Security testing will be part of the Integrated Application Test Campaign.

1. Client/Server Security – 62351-3/62351-4/-6  
     
   Environment  
   1. Provide proof of support for coexistence of simultaneous of secure and non-secure interactions for the secure implementations.
   2. “Secure clients” will connect to the “secure servers” while the server is participating in the integrated application using non-secure associations. The “secure client” to “secure server” will be over a 62351-3 and Certificate based application ACSE association per 62351-4.
   3. “Secure Clients” must participate in the integrated application using non-secure associations simultaneously to (b).
   4. Vendors will provide their own certificates for exchange (e.g. CA and actual certificates). This will allow the verification of multiple X.509 certificate file formats as part of the IOP. Vendors must also bring replacement certificates and a CRL.

Test Cases

* 1. Non-secure proof of life will be provided through establishment of integrity reporting of pre-existing DataSets.
  2. Secure test cases (Herb to write up):
     1. Association establishment
     2. Association release
     3. Cable Pull (needs documentation of TCP\_Keepalive value)
        1. Server
        2. Client
     4. Revocation of a certificate
     5. Attempt to establish a connection with a revoked certificate
     6. Attempt to establish a connection with an unexpected certificate.
     7. Data transfer

1. RBAC – 62351-8, 62351-90-1
2. Syslog – (Siemens, GE, SISCO, Palo Alto, CISCO)- Security event centric test cases. Siemens to make a first pass.
3. Radius (placeholder)
4. SNMPv3 testing and/or IEC 62351-7 – Frances to assist, Herb. User or TSM/TLS (probably not available yet in implementation). Probably means User authentication.
5. EAP Testing  
   1. Define and enforce access controls at EAP
   2. Threat detection
      1. Layer 7
      2. Known threats
      3. Intrusion detection
      4. Role based access/logging of traffic – Palo Alto to develop
   3. Resiliency of EAP – in process
   4. Syslog
   5. SNMP/Security MIBs
   6. MMS, R-GOOSE, L2-GOOSE   
      
   7. L2-GOOSE Performance Testing through the infrastructure
   8. Access control to EAP devices