Cryptographic Key Management for SCADA Systems, Issues and Perspectives

Ludovic Piètre-Cambacédès[1,2], Pascal Sitbon[1]
[1]*Electricité de France*, [2]*TELECOM ParisTech*
{ludovic.pietre-cambacedes, pascal.sitbon}@edf.fr

Abstract

This article focuses on cryptographic Key Management Systems (KMS) for SCADA systems environments. It first gives a generic view on the constraints, requirements and desired technical properties in SCADA contexts. Then, the most widespread solutions are presented, before discussing how they meet such conditions. The work done by different initiatives on this issue is also introduced. Finally, perspectives and research directions are proposed in consequence. The article aims at presenting open issues on the area, to foster discussion and research, according to the authors' view.

1. Introduction

The technical landscape of the electrical power infrastructure is changing considerably fast, driven by drastic market evolutions and the growing usage of information technologies. These changes directly impact the computer systems, generally referred as SCADA (Supervisory, Control and Data Acquisition) systems, which control and monitor its industrial components [1]. From closed, isolated and proprietary architectures, the systems are getting standardized and interconnected, allowing new functionalities and cost-effectiveness. Unfortunately, this also leads to new vulnerabilities, which, combined with evolving threats, turn SCADA cybersecurity into a priority and a permanent challenge [2].

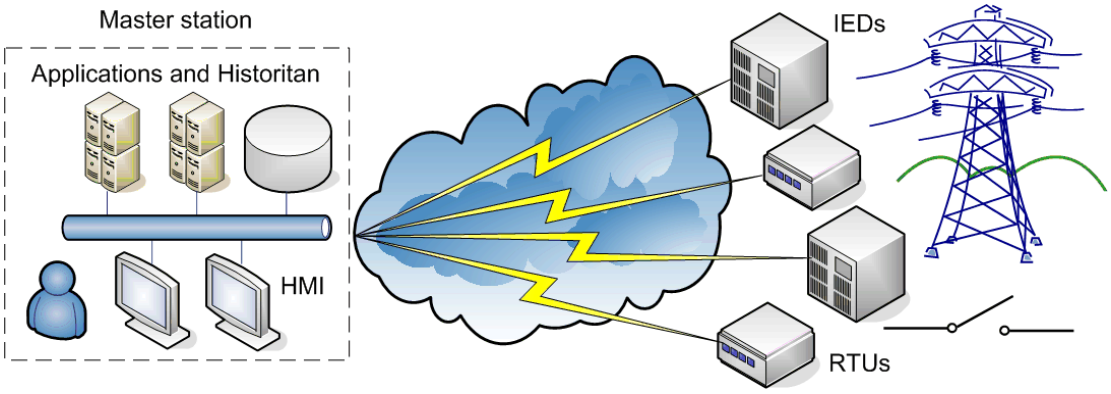
Cryptography has in this respect a major role to play. Nevertheless, encryption may be the "easy" part. If a lot is already under discussion about encryption or authentication for SCADA systems [3][4], most of the proposed mechanisms suppose keys already in place ; however, their management is still an open issue.

Section 2 defines briefly a typical SCADA architecture before identifying the specific constraints and characteristics impacting KMS. In section 3, the most used KMS solutions are presented and examined through the prism previously proposed. Section 4 sums up how different SCADA-related initiatives tackle the KMS issue. Section 5 identifies the remaining challenges and provides potential areas of investigation. Section 6 concludes the article.

2. SCADA systems context and specificities

A SCADA system can be globally seen as a central master system that monitors and controls a large set of remote points, spread-out over a wide area and generally called Remote Terminal Units (RTUs). RTUs can be, for example, circuit breaker controllers, voltage regulators or protective relaying devices, and usually locally control one or more actuators and sensors. HMI (Human Machine Interface), historian and support

applications at the master side provide information to operators in the control center to



make appropriate supervisory decisions, control actuators or readjust their parameters.

Figure 1. A simplified SCADA architecture

Secure communications are often required between master systems and RTUs. Information like open/close breaker orders or electrical measures for the grid global balance can be highly sensitive. Cryptography being more and more considered as an appropriate solution to ensure their authenticity and integrity, key management comes naturally into consideration. Key management implies different services such as generation, registration, distribution, installation, storage, retrieval, renewal, revocation, archiving or destruction [5].

