Long Term Cybersecurity research
Summaries of joint US-NL projects granted under the
DHS-NWO/V&J research cooperation initiative (2013-2014)

Project number	**628.001.023**
Principal Investigators	*Sandro Etalle (University of Eindhoven, NL)* *Alfonso Valdes (University of Illinois at Urbana Champaign, US)*
Project title	**IN-DEPTH DEFENSE OF SCADA AND INDUSTRIAL CONTROL SYSTEMS**

Scientific summary

SCADA and ICS formerly relied on isolated systems and proprietary protocols, but are increasingly interconnected and employ open protocols or legacy protocols encapsulated in TCP/IP. From smart grids to advanced automated manufacturing, these trends provide an opportunity for vastly increased system performance, but may also expose these systems to cyber-attacks. The situation is exacerbated in that for many reasons, enterprise security practices do not always transfer well to SCADA and ICS.
On the other hand, these systems are characterized by regular communication patterns and comparatively simple protocols (compared to enterprise systems). Intrusion detection techniques that are not widely used in enterprise systems because of false positives (for example, learning-based anomaly detection) or intractability (intrusion detection based on exceptions to a formal specification of correct system behavior) may be applicable in these environments. This work builds on complementary anomaly detection and specification-based detection work that has been going on at the University of Eindhoven (NL) and the University of Illinois (US) to develop a blended system to secure SCADA and ICS. The developed security technology will be made available in an open framework (currently envisioned to be extensions to the BRO IDS).