Combinaison de test et de vérification pour les CPS adaptatifs

Spécialité : Informatique

Encadrement

Prof. Dr. O. Kouchnarenko olga.kouchnarenko@femto-st.fr - Directrice
Dr. F. Dadeau frederic.dadeau@femto-st.fr – Co-encadrant

Equipe de recherche

VESONTIO
Département d'Informatique des Systèmes Complexes
Institut FEMTO-ST, UMR CNRS 6471

Contact : Dr. Frédéric Dadeau frederic.dadeau@femto-st.fr

Description du sujet

Les Systèmes Cyber Physiques (CPS) sont des systèmes contrôle-commande interconnectés, successeurs des systèmes embarqués, ayant pour caractéristique le contrôle des entités physiques par le logiciel. On en trouve dans les systèmes intelligents tel que les véhicules autonomes, les smart-grids, la domotique, ou encore les systèmes robotiques. Ces systèmes peuvent être modélisés par des composants communicants dont les comportements sont le plus souvent décrits par des règles spécifiant la réaction du système aux envois de données remontées par des capteurs, et provoquant des évolutions du système (par exemple, reconfiguration de composants, mise à jour de l'état interne du système, etc.) [1,3]

Comme tous les systèmes, les CPS présentent des besoins de sûreté de fonctionnement et de sécurité [2]. En particulier, il est nécessaire de s'assurer de la conformité du système au cahier des charges, par le biais de propriétés fonctionnelles du systèmes (invariants, propriétés temporelles), ou de propriétés de sécurité (contrôle d'accès, intégrité des informations, disponibilité des services) [5]. Dans une large majorité de cas, les configurations du système sont en nombre infini et ainsi les techniques de vérification classiques, basées sur une exploration exhaustive des états du système (model-checking), sont inapplicables.

La vérification à l'exécution consiste à analyser à l'exécution (monitoring) les traces du système pour déterminer si celui-ci se comporte conformément aux exigences, formalisées par des propriétés sur ces traces [4]. Le test actif consiste à créer des traces d'exécution spécifiques qui vont chercher à provoquer la réaction du système en vue de s'assurer de son bon fonctionnement.

Nous proposons dans cette thèse de combiner des approches de vérification à l'exécution (test passif/monitoring) et de génération de tests (test actif) pour valider les systèmes cyber-physiques. Cette combinaison s'appuiera sur un modèle du système, et un ensemble de propriétés fonctionnelles et de sécurité, exprimées dans un langage ad hoc. Ces artefacts seront ensuite utilisés pour la génération automatique de tests, en utilisant des techniques telles que le fuzzing de données, ou des critères de sélection de test structurels du modèle ou de la propriété [6]. De plus, des techniques de vérification statiques pourront être utilisées par la validation de la cohérence globale des règles décrivant le comportement du CPS (détection de non-déterminisme, deadlocks, etc.), fournissant ainsi un retour sur l'implantation des différents composants.

Plan des travaux

- état de l'art sur les CPS et les approches de vérification & validation
- extension du modèle à composants pour la modélisation des CPS et des propriétés considérées
- génération de tests à partir des propriétés
- évaluation des propriétés à l'exécution et fuzzing de données
- évaluation expérimentale

Références bibliographiques

[1] S. K. Khaitan and J. D. McCalley, "Design Techniques and Applications of Cyberphysical Systems: A Survey," in IEEE Systems Journal, vol. 9, no. 2, pp. 350-365, June 2015.

[2] J. Shi, J. Wan, H. Yan and H. Suo, "A survey of Cyber-Physical Systems," 2011 International Conference on Wireless Communications and Signal Processing (WCSP), Nanjing, 2011, pp. 1-6.

[3] De Lemos, R., Giese, H., Müller, H.A., Shaw, M., Andersson, J., Litoiu, M., Schmerl, B., Tamura, G., Villegas, N.M., Vogel, T., et al.: Software engineering for self-adaptive systems: A second research roadmap. In: Software Engineering for Self-Adaptive Systems II. Springer (2013) pp. 1–32.

[4] Kouchnarenko, O., Weber, J.F.: Adapting component-based systems at runtime via policies with temporal patterns. In 10th Int. Symp. on Formal Aspects of Component Software, FACS 2013, Nanchang, China, October 27-29, 2013, Revised Selected Papers. Volume 8348 of LNCS. Springer (2014) pp. 234–253.

[5] M. Rocchetto and N. O. Tippenhauer, "Towards Formal Security Analysis of Industrial Control Systems", in Proceedings of ACM Asia Conference on Computer and Communications Security (ASIACCS), 2017.

