Received: 10 February 2018 | Revised: 17 March 2018 | Accepted: 19 March 2018

DOI: 10.1002/itl2.44

LETTER

WILEY

Cyber-physical architecture assisted by programmable networking

Jose Rubio-Hernan[1] | Rishikesh Sahay[2] | Luca De Cicco[3] | Joaquin Garcia-Alfaro[1]

[1]IMT, Institut Mines-Telecom, Université Paris-Saclay, Evry, France
[2]Department of Applied Mathematics and Computer Science, DTU, Technical University of Denmark, Lyngby, Denmark
[3]Dipartimento di Ingegneria Elettrica e dell'Informazione, POLIBA, Politecnico di Bari, Bari, Italy

Correspondence
Joaquin Garcia-Alfaro, IMT, Institut Mines-Telecom, Université Paris-Saclay, Evry, France.
Email: joaquin.garcia_alfaro@telecom-sudparis.eu

Funding Information
CNI chair of the Institut Mines-Telecom, https://www.chairecyber-cni.org/. Cyber-CNI Chair of the Institut Mines-Telecom.

Cyber-physical technologies are prone to attacks in addition to faults and failures. The issue of protecting cyber-physical systems should be tackled by jointly addressing security at both cyber and physical domains in order to promptly detect and mitigate cyber-physical threats. Toward this end, this letter proposes a new architecture combining control-theoretic solutions together with programmable networking techniques to jointly handle crucial threats to cyber-physical systems. The architecture paves the way for new interesting techniques research directions and challenges which we discuss in our work

KEYWORDS

control theory, cyber-physical systems, programmable networking, software-defined networks, supervisory control and data acquisition

1 | INTRODUCTION

Cyber-physical systems (CPS) integrate physical infrastructures over computing network resources, in an effort to reduce complexity and costs of traditional control systems. Modern industrial control systems are a proper example. They have evolved from networked control systems that route their underlying information in terms of physical measurement and feedback control. Traditional security, from a network and computing security standpoint, is able to cover cyber threats, but fails at addressing physical threats. Control-theoretic solutions, combined with network computing security techniques, can lead to powerful solutions to cover both physical and cyber-physical attacks at the same time.[1–3] Nevertheless, guaranteeing the resilience of these systems (ie, to keep offering critical functionality under attack conditions) is still an open and critical problem to solve.[4] We argue that the use of *Programmable Networking* (PN) is a plausible solution to efficiently handle such a problem.

PN is a paradigm to manage network resources in a programmatic way. It can be used to decouple static network architectures and ease their management. Additionally, it facilitates the decentralization of network control and processing of network data. Control and data domain can be reprogrammed dynamically to enforce novel network applications and functionalities. Software-Defined Networking (SDN)[5] is a promising technology associated to the concept of PN. The use of PN allows decoupling the control domain from the data domain.[6] Novel network functionality can be devised and deployed depending on the current requirements. This includes the enforcement of protection schemes to recover the system elements from attacks.[7–9] The use of PN increases the visibility of controllers in terms of failure and attacks. It enables network operators to take control over the network flows based on dynamic conditions.[10] It also allows to control data domain devices from application-layer controllers, hence increasing the flexibility in terms of network reconfiguration. For instance, applications at the control domain can dynamically deploy policies over the networked devices via high-level programming languages.[11]

In this letter, we present a novel approach toward the development of a programmable cyber-physical system. Network and physical controllers get connected toward coordinating resilience strategies, for example, to maintain the resilient properties of the system under failure and attacks, at any layer of the resulting architecture. The proposed architecture is experimentally

