Chapter 8
Standardisation and Deployment

8.1 Introduction

Following the discussion of the components of the Autonomic Cooperative System Architectural Model (ACSAM) in the prior chapters, especially including the Autonomic Cooperative Networking Protocol (ACNP) along with its pertinent Autonomic Cooperative Behaviour (ACB), as well as complemented with the aspects of implementation and simulation, this chapter is intended to provide the relevant insight into the field of standardisation and deployment. To this end, certain concepts of interest are analysed and the contents is structured in such a way that it opens with more standardisation orientated elements while towards the end it naturally becomes rather shifted towards the issue of deployment. Both the components appear to be sufficiently balanced thanks to the aspect of architectural commonalities. In particular, first of all the question of the Autonomic Future Internet is discussed with a special emphasis being put on the related standardisation within the Industry Specification Group (ISG) on Autonomic network engineering for the self-managing Future Internet (AFI), functioning under the auspices of the European Telecommunications Standards Institute (ETSI). Then, the Machine-to-Machine (M2M) communications are analysed also based on the ETSI standardisation efforts and the concept of Software Defined Networking (SDN) follows, which shifts the focus a little bit towards deployment aspects. After this turning point, both the Emergency Systems and Vehicular Networks are brought up, to outline certain architectural elements as viewed from the deployment angle.

8.2 Autonomic Future Internet

The Future Internet is becoming one of the most desirable concepts, sought after by various research and development communities. The interest in this topic, being substantial, seems at least steady if not rapidly increasing, most likely due

M. Wódczak, *Autonomic Computing Enabled Cooperative Networked Design*,
SpringerBriefs in Computer Science, DOI 10.1007/978-1-4939-0764-9_8,

to the fact that referring to the future in the very name of the said concept makes it appear continually evolvable and open-ended. This way the drive for innovation is continuous and a wide variety of different incarnations of the Future Internet are being put forward. Essentially, as the foreseen number of devices to be interconnected worldwide is expected to grow more and more drastically, the proposed Autonomic Cooperative System Architectural Model (ACSAM) advocates for a completely autonomic design, allowing for full self-manageability. In fact, as outlined in this book, the notion of self-management is perceived as the key enabler for the instantiation of efficient networking, and the cooperative one in particular. Clearly, given the availability of the enormous addressing space offered by IPv6, it is claimed that the Internet of Things (IoT) will enable virtually any networked element to feature its own Internet Protocol (IP) address. Thus, the density of communication-ready devices will most obviously translate into low power transmission schemes, potentially making the way not only for the Autonomic Cooperative Behaviour (ACB) based Autonomic Cooperative Networking Protocol (ACNP) but the whole ACSAM. To this end, however, a strong standardisation orientated effort in indispensable.

Such an effort has been accordingly undertaken by the Industry Specification Group (ISG) on Autonomic network engineering for the self-managing Future Internet (AFI), operating under the auspices of the European Telecommunications Standards Institute (ETSI) [2].[1] As such, the ETSI ISG AFI was established in response to a commonly agreed consensus that both the prior developments and concepts, as well as the numerous efforts ongoing at that time, intended to achieve the very identical goal of instantiating autonomic and self-managing networking, urgently demanded the relevant dose of harmonisation in the context of the rapidly progressing and advancing design of the Future Internet [18]. Given the above background and reasoning, the structure of the ETSI ISG AFI was arranged according to specific Work Items (WIs) being the basis for the preparation of the ETSI Group Specifications (GSs), to be further upgraded to the ETSI Technical Specifications (TSs). Looking from the present perspective, thus far, the ETSI ISG AFI has finalised the first two ground-laying WIs outlining the scenarios, use cases, and requirements for autonomic/self-managing Future Internet [5], as well as defining an architectural reference model for autonomic networking, cognitive networking, and self-management as required by autonomic network engineering for the self-managing Future Internet [6]. Given the completion of the cited ETSI Work Items, the AFI continues the standardisation process in the area of autonomic reference architectures, analysis of requirements, and specification of implementation-oriented solutions [18].