SCADA systems have several characteristics that structure and make key management a non-trivial issue. For example, they can supervise thousands of remote points; Automatic Metering Infrastructures (AMIs) can imply millions. Table 1 proposes a view of the specific constraints, functional requirements and desired technical properties to consider when designing KMS [5][6][7]. They are not necessarily cumulative or systematic, but rather describe the general situation.

Table 1. Scada KMS constraints and desired properties

Short designation	Description
Environment/technical constraints	
Long life span	Long duration of industrial materials
Low resources	Limited CPU and memory resources
Proprietary technologies	Proprietary hard/software, protocols
Limited access	Difficult access for maintenance
Physical insecurity	No specific physical protection
Poor time synchronization	Poor time synchronisation
Long distance	Long distance between entities
Numerous entities	High number of entities
Low bandwidth	Low bandwidth channels
Latency	Latency / near-real time constraints
Asymmetric communications	E.g. master-slave protocols

Use of dialup	Use of dial-up modems
Little skills	Few cyber-security skilled personnel

Functional requirements	
High availability	Typically for control functions
Easy replacement	Replacement should be easily done
Malleability	Fit to divisions, take-overs…
Scalability	Management scalability
Desired technical properties	
Key authentication	Key authentication
Source authentication	Source authentication
Destination authentication	Destination authentication
Replay protection	Replay protection
Key freshness	Key freshness
Perfect Forward Secrecy	Perfect Forward Secrecy
Small number of messages	Few messages in KMS exchanges

3. A macroscopic key management survey

3.1. The four canonical KMS

In each case, the goal is to fix a short term session key KAB (or set of keys) between A and B to establish a secure channel.

3.1.1. A - Key-server based: Two variants exist, depending on K_{AB} generation: Key Distribution Center (KDC) and Key Translation Center (KTC) (see Fig. 2). In the first one, K_{AB} generation is done by a trusted KDC that is supposed to have pre-shared keys with A and B. A asks the KDC to generate K_{AB} (step 1). The KDC distributes K_{AB} to A and B using the pre shared-keys it shares with each entity (steps 2 and 3). K_{AB} can be distributed to B through A if the KDC does not have a direct access (step 3'). In the second variant, K_{AB} generation is done by the initiating entity. A enciphers K_{AB} with its key pre-shared with the KTC, and sends it to the KTC (step 1). This one deciphers it, and re-enciphers it with the key it shares with B. Finally, it the KTC can either forward it directly to B (step 2), or send it back to A, who transmits it to B (steps 2' and 3'). B deciphers it and gets K_{AB}.

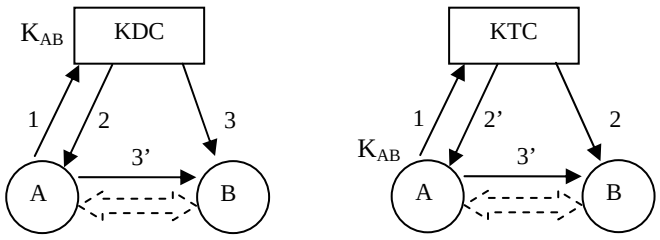


Figure 2. Key server based KMS

The first scheme was proposed by Needham-Schroeder [8] thirty years ago, and has been broken and fixed several times [9]. It has inspired a more robust system, Kerberos [10], based on time-stamped tickets and widely used today in its fifth version [11].

3.1.2. B - Point-to-point architectures: Such KMSs can be seen as sets of point-to-point trust relations, established on the basis of pre-shared symmetric long term keys. These long-term keys allow the establishment of temporal communication keys through automated negotiation. Classical exchanges suppose two or three passes (Fig. 3), offering unilateral or bilateral authentication. They imply the use of random numbers ("nonces") and/or time dependent parameters [5][12]. "Aggressive mode" can reduce exchanges to one-step processes. Repetition of this atomic structure can lead to hierarchical architectures, where each node can communicate with a limited set of nodes, hierarchically organized.

Figure 3. Point-to-point KMS

3.1.3. C – Standard PKI: Public Key Infrastructure (PKI) designates the set of components, protocols and procedures necessary to manage certificates and asymmetric keys lifecycles. The same services listed at the end of page 1 are offered, but in a way closely linked to the possibilities of asymmetric cryptography (public and private keys, off-line verification, etc.).