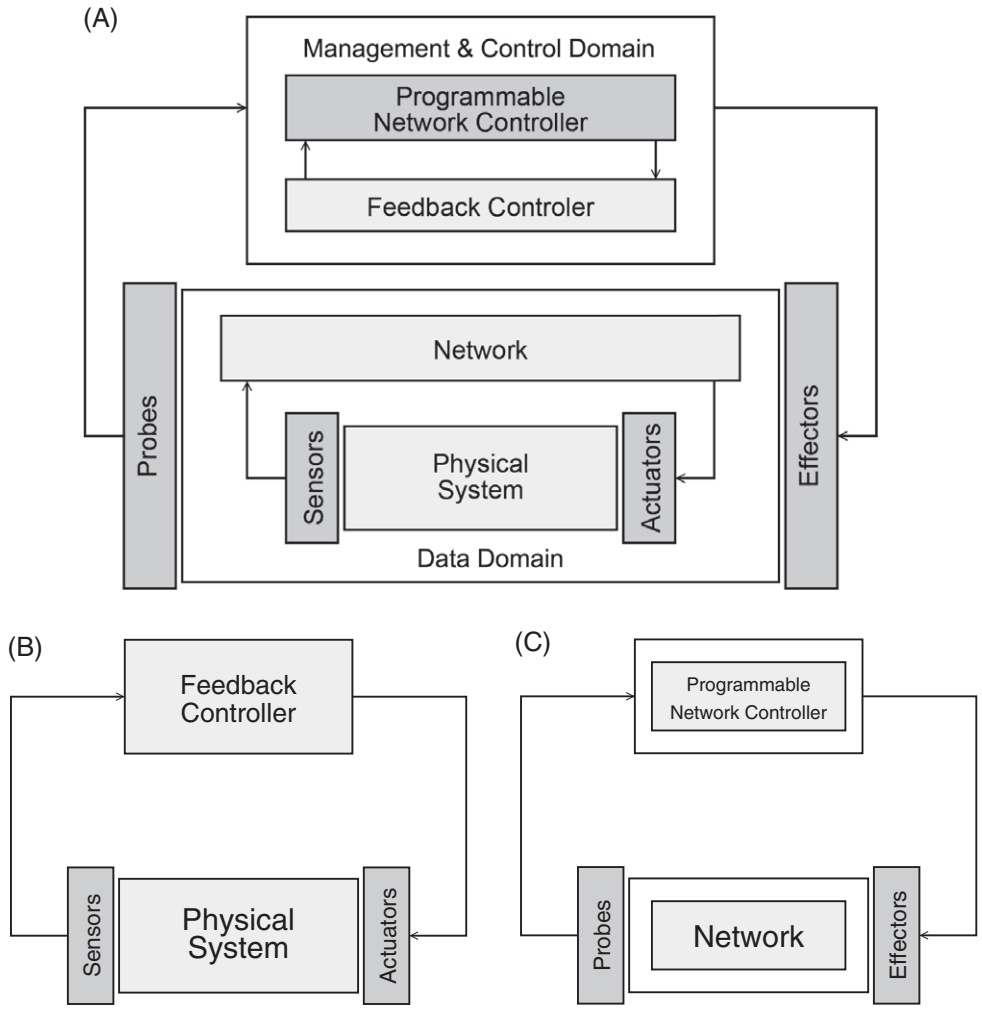

FIGURE 1 Proposed architecture. (A) Proposed architecture, combining feedback control and programmable networking, (B) closed-loop feedback control, and (C) programmable networking

validated by means of current programmable and cyber-physical technologies. More specifically, we show a proof-of-concept design combining SCADA (Supervisory Control And Data Acquisition) protocols and SDN-enhanced topologies, in order to evaluate the improvement of detection and mitigation capabilities of the resulting system.

The remaining sections of this letter are organized as follows. Section 2 presents our envisioned architecture. Section 3 discusses about the advantages and limitations of our proposal, with respect to experimental feasibility of our work. Section 4 closes the letter with some conclusions and perspectives of future work.

2 | OUR PROPOSAL

2.1 | Combining 2 complementary paradigms

CPS and PN are 2 complementary paradigms, but often separately addressed by 2 different research communities (control and computing-network communities). Both paradigms use similar elements, that can be presented either following control-theoretic architectures[12] or via computer-based programmatic definitions.[13] In the control community, CPS are regarded as a particular class of networked-control systems[12] (cf., Figure 1). Particularly, feedback control is managed by the following elements. *Controllers*, located within the cyber layer of the system (ie, the layer related to the network and computing resources), monitor and supervise information produced by physical *sensors* reporting measurements from physical processes. Based on the sensor measurements, controllers dynamically compute corrective actions which are put in place by system *actuators*, to steer the physical processes to the desired states.

PN can be represented using similar elements and definitions,[13] as depicted in Figure 1. In such a representation, the controller is governed by software elements, supervising both the *management* and the *control* domains of a programmable architecture. The controller manages the behavior of all the interactions at the *data domain*, where network elements (eg, network switches)

follow some precise policies directed by the controller (eg, to enforce routing and security strategies). The remaining elements of the network get permanently monitored by the controller, and orchestrated via control policies to improve, for example, the routing of traffic or the enforcement of network security countermeasures. To conduct monitoring at the data domain, several network probes (referred to as probes in Figure 1) report networking measurements to the controller.

