Fraunhofer
FOKUS

FRAUNHOFER INSTITUTE FOR OPEN COMMUNICATION SYSTEMS FOKUS

RACOMAT

Contact
Johannes Viehmann
System Quality Center – SQC
Phone. +49 30 3463-7274
Fax +49 30 3463-99 7274
johannes.viehmann
@fokus.fraunhofer.de

Fraunhofer FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin
Germany

www.fokus.fraunhofer.de

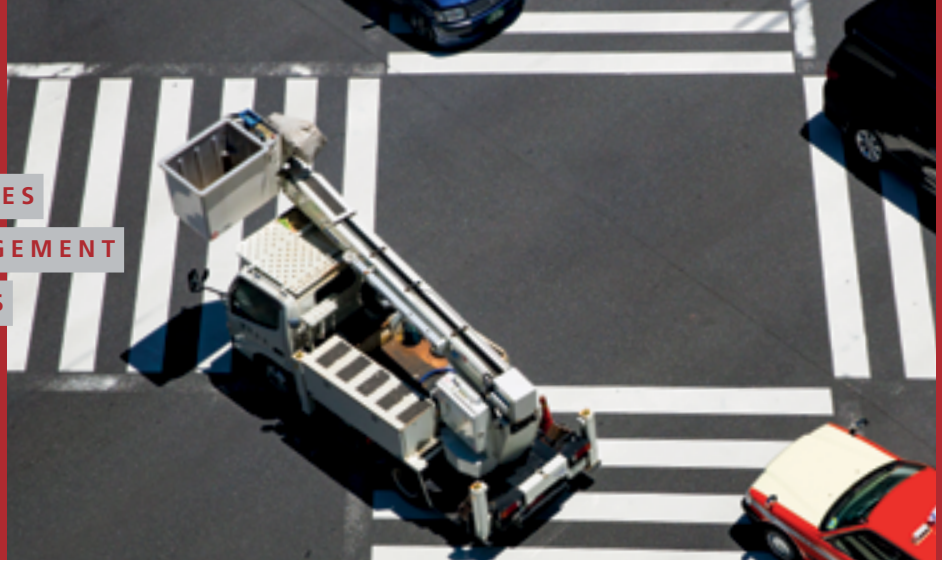
RACOMAT
Risk Assessment
COMbined with
Automated Testing

Networked information and communication systems are omnipresent in our everyday life: In industrial production or in critical infrastructures such as power supply or the banking sector, we are already highly dependent on them. With new technologies, such as autonomous vehicles, their importance will continue to grow. The direct, existential well-being of persons is thereby increasingly entrusted to information and communication systems. The requirements for their safety and reliability are correspondingly high. RACOMAT is a tool for the risk management of such systems, which combines security tests with a component-based, compositional risk assessment. This makes automation possible from risk modeling to safety testing.

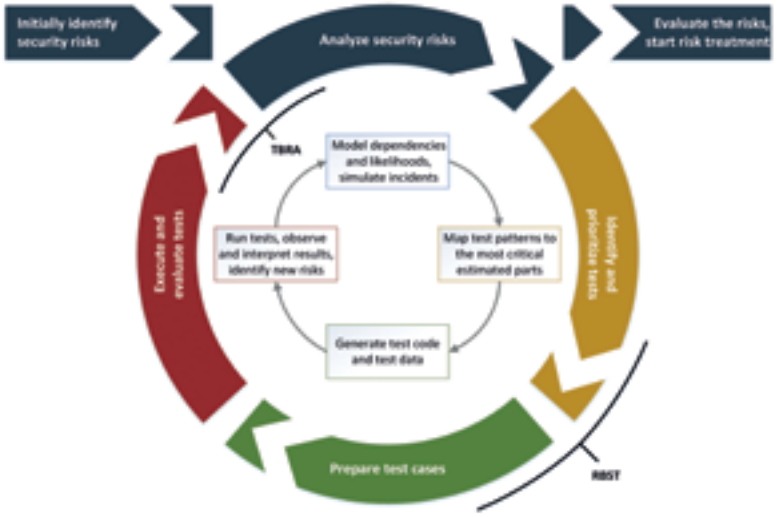
The RACOMAT Tool

In order to model and visualize a risk image, the RACOMAT tool uses intuitive risk graphs. RACOMAT supports the identification of potential vulnerabilities and threats with existing expertise from existing libraries. The RACOMAT tool calculates how much effort is required for security testing in order to improve the quality of the risk image by reducing uncertainties, starting from a total budget for the risk assessment. Security test patterns and tool-generated system models are used to perform automatic or at least semi-automatic testing. A more compact presentation with a focus on the economic aspects makes sense for further risk management, i.e. for risk evaluation and risk treatment. The RACOMAT tool provides the management with a dashboard that expresses the risks as expected costs per unit of time, and functions to plan and control the risk management.

THE RACOMAT TOOL ENABLES A SUCCESSFUL RISK MANAGEMENT EVEN IN COMPLEX SYSTEMS



Risk assessment procedure



RACOMAT makes it possible to model business scenarios and to link the business process models with the underlying technical infrastructure so that the impact of technical risks on the core business can be analyzed. Using domain-specific wizards, this can also be automated to a certain extent. For the finance and banking sector, such an assistant has already been developed as a plug-in.

Risk management according to industry standards

The RACOMAT Tool supports ISO 31000 compliant risk management. It suggests an iterative approach to risk assessment. An initial, coarse risk image is gradually improved in several rounds. The concepts of risk-based security testing (RBST) and test-based risk assessment (TBRA) are linked to combine the strengths of both approaches.

Iterative Risk Management

1. Develop the initial risk model based on literature, empirical values and expert assessment
2. Use event simulations to calculate the consequences and overall risks of threats
3. Select threat scenarios with the greatest uncertainties that should be analyzed in detail using security tests
4. Generate required test cases
5. Perform tests and use the results to improve the risk model
6. Once again, use an improved risk model to carry out event simulations in order to determine overall risks more precisely

– Continue with step 3 until the budget for the risk analysis is exhausted

7. Final risk evaluation and measures to reduce unacceptably high risks

jda | 1307 (Fotos: iStock – oluolu3)