Figure 4. Key pairs generation and registration, before mutual authentication

A trusted entity, the Certification Authority (CA), is in charge of binding identity information with the public keys of communicating entities, into structures called certificates by electronic signature. The CA has itself a certificate, either self-signed (step 1), or signed by a higher rank CA. The CA private key is used to sign entity certificates during a preliminary registration process (steps 2, 2', 3, 3'). In this process, key pair are generated for the entities (by themselves or centrally) and the public key is signed by the CA and associated with their identity, after verification. The resulting structures are certificates, which can be used along with entities' private keys to authenticate them, establish keying material, etc.

PKIs are widely used and constitute a dominant paradigm of key management. Most of the PKI service and solution providers have adopted the X509v3 standard [13], and generally its PKIX derivation [14]. Web server authentication, electronic identity cards or passports, and numerous on-line applications rely on standardized PKI. PKIs are particularly adapted to open and distributed environments, and offer a natural hierarchical division of trust,

signatures and non-repudiation services. Unfortunately, X509 and PKIX are heavy and complicated [15], leading to implementation, interoperability and cost issues, especially for large deployments. Awkward naming, poorly efficient revocation systems, and high cryptographic computation costs are serious drawbacks of standard PKIs [16][17].

3.1.4. D - "Customized" PKI: PKI can be "customized" for specific environments. For instance, revocation can be based on fast expiration instead of Certificate Revocation Lists [14]; the control over entities offered by SCADA environments can also allow simplified naming systems and certificate formats. Nevertheless, the difficulty to design secure systems out of the scrutinized standard world should not be under evaluated. Evolution, interoperability and maintenance costs should also be considered.

3.2. KMS comparison for SCADA systems

The Key Management System families A, B, C and D meet differently Table 1 elements. Table 2 proposes a comparison along those criteria, with the following convention: "--" means that the considered solution is strongly inappropriate to meet the given criteria or property, "-" corresponds to "rather inappropriate", an empty box indicates a neutral impact, "+" and "++" correspond respectively to appropriate and strongly appropriate solutions. Brackets are used when the given evaluation applies only for specific implementations. Note that this evaluation is based on the authors' general experience and views, not on objective and dedicated experimentations or tests.

Table 2. Comparison of the four KMS families

	A	B	C	D
Long life span	+	+	(-)	(-)
Low resources		++	-	-
Adapt to proprietary technologies		++		++
Physical entities insecurity			-	-
Poor time synchronisation	(-)	(-)	-	
Numerous entities		--	--	-
Low bandwidth	-	+	-	(-)
Latency sensibility			-	-
Asymmetric communications	-			
Use of dialup	--	+		
High availability	-			(+)
Easy replacement	+	+	-	(-)
Malleability	-	+		
Management scalability		-		
Little cyber-security skills			--	(--)
Key authentication	+	(+)	+	+
Source authentication	+	+	+	+
Destination authentication	+	+	+	+
Replay protection	+	(+)	+	+
Key freshness	+	(+)	(+)	(+)

Perfect Forward Secrecy	+	(+)	(+)	(+)
Small number of KMS messages	--	+		

3.3. Good old ways for SCADA KMS?

Following a straightforward negative vs. positive evaluation count for each KMS in Table 2, PKI-based KMS (C, D) should be considered carefully whereas symmetric key KMS (A, B) seem more attractive. However, best-practices should apply as recommended and summarized in [18]. Moreover, RFC4107 [7] helps in choosing between automatic and manual KMS. Although the first option is strongly recommended in [7], it indicates that a manual approach can be suitable in cases sharing similarities with SCADA contexts. Data values and deployment scales can limit this option relevance.

4. KMS in power industry initiatives

The following section provides an overview on how the key management issue is presently being addressed in different relevant SCADA cyber security initiatives.

4.1. IEC TC57 WG15 work and choices – IEC 62351

Working Group 15 of Technical Committee 57 of the International Electrotechnical Commission (IEC) develops standards for end-to-end cyber-security of the electric system, in particular for the communication protocols defined within TC 57. This refers to the 60870-5, -6, 61850, 61968 and 61970 IEC standard series. The results are regrouped under a Technical Specification [3], presently divided into 7 parts. Reference [19] provides an overview of the work already accomplished. No general KMS has been specified, but related design choices for security mechanisms partly define key management aspects.

Table 3. Key management aspects of IEC 62351

62351 part	*Security mechanism*	*Key management aspects*
Part 3: TCP/IP Profiles	SSL/TLS with specific parameters	Suppose an x509 PKI; CA considerations are explicitly given. The use of self-signed certificates is not specified.
Part 4: MMS Profiles	Electronic certificates	All profiles imply the use of a standard x509 PKI.
Part 5: 60870-5 Profiles	Challenge-response authentication	Two levels of symmetric keys: Session keys, and Update keys to change the former ones, and supposed pre-shared by an unspecified mechanism
Part 6: 61850 Profiles	Digital signatures	For non-routable profiles that have strong time constraints (< 4 ms), specific digital signature authentication is proposed, with specific client certificates, and optional server certificates.