In particular, the third Work Item was created which is subdivided into the following branches under the titles of “Autonomicity-enabled NGN Reference Architecture (fixed/wired networks)”, “Autonomicity-enabled Broadband

[1] In fact, since its very co-founding, the author of this book has been actively serving as a Vice-Chairman and Rapporteur of ETSI ISG AFI.

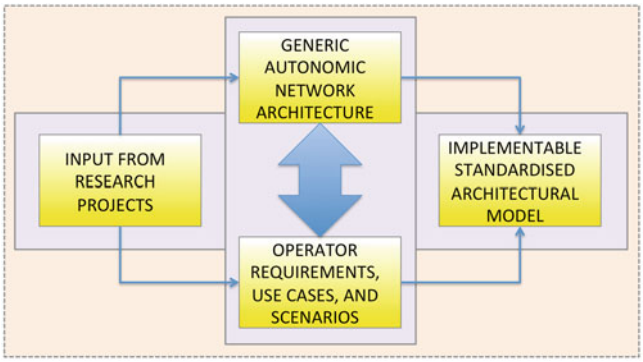

Fig. 8.1 AFI standardisation

Forum (BBF) Reference Architecture", "Autonomicity-enabled Mobile Network Architecture (3GPP and Non-3GPP)", as well as "Autonomicity-enabled Wireless Ad-Hoc/Mesh/Sensor Network Architecture".[2,3] Given the fact that the ETSI ISG AFI effort is becoming more and more widespread, certain standardisation methodology was assumed by the body itself [18]. Such a methodology may be perceived a result of the general context of research projects the ETSI ISG AFI was set in from the very outset, as originally it was spawned by the European Union Framework Programme Seven (EU FP7) project on Exposing the Features in IP version Six protocols that can be exploited/extended for the purposes of designing/building Autonomic Networks and Services (EFIPSANS). Consequently, as depicted in Fig. 8.1, the input from the said research projects is welcomed to contribute to the refinement of the Generic Autonomic Network Architecture, as well as the operator requirements, use cases, and scenarios, through a tight interaction between the two relevant WIs. Following, an implementable standardised architectural model is being devised as the main and most comprehensive outcome. In fact, the whole book contains the author's contribution to the instantiation of such a model in the form of ACSAM. The reader is referred to previous chapters for the explanation of the original workings of GANA along with the proposed extensions.

[2]The author of this book serves as the Rapporteur of ETSI on the "Autonomicity-enabled Wireless Ad-Hoc/Mesh/Sensor Network Architecture".

[3]As mentioned before, currently, the word "autonomicity" does not seem to exist in the dictionaries of the English language. For this reason, even though this word is now being coined within the ETSI ISG AFI, the author of this book personally avoids using it apart from the officially cited titles of the GSs-to-be. Apart from linguistic purity, however, there indeed appears to exist a semantic gap in this respect and this word might gain common approval much sooner than expected.

8.3 Machine-to-Machine

Going further into the realm of automation it transpires that, most obviously, autonomic networking has much more to do with the concept of the Machine-to-Machine (M2M) system than anybody could expect, at least from the architectural perspective being the main theme of this book. In fact, based on the definition provided by ETSI, the M2M communication is established between two or among more entities and it is assumed to be organised without a need for any direct human intervention [7]. What is more, as the related M2M services are to automate the relevant decision making and communication processes, the overall concept falls immediately in line with the already explained paradigm of self-manageability, resembling the operation of the human Autonomic Nervous System (ANS), so inherent in autonomic networking [18]. Such a characteristic feature is especially important in the case of highly complex networked systems, where the network nodes might be represented by M2M devices, and where automation is the only way forward in terms of a sustainable and durable system operation. The main components of an M2M system may be decomposed into the ones belonging with the M2M Device and Gateway, as well as the ones belonging with the M2M Network [8]. While typically an M2M Device would connect to the network over a Gateway, a direct connection is also possible, as long as the proper functionality is properly implemented. The two network related functional blocks deal with interconnectivity, as opposed to the service layer providing all the abstraction required for M2M Applications.

