WW ENGINEERING MONTHLY NEWSLETTER – DECEMBER 2017

Hi team,

As I was getting out of bed on Sunday morning I received a text message from Jerry which said "Did you know Thales is acquiring Gemalto?" Needless to say I jumped out of bed, surprised, opened my mailbox and read all about the BIG ANNOUNCEMENT that Thales is acquiring Gemalto for a staggering €4.8 billion! We will be watching the developments and updates from Thales Corporate folks and our own execs but all I can say or think is "Never a dull moment!" With the new DBU going live on January 1st 2018 and a major acquisition in data security closing in the 2H-2018 I can only imagine that 2018 and beyond are going to be interesting and exciting times for us. But let this not be a distraction for us. We should remain focused on executing our roadmaps as planned.

A HUGE thank you to all of you for your efforts in 2017 product delivery! I wish you all Happy Holidays and the very best for 2018.

-Ashvin

This month's newsletter includes several great articles and stories:

- PS10K DfX Manufacturing Test Strategy – An update by Jerry Wardrop
- nShield Adrastea Release – An update from Nick Stoppard
- Connect XC remote Administration feature for supporting Microsoft Azure Raw – An update from Nick Stoppard
- Integration of Thales Security Products in the Pivotal Cloud Foundry Platform – An update from Arup Biswas
- Tools initiative, Fabric and more – An update from Mark Hicken
- Pune,, India office move – An update by Anirudh Mavinkurve and Mahesh Mohan

PS10K DFX MANUFACTURING TEST STRATEGY

Jerry Wardrop (Jerry.Wardrop@THALESESEC.NET) reports…

The payShield 10000 DfX Test Strategy focuses on early failure detection at the Printed Circuit Board Assembly (PCBA) level and relies on three manufacturing approaches; color Automated Optical Inspection (AOI), Automated X-Ray Inspection (AXI), and In-Circuit Test (ICT). Color AOI applies high definition color monitoring of all components being physically placed on the board; correct part, orientation, and location placement. If a part is incorrect or misplaced during manufacturing, an alarm is triggered and the line stops for resolution. AXI is automated X-Ray inspection of high density Ball Grid Array (BGA) components are inspected for proper placement and solder adhesion. For example, the main processor has 1295 solder balls on the underside of the component and each must be properly aligned on all three axis and properly soldered. The AXI is used to verify the placement and to measure adhesion to manufacturer's specification for the part. ICT is a process where a functional test fixture is created, unique for each board, and allows for comprehensive electrical testing (Joint Test Action Group JTAG) at the board level. These three processes ensure consistent high quality manufacturing for each PCBA manufactured.

The picture illustrates the payShield 10000 production test strategy and the AOI, AXI, and ICT steps. Once passed, the PCBA's are then sub-assembled with memory, lids, and installed into a chassis for Functional Configuration