4.2. DNP3 User Group - Secure DNP3 v1.0

The secure version of DNP3, a widely used protocol in the North American power grid, is developed by the DNP User Group. Version 1 of the specifications was released in 2007 [20] and it is similar to IEC62351 part 5. A two-level key scheme ensures user and data authentication for the DNP3 protocol. A long-term key is supposed to be pre-shared between the entities. Some future work may specify a KMS to do so, but today this is left to user responsibility.

4.3. The IEEE P1689 draft

The IEEE Power Engineering Society Substations Committee is currently working on P1689, a "Trial Use Standard for Retrofit Cyber Security of Serial SCADA Links and IED Remote Access". It uses Cryptographic Modules (CM) to ensure message authentication and maintenance CM to secure the related ports. Annex gives KMS functional requirements [4].

4.4. Smart meters initiatives

Smart meters leverage information technologies to optimize metering processes and new services. Italy has already rolled out 27 million units, but others large deployments are on their way in the USA or in Europe [21]. Recently, a dedicated security engineering task force, called AMI-SEC, has been created in the USA to produce common security specifications for utilities, that may include KMS aspects, presently studied [22]. For example, reference [23] compares classical solutions before devising an original symmetrical key distribution system.

5. Challenges and technical perspectives

5.1. Room for specific SCADA KMS?

Besides the initiatives previously discussed, several specifically designed KMS have been proposed. In 2002, the US Sandia National Labs proposed a hybrid of B and D KMS [24]. Sandia has also integrated a KMS proprietary solution to a G.E. SCADA [25]. In 2006, Dawson et al. proposed "A Key Management Architecture for SCADA Systems" [6], close to KMS A. Unfortunately, these solutions do not meet all Table 1 criteria, and none have led to real deployments.

5.2. Some technical perspectives

5.2.1. ECC and the key size debate: When asymmetric cryptography is considered, Elliptic Curves Cryptography (ECC) emerges as an interesting alternative to RSA for SCADA environments [24][26]. With smaller required key sizes, it appears more suited for low resources and low bandwidth contexts [27]. Regarding the key size question, several SCADA characteristics have contradictory influences: for example, limited computation power and time constraints tend to limit key size, whereas the long lives of industrial equipment would argue for longer keys. Risk analysis, serious references (e.g. [28]) and national agencies' recommendations should be used.

5.2.2. Low-computational cost and zero-knowledge authentication algorithms: Recently standardized protocols like GPS1, GPS2, GQ or GQ2 [12] should also be

considered, due to their low computational cost and their zero-knowledge properties [29]. The distribution of the initial keying material may still constitute an issue.

5.2.3. Password Authenticated Key Exchange (PAKE) protocols: PAKE protocols are based on passwords (weak secrets), allowing the negotiation of one or several strong secrets (cryptographic keys) used to authenticate the exchange and other uses. Contrary to traditional password mechanisms, they cannot be brute-forced. They have recently been standardized [5]; one of them, SRP, is already widely available for applications like TLS, SSH and telnet [30]. PAKE protocols are not KMS, but may substitute the secure key distribution problem by a password management problem, which could be easier for Utilities.

5.2.4. Smartcards: Smartcard microprocessors are a cost-efficient and secure way to implement cryptographic algorithms; they can protect cryptographic key material and provide trustable security services in communication architectures. It would make a lot of sense to introduce their use in SCADA environment for field devices, including for machine-to-machine authentication and integrity protection mechanisms. The idea have already been introduced for industrial plant network communications [31][32][33][34] and may be transferable quite directly in SCADA systems context.

5.2.5. Key management for sensor networks, a pertinent source of inspiration: There are two simple reasons for this statement: first, sensor networks can be part of SCADA systems; secondly, some of their design constraints are very similar, in particular, CPU or memory limitations, high numbers of nodes, and proprietary hard/software. Wireless sensor network (WSN) constraints tend to be even closer. Research efforts on KMS for WSN are prolific, with ideas that could find their way into the SCADA domain. Approaches based on delayed key disclosure like TESLA [35] have been punctually studied for SCADA [36] or considered for AMI [23], but the potential remains unexploited. Variants such as SPINS protocols [37], key agreements using identity-based cryptography [38][39], SECK [40] and many more should be considered. Camtepe et al. [41] gives a survey of key distribution for WSN, but a closer look would definitely be worth the effort. Alcaraz et al. [42] classifies them and gives useful selection criteria.

