29th Annual INCOSE
international symposium
Orlando, FL, USA
July 20 - 25, 2019

Applying Feature-Based Systems and Software Product Line Engineering in Unclassified and Classified Environments

James K. Teaff, ME, CSEP
Raytheon Intelligence, Information and Systems
16800 Hughes Dr., Aurora, CO 80011 USA
+1-303-344-6000
James.K.Teaff@Raytheon.com

Dr. Bobbi Young
Raytheon Missile Systems
1151 E Hermans Rd.
Tucson, AZ 85756 USA
+1-520-794-9022
Bobbi.Young@Raytheon.com

Dr. Paul Clements
BigLever Software, Inc.
10500 Laurel Hill Cove, Austin TX 78730 USA
+1-512-777-9552
pclements@BigLever.com

Abstract. Global aerospace and defense companies are reaping the benefits of feature-based systems and software product line engineering and management (FBPLE) in those situations where production must seamlessly span unclassified and classified environments (Gregg et al. 2014) (Gregg et al. 2015) (Krueger et al. 2014) (Lanman et al. 2011). These benefits include leveraging company talent while awaiting access to classified material; leveraging employees who are members of other sovereign states; and optimizing system production and maintenance for export / import. In this whitepaper we present the architectural design and accompanying business processes for a PLE factory and its artifacts that comprise unclassified and classified digital assets[1]. These digital assets are used in automated generation of unclassified and classified product instances. All production activities occur within a single logical enterprise spanning multiple information systems comprising multiple security zones[2].

[1] Digital assets are artifacts that can be managed on an information system, and include software, hardware design specifications, bills of materials, team schedules & other management artifacts, and more.

[2] A security zone in this context is a collection of one or more information system segments with rules-driven control of inbound and outbound traffic, establishing a perimeter within which sensitive or classified information is processed.

This document does not contain technology or Technical Data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Introduction

As aerospace and defense companies expand their product offerings in the commercial and foreign sovereign state markets, systems and software product lines have expanded production into an enterprise spanning multiple information systems at different classification levels and adhering to different security classification guides, e.g. unclassified, secret, and top secret. Inherent in this expansion is the need to protect the confidentiality and integrity of the deliverable system elements within the enterprise while simultaneously enabling efficient production of system elements at all classification levels. This paper describes the business architecture and system architecture for implementing feature-based systems and software product line engineering and management (FBPLE) in this challenging context.

Systems engineers correctly focus much of their attention on the deployed products in their product portfolio. Of equal importance in a product line engineering (PLE) context is the architecture of the PLE factory that assembles the deployed products. Analogous to a hard goods factory that generates automobiles in different configurations from an inventory of assets, a PLE factory is a collection of assembly lines that automatically generates, tests, and deploys variations of systems from an inventory of digital assets (Flores et al. 2012). Industry has shown that application of this PLE factory paradigm provides an organization with greater agility to meet market demands and provides a competitive advantage with capability-rich offerings in a cost-efficient fashion, including a tenfold or more improvement in the ability to field new features and provide ongoing maintenance of complex systems of systems (Gregg et al. 2014) (Flores et al. 2012).

Historically, classified products for each government customer are developed in isolation by aerospace and defense companies, primarily due to the protocols levied by each customer to protect the confidentiality and integrity of the deliverable system elements as depicted in Figure 1.

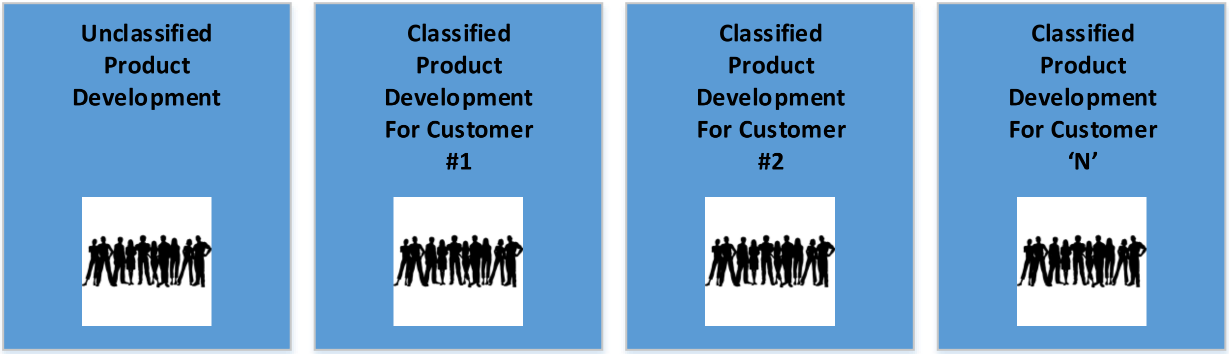
Unclassified Product Development
Classified Product Development For Customer #1
Classified Product Development For Customer #2
Classified Product Development For Customer 'N'

Figure 1. As-Is Business Architecture

Characteristics of this as-is business architecture include:

- Product development for a customer's system is performed only by those people with a security clearance granted by that specific government customer, e.g. secret, or top secret.
- Product development is performed within information systems adhering to the physical security and cybersecurity controls required by a specific government customer. This typically results in aerospace and defense companies standing up separate system devel-

opment environments for each government customer; and at times multiple system development environments for the same government customer.

- Digital assets cannot be shared between product development teams without prior written agreements with the applicable government customers.
- Digital assets are transferred between information systems adhering to a manually intensive business process which is lengthy, expensive and prone to human error.

These characteristics have driven a number of undesirable effects:

- Each product development requires a dedicated team operating within separate (disconnected) information systems placing a burden on staffing and resource expenses.
- Digital asset reuse is ad-hoc, using clones pulled from either unclassified shared asset libraries, and/or clones from shared asset libraries at the same security classification.
- Product development teams maintain their clones in isolation, or at best return and merge their clones into the originating shared asset library, with attendant errors, inefficiencies, lack of agility, and significant increases in new feature development and maintenance costs over time (Krueger et al. 2013).