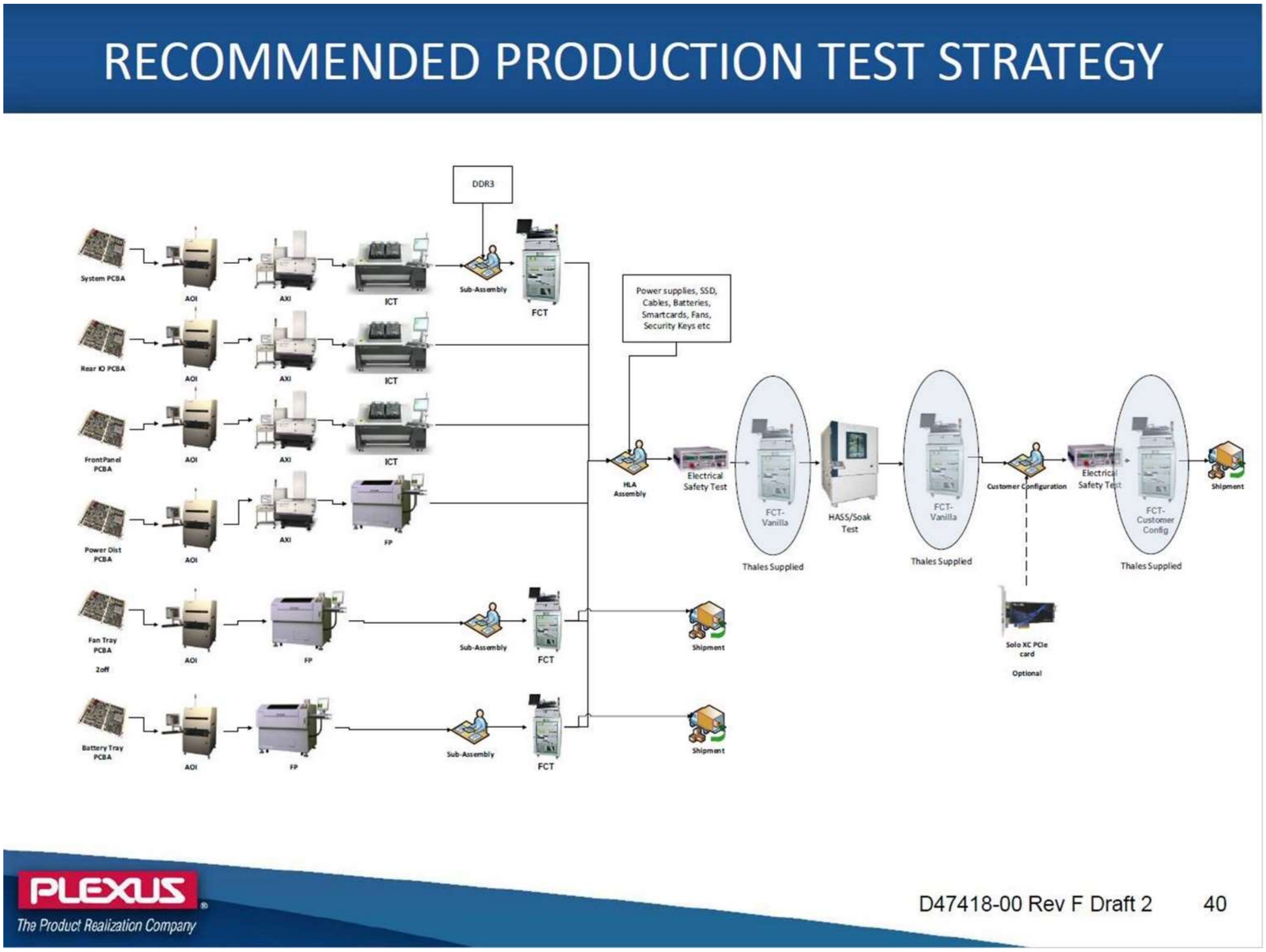
Testing (FCT). FCT is the first set of functional production tests performed against the system as a whole. If pass, the remaining high level assembly components (fans, battery, power supplies, etc.) are installed and an electrical safety test for shock is performed.

The remaining steps in the process are also FCT type tests specific to Thales for product Warranting and Licensing. This is where the Trust is injected into the product, which is then used throughout the life of the product to validate all subsequent code being loaded and operating. Licensing is the process of enabling functionality (commands, algorithms, key length, and performance) purchased by the customer.

During the final steps, initial Highly Accelerated Life Test (HALT) testing is performed for enhancing product reliability by determining the stress-related margins that the product can be subjected to before failure occurs. This is a very important step in the design process for ensuring the product will meet or exceed customer environments. Routinely, newly manufactured product will be subjected to Highly Accelerated Stress Screening (HASS), more vibration testing, to ensure the product manufactured is within the HALT-defined margins. More regular application of HALT and HASS testing is intended in the strategy to reduce infant mortality failures experienced by our customers.

As illustrated, there are three Thales supplied FCT steps which are traditionally performed by our internal New Product Introduction (NPI) team. The first, configures the payShield 10000 to a “vanilla” state with no specific application personality. The second FCT step, when executed, verifies the HASS test results for compliance and the third FCT step executes the Thales production tests performed against the unit configured specifically to a sales order. We are evaluating these last three steps to reduce the number and amount of “Thales touches” to the product as a method for increasing the manufacturer’s ability to perform failure analysis on returned units.