6. Conclusion

If no unique “one-size-fits-all” solution exists, this paper gives some generic characteristics and constraints to choose or design appropriate KMS for SCADA contexts. None of the four canonical families examined appear to be adequate, even if symmetric key based options may have a slight advantage in our analysis on a good-engineering practices point of view. To our knowledge, the most concerned standardization bodies and initiatives have not yet achieved convincing results or real-world deployments on this issue. This article has pointed out the main difficulties to address but also has opened the discussion to adjacent security domains, like WSN, ECC or PAKE protocols, bringing new technical perspectives and inspiration to design appropriate SCADA Key Management Systems.

7. References

[1] Ronald L. Krutz, Securing Scada Systems (1st ed.), John Wiley & Sons, 2005, ISBN 0764597876, pp.1-22.

[2] US General Accounting Office, Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems, Report to Congress, GAO-04-354, 2004.

[3] IEC (International Electrotechnical Commission), Power system control & associated communications - Data & communication security, IEC62351 part 1 to 7, Technical Specification, 2007.

[4] IEEE (Institute of Electrical and Electronics Engineers), Trial Use Std. for Retrofit Cyber Security of Serial SCADA Links and IED Remote Access, P1689, Draft, 2007.

[5] IEC/ISO, IT Security techniques - Key management, IEC/ISO11770, International Standard.

[6] R. Dawson, C. Boyd, E. Dawson and JMG. Nieto, "SKMA, A Key Management Architecture for SCADA Systems", Proc. of the AISW-NetSec workshop, ACM, 2006.

[7] S. Bellovin, R. Housley, "Guidelines for Cryptographic Key Management", RFC 4107, IETF, 2005.

[8] R. Needham, M. Schroeder, "Using Encryption for Authentication in Large Networks of Computers" Communications of the ACM, Vol. 21, pp. 993-999, 1978.

[9] G. Lowe, "An attack on the Needham-Schroeder public key authentication protocol", Information Processing Letters, vol. 56(3), pp. 131-136, 1995.

[10] B. C. Neuman, Theodore Ts'o, "Kerberos: An Authentication Service for Computer Networks", IEEE Communications, volume 32/9, pp33–38, 1994.

[11] C. Neuman, T. Yu, S. Hartman, , K. Raeburn, "The Kerberos Network Authentication Service (V5)", RFC 4120, IETF, 2005.

[12] IEC/ISO, IT - Security techniques - Entity authentication, IEC/ISO9798-5:2004, International Standard.

[13] ITU (International Telecommunication Union), "Information Technology - Open Systems Interconnection - The Directory: Authentication Framework", ITU-T Recommendation X.509, 2005.

[14] IETF, PKIX Charter Requests For Comments (RFCs), http://www.ietf.org/html.charters/pkix-charter.html

[15] P. Gutmann, X509 Style Guide, October 2000, http://www.cs.auckland.ac.nz/~pgut001/

[16] N. Ferguson, B. Schneier, Practical Cryptography (1st ed.), Wiley, ISBN 0471223573, pp. 315-345, 2003.

[17] P. Gutmann, "Everything you never wanted to know about PKI but have been forced to find out", 2001, http://www.cs.auckland.ac.nz/~pgut001/pubs/pkitutorial.pdf

[18] B. Kaliski, "Learning to SKI Again: The Renaissance of Symmetric Key Infrastructures", Proc. RSA Conference, San Francisco, USA, 2007.

[19] L. Piètre-Cambacédès, C. Chalhoub, F. Cleveland, "IEC TC57 WG15 – Cyber security standards for the power system", Proc. of CIGRE D2 Colloquium, Luzern, 2007.

[20] DNP User Group, Secure DNP3 specifications, DNP User Group Library (www.dnp.org), 2007.

[21] J. Lund, "Learning from European Advanced Metering Deployments", Utility Automation & Engineering, June 2007

[22] EnerNex corporate communications, "EnerNex Announces Formation of AMI-SEC Task Force", Oct. 2007.

[23] G. Gilchrist & D. Highfill, "Key Management and Cryptography for Advanced Metering Infrastructures (AMI) and Other Large, Low Power Networks", Proc. of the S4 2008 Conference, Miami, 2008.

