

## 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](http://www.sandc.com)

---

#### NOTICE OF CONFIDENTIALITY:

This message may contain information that is considered confidential and which may be prohibited from disclosure under applicable law or by contractual agreement. The information is intended solely for the use of the individual or entity named above. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of the information contained in or attached to this message is strictly prohibited. If you have received this email transmission in error, please notify the sender by replying to this email and then delete it from your system.