Stay tuned, as I am intending to include the DfX Test Strategy as a topic for a future payShield 10000 raising awareness session.



RECOMMENDED PRODUCTION TEST STRATEGY

PLEXUS
The Product Realization Company

D47418-00 Rev F Draft 2 40

NSHIELD ADRASTEA RELEASE:

Nick Stoppard (nick.stoppard@thales-esecurity.net) reports:

ADRASTEA is one the most important and complex releases that Cambridge engineering have undertaken in recent years. The GA release is scheduled for March 2018 with its primary aim being eIDAS certification for nShield and will:

- Provide a secure logging capability which is compliant with the needs of eIDAS certification
- Provide a method a synchronising time being used in the logs from different HSMs
- Merge the Solo XC and Solo firmware onto a single common baseline ensuring the HSMs have a common feature set
- Prepare the merged firmware for FIPS 140-2 Level 2 and 3 certification
- Prepare the software for Common Criteria certification
- Fix known vulnerabilities and provide patch releases for old versions
- Continue to drive improvements into the CI/CD system and automated testing

The largest customers for Adrastea will be those that recognise an immediate need for these future certifications (Common Criteria and FIPS).

The majority of ADRASTEA features will be dev complete by the end of the 2017 and will therefore be ready for final IVVQ. In order to mitigate risks associated with final IVVQ we are currently performing early Software TRRs (end of dev checklist) on all features before Christmas (even if the feature is not completed), to check for remaining work and allow IVVQ to get prepared early. In addition, it is planned to bolster IVVQ resource and accelerate early testing on the firmware merge activity.

For this release the biggest risks and potential mitigations marked in red are as follows:

- Features working on Solo XC after the merge is complete
  - ***Ensure IVVQ are aligned to perform early system testing on the new XC merged firmware over Christmas (automated tests) and early next year. This will give us early indications of any issues.***
- CI/CD system – moving from Jenkins CI to bamboo CI (with CMake) involves significant risk
  - ***Maintain the Jenkins CI up and running so it can continue to be of use should problems occur. The new CI/CD team (team Marx) are on standby to support the release when needed.***
- IVVQ effort – Resource and time are constrained and given recent issues with Saturn we need to ensure tests are not overlooked.
  - ***Start to write the test plan early and review this. Also, ensuring that all dev teams are available 100% during the IVVQ phase to perform their own testing as well and continue to build up the automated testing (as opposed to jumping onto working on the next release).***
  - ***Ensure a sufficient level of governance attached to all gated processes***
- Impact on ADRATEA resources of other high priority projects e.g. Azure Raw
  - ***Ensure that we do not over commit ADRASTEA engineering resource to other projects***
- Christmas holidays leading to slow ramp up in new year
  - ***Brief all teams and managers on the importance of maintaining momentum when returning after break***
- Impact of reliability issues with Connect XC have used most of our schedule contingency, so there is no project schedule reserve remaining.
  - ***Ensure our schedules and metrics are reviewed frequently so mitigation actions can be taken immediately***

In addition to the large risks stated above, we must be cognisant of lower risks that may prove to be significant and must therefore keep assessing our entire register, retiring or providing mitigation to those risks that demand attention.

From the perspective of our business we understand that ADRASTEA will be a major milestone, merging complex firmware and acquiring certifications that are demanded by the market in the information security domain. It is from this understanding that we have dedicated the majority of our engineering resources in Cambridge and Crawley to deliver this important project for our business.

AZURE RAW

Microsoft Azure Raw Project

Nick Stoppard (nick.stoppard@thales-esecurity.net) reports:

Over the past few months UK Engineering, Technical Directorate and Product Management Group have launched an initiative to provide MS with a remote administration capability through a separate serial port located on the mother board accessed via the rear panel of the Connect XC. This will provide MS with the ability to offer HSM's as a service to selected customers. MS will be able to remotely recover, purge and reassign HSM's after a tenant has reached the end of their leasing contract. Tenants will retain full ownership of their key material, the ability to create/manage their security world, and continue to be able to purge all key material and therefore sterilise their footprint on the Azure Raw HSM at the end of leasing.