To expand into global markets, aerospace and defense companies are finding they need a better factory that can securely assemble and deliver both unclassified and classified versions of their products. The architecture drivers for this new-and-improved PLE factory are:

- Provide the ability for all employees across the globe to perform product development via a virtual office while protecting the confidentiality and integrity of customer-specific digital assets using cybersecurity controls, i.e. a multiple information system security zone enterprise.

- Enable fully automated assembly of all product variants by a single product development team in a consolidated virtual PLE factory vs. individual development teams and information systems for each customer. Figure 2 depicts the target business architecture.

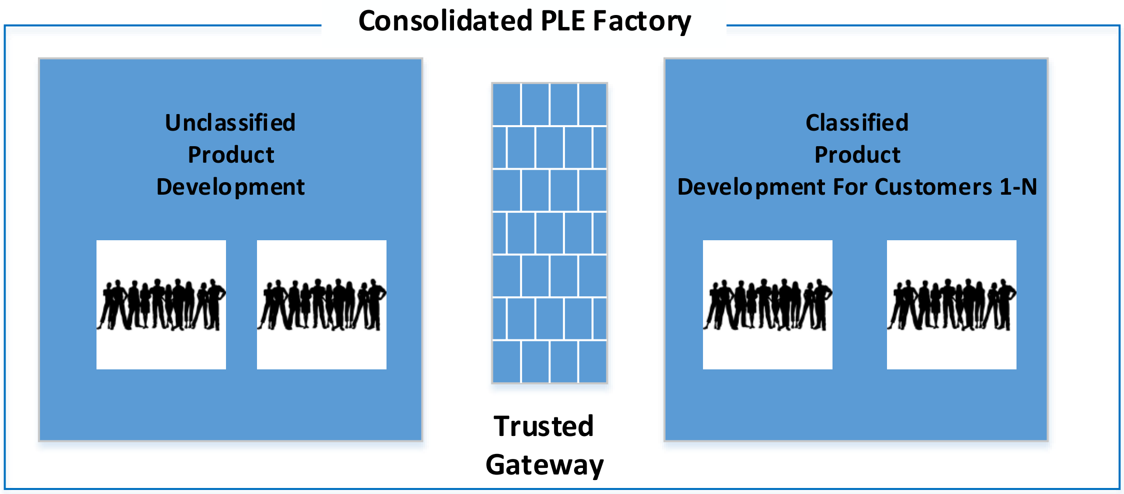
Consolidated PLE Factory
Unclassified Product Development
Trusted Gateway
Classified Product Development For Customers 1-N

Figure 2. Target Business Architecture

This document does not contain technology or Technical Data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Based on the security requirements for a PLE factory generating classified products, we derived the following as part of our architecture vision to account for multiple security zones:

- All production for a delivered system occurs within a single product line's enterprise and by a single team; no production occurs within a separate information system except where contractually required (e.g. final acceptance tests). Note that with this architecture vision statement we specifically prohibit the as-is practice of having a separate engineering team and a separate information system for development of each individual product instance.
- Digital asset creation and maintenance is primarily performed in an unclassified environment, thus providing the ability to import / export the system internationally, as well as leverage a broad company talent base, including employees that are waiting for access to classified material; and employees who are members of any sovereign state. Contrast this with the current practice of all asset creation – including unclassified asset creation – being performed within a classified security zone.
- Classified digital asset creation and maintenance occurs within a dedicated information system security zone for each classification level, e.g. secret, top secret.
- Automation is used to transfer digital assets across the production line's information system security zones except for when an asset requires a security-approved "human-in-the-loop" business process, in which case a business process management tool is used to increase the efficiency of the security approval.

What Is Feature-Based Systems and Software Product Line Engineering?

Systems and software product line engineering (PLE) is a way to engineer a portfolio of related products in an efficient manner, taking full advantage of the products' similarities while respecting and managing their differences (Krueger et al. 2013) (Clements et al. 2002). By *engineer* we mean all of the activities involved in planning, producing, delivering, and deploying, sustaining, and retiring products. Modern PLE has incorporated lessons learned over the past decades and resulted in an advanced set of explicitly defined product line engineering and management solutions, forming what the community has termed feature-based systems and software product line engineering and management – or more simply feature-based PLE (FBPLE) (Krueger et al. 2013) (Krueger et al. 2017). FBPLE is based on the concept of features that describe unique product instance characteristics; and it relies on automated digital asset variation creators - PLE factory configurators - to instantiate specific configurations of digital assets across all aspects of the system development lifecycle (Krueger et al. 2013). Figure 3 illustrates these concepts. The shared digital assets, the feature catalog, the bills-of-features, the processes related to creation and evolution, and the staffed roles to carry it all out make up the PLE factory. Once the factory's assembly line capability is established, products are instantiated – derived from the shared digital assets and configured according to a bill-of-features – rather than manually created.