In particular, it is assumed that the primary function of a Machine-to-Machine Device is to execute the said Machine-to-Machine Applications on the basis of service capabilities such as certain common functions to be shared after having been exposed through open interfaces, with the aid of the core network functionality. Yet, at the same time, it is expected that the workings of the networked parts of the Machine-to-Machine system be hidden, on its both ends, i.e. the M2M Device and Gateway, as well as the M2M Network related ones, where the M2M Applications are residing, as indicated in the latest ETSI Technical Specification of the Machine-to-Machine functional architecture [8]. Originally, apart from the collaborative approach to be introduced in the following paragraphs, there are two aforementioned legacy connection modes. The main difference between the two consists in the registration, authentication, authorisation, management, and provisioning procedures taking place either directly or with the aid of the Gateway acting as a Proxy. Interestingly, the networked part pertaining to the M2M Device and Gateway side is denoted as M2M Area Network which may employ technologies ranging from Personal Area Networks (PANs) to Local Area Networks (LANs). The Access Network, in turn, may include both wired and wireless technologies, while the Core Network is responsible for IP connectivity, roaming, service and network control functions, as well as interconnection with other networks [8].

As proposed in Fig. 8.2, describing a modified Machine-to-Machine functional architecture, it appears that it would readily accommodate the idea of collaborative transmission which could be taking place mostly between or among the M2M Cooperative Gateways providing the connectivity for the M2M Devices over the M2M Access and Core network. This way, not only would the M2M Gateways become capable of expressing the Autonomic Cooperative Behaviour, but, what is more, the M2M Devices implementing the Gateway functionality could express their willingness to carry and forward traffic. All this remains very much in line with the instantiation of autonomics by means of the Autonomic Cooperative Networking Protocol, as advocated for earlier in this book. Certainly, entering Autonomic Cooperative Behaviour would mean the necessity for the M2M Devices or Gateways to implement the functionality of Autonomic Cooperative Nodes so that the whole set-up could work under the umbrella of the Autonomic Cooperative System Architectural Model. In particular, it looking at the variety of the use cases defined for Machine-to-Machine communications [7], this technology may go hand-in-hand with the Internet of Things, referred to in the previous section, or, at least, become one of its key enablers. This is mostly so because, similarly to the Autonomic Future Internet, the rationale behind Machine-to-Machine is quite generic making both approaches, in some sense, technology agnostic and, thus, highly interoperable, especially when the architectural models are concerned.

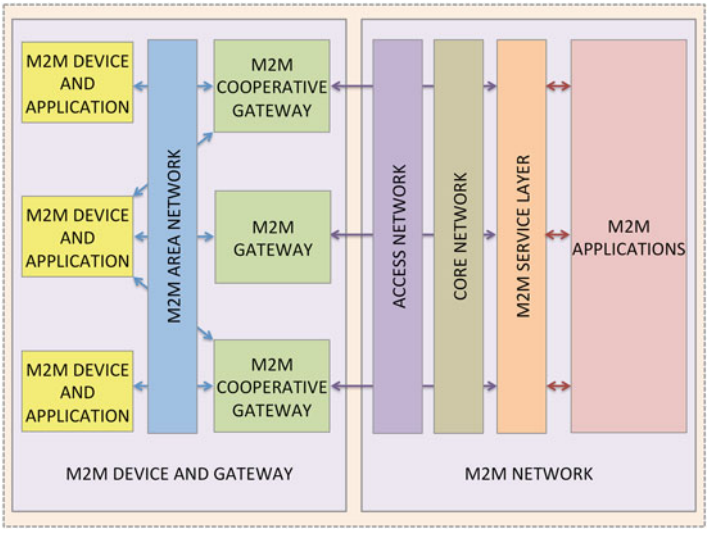

Fig. 8.2 M2M functional architecture with ACB

8.4 Software Defined Networking

Given the already mentioned complexity of the current and future networked systems, quite expectedly, there are other technologies developed entirely with the intention of taking the human out of the configuration and management processes to the highest possible extent, thereby increasing the overall stability and scalability of such advanced designs. Once again, following the rationale behind the Machine-to-Machine and, most importantly, very much as it is the case for autonomics itself, also the concept of Software Defined Networking (SDN) emphasises the fact that the distributed character of today's systems demands certain dose of an urgent intervention in terms facilitating their configurability, not to even mention the related manageability. The reason for such a need may be fairly easily explained on the basis that nowadays the most sophisticated policies and tasks might still be implemented only with the use of the legacy Command Line Interface (CLI), allowing, at most, for the use of a limited set of low-level device configuration directives [9]. Even if it was possible to perform the overall configuration in such a way, the changing state of the continually evolving networked system would still remain not properly addressed. A while ago such a problem seemed to have been solvable with the aid of introducing some automation with the aid of the so-called dynamic scripting approaches but, apparently, taking into account the technological progress, it may no longer be the case.