2.2 | Toward resilient control systems

A crucial goal of both cyber-physical designs and PN is to ensure resilient control systems. Resilience is a property that has been studied for many years in different areas of knowledge. Laprie[14] defines the resilience of a system as *the persistence of dependability when facing changes in the system*. Dependability has also been expressed by Ellison et al. as the *avoidance of failures that are unacceptably frequent or severe*.[15] From these 2 definitions, we see that resilience deals with the management of operational functionality that is crucial for a system, and that cannot be stopped; in other words, system functionality that shall be properly accomplished. For instance, the cooling service of a reactor in a nuclear plant is a proper example of a critical functionality.

Other system functionalities may be seen as less important. They can even be temporarily stopped or partially accomplished. Such type of functions can be seen as secondary functions. A printing service for employees in the aforementioned nuclear plant scenario is a proper example of a secondary function. Another important element to take into consideration is the severity of failures. The more severe a failure is, the more it will affect the related system. Also, the more severe the failure, the harder it will be for the system to recover the nominal system functionalities. Several works have focused on these issues when addressing the survivability of critical system functionalities (see, for instance, Reference 16 and citations thereof).

Finally, a resilient control system shall able to[17]: (1) detect undesirable threats; (2) minimize the impact of such threats; and (3) mitigate them (ie, recover to normal operation in a reasonable time). Solutions include the use of redundancy (eg, use of software replicas), the enforcement of system segmentation, and the inclusion of different levels of protection (eg, secure handshakes, message signatures, and encryption). In the end, the goal is to include enough security measures to closing the system monitoring loop with additional responses that mitigate the undesirable events. In other words, inclusion of mitigation techniques to keep processes in a normal operating state while the system is confronted to failures and attacks. The challenge of satisfying those previous requirements on a cyber-physical system is the difficulty of properly differentiating failures from attacks, since their underlying security models (eg, in terms of mitigation) differ as well.

2.3 | Cyber-physical architecture assisted by PN

Taking into account the aforementioned descriptions and goals, in this section we propose a resilient cyber-physical architecture assisted by PN. The proposed architecture allows creating a cross control layer between the physical and the cyber layers. The resulting design aims to handle different security models, for example, from a security and safety standpoint. For instance, it enables adaptive and dynamic mitigation of threats. Moreover, it makes it possible to differentiate between failures, accidents, and attacks prior enforcing the mitigation strategies.

The use of PN allows to have a high level of abstraction while analyzing the system threats (contrary to traditional solutions anchored at the data domain), moving the defense at the same level of cyber-physical adversaries, assumed to be entities with physical and cyber knowledge.

Figure 1A shows our proposed framework of a PN-assisted cyber-physical system. The framework contains different components of PN technologies and CPS: (1) The data domain is mainly comprised of 2 subspaces: A physical space composed by *physical sensors and actuators*, which are used by the CPS to communicate with the physical processes located in the physical system (also located in the physical space). These devices communicate with the Feedback Controller to manage the physical processes; Also a network space composed by *PN switches*, which are programmable network switches controlled dynamically. This dynamic control enables us to minimize the deployment cost of the network framework, as to improve and manage many other network features,[18] for example, Quality of Service (QoS) and security requirements. PN switches use a centralized framework with an interface to control and manage all the network features dynamically; (2) The management and control domain contains 2 different controllers working on a joint and coordinated way, to fully cover the control of the resulting framework. The controllers are: (1) a *Feedback Controller* and (2) a *Programmable Networking (PN) controller*.

The Feedback Controller is made of 2 subcomponents: (1) the feedback controller that is in charge of enforcing the dynamical control objectives (fast dynamics are involved); (2) A supervisor controller that communicates in a bidirectional way with the PN controller in the following way. The PN controller, based on measurements provided by probes and feedback provided by the Feedback Controller, is able to detect a possible threat acting on the control path. In response to such a threat, the PN controller provides a corrective measure to mitigate the impact. The PN controller can be seen as a computing entity that is located at an

external location (eg, a kind of Network Operating System[5]). For instance, it provides resources and abstractions to manage the system using a centralized or a decentralized model.[19]

