Marc Vauclair

From: OpenSG SG Security WG Embedded Systems Security Task Force [OPENSG-SGSEC-EMBSYSSEC-TF@SMARTGRIDLISTSERV.ORG] on behalf of Khera, Rohit [Rohit.Khera@SANDC.COM]
Sent: Wednesday, July 27, 2011 23:28
To: OPENSG-SGSEC-EMBSYSSEC-TF@SMARTGRIDLISTSERV.ORG
Subject: Note from DCSSI around TRNG methods in BSI AIS 31
Attachments: image001.jpg; NOTE-05_Evaluation_AIS31_en.pdf

Attached is the note from DCSSI (France) around use of TRNG functionality classes outlined in BSI AIS 31 that was referenced on the call today

Significantly, this document questions statistical modeling of physical random sequences in AIS 31 based on model assumptions of their underlying distributions, and recommends DRBG post processing on output sequences (Refer to section 5 ‘Reservation on the Method AIS31’)

Regards

Rohit Khera
Product Innovation
S&C Electric Company
510 749 5689
1135 Atlantic Avenue
Suite 100
Alameda, CA 94501-1174
USA
www.sandc.com