Most likely, this is why, the concept of Software Defined Networking has emerged most recently to gain a potentially unprecedentedly rapid growth in interest. This technology assumes the separation of both the data plane and the control plane in the current understanding [9]. In other words, the behaviour of the whole network is expected to be, not only orchestrated but, in fact, dictated by a central software programme, referred to as the controller, and assuming the role of the system brain, operating in the very control plane. At the same time, all the other network nodes are becoming basic packet forwarding devices, functioning in the data plane, in turn. Interesting and appealing as it might be, the concept of Software Defined Networking, at least at first sight, might not immediately and straightforwardly integrate into the reasoning stemming from the Generic Autonomic Network Architecture (GANA). Such a risk could result from the fact that while SDN clearly advocates for a centralised approach, the GANA Reference Architecture is, quite the contrary, highly distributed, just like the pre-SDN solutions. This issue may be addressed with the aid of making certain formal alignments between both the GANA and SDN frameworks [3]. As far a the former is concerned, there already exist elevated nodes of the network level type, according to the assumed abstraction, orchestrating their pertinent network domains, while the latter would need to maintain network segmentation with the aid of domain controllers. Given such an assumption, certain simplification to GANA may be proposed, too.

In particular, the programmability offered by SDN comes in handy allowing for run-time software composition. In other words, the elevated Autonomic Cooperative Nodes (ACNs), each assuming the functionality of a controller, may be entitled to execute more complicated programmes in order to fulfil the requirements of the Autonomic Cooperative System Architectural Model (ACSAM), communicated through Autonomic Cooperative Networking Protocol (ACNP). As outlined in Fig. 8.3, in the case of such an SDN-enabled Autonomic Cooperative System Architectural Model, the functionality of plain Autonomic Nodes (ANs) is proposed to be limited up to the function level of the GANA abstraction, while for the Autonomic Cooperative Nodes, intended to express the Autonomic Cooperative Behaviour, the full four-level abstraction would be maintained. In fact, the number of the available levels of abstraction could be part of the said programmability, and once promoted to the role of ACN, the functionality of an AN would become autonomically elevated, which, potentially, would be also the case the other way round. Such a change of role could be triggered by a dynamic network reconfiguration caused, for example, by some external policy-related factors, or be conditioned by an internal shift resulting from the willingness to carry and forward traffic parameter of the Optimised Link State Routing (OLSR) protocol, being the basis for the Autonomic Cooperative Networking Protocol.