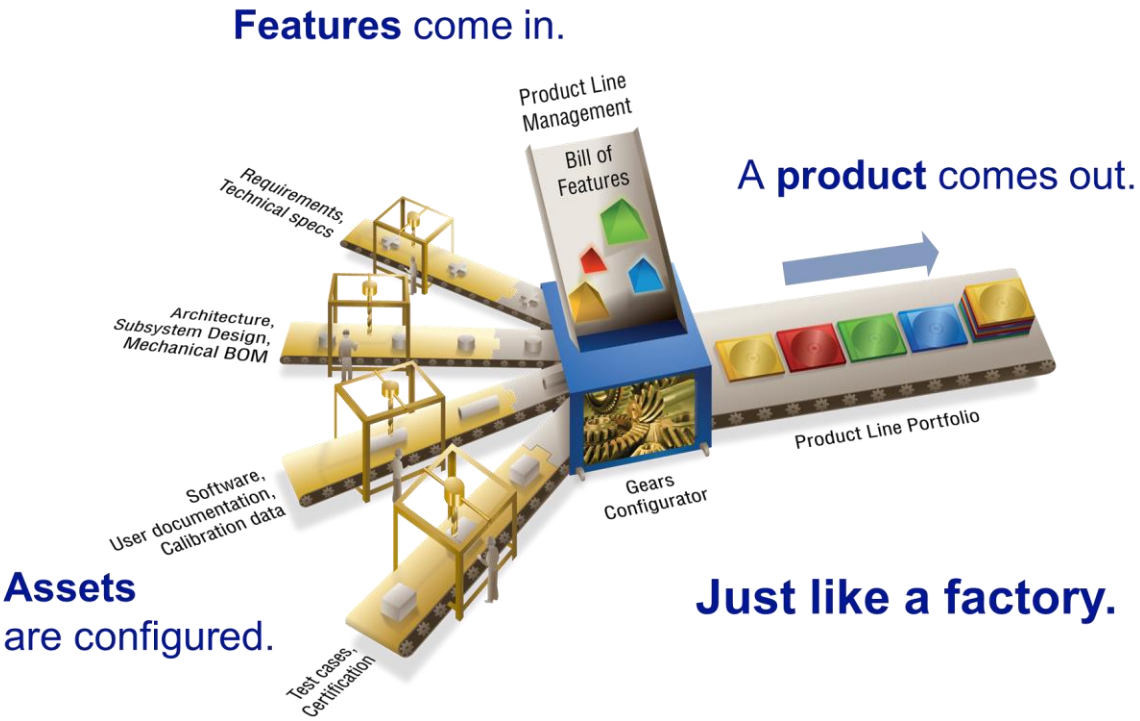

Figure 3. PLE Factory. Figure © BigLever Software, Inc. Used with permission.

Multiple Security Zones Pilot Example: Integrated Air and Missile Defense (IAMD)

In order to maintain the confidentiality and intellectual property of our respective customers and companies, rather than describing our actual PLE factories and products we illustrate our application of FBPLE by using a fictitious but realistic example from the Integrated Air and Missile Defense (IAMD) domain: a system for integrated air and missile defense called GloboShield as we previously described in (Young et al. 2018). GloboShield's mission is to provide a fully integrated capability to protect a theater from air and missile attack by detecting, tracking, identifying, and destroying airborne threats. Such a system includes sensors, displays, planning functions, threat evaluation, health and status monitoring, communication with other friendly command and control systems for information exchange, and more. A product variant implementation consists of a mix of hardware, software, and people elements. Figure 4 is a sketch of a system architecture view for GloboShield, identifying its major subsystems. (The figure does not tell the whole architectural story. It does not show behaviors or execution-time relationships among the subsystems; other architectural views do that. For the purposes of our discussion, we will let the figure stand in for the entire range of useful architecture documentation.)

This document does not contain technology or Technical Data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

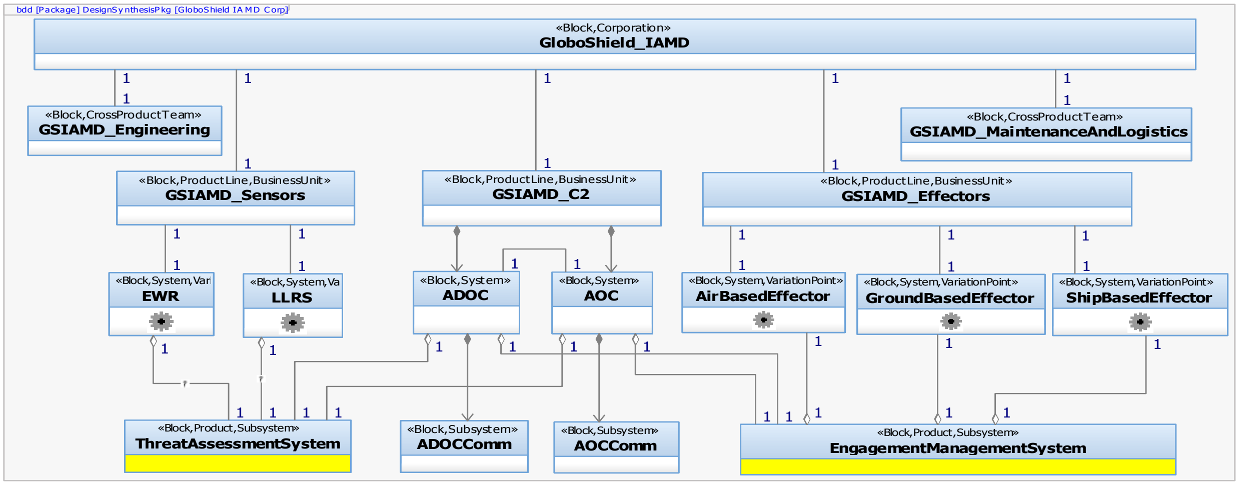
bdd [Package] DesignSynthesisPkg [GloboShield IAMD Corp]
«Block,Corporation»
GloboShield_IAMD
«Block,CrossProductTeam»
GSIAMD_Engineering
«Block,CrossProductTeam»
GSIAMD_MaintenanceAndLogistics
«Block,ProductLine,BusinessUnit»
GSIAMD_Sensors
«Block,ProductLine,BusinessUnit»
GSIAMD_C2
«Block,ProductLine,BusinessUnit»
GSIAMD_Effectors
«Block,System,Vari
EWR
«Block,System,Va
LLRS
«Block,System»
ADOC
«Block,System»
AOC
«Block,System,VariationPoint»
AirBasedEffector
«Block,System,VariationPoint»
GroundBasedEffector
«Block,System,VariationPoint»
ShipBasedEffector
«Block,Product,Subsystem»
ThreatAssessmentSystem
«Block,Subsystem»
ADOCComm
«Block,Subsystem»
AOCComm
«Block,Product,Subsystem»
EngagementManagementSystem
1

Figure 4. Fictitious GloboShield Architecture

GloboShield is a product line. Customers can order GloboShield in different configurations, and with different levels of capability. For example, each product has different sensor and weapon systems, as well as different organizations for managing air and missile defense. In addition, GloboShield provides options for its Threat Assessment capability. The customer may:

- Choose or omit the Threat Determination service to identify a threat that could be an air-breathing target (ABT) and/or a theater ballistic missile (TBM).
- Choose or omit, in addition to the Threat Determination service, a Threat Ranking and/or a Threat Warning service.

Each instance of GloboShield will have its own requirements, system architecture, software code, documentation, and more, that reflect the product choices outlined above as well as many others.

