Increasingly, chips are being utilized in applications where security is a key aspect: banking, price tagging, pay-tv, etc. Security is important, as privacy, personal integrity, and money is involved. Security requires as little observability and controllability of on-chip data as possible, in order to withstand even advanced high-tech hackers. In addition, we as IC design community want of course that our intellectual property in the design itself is protected from copying by others. Good manufacturing test quality on the other hand depends on good controllability and observability of on-chip data. Design-for-Testability hardware is added to most ICs to enhance the internal controllability and observability and hence enable high test quality. Are these two aspects indeed contradictory, and can we have only one at a time? If that is the case, isn’t the product quality of secure chips on which we store our virtual money or personal data in jeopardy? In this panel session, we will discuss with representatives from the secure industry (who typically hide from publicity) and test solution providers how they untie this knot, and what challenges are still ahead.

Moderator : Brian Chess, Fortify (Los Altos, CA, USA)
Panelists : Herve Fleury, Philips Semiconductors (Caen, France)  
Rohit Kapur, Synopsys (Sunnyvale, CA, USA)  
Steve Pateras, LogicVision (San Jose, CA, USA)  
Laurent Sourgen, ST Microelectronics (Rousset, France)
Organizer : Erik Jan Marinissen, Philips Research (Eindhoven, The Netherlands)

The panel will follow the traditional panel format: five-minute position statements by all panelists, followed by an interactive discussion between panelists and audience.