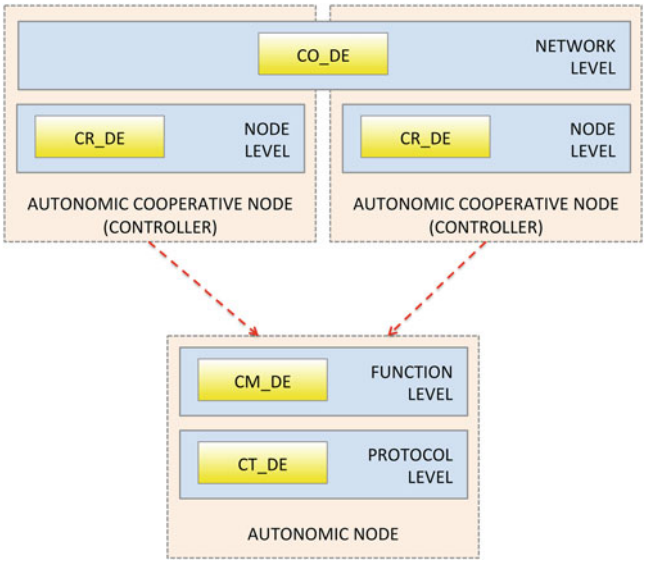

Fig. 8.3 SDN and ACB

8.5 Emergency Systems

Moving a bit from the being standardised architectural components towards a more deployment related context, it appears impossible not to discern the importance of the latest advancement in the development of the novel infrastructure for the emergency system of the future [1]. It is especially conspicuous in the ad hoc or mesh part of such a system, where the devices carried by the First Responders (FRs) seek seamless and on-demand connectivity [12]. For this very reason, emergency networks, formed by such FRs operating in the area of incident, seem to have become a very relevant field for the application of the previously introduced concepts related to the Autonomic Cooperative System Architectural Model (ACSAM). It especially holds true for numerous small groups of FRs, coordinated by their respective Chief First Responders (CFRs), as there appears to arise a correspondence between the topics of human resource and network resource management [11]. Such groups may be assumed to contain from four through six FRs which immediately translates into the following options when the preferred network topology is concerned [14]. In particular, as the FRs would normally gather around the CFR and, most naturally, form the topology of a star, a multi-hop communication between the CFR and its FRs might not be the predominant case. On the other hand, the possibility of instantiating the multi-hop communication cannot be obviously excluded, especially when a group of FRs is more spread apart by forming almost a line. What is more, the option of having bigger or merging and splitting trams of FRs might be more realistic than expected [17].

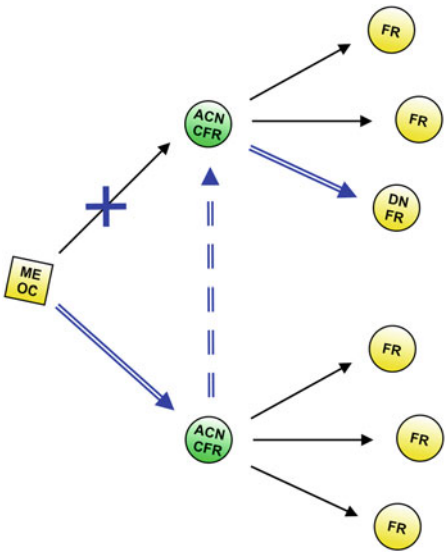

Fig. 8.4 Supportive cooperation between CFRs acting as ACNs

This brings about the question of how such a system should be orchestrated given the harsh characteristics of the environment it is expected to operate in [15]. In principle, the implementation of the Autonomic Cooperative System Architectural Model, supported by the inclusion of the Autonomic Cooperative Networking Protocol and Autonomic Cooperative Behaviour, seems to be the proper way forward. In fact, one should note that, apart from CFRs and FRs, there also exist both the Emergency Operations Centre (EOC) and the Mobile Emergency Operations Centre (MEOC). While the former is located at a fixed site, the latter is mobile so that it can be relocated to the area of incident. As a result, the cooperation between or among CFRs may be perceived from both the angle of supportive and collaborative protocols, as introduced and defined in Sect. 4.2. Looking from the supportive action perspective, it is typically assumed that the process of communication between two FRs belonging to two separate FR teams would be assisted solely by their respective CFRs, communicating not directly but over the MEOC, as outlined in Fig. 8.4. Such an assumption would need to be relaxed as there may appear a potential lack of communication with the Mobile Emergency Operations Centre, even though such a case would be presumably rare. Moreover, for legacy reasons, related to the hierarchy of a consolidated management of distinct FR teams, it would be required that solely a given CFR can communicate and, thus, route the data coming from the Emergency Operations Centre towards a given FR team.

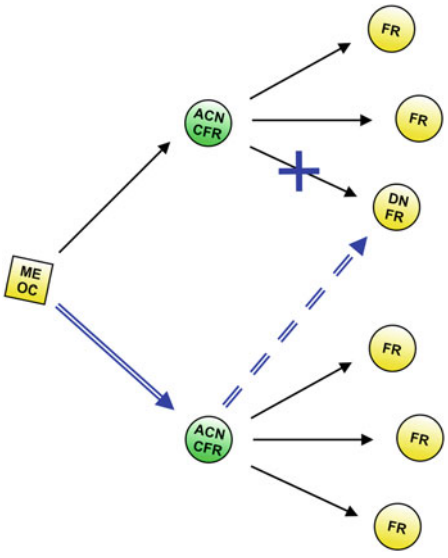

Fig. 8.5 Back-up operation of supporting CFR

From the Autonomic Cooperative System Architectural Model perspective, however, there are no clear arguments against the establishment of a logical