Production Scenarios for GloboShield across Multiple Security Zones

We use a set of production scenarios as an architectural design aid, synthesizing from them a set of factory architectures, each of which satisfies a different set of customer security requirements. First, a few United States Government definitions to better understand the production scenarios:

- Data Sharing: The authorization (by the information owner) to release classified data or information to an external system or program.
- Co-Processing: The use of a single information system (IS) to support distinct programs or efforts while maintaining the ability to distinguish the unique information, data, or intellectual property associated with each contract or effort for purposes such as program-specific data destruction or data sharing.
- Co-Mingling: The use of a single IS to support distinct contracts or efforts without the ability to distinguish the unique information, data, or intellectual property associated with each contract or effort for purposes such as program-specific data destruction or data sharing.
- Data sharing agreement: A unidirectional (one-way), agreement that allows a program to share classified information with another program. A data sharing agreement from

Program A to Program B allows sharing of Program A classified information and data with Program B.

Within the Globoshield example, classified information appears in the combination of sensors and weapons that are used for each customer base depending on ITAR restrictions and security classifications. In order for our GloboShield product line to be launched using harvested classified assets from pre-existing programs, as well as to continuously deliver product variants to various classified customers, multiple bidirectional agreements are brokered with the government agencies involved, (essentially this is a set of unidirectional data sharing agreements). However, in certain circumstances contractual obligations and security requirements mandate classified assets for an individual classified customer be manipulated solely within a dedicated information system, in which case a unidirectional agreement is brokered. This agreement allows the classified product variant to use common production line assets, and then use classified customer-specific assets within its unique production line segment. Additionally, each PLE factory adheres to co-processing security requirements, tracking via meta-data the information associated with each customer, giving us the most flexible security arrangement and broadest applicability. Information is automatically exchanged between the security zones via a trusted gateway system[3]. Note that we purposefully architect solutions where a human-in-the-loop business process is no longer required.

Production Scenario: Bidirectional Data Sharing Agreements with Co-Processing

In our base production scenario four GloboShield product instances are delivered – two unclassified product instances for international sales to sovereign states; and two secret classified product instances containing merged unclassified and secret classified digital assets (e.g. GloboShield customer-specific classified sensor algorithms) for classified customers. Figure 5 depicts the scenario. The PLE factory is operated with bidirectional data sharing agreements across all secret classified customers. Two information system security zones are established – an unclassified zone and a secret classified zone – represented as red dashed lines. The factory's production line is split into two daisy chained assembly line segments, one per security zone. Files are automatically and securely transferred between information system security zones via a trusted gateway system based on a synchronization event, e.g. a new software version delivery.

[3] A trusted gateway system provides secure, automated file transfers. The gateway provides rules-driven deep inspection of file contents and meta-data, transferring only those files allowed by security policies.

This document does not contain technology or Technical Data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

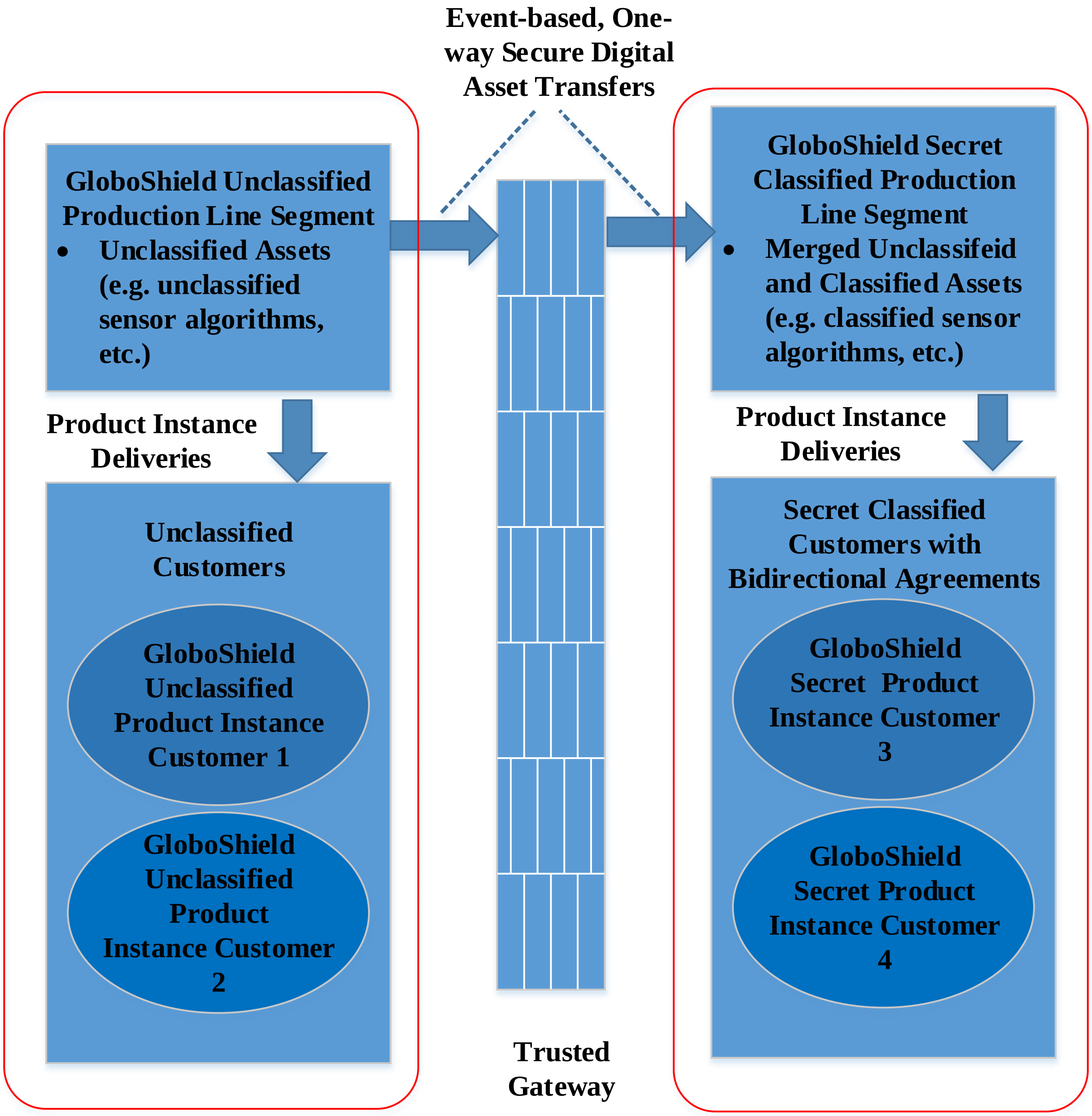
Event-based, One-way Secure Digital Asset Transfers
GloboShield Unclassified Production Line Segment
• Unclassified Assets (e.g. unclassified sensor algorithms, etc.)
Product Instance Deliveries
Unclassified Customers
GloboShield Unclassified Product Instance Customer 1
GloboShield Unclassified Product Instance Customer 2
Trusted Gateway
GloboShield Secret Classified Production Line Segment
• Merged Unclassifeid and Classified Assets (e.g. classified sensor algorithms, etc.)
Product Instance Deliveries
Secret Classified Customers with Bidirectional Agreements
GloboShield Secret Product Instance Customer 3
GloboShield Secret Product Instance Customer 4