[6] K. Cabrera Castillos, F. Dadeau, and J. Julliand. Coverage Criteria for Model-Based Testing using Property Patterns. In A. Petrenko and H. Schlingloff, editors, MBT 2014, 9th International Workshop on Model-Based Testing (co-located with ETAPS 2014). Grenoble, France. April 2014.

Combining test and verification for adaptative CPS

Specialty: Computer Science

Supervisors
Prof. Dr. O. Kouchnarenko <olga.kouchnarenko@femto-st.fr>
Dr. F. Dadeau <frederic.dadeau@femto-st.fr>

Research Team
VESONTIO
Département d'Informatique des Systèmes Complexes
Institut FEMTO-ST, UMR CNRS 6471

Contact: Dr. Frédéric Dadeau – frederic.dadeau@femto-st.fr

Description

Cyber-Physical Systems (CPS) are interconnected control-command systems, inheriting from embedded system. They are characterized by the control of physical entities via the software. They can be smart systems, such as autonomous vehicles, smart-grids for power management, domotics or robotics systems. These systems can be modelled by communicating components whose behaviors are, most of the time, described by rules specifying the reaction of the system to data retrieved by various sensors, thus triggering the evolution of the system state (e.g. component reconfiguration, update of the internal system state, etc.) [1,3].

As for all systems, CPS are in need for safety and security [2]. Especially, it is mandatory to ensure the conformance of the system w.r.t. the initial informal requirements, or w.r.t. functional properties (access control, data integrity, service availability, etc.) [5]. In a large majority of cases, system configurations are infinite and thus, classical verification techniques, based on an exhaustive exploration of the system states (such as model-checking), can not be applied.

Runtime checking consists in analysing, at run-time, traces of the system's execution to determine if this latter behaves as expected, w.r.t. a given set of trace properties [4]. This represents a passive testing approach. Active testing, on the opposite, consists in building specific execution traces that will ensure the system's reaction to check if it reacted in the appropriate way.

We propose, in this thesis, to combine runtime checking approaches (passive testing/monitoring) with test generation approaches (active testing) to validate cyber-physical systems. This combination will rely on a model of the system and a set of both functional and security properties, expressed in an ad hoc language. These artifacts will then be used for automated test generation, by using techniques such as data fuzzing, or dedicated coverage criteria such as model coverage or property coverage [6]. In addition, static verification techniques will be used to ensure the global coherence of the rules describing the behavior of the CPS (non-determinism detection, deadlocks, etc.) providing a useful feedback on the implementation of the various components.

Roadmap

- State of the art on CPS and existing verification & validation approaches
- Extension of a component model for the CPS and the considered properties
- Test generation from the properties
- Runtime evaluation of the properties and data fuzzing
- Experimental evaluation

Bibliography

[1] S. K. Khaitan and J. D. McCalley, "Design Techniques and Applications of Cyberphysical Systems: A Survey," in IEEE Systems Journal, vol. 9, no. 2, pp. 350-365, June 2015.

[2] J. Shi, J. Wan, H. Yan and H. Suo, "A survey of Cyber-Physical Systems," 2011 International Conference on Wireless Communications and Signal Processing (WCSP), Nanjing, 2011, pp. 1-6.

[3] De Lemos, R., Giese, H., Müller, H.A., Shaw, M., Andersson, J., Litoiu, M., Schmerl, B., Tamura, G., Villegas, N.M., Vogel, T., et al.: Software engineering for self-adaptive systems: A second research roadmap. In: Software Engineering for Self-Adaptive Systems II. Springer (2013) pp. 1–32.

[4] Kouchnarenko, O., Weber, J.F.: Adapting component-based systems at runtime via policies with temporal patterns. In 10th Int. Symp. on Formal Aspects of Component Software, FACS 2013, Nanchang, China, October 27-29, 2013, Revised Selected Papers. Volume 8348 of LNCS. Springer (2014) pp. 234–253.

[5] M. Rocchetto and N. O. Tippenhauer, "Towards Formal Security Analysis of Industrial Control Systems", in Proceedings of ACM Asia Conference on Computer and Communications Security (ASIACCS), 2017.

[6] K. Cabrera Castillos, F. Dadeau, and J. Julliand. Coverage Criteria for Model-Based Testing using Property Patterns. In A. Petrenko and H. Schlingloff, editors, MBT 2014, 9th International Workshop on Model-Based Testing (co-located with ETAPS 2014). Grenoble, France. April 2014.