

# Third Dutch Process Control Security Event

On June 4<sup>th</sup>, 2009, the third Dutch Process Control Security Event took place in Amsterdam. The event, organised by the Dutch National Infrastructure against Cybercrime (NICC), attracted both Dutch process control experts and members of the European SCADA and Control Systems Information Exchange (EuroSCSIE). A set of plenary sessions and parallel workshops addressed a wide range of topics. Seán McGurk, the Director of the US Department of Homeland Security (DHS) discussed in his keynote speech the US Control Systems Security Programme (CSSP). Later, in a subsequent workshop, he answered a set of questions by the audience about cyber security and the benefits of international cooperation. Nate Cube, CTO and Co-founder of Wurdtech Security Technologies, discussed the cyber vulnerabilities of process control systems based upon the Industrial Cyber Security Vulnerability Database. A set of parallel workshops followed. We will highlight some of them.

The EuroSCSIE had issued a short questionnaire to Process Control/SCADA manufacturers, vendors, system integrators and support organisations. The objective was to get an understanding on how information security is perceived by these companies regarding both their products and services, and their internal processes. Stefan Lueders of CERN presented the background and structure of the questionnaire. Eric Luijff of NICC, TNO presented the analysis of the returned questionnaires. The questionnaire results reveal that the manufacturers, vendors, system integrators and support organisations still can improve a lot in the area of information security. As such, these results are an important step to seek the dialogue about increasing security between the end users/operators of the process control systems and the product/services companies.

**Annemarie Zielstra**

Programme manager

NICC

[annemarie.zielstra@ictu.nl](mailto:annemarie.zielstra@ictu.nl)



In another workshop, the human behaviour aspects in information security were discussed. Responsibility alone is not enough to address the cybercrime issues; ownership is the key! Both personnel and management need to be closely associated with addressing cybercrime. A subsequent workshop discussed how one can convince management. The secret: let them feel a little less comfortable and a little bit more insecure.

Since early 2009, the NICC works on a Dutch national roadmap to secure process control systems. The US roadmaps are considered as examples, but the Dutch approach will be a cross-sector approach with a very practical aim. The first outlines were sketched. The roadmap centres on the end user and will be very pragmatic. The intent is to follow-up the outlines of the roadmap in 2009 and have it agreed by a broad range

of stakeholders: manufacturers, system integrators, service organisations, end users from the critical sectors, government agencies, research and development. The objective of the roadmap will be that in eight year's time any unauthorised use of process control systems cannot lead to serious disruption of critical infrastructure supply. One aspect will be incident registration of cyber security incidents in process control/SCADA systems. It was indicated that such a registration will start soon by a way of trial.



At the end of the event, Annemarie Zielstra, Programme Manager of NICC and Seán McGurk signed an agreement which allows Dutch public and private parties to take part in the DHS Industrial Control Systems Cyber Security Advanced Training which includes a red team/blue team exercise. The training will take place in November, 2009.

All attendees were very pleased with the interaction they had with their colleagues from other companies and the content of the workshops. They are looking forward for the 4<sup>th</sup> event!

**RED BLUE TEAM TRAINING**

Control Systems Cyber Security Advanced  
 and private organizations linked to the  
 nation Exchange.

Where: Control Systems Analysis Center loc  
 Who Should Attend: Control System Engine  
 IT personnel, Network Engineers and manag  
 responsible for critical infrastruc

training on protecting and securing control systems