rules, a unique hybrid system is obtained. A critical relation is then defined which describes the occurrence of safety-critical situations in the composed hybrid system. Studying safety in multi-agent ATM scenarios then translates to studying critical observability of the obtained (composed) hybrid system with respect to the critical relation.

Although formally sound, this approach is hardly applicable to realistic scenarios because of the large number of variables involved. To overcome these difficulties we proposed algorithms based on bisimulation theory, widely used in the area of formal methods to mitigate software verification.

We analysed the Terminal Maneuvering Area (TMA) T1 operation, a procedure selected within the MAREA consortium as a benchmark, exhibiting most relevant features arising in the novel SESAR 2020 Concept of Operation. We considered a scenario involving 25 agents, comprising more than 1.68 x 10^{18} discrete states. We showed that this procedure is not critically observable. This implies that there are safety-critical configurations which cannot be detected by pilots or air traffic controllers. In other words, in some situations, not only is the human operator's awareness of a safety critical situation incorrect, but furthermore, it cannot be improved before a safety-critical situation occurs. This analysis also proposed alternative solutions which ensure safety of the procedure.

We wish to thank Henk Blom and Mariken Everdij (NLR) for fruitful discussions on this paper.

Link:
http://dews.univaq.it/

References:
[1] E. De Santis et al: "Critical Observability of a Class of Hybrid Systems and Application to ATM systems", in "Stochastic Hybrid Systems: Theory and Safety Critical Applications", LNCIS 337
[2] E. De Santis et al: "Final modelling and analysis of SESAR 2020 ConOps", Report MAREA D4.4, http://complexworld.eu/wiki/File:D4.4-v1.0.pdf
[3] Resilience Engineering Perspectives, Preparation and Restoration, Vol. 2, Ashgate, England, 2009.

Please contact:
Elena De Santis, Maria Domenica Di Benedetto and Giordano Pola, Center of Excellence for Research DEWS, University of L'Aquila, Italy.
E-mail: {elena.desantis, mariadomenica.dibenedetto, giordano.pola} @univaq.it

Security in the Era of Cyber-Physical Systems of Systems

by Stamatis Karnouskos

Critical infrastructures are increasingly equipped with modern Cyber-Physical Systems (CPS) and Internet-based services that enhance their functionalities and operation. However, traditional security practices fall short when it comes to addressing the multitude of security considerations, not only at individual system but also at system-of-system level. The creation of recent sophisticated tools, such as Stuxnet, Duqu, Flame, and the Mask, is the prequel to a nightmare in a CPS-dominated future.

The existence and utilization of highly complex tools such as Stuxnet, Duqu, Flame, and the Mask in real-world attacks demonstrate that we have entered the era of sophisticated cyber warfare. The concern is that the Cyber-Physical Systems (CPS) [1] monitoring and controlling critical infrastructures such as the smart grid [2] may be susceptible to cyber-terrorism, and that even small criminally inclined groups would be able to create attacks with asymmetrical impact. Since the majority of the world's SCADA/DCS and PLC systems can be found in high-tech industrial facilities in Europe, US and Japan, it is imperative to invest in security as a process. Adequately addressing security in the cyber-physical system era, however, poses a significant challenge.

Attacks such as that of Stuxnet relied on a number of existing vulnerabilities, some of which dated back two years [3]. Updates should have been applied during that time, but owing to the "air-gap" isolation they were considered unnecessary. Additionally, many of the industrial infrastructures that employ CPS are long-lived with life times of 10+ years. This means updates are not always possible (for older systems), or are not implemented as often owing to the lengthier testing time and the fear of unwanted side effects. However, these poorly defended, poorly patched and poorly regulated systems will be the first ones that will be used as Trojan horses to attack the more modern systems with zero-day attacks. ``Don't touch a running system" may not apply in the CPS era.

Modern CPSs do not constitute a monolithic platform and are not developed by a single stakeholder. On the contrary, they consist of various hardware and software parts "glued" together to perform the required tasks. Hence the first problem that arises is how to trust the individual parts of the CPS and how to guarantee a deterministic behaviour. Addressing security only at hardware or software levels is not enough. The operational context also needs to be considered for safety and dependability reasons. Even if both are fully certified and addressed, there is still no guarantee that actions that compromise a CPS will not occur during its lifetime – hence adequate security measures also need to be taken in the operational context.