Prior to formally launching this project the engineering and technical teams have worked towards a demonstrator which will be shipped to MS before Christmas. The final development day for this demo will be the end of the current sprint which is the 19th of December. Following this sprint, the lids will be fastened down on four Connect XC's ready for shipping on 21/22 December. Team Starbug, led by Hamish Cameron, is currently testing the Connect XC's with new firmware images that include the latest iteration of the serial Command Line Interface. It is envisaged that sufficient functionality will be available via the serial port to demonstrate the concept in sufficient detail prior to Xmas. Last week, John Hartley gave a high level demo of Azure raw to Microsoft which appeared to go well!

For the Azure GA, Hardware/software/IVV estimates are suggesting that its release date may be coincidental with the ADRASTEA release currently scheduled for March 2018 which means there is a strong possibility that we can snap one to the other for an integrated version 12.50 release.

So far the Azure Raw project has demonstrated that Engineering, Technical Directorate and Product Management are operating seamlessly in an integrated manner alongside on of most important customers. The results of this close cooperation is a concept demonstration to MS which will provide our business with a solid foundation and enhance our position for future sales of Connect XC!

TOOLS INITIATIVE, FABRIC AND MORE

Mark mark.hicken@thales-esecurity.net, reports…

- **Tooling**: DevOps have the Global BitBucket/Git and Artifactory repos up and running and AuthN is available WW. We're now working on build portability i.e. config as code for Building Blocks for all new BB's
- **Tools Initiative**: After a short break the Tools Initiative will restart monthly meetings in the New Year to plan out the major tooling changes for 2018. This will drive further consolidation of our toolchains around Git, Bamboo for CI/CD and Artifactory
- **Fabric**: We're building a consistent light weight approach to capturing Portfolio Needs and breaking them down into Features delivered through Building Blocks:
    - Progressing with TD and PMG the use of Product Increment Proposals to capture Product needs in a consistent way across the Portfolio
    - Feature Design Descriptions are in development by the DA's on Lucy and VTS to capture high level designs which will be based on Product Increment Proposal Needs.

- **Export Control**: Quotes are coming in via our UK supplier for a solution based on our development sites in India, US and UK.

SAN JOSE ENGINEERING TEAM VISITS THE PIVOTAL OFFICE IN SAN FRANCISCO TO DISCUSS THE INTEGRATON OF THALES SECURITY PRODUCTS IN THE PIVOTAL CLOUD FOUNDRY PLATFORM

Arup Biswas (abiswas@thalesesec.net) reports:

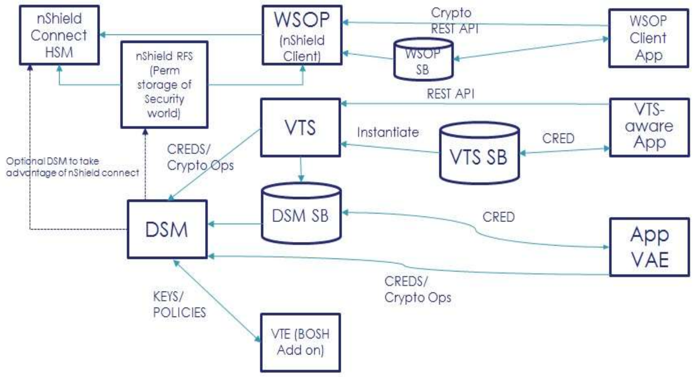
On Nov. 1st and 2nd Rajesh Gupta, Anand Ozarkar, Feng Xu, Alvin Abad and Arup Biswas visited the Pivotal office in San Francisco for discussing the architecture and integration of Thales e-Security products into the Pivotal Cloud Foundry platform.