Figure 5. Bidirectional Data Sharing Agreement with Co-processing Production Abstract

Production Scenario: Mixed Data Sharing Agreements

In this production scenario we build on the base production scenario described above by introducing a mix of classified customers (e.g. secret and top secret) whose security requirements require operating with a mix of unidirectional and bidirectional data sharing agreements. Figure 6 depicts the scenario. In this production scenario a total of five GloboShield product instances are delivered – two unclassified product instances for export to sovereign states; and three product instances containing merged unclassified and secret plus top secret classified digital assets for the secret and top secret classified customers. Three information system security zones are established – an unclassified zone, a secret classified zone, and a top secret classified zone, each of which complies with a specific set of security requirements – represented as red dashed lines. The factory's production line is split into multiple daisy chained segments, one per security zone. As in our base production scenario, files are automatically and securely transferred between security zones via a trusted gateway system based on a synchronization event.

The secret classified government customers for GloboShield product instances 3 and 4 have bi-directional data sharing agreements and can merge the unclassified and secret classified digital assets (Secret Classified Production Line Segment A). The top secret classified government customer for GloboShield product instance 5 only has a unidirectional data sharing agreement with the two secret classified customers. Therefore, production for that customer operates within its own top secret classified production line segment deployed within its own security zone (Top Secret Classified Production Line Segment B). This top secret classified environment can merge digital assets from Classified Product Line Segment A with its own customer-specific classified digital assets in its dedicated Top Secret Classified Production Line Segment B as it has a unidirectional data sharing agreement. However digital assets from Top Secret Classified Production Line Segment B cannot be shared back to the originating secret classified production line segment because there is no data sharing agreement in that direction and it is operating at a higher security level. Note that this production line architecture is easily extensible; for example when another top secret classified contract for GloboShield product instance #5's customer is launched, the new product variation development is executed within the security zone and production line segment already instantiated for that classified customer.

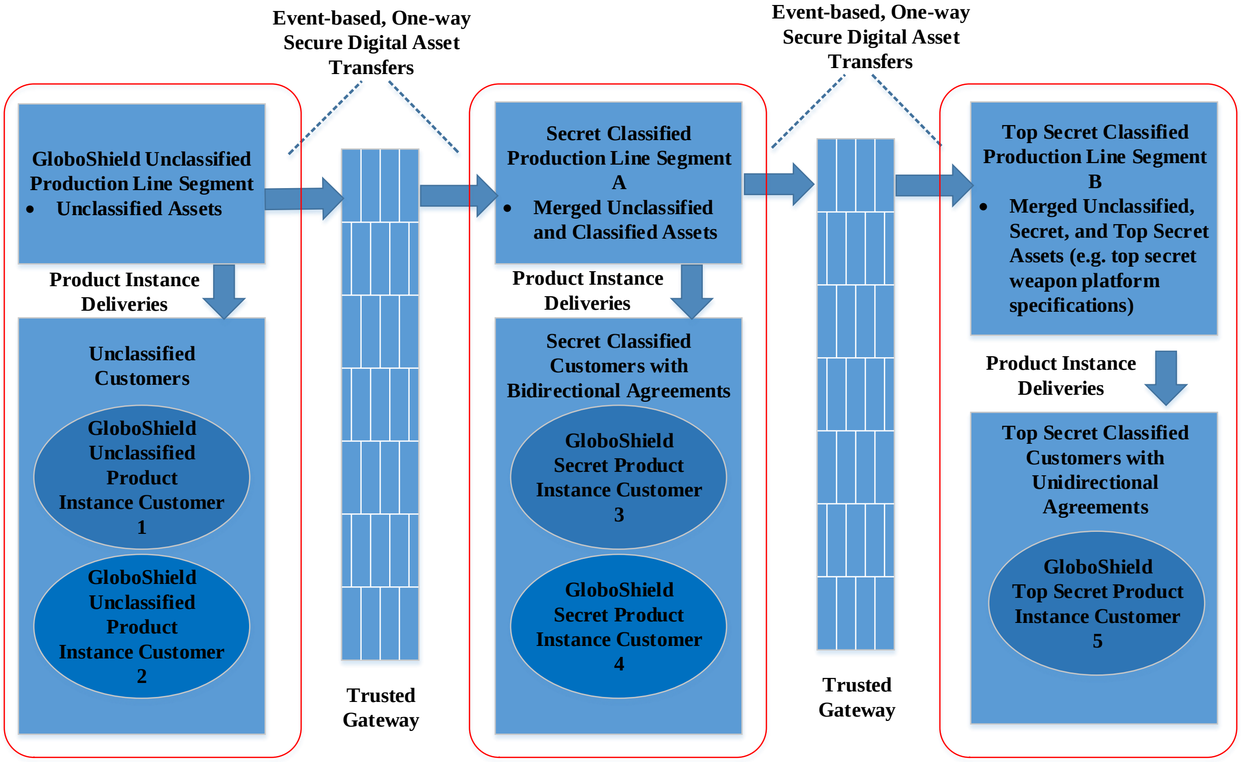
Event-based, One-way Secure Digital Asset Transfers
Event-based, One-way Secure Digital Asset Transfers
GloboShield Unclassified Production Line Segment
• Unclassified Assets
Product Instance Deliveries
Unclassified Customers
GloboShield Unclassified Product Instance Customer 1
GloboShield Unclassified Product Instance Customer 2
Trusted Gateway
Secret Classified Production Line Segment A
• Merged Unclassified and Classified Assets
Product Instance Deliveries
Secret Classified Customers with Bidirectional Agreements
GloboShield Secret Product Instance Customer 3
GloboShield Secret Product Instance Customer 4
Trusted Gateway
Top Secret Classified Production Line Segment B
• Merged Unclassified, Secret, and Top Secret Assets (e.g. top secret weapon platform specifications)
Product Instance Deliveries
Top Secret Classified Customers with Unidirectional Agreements
GloboShield Top Secret Product Instance Customer 5