Together, both controllers manage the data domain. The Feedback controller manages the physical system through physical sensors and actuators deployed at the physical layer. Also the PN controller estimates and manages the data domain through network probes and effectors—deployed at the management and control domain. It is worth noting that the PN controller uses system identification tools to estimate the behavior matrices of the physical system. As a result, it can compare the *nominal cyber-physical system model* (ie, the behavior matrices) with the model estimated by the Feedback Controller. The correlation between both estimations allows to detect anomalies in the system (cf., Reference 19 for a sample technique based on the same principle). Notice that such anomalies can either be unintentional failures, or stealthy attacks disguised by intentional modifications produced by a malicious entity that intends to disrupt the physical system.[3,20] Assuming a system with appropriate measure to detect both failures and attacks, the PN controller can react to those anomalies, by enforcing some *mitigation* policies. At the data domain, we have *network probes and effectors*, conducting data monitoring—if instructed by the control domain. Network probes monitor the traffic in the data domain and provide the information to the PN controller. The PN controller analyzes the information and forwards control actions to the effectors. Network rules at the control domain are responsible for enforcing such actions. For instance, when a network probe finds tampered traffic in a network path, it provides the tampered information to the control domain. Then, the PN controller, located at the control domain, checks for the available resources in, for example, a path lookup component, and provides new routes to enforce the action. For instance, it may redirect the tampered traffic to provide fair share of network bandwidth with respect to legitimate traffic.

Another important component of the management and control domain is the *Path Lookup*. Paths in the framework are precomputed. Normally, a list of paths is maintained at the control domain. The path lookup component maintains a table of paths (from the ingress switch to the egress switch) sorted according to the quality of service provided by the paths, associated to unique labels. Paths are later assigned to flows based on the traffic class that they belong to. This is a crucial component of the overall system. Resiliency to attacks can be implemented by using multipath communication between cyber-physical system components or by activating new paths (even suboptimal) to evade an attack. For example, legitimate flows are assigned to high priority paths while suspicious flows are assigned to paths containing middleboxes or paths having longer hops and narrower bandwidth, to finally forward the malicious flows through paths which lead to a sinkhole.

2.4 | Use case

In this section, we describe an *autonomous urban bus transportation infrastructure* in order to show a specific example illustrating our approach. This scenario has 2 complementary domains: (1) data domain encompassed by the physical system (ie, buses, stations, and bus stops) where sensors and actuators used to manage and control the physical infrastructure and whose data are forwarded to the Feedback Controller through a PN (eg PN switches, servers); (2) and control domain, where the Feedback Controller automatically analyzes the data received from the physical system (ie, bus, stations, and bus stops) using a feedback algorithm to correctly coordinate the traffic and rectifying errors in real time. In addition, a supervisor component in the Feedback Controller handles the data received from the sensors (located, for instance, at the buses) and the data computed by the feedback algorithm. The goal is to communicate with the PN controller to build a global view of the system. The supervisor component at the Feedback Controller acts as an interface between the PN controller and the Feedback Controller to have the communication. The PN controller manages the network, modifying traffic and security rules to handle network threats. It also collects data whose trust is validated using the information sent by the supervisor of the Feedback Controller. This coordination allows to have a real control of all the components located in the Data domain, that is, to manage more efficiently any possible disruption, such as bus disruptions produced by errors or attacks, including speeding, wrong positioning, or diversion to wrong circulation paths.

3 | VALIDATION AND DISCUSSION

To validate the feasibility of our proposal, we are currently implementing a proof-of-concept prototype based on the architecture proposed in this letter. The prototype combines the components of a cyber-physical system together with PN technology. It builds upon *Mininet,*[21] a network emulator tool which provides a rapid prototyping for PN. The protocol used to instantiate the PN techniques is OpenFlow. It allows controlling the path of the network traffic through PN switches. For the implementation of cyber-physical system, we use the SCADA Modbus protocol.[22] Further information about the proof-of-concept prototype and ongoing results is available online.

