch, Podelwitz und Leipzig können Feuerwehr, Rettungsdienst und Katastrophenschutzeinheiten im Notfall zuverlässiger und schneller alarmiert werden.
+++ Neuer **Vorstandsvorsitzender des PMeV** ist Bernhard Klinger, Vice President Geschäftsentwicklung von Hytera Mobilfunk Deutschland. Der bisherige stellvertretende Vorsitzende folgt auf Dr. Klaus Hütten (e*Message), der nicht erneut kandidierte.
+++ Zum Schutz von Einsatzkräften und Bürgern sowie für eine optimierte Aufklärung von Straftaten stattet **Motorola Solutions** die Bundespolizei schrittweise mit **2.300 Videolautsprechermikrofonen Motorola Si500** mit integrierter Bodycam aus. Die intuitiv bedienbaren Lösungen ermöglichen eine zuverlässige Sprachkommunikation, Video- und Audioaufzeichnung sowie eine Bilderfassung. Die Videos und Fotos werden gesetzeskonform in digitale Beweissicherungssysteme hochgeladen.
+++ In der **Katwarn-App** werden nun Warnungen des modularen Warnsystems (MoWaS) des Bundes angezeigt. Die **Warn-App NINA** wiederum empfängt Meldungen des Warnsystems Katwarn. Durch die **wechselseitige Bereitstellung** sind Gefahrenmeldungen beider Systeme deutschlandweit verfügbar.
+++ Norwegen und Schweden sind weltweit die ersten Länder, die ein **grenzüberschreitendes Notfallkommunikationsnetz** betreiben und nutzen. Die Entwicklung des Inter-System-Interface-Projektes (ISI) startete 2016, am 1. Februar dieses Jahres wurde es live geschaltet. Die Leitstellentechnik kommt von Frequentis.
+++ Das **Ad-hoc-System ES-100** von **Hytera** bietet schnelle Funkversorgung im Katastrophenfall. Das Herzstück eines ES-100-Ad-hoc-Systems bildet ein Netz aus mindestens zwei E-pack-100-Einheiten, die Funkgerät, Repeater und Mesh-Netzknoten in nur einem Gerät vereinen.