Trust is a fundamental issue to consider. As an example, CPS hardware compo-

nents can be used as carriers of attacks and entry points to a system. Common attacks utilize "trusted" parts of a system, such as USB ports, the Ethernet card, the battery etc. to host and execute malicious code that bypasses the operating system's guards. Digitally signed software should not be blindly trusted either. As an example, Stuxnet installed two kernel drivers that were digitally signed by valid certificates that were stolen from two different issuing companies. Real time online validation of certificates may limit the exposure window.

Software and hardware security are not the only issues to be considered; human users must be included in the process. Security clearance on people does not imply security on their accompanying assets. In the Stuxnet case [3], a trustworthy employee with an unknowingly rootkited laptop or an infected USB flash drive would be enough to spread the malware. This could be, for instance, a contractor carrying a personal device, who is assigned to do maintenance on a facility.

Lack of security-considerations at CPS development time may lead to insecure software with bugs that may result in unpredictable system behaviour or, even worse, a controllably malicious operational behaviour. Other pitfalls may also be possible, as demonstrated by the Stuxnet [3], which was able to take advantage of something that should never have existed in the first place, i.e., default hard-coded access accounts and passwords in industrial PLCs.

It is interesting that we place so much trust on CPS systems even when some of their complex operational stages may not be secure. Stuxnet impersonated the normal behaviour of the PLC, and any network management system or control room operator would have been unlikely to see a rogue PLC as its signals were faked [3]. As such, only the independently observed physical process and that reported by the Stuxnet-infected PLC data would mismatch. Hence, safeguards need to be in place, not only on individual CPS, but also on the processes in which they participate. This requires system-of-system wide behaviour monitoring and checks for anomalies. Heuristics for estimating behaviour deviation may provide hints, which should be assessed and analysed in conjunction with other metrics. This is challenging but probably achievable to some degree if the process is under the control of a limited number of stakeholders. However, in the envisioned widely collaborative CPS systems-of-systems this is a daunting task.

In CPS system-of-systems it will be difficult to do holistic code reviews, systematic testing and checks at design and runtime [2]. Hence, software "bugs" which may have a tangible impact on the physical world will happen more often, while their impact will be hard to assess. It is not clear how much effort will need to be invested in designing and integrating software for such complex system of systems versus testing it. Additionally, the range of qualifications that will be required by future engineers to perform these tasks will have to be broader and more in-depth which is challenging. Automatic tools that do the model checking as well as detect potential safety-critical issues on large scale multi-dimensional applications will be needed.

CPSs control real-world infrastructures and thus have a real-world impact. Dependability in CPS and their ecosystems will be the key factor for their application in critical systems; it will determine to what extent our core critical infrastructure will be vulnerable in the future. The CPS era is in need of solutions that will support it at device, system, infrastructure and application level [1]. This includes the whole lifecycle from cradle-to-grave of its components and services. This is a grand challenge and includes multi-disciplinary engineering, modelling, emergent behaviour, human interaction etc. Finally, it has to be kept in mind that security is a multi-angled process in which vulnerability and risk analysis may dictate what is an acceptable level. Solutions focusing asymmetrically on particular aspects, whilst neglecting others, may give a false sense of safety and security, which will be shattered by reality as Stuxnet, Duqu, Flame, and the Mask have recently demonstrated.

References:

[1] "Cyber-Physical Systems: Driving force for innovation in mobility, health, energy and production". Tech. rep., Acatech – German National Academy of Science and Engineering, 2011

[2] S. Karnouskos: "Cyber-Physical Systems in the SmartGrid", in IEEE 9th International Conference on Industrial Informatics (INDIN), Lisbon, Portugal, 2011

[3] S. Karnouskos: "Stuxnet Worm Impact on Industrial Cyber-Physical System Security", in 37th Annual Conference of the IEEE Industrial Electronics Society (IECON), Melbourne, Australia, 2011.

Please contact:

Stamatis Karnouskos
SAP, Germany
E-mail: stamatis.karnouskos@sap.com