For the time being, the PN controller of the prototype instructs the network probes of a cyber-physical system (eg, autonomous vehicles) to monitor traffic from data domains, in order to investigate the existence of malicious traffic evidences. More

specifically, the PN controller receives traffic header details (such as source IP address, destination IP address, and protocol) along with payload data containing networked-feedback measurements from the physical domains. The PN controller cooperates with the Feedback Controller. It analyzes anomalous details and may share information with the Feedback Controller. Whenever the level of suspicious events reaches a configurable threshold, the PN controller may decide to send the measurements to, for example, quarantine subnetwork, by redirecting the suspicious traffic through alternative routing paths.[23] This solution, based on the path lookup module of *framework*, uses network traffic labeling to mark down the suspicious events. This is implemented in practice by adding an additional functionality to the *Mininet* PN controllers that deploys mitigation rules to handle suspicious traffic at the edge of the PN switches of the cyber-physical system. The redirection of traffic is enforced by the network effector of the system, in order to enable quarantining plans. Some more practical details and video captures of the proof-of-concept prototype are available online at http://j.mp/TSPCPSDN.

The aforementioned prototype validates the architecture proposed in this letter. It promotes cooperation between controllers located at both management and control domains of a cyber-physical system. Nevertheless, further analysis is required with respect to the duality of goals of each controller paradigm represented in the architecture depicted in Figure 1A. In some cases, the 2 combined paradigms may be driven with different objectives. A more thorough study shall be conducted to identify how the controllers achieve a common goal (eg, guaranteeing cyber-resilience of the underlying system) withing interfering their primary objectives (ie, networking and physical control objectives). To make a concrete example, the Feedback Controller can report an anomalous deviation of the sensor readings from the nominal behavior as a feedback to the PN controller. This issue could be due to sensors being faulty or due to an attack whose actions affect the control paths. The Feedback Controller alone is not able to distinguish between the 2 events since it has no view of the underlying network (information hiding). In response to such a situation, the Feedback Controller sends an alert signal to the PN controller which verifies if the control path (which is unknown to the Feedback Controller) is likely to be under attack. In case of an attack is detected by the PN controller, it puts in place the corrective measures (ie, segregate malicious traffic programmatically) and sends a signal to the Feedback Controller, to report that a corrective action has been taken into account. Notice that sophisticated attacks to the system could escape the detectors running solely in the cyber-layer. When this is managed as well by the Feedback Controller, stealthy attacks hidden as failure and faults will be identified. A more precise evaluation of this type of scenarios will be provided in a forthcoming publication.

4 | CONCLUSION

This letter shows that PN and feedback control can be combined together in order to build higher resilient CPS. We argued that our PN-assisted cyber-physical architecture, improves detection and mitigation of cyber-physical attacks. It allows cooperation between traditional Feedback Controllers and PN devices, to allow more efficient mitigation of threats (eg, by providing evidences about stealthy cyber-physical attacks disguised as failures and faults). Next steps include a more thorough analysis about the cooperation of controllers, as well as investigation about the effective activation of cyber-physical resilience by combining novel detection and mitigation strategies.

ACKNOWLEDGMENTS

This article was partially supported by the Cyber-CNI Chair of the Institut Mines-Telecom (http://chaire-cyber-cni.fr/)

ORCID

Joaquin Garcia-Alfaro http://orcid.org/0000-0002-7453-4393

REFERENCES

1. Pasqualetti F, Dorfler F, Bullo F. Control-theoretic methods for cyberphysical security: geometric principles for optimal cross-layer resilient control systems. *IEEE Control Syst*. 2015;*35*(1):110-127. https://doi.org/10.1109/MCS.2014.2364725.
2. Mo Y, Weerakkody S, Sinopoli B. Physical authentication of control systems: designing watermarked control inputs to detect counterfeit sensor outputs. *IEEE Control Syst*. February 2015;*35*(1):93-109. https://doi.org/10.1109/MCS.2014.2364724.
3. Rubio-Hernan J, De Cicco L, Garcia-Alfaro J. Adaptive control-theoretic detection of integrity attacks against cyber-physical industrial systems. *Trans Emerg Telecommun Technol*. 2017. https://doi.org/10.1002/ett.3209.
4. Urbina D, Giraldo J, Cardenas A, Valente J, Faisal M, Tippenhauer N, Ruths J, Candell R, Sandberg H. Survey and new directions for physics-based attack detection in control systems. Grant/Contract Reports (NISTGCR), National Institute of Standards and Technology (NIST); 2016; 1–37. https://doi.org/10.6028/NIST.GCR.16-010.
5. Kreutz D, Ramos F, Verissimo P, Rothenberg C, Azodolmolky S, Uhlig S. Software-defined networking: a comprehensive survey. *Proc IEEE*. 2015;*103*(1):14-76. https://doi.org/10.1109/JPROC.2014.2371999.