Figure 6. Mixed Data Sharing Agreements Production Abstract

PLE Factory Architecture

With the described production scenarios, we establish our primary PLE factory architecture pattern: a daisy-chained set of production line segments residing within a single global enterprise divided into multiple information system security zones. The key systems engineering problem to solve for the multiple security zone PLE factory is to securely synchronize the evolution of unclassified and secret or top secret classified digital assets as each undergoes their natural ongoing development over time; i.e. temporal baseline management. Synchronization points occur when the overall production line (including both classified and unclassified portions) needs to be run to support some event. The event might be an upcoming release, or the next point in a regular development cadence – the team's operating rhythm. Moreover, architecturally the synchronization must be fully automated, no longer requiring human-in-the-loop security reviews, manual file transfers between information systems, etc.

Temporal Baseline Management across Multiple Security Zones

Organizations building a portfolio of products have to deal with the concerns illustrated in Figure 7: managing the life cycle of each product (vertical axis), evolving the portfolio over time (horizontal axis), and managing the plurality of products (outward-pointing axis) (Krueger et al. 2013). Evolution in a multiple security zone context brings an additional complexity, as evolution happens in each of the different information system security zones, and versions must be coordinated over time per the team's operating rhythm and customer delivery cycles to produce a consistent whole without compromising security protocols.

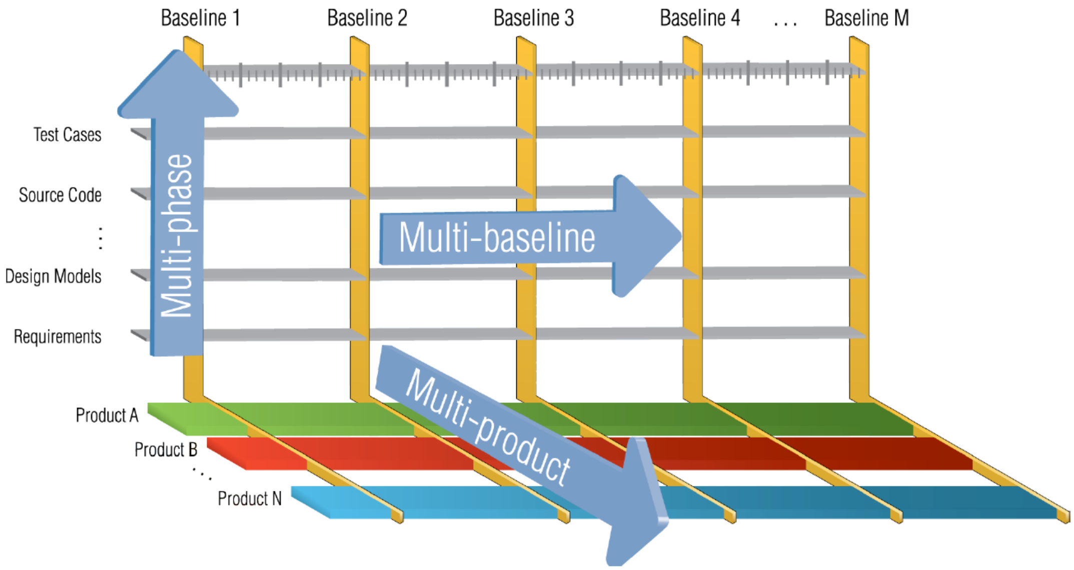

Figure 7. The Three Dimensions of a Complete PLE Solution. Figure © BigLever Software, Inc. Used with permission.

All of the digital assets in the production line naturally evolve over time. Development is performed on digital assets using a variety of tools, selected by the organization for each asset type: e.g., DOORS for requirements, MagicDraw for engineering models, Apache Eclipse for code, and so forth. Production lines additionally include files created by the PLE factory itself. These files represent the factory's feature models, feature and product profiles, digital asset file locations, and more. These PLE factory files also evolve over time.

FBPLE temporal management is based on the concept of a temporal baseline, which is essentially a production-line-segment-level baseline that comprises the set of file baselines of each of the digital assets and the PLE factory files. Temporal baselines are used to define and create any version of any product at any time and are managed using any industry standard configuration management (CM) system. Figure 8 illustrates the design for a PLE factory that spans an unclassified and a classified environment as in production scenario #1.