connection over another CFR, as long as such an operation remains transparent to the system, making the human hierarchy look as if nothing had changed. In fact, as outlined in Fig. 8.5, should one of the CFRs be unable to communicate with its FRs, the system would offer support through the autonomic switching to a back-up mode, where another CFR could be exploited as an intermediary entity, allowing for communication with MEOC. In fact, to enable switching between different operation modes, not only would it be necessary to monitor the links between CFRs and their corresponding FRs, but the system would need to be autonomically notified about a potential availability of another CFR to serve the FR or FRs not belonging to his own team [17]. Having the relevant global data related to the network parameters, MEOC would even have some leeway to arrange for collaboration still before link degradation occurs, making the use of the Cooperative Re-Routing Decision Element CR_DE, working closely with the Resilience and Survivability Decision Element RS_DE, as well as the Fault Management Decision Element FM_DE, according to the logic described in Sect. 6.5 [16]. Such an assistance of an external CFR in the communication between MEOC and a given FR, done by means of instantiating the Autonomic Cooperative Behaviour, in a way transparent to the system and not affecting the hierarchy, is presented in Fig. 8.6.

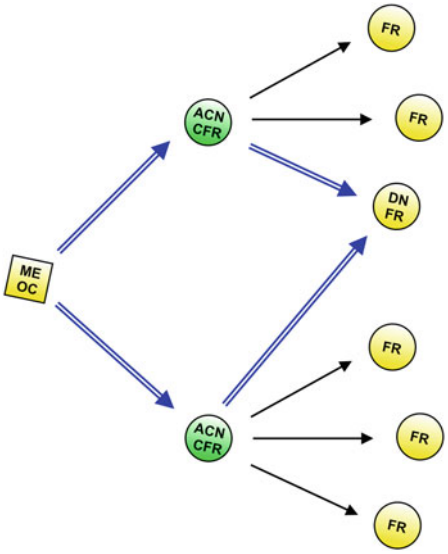

Fig. 8.6 ACB expressed by two CFRs

8.6 Vehicular Networks

As the latest cutting edge technologies for mobile communications, offering better transmission capabilities, are being devised globally, the concept of a world-wide deployment of efficient vehicular systems is becoming more and more crystallised [10]. On the one hand, certain advancement in this direction may be observed both in the case of the Physical Layer, as well as the Medium Access Control Layer, where the emphasis is generally laid on the provision of wider bandwidth and lower transmission latencies. On the other hand, however, one needs to remember about the Network Layer, where the aspects of autonomic networking and collaborative communication seem to gain increasingly significant attention these days. In fact, as advocated for throughout the whole chapter, self-management and autonomics should be perceived as the core elements of the ubiquitous network of the future [4]. Such a ubiquity means, that, undoubtedly, vehicular systems will become the key element of the global networking ecosystem and it is crucial to ensure that the relevant technologies are included in their development from the very outset. A distinctiveness of the vehicular networks may be related to their high complexity in terms of topology control and service provision [10]. Therefore, certain dose of autonomics is required for the purposes of guaranteeing smooth and robust system operation. Primarily, it is expected that there will be a need for the vehicles to express autonomic configuration capabilities in order to address the issues of rapid topology changes and distributed system nature.

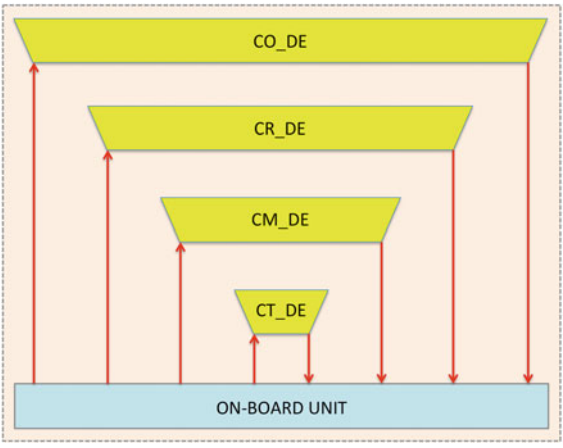

Fig. 8.7 Interaction between DEs and OBU

What is more, the very relevant question of self-management needs to be answered so that it would be possible to understand how the networked nodes, i.e. vehicles, can express the Autonomic Cooperative Behaviour and manifest it through, for example, the ability of employing the Autonomic Cooperative Networking Protocol [13]. Undoubtedly, such a system needs to be stable and

