BSSE System and Software Engineering

Dr. Rainer Gerlich

Automated System Verification and Validation

"To be sure the system will really work as expected and when needed"

The progress in the area of hardware and software technology allows to make components more intelligent and to synthesize larger and complex systems out of a number of such components. While previously the components acted independently, they now can communicate due to their higher intelligence. This gives a high potential to tune and optimise a system's properties. However, this higher complexity also introduces additional risks. The more components are involved and the more functionality is provided the higher is the chance that the overall system's state becomes inconsistent and faulty. Consequently, then the system will fail to work, probably in situations which are critical for a mission.

Such situations could recently well be observed during the start preparations of Formula-1 races: a number of times the start support system failed. Being asked for the reason officials stated on TV that hundreds of tests would have been needed, but were not executed. Becoming aware of the problem and being again faced with it during training, the most important tests have been executed just during the night before the race started. However, a number of weeks later the problem still seems to exist.

This problem is just a consequence of introducing more intelligence into systems for reasons of optimisation and system tuning. In case of cars it is e.g. a matter of "Engine Management" to reduce fuel consumption and environmental pollusion, and to increase an engine's power, or to support the pilot for engine management during the start phase.

The problem of the Formula-1 start support system is typical for systems including software. Software allows to provide complex functionality, but it is very difficult to prove that the software is correct. If a number of components is involved, the complexity is beyond what man can understand. The problem even becomes more complex by impact of timing conditions. Therefore a formal and representative approach has to be applied which allows to automatically exploit the system's behaviour under normal, stress and fault conditions.

Such an approach should not require much effort per test case, otherwise it would be impossible to do a complete verfication and validation of the system within a reasonable time. Consequently, an automated approach is the best choice which stimulates the system by "good" and "bad" inputs and evaluates the results.

If the system is under development, automated production of a representative software prototype (RSP) will help to find the optimum system architecture. If a system has been already finished an automatically constructed RSP will help to identify potential problems and risks.

BSSE has developed the technologies "ISG" (Instantaneous System and Software Generation) and "ASaP" (Automated Software Production) for automated production of software, covering automated construction of systems like real-time systems, embedded systems and distributed systems, and of RSPs. Both technologies imply automated verification and validation (V&V). ISG and ASaP take system specifications and either generate the complete system infrastructure and the means for V&V, or a test environment for automated stimulation of the system or software and automated evaluation of test results. By these technologies not only a system's functionality and behaviour can be exploited, but also its performance and the impacts by varying timing conditions and faults.

Hence, ISG and ASaP allow to fully investigate a system's "good" and "bad" properties. This is considered as a significant contribution towards avoidance of situations like the ones described above in case of Formula-1.

Point of Contact:

Dr. Rainer Gerlich BSSE System and Software Engineering
Auf dem Ruhbuehl 181
88090 Immenstaad, Germany

Voice: +49/7545/91.12.58
Fax: +49/7545/91.12.40
Mobile: +49/171/80.20.659

e-mail: gerlich@t-online.de
URL: http://home.t-online.de/home/gerlich