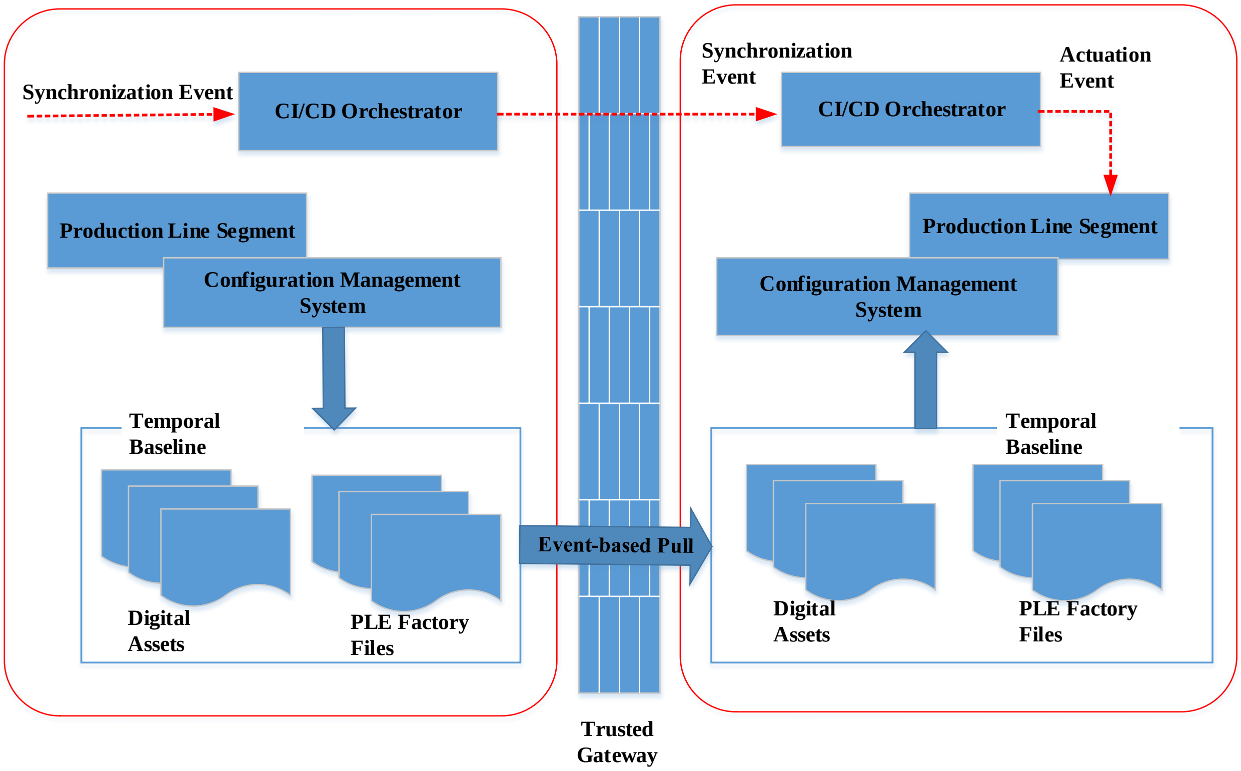

Figure 8. Digital Asset Temporal Management across Unclassified and Classified Security Zones

This pattern is iteratively applied to daisy chain two or more classified environments as in production scenario #2. Automation to support file transfers and CM system actions is provided by an industry standard continuous integration / continuous deployment (CI/CD) orchestrator within each security zone. Configuration management system branching and merging techniques are used in production line segments containing classified assets in much the same way they're used in strictly unclassified production lines, with one restriction: no branching or merging can take place between the classified and unclassified environments, or between classified environments at different classification levels, i.e. the CM systems operate in isolation within their security zones.

The digital asset temporal management business process first iteration is:

- Create an unclassified production line and perform development in the unclassified environment, with no classified information present.
- When the development in the unclassified environment is completed to the point where the shared asset supersets and PLE factory files cannot be further developed without the addition of the classified information:
    - Create classified production lines in the classified environments.
    - Create a copy of the unclassified production line segment and securely pull it into the classified environment thru the trusted gateway system.
    - Merge the unclassified production line segment into the classified production lines.
- Perform development in the classified environments on the classified digital assets, as needed. Unclassified digital assets should continue to be maintained in the unclassified environment.

The ongoing business process to support synchronization events for digital assets and associated PLE factory files is:

- Create a temporal baseline of the files across all of the different environments in the extended enterprise.
- Take a snapshot of the unclassified production line, create a physical copy of it, and securely pull the copy into the classified environment via the trusted gateway system.
- Perform a merge of the physical copy of the unclassified production line segment with the classified production line segment.
- The newly merged classified production line is actuated (run) for each of the classified product instances.
- Repeat for downstream daisy-chained classified production line segments.

Production Line Modular Design

Recall that the temporal baselines transferred between security zones comprise the PLE factory files and digital assets for a specific production line segment – essentially a factory sub-assembly line. A taxonomy for feature-based PLE is described in (Krueger et al. 2017), which enables the creation of a modular design for a PLE factory as a set of sub-assembly lines. Our design for the GloboShield Factory is comprised of a set of production lines, which in turn have Feature Models; Feature Profiles – which are discrete selections of Features used in the Bills-of-Features Portfolio; the Bills-of-Features itself which specifies product instances as collections of Feature Profiles and digital assets; the digital assets themselves; and the Business Rules or constraints for the factory, which specify valid/invalid combinations of Features, etc. The GloboShield PLE Factory for production scenario #1 is designed as a set of sub-assembly lines: an unclassified sub-assembly line; and a secret sub-assembly line that imports the unclassified sub-assembly line, as depicted in Figure 9. This pattern is repeated for each daisy-chained sub-assembly line as in production scenario #2. Each downstream sub-assembly line in the daisy-chain imports the upstream sub-assembly lines, thus making the imported Features, Feature Profiles, Bills-of-Features, Assets, Business Rules, et al. available for that sub-assembly line.