[24] C. Beaver, D. Gallup, W. Neumann & Torgerson M., "Key management for SCADA", Technical Report SAND2001-3252, Sandia National Laboratories, 2002.

[25] D. Holstein, J. Tengdin, J. Wack, R. Butler, T. Draelos, P. Blomgren, Cyber Security for Utility Operations, NETL Project M63SNL34, Final Report, 2005.

[26] Robert J. Lambert, "ECC and SCADA Key Management", S4 (SCADA Security Scientific Symposium) Conference, Digital Bond ed., 2007.

[27] S. Hankerson, A. Menezes, Guide to Elliptic Curve Cryptography, Springer-Verlag, Berlin, Germany, 2004.

[28] ECRYPT (European Network of Excellence in Cryptology), ECRYPT Yearly Report on Algorithms and Keysizes (D.SPA.10), ECRYPT IST European Project, 2005.

[29] Jean-Jacques Quisquater, Louis C. Guillou, Thomas A. Berson, "How to Explain Zero-Knowledge Protocols to Your Children", Proc. of Crypto '89, Springer, pp..628-631, 1990.

[30] T. Wu, "The SRP Authentication and Key Exchange System", RFC 2945, IETF, 2000.

[31] P. Palensky and T. Sauter, “Security considerations for FAN-Internet connections,” in Proc. IEEE Workshop on Factory Communication Systems, Porto, pp. 27–35, 2000.

[32] T. Sauter and Ch. Schwaiger, “Achievement of secure Internet access to fieldbus systems”, Microprocessors and Microsystems Journal, Elsevier, Vol. 26, Issue 7, 2002.

[33] C. Schwaiger and A. Treytl, “Smart card based security for Fieldbus systems”, in Proc. International IEEE Conference Emerging Technologies and Factory Automation 2003 (ETFA’03), vol. 1, pp. 398–406, 2003.

[34] M. Lobashov, G. Pratl, and T. Sauter, “Implications of power-line communication on distributed data acquisition and control systems”, in Proc. International IEEE Conference Emerging Technologies and Factory Automation 2003 (ETFA’03), vol. 2, pp. 607–613, 2003.

[35] A. Perrig, R. Canetti, J. Tygar & D. Song, “Efficient authentication and signing of multicast streams over lossy channels”, Proc. of the IEEE S&P Symp., IEEE CS, 2000.

[36] Y. Wang, B. Chu, “sSCADA: Securing SCADA Infrastructure Communications”, IACR Eprint, 2004.

[37] A. Perrig, R. Szewczyk, V. Wen, D. Culler and J. Tygar, “Spins: Security protocols for sensor networks”, Wireless Networks Journal (WINE), September 2002.

[38] G. Yang, C. Rong, C. Veigner, J. Wang, and H. Cheng, “Identity-Based Key Agreement and Encryption for Wireless Sensor Networks”, IJCSNS International Journal of Computer Science and Network Security, Vol.6 No.5B, 2006.

[39] D. Boneh, M. Franklin, “Identity-based encryption from the weil pairing”, Proceedings of CRYPTO’01, Springer, 2001.

[40] M. Chorzempa, J-M. Park, M.Eltoweissy, “Key management for long-lived sensor networks in hostile environments”, ACM Computer Communications, Volume 30, Issue 9, pp. 1964-1979, 2007.

[41] A. Camtepe, B. Yener, “Key distribution mechanisms for wireless sensor networks: a survey”, Technical Report 05-07, Rensselaer Polytechnic Institute, 2005.

[42] C. Alcaraz & R. Roman, “Applying Key Infrastructures for Sensor Networks in CIP/CIIP Scenarios”, Proceedings of CRITIS’06 Conference, Springer, 2006.

Authors

Ludovic Piètre-Cambacédès has been working as a research-engineer on computer security at Electricité de France (EDF) since 2001. He’s particularly involved in architecture and technical recommendations for the cyber security of EDF critical infrastructures. He has taken part in different European research projects and contributes as an expert to several normative and collaborative international initiatives fostering cyber security for power utilities (e.g. CIGRE, IAEA or IEC).

Pascal, CISSP, ISO27001 Lead Auditor, graduated from ENSIMAG, a French Grande Ecole (equivalent of MS in Computer Science), has 10 years of experience in IT, including 7 years in IT security. His main interests are IT security, including technical, organizational as well as management themes, and Industrial Control Systems. He is currently working at EDF R&D as a cyber security expert and research engineer.