scalable, and, thus, large-scale vehicular networks should express self-management through efficient and effective self-configuration and self-management so that it would be capable of functioning by itself without any necessity for a specific external human intervention during the majority of its operation time [4]. The incorporation of a relevant communication logic may be facilitated with the aid of the components of the Autonomic Cooperative System Architectural Model (ACSAM) building on top of the notion of the Autonomic Control Loop (ACL) of Generic Autonomic Network Architecture (GANA) [18]. In other words, as outlined in Fig. 8.7, the basic idea would be that the interaction with the GANA Decision Element (DE) is taking place on all the levels, where the ACLs allow to orchestrate their respective Managed Entity (ME), implemented within the On-Board Unit (OBU). A question may arise, however, in what way should the On-Board Unit be perceived when it comes to the interfacing with the Autonomic Cooperative System Architectural Model, as, in general, it would seem that it could be treated as a Managed Entity on some level of the Generic Autonomic Network Architecture abstraction.

In fact, as such, the On-Board Unit appears to be much more of a networked device, featuring certain dose of additional capabilities. This way, being rather a composition of various protocols and manageable routines, the On-Board Unit should not be seen as a singe Managed Entity. Quite the contrary, similarly to network routers, the Autonomic Cooperative System Architectural Model would need to be then integrated into the OBU in order to orchestrate its operation from the inside. This way, going through various levels of abstraction, the vehicles of a Vehicular Ad-hoc NETwork (VANET) would be able to form Virtual Cooperative Sets in order to instantiate the Virtual Multiple Input Multiple Output technology enabled Distributed Spatio-Temporal Block Coding for the needs of expressing Autonomic Cooperative Behaviour. Such Autonomic Cooperative Behaviour would be composed with the use of the Optimised Link State Routing (OLSR) based Autonomic Cooperative Networking Protocol (ACNP) under the overall umbrella of Autonomic Cooperative System Architectural Model. Particularly, as the ACNP is an inherently proactive solution, it would comply with the autonomic environment of VANET, not only because of being integrated with collaborative transmission, but also thanks to maintaining the OLSR feature of willingness to carry and forward traffic, meant as an enabler for Autonomic Behaviour (AB), in general [10]. The orchestration going on within the Autonomic Control Loop would then involve the acquisition of the relevant monitoring data, as well as the application of certain algorithms, potentially having the flavour of policies [17].

8.7 Conclusion

In this chapter, the relevant insight into the field of standardisation and deployment was provided. For this reason, the concepts of interest analysed in the consecutive sections were structured accordingly, so that the whole chapter could

have been opened with the rather standardisation orientated topics, while towards the end it started naturally becoming to lean towards the issue of deployment. An utmost attention was paid to present both the components in a sufficiently balanced manner. Such a presentation was facilitated by the fact of the existence of numerous architectural commonalities. In particular, first the phenomenon of the Autonomic Future Internet was discussed with a special emphasis having been laid on the related standardisation within the ISG AFI, operating under the auspices of the European Telecommunications Standards Institute. Then, the Machine-to-Machine (M2M) communications were analysed mostly on the basis of the ETSI standardisation efforts and the concept of Software Defined Networking (SDN) followed, which shifted the focus more towards the deployment aspects. Eventually, both the Emergency Systems and Vehicular Networks were brought up, to outline certain architectural advancements as viewed from the deployment perspective.