6. Open Networking Foundation. Software-defined networking: the new norm for networks. Technical Report; 2012.
7. Shin S, Porras P, Yegneswaran V, Fong M, Gu G, Tyson M. FRESCO: modular composable security services for software-defined networks. Paper presented at: Proceedings of the ISOC Network and Distributed System Security Symposium (NDSS). San Diego, CA, United States; 2013.
8. Fayaz S, Tobioka Y, Sekar V, Bailey M. Bohatei: flexible and elastic DDoS defense. Paper presented at: 24th USENIX Security Symposium (USENIX Security 15), USENIX Association. Washington DC, United States; 2015; 817–832.
9. Li J, Berg S, Zhang M, Reiher P, Wei T. Drawbridge: software-defined DDoS-resistant traffic engineering. Paper presented at: Proceedings of the 2014 ACM Conference on SIGCOMM, ACM: New York, NY; 2014; 591–592, https://doi.org/10.1145/2619239.2631469.
10. Al-Fares M, Radhakrishnan S, Raghavan B, Huang N, Vahdat A. Hedera: dynamic flow scheduling for data center networks. Paper presented at: Proceedings of the 7th USENIX Conference on Networked Systems Design and Implementation, NSDI'10, USENIX Association, Berkeley, CA; 2010.
11. Sahay R, Blanc G, Zhang Z, Debar H. ArOMA: an SDN based autonomic DDoS mitigation framework. *Comput Secur*. 2017;*70*(Supplement C):482-499.
12. Lindberg M., Arzen K. Feedback control of cyber-physical systems with multi resource dependencies and model uncertainties. Paper presented at: 2010 31st IEEE Real-Time Systems Symposium. San Diego, CA, United States; 2010; 85–94.
13. Matni N, Tang A, Doyle J. A case study in network architecture tradeoffs. Technical Report; 2015.
14. Laprie J. From dependability to resilience. Paper presented at: 38th IEEE/IFIP International Conference on Dependable Systems and Networks. Anchorage, Alaska, United States; 2008.
15. Ellison R, Fisher D, Linger R, Lipson H, Longstaff T. Survivable network systems: An emerging discipline. Technical Report, Software Engineering Institute, Carnegie-Mellon University, Pittsburgh, PA; 1997.
16. Linger R, Mead N, Lipson H. Requirements definition for survivable network systems. Paper preseted at: Proceedings of Third International Conference on Requirements Engineering, IEEE; 1998; 14–23.
17. Queiroz C. A Holistic Approach for Measuring the Survivability of SCADA Systems [PhD thesis]. Melbourne, Australia: RMIT University, 2012.
18. Sharma S. Programmable Ethernet Switches and Their Applications [PhD thesis]. Stony Brook, NY: State University of New York at Stony Brook; 2008.
19. Rubio-Hernan J, De Cicco L, Garcia-Alfaro J. Event-triggered watermarking control to handle cyber-physical integrity attacks. Paper presented at: 21st Nordic Conference in Secure IT Systems (NordSec 2016), Oulu, Finland, Springer; 2016; 3–19. https://doi.org/10.1007/978-3-319-47560-8.
20. Rubio-Hernan J, De Cicco L, Garcia-Alfaro J. On the use of watermark-based schemes to detect cyber-physical attacks. *EURASIP J Inform Secur*. 2017;*2017*(1):8. https://doi.org/10.1186/s13635-017-0060-9.
21. Lantz B, Heller B, McKeown N. A network in a laptop: rapid prototyping for software-defined networks. Paper presented at: 9th ACM SIGCOMM Workshop on Hot Topics in Networks, New York, NY: ACM; 2010; 19:1–19:6. https://doi.org/10.1145/1868447.1868466.
22. Modbus Organization. Official modbus specifications. 2016. http://wwwmodbusorg/specsphp. Accessed March 1, 2018.
23. Hachem N, Debar H, Garcia-Alfaro J HADEGA: a novel MPLS-based mitigation solution to handle network attacks. Paper presented at: 31st IEEE International conference on Performance Computing and Communications (IPCCC 2012), IEEE; 2012; 171–180, https://doi.org/10.1109/PCCC.2012.6407750.

How to cite this article: Rubio-Hernan J, Sahay R, De Cicco L, Garcia-Alfaro J. Cyber-physical architecture assisted by programmable networking. *Internet Technology Letters* 2018;1:e44. https://doi.org/10.1002/itl2.44