Outline of the activities:

On day one, we started by presenting the use case discussed at the digital factory meeting in Paris. This discussion invoked many questions from Pivotal side regarding different products in TeS. The day ended with hands-on training with the PCF development environment. On day two, we had an in depth technical discussion with the Pivotal application architect. It was an interactive session with lots of questions from both sides. We discussed various design choices for each of the component. At the end of this discussion, we arrived at the system-level integration architecture for the Thales e-security products. This was followed by another in-depth discussion with the BOSH architect from Pivotal. During this session, we discussed the BOSH architecture and specifically the use case of Vormetric Transparent Encryption (VTE) as a BOSH add-on. We identified several issues including a blocker at this time. We ended day two with more hands-on training.

TeS-PCF Integration Architecture:

The following diagram depicts different components for the PCF integration. PCF platform uses service broker to instantiate a service. An application binds to a service using the service broker, which instantiates the service, provides the application with the service location and other credentials and goes away. Application can then interact with the service using the service interfaces.



Legends:

SB: Service Broker
VTS: Vormetric Tokenization Server
VAE: Vormetric Application Encryption
VTE: Vormetric Transparent Encryption
WSOP: Web Services Option Pack (nShield)
DSM: Data Security Manager

EXODUS TO RMZ WESTEND – INDIA TEAM OFFICE RELOCATION UPDATE

Anirudh Mavinkurve (amavinkurve-c@thalesesec.net) reports…

The Pune team has moved to a new office in the WestEnd building at Aundh Pune. The move was conducted on the weekend for 18th and 19th November, 2017. Bhupathi K was the *prime mover* (pun intended), assisted by other able members of the team.

The task at hand was to move equipment, people, and belongings and set up the new place all in one go.

An able team of volunteers was assembled and readied for the D day. On day minus one everything at the old office was packed and ready to move! And so it began!

Day 0:

Step 1 – movers and packers take everything to the new location, supervised by our volunteers

Step 2 – food 😉

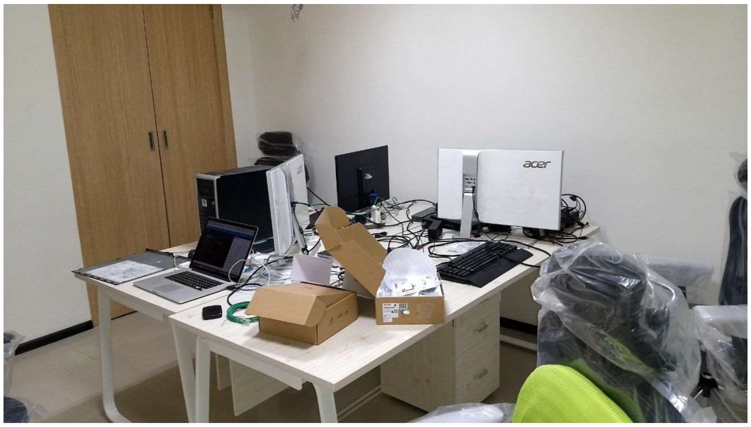
Step 3 – Partial unpacking – everyone's monitors assembled and placed at their desks!

The cafeteria:

Step 4 – coffee ☺

Step 5 – setup for the entertainment room. Yep, you heard that right. We have an entertainment room at the new office – with a 1080p projector, state of the art surround sound system and the works. Oh, and it also doubles up as a conference room.

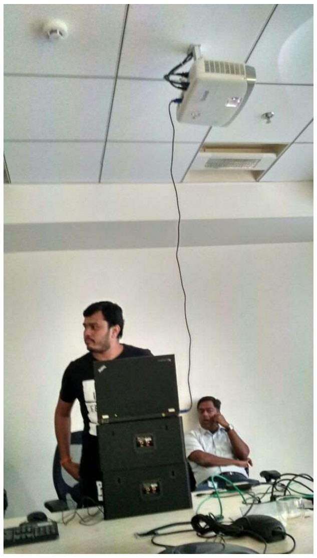
Our network operations center (Anirudh's office temporarily converted):



Overall it was handled quite well – no loss of work!

And we were up and running in time for Ashvin's visit:

Shrikant ended up stacking his laptop on a couple of speakers to make it reach the cable:



Shrikant ended up stacking his laptop on a couple of speakers to make it reach the cable:

You can take us out of the garage, but not the garage out of us… 😆