References

1. Calarco, G., Casoni, M., Paganelli, A., Vassiliadis, D., & Wódczak, M. (2010). A satellite based system for managing crisis scenarios: the E-SPONDER perspective. In *5th Advanced Satellite Multimedia Systems Conference*. Italy: Cagliari.
2. Chaparadza, R., Ciavaglia, L., Wódczak, M., Chen, C.-C., Lee, B. A., Liakopoulos, A., et al. (2009). ETSI industry specification group on autonomic network engineering for self-managing future internet (ETSI ISG AFI). In G. Vossen, D. Long, & J. Yu (Eds.), *Springer Lecture Notes in Computer Science (LNCS): Web Information Systems Engineering* (Vol. 5802/2009). *10th International Conference on Web Information Systems Engineering* Poland: Poznań.
3. Chaparadza, R., Meriem, T. B., Radier, B., Szott, S., Wódczak, M, Prakash, A., et al. (2013). SDN enablers in the ETSI AFI GANA reference model for autonomic management and control (emerging standard), and virtualization impact. In *5th IEEE MENS at GLOBECOM 2013*. Atlanta: Georgia.
4. Chaparadza, R., Papavassiliou, S., Kastrinogiannis, T., Vigoureux, M., Dotaro, E., Davy, A., et al. (2009). Creating a viable evolution path towards self-managing future internet via a standardizable reference model for autonomic network engineering. In G. Tselentis, J. Domingue, A. Galis, A. Gavras, D. Hausheer, S. Krco, V. Lotz, and T. Zahariadis (Eds.) *Chapter in the book: "Towards the Future Internet - A European Research Perspective"* IOS Press, ISBN: 978-1-60750-007-0. Also published at the Future Internet Assembly 2009 in Prague.
5. ETSI GS AFI 001 V1.1.1. (2011). *Autonomic network engineering for the self-managing Future Internet (AFI); scenarios, use cases and requirements for autonomic/self-managing future internet*. ETSI Group Specification, France.
6. ETSI GS AFI 002 V1.1.1. (2013). *Autonomic network engineering for the self-managing future internet (AFI); generic autonomic network architecture (an architectural reference model for autonomic networking, cognitive networking and self-management)*. ETSI Group Specification, France.
7. ETSI TS 102 689 V1.1.1. (2010). *Machine-to-machine communications (M2M); M2M service requirements*. ETSI Technical Specification, France.
8. ETSI TS 102 690 V2.1.1. (2013). *Machine-to-machine communications (M2M); functional architecture*. ETSI Technical Specification, France.

9. Hyojoon K., & Feamster, N. (2013). Improving network management with software defined networking. *IEEE Communications Magazine*, *51*(2), 114–119.
10. Li, J., Wódczak, M., Wu, X., & Hsing, T. R. (2012). Vehicular networks and applications – challenges, requirements and service opportunities. *Academy Publisher Journal of Communications (JCM)*, *7*(5), 365–373.
11. Vassiliadis, D., Garbi, A., Calarco, G., Casoni, M., Paganelli, A., Morera, R., et al. (2010). Wireless networks at the service of effective first response work: the E-SPONDER vision. In *EEE International Symposium on Wireless Pervasive Computing*. Italy: Modena.
12. Wódczak, M. (2011). Autonomic cooperation in Ad-hoc environments. In *5th International Workshop on Localised Algorithms and Protocols for Wireless Sensor Networks (LOCALGOS) in conjunction with IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS)*. Spain: Barcelona.
13. Wódczak, M. (2011). Autonomic cooperative networking for wireless green sensor systems. *International Journal of Sensor Networks (IJSNet)*, *10*(1/2), 83–93.
14. Wódczak, M. (2011). Deployment aspects of autonomic cooperative communications in emergency networks. In *3rd International Congress on Ultra Modern Telecommunications and Control Systems, IEEE ICUMT*. Hungary: Budapest.
15. Wódczak, M. (2011). Resilience aspects of autonomic cooperative communications in context of cloud networking. In *IEEE First Symposium on Network Cloud Computing and Applications*. France: Toulouse.
16. Wódczak, M. (2012). Autonomic cooperative communications for emergency networks. In *4th IEEE MENS at GLOBECOM 2012*. Anaheim: California.
17. Wódczak, M. (2012). *Autonomic cooperative networking*. New York: Springer.
18. Wódczak, M., Meriem, T. B., Radier, B., Chaparadza, R., Quinn, K., Kielthy, J., et al. (2011). Standardizing a reference model and autonomic network architectures for the self-managing future internet. *IEEE Network*, *25*(6), 50–56.