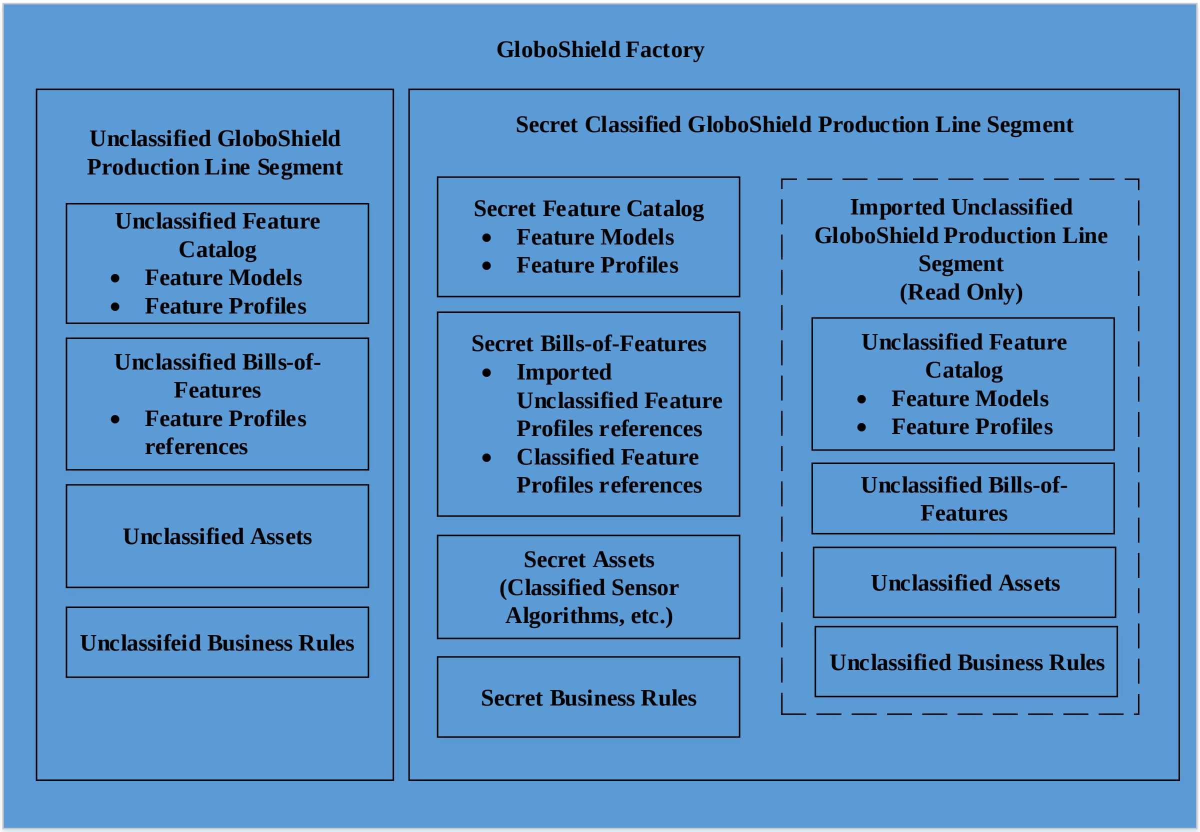
GloboShield Factory
Unclassified GloboShield Production Line Segment
Unclassified Feature Catalog
• Feature Models
• Feature Profiles
Unclassified Bills-of-Features
• Feature Profiles references
Unclassified Assets
Unclassifeid Business Rules
Secret Classified GloboShield Production Line Segment
Secret Feature Catalog
• Feature Models
• Feature Profiles
Secret Bills-of-Features
• Imported Unclassified Feature Profiles references
• Classified Feature Profiles references
Secret Assets (Classified Sensor Algorithms, etc.)
Secret Business Rules
Imported Unclassified GloboShield Production Line Segment (Read Only)
Unclassified Feature Catalog
• Feature Models
• Feature Profiles
Unclassified Bills-of-Features
Unclassified Assets
Unclassified Business Rules

Figure 9. GloboShield Sub-Assembly Lines Design

Summary

PLE factories that span multiple security zones unlock numerous organizational benefits, including decreased computing system expense; leveraging company talent while awaiting access to classified material, and leveraging employees who are members of other sovereign states; plus optimizing production and maintenance for export / import. Additionally, a single enterprise of daisy-chained production line segments prevents organizations reverting to clone-and-own or clone-and-return behaviors, as when they had separate factories for each product instance. We illustrated implementing multiple information system security zone production lines using an example from the Integrated Air and Missile Defense domain: a fictitious system for integrated air and missile defense called GloboShield. Production scenarios requiring multiple information system security zones were presented, with each scenario complying with different customer security classification guides and different data sharing agreements. The mechanics of temporal baseline management in a multi-security-zone PLE factory while protecting the confidentiality and integrity of its digital assets were presented, and included: (1) creating and deploying a daisy chain of production line segments in information systems that are serially connected through trusted gateway systems creating a single enterprise system; and (2) application of factory tooling to periodically create temporal baselines in each production line segment and merge them across each factory sub-assembly line. Digital asset and PLE factory file export, transport, and merge are accomplished through judiciously designing the production line segments within the factory tools using modular packaging of feature models, digital assets, etc.

References

1. Krueger, C et al. 2013, ‘Systems and software product line engineering’, *Encyclopedia of Software Engineering*, Philip A. LaPlante ed., Taylor and Francis, in publication, retrieved from <www.biglever.com/extras/PLE_SE_Encyclopedia_2013.pdf>, Austin, US.

2. Krueger, C et al. 2017, ‘Enterprise feature ontology for feature-based product line engineering and operations’, *Proceedings of SPLC 2017*, Sevilla, Spain.

3. Flores, R et al. 2012, ‘Mega-scale product line engineering at General Motors’, *Proceedings of SPLC 2012*, Salvador, Brazil.

4. Gregg, S et al. 2014, ‘Lessons from AEGIS: Organizational and governance aspects of a major product line in a multi-program environment’, *Proceedings of SPLC 2014*, Florence, Italy.

5. Gregg, S et al. 2015, ‘The more you do, the more you save: the superlinear cost avoidance effect of systems and software product line engineering’, *Proceedings of SPLC 2015*, Nashville, US.

6. Lanman, J et al. 2011, ‘Employing the second generation software product-line for live training transformation’, *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC),* Orlando, US.

7. Clements, P, Northrop, L 2002, ‘Software product lines: practices and patterns’, *Software Engineering Institute*, Carnegie Mellon University, Pittsburgh, US.

8. Young, B. et al. 2018, ‘Product Line Engineering Meets Model Based Engineering in the Defense and Automotive Industries’, *Proceedings Systems and Software Product Line Conference 2017*, Spain 2017.

9. Krueger, C et al. 2014, ‘Second generation product line engineering takes hold in the DoD’, *CrossTalk The Journal of Defense Software Engineering*, in publication, retrieved from <www.crosstalkonline.org/issues/janfeb-2014.html>, US.

Biography

James Teaff, M.E. wrote his first line of code as a professional in the early 80’s while working for a tech startup. Subsequently over the past three decades he has worked for numerous aerospace and defense companies across the full system development lifecycle, from principal investigator and proposal writer to IPT lead, chief architect, requirements analyst, Scrum Master, programmer, tester, 2nd tier O&M support, and more. James holds a Master of Engineering in Engineering Management from the University of Colorado, and a Bachelor of Science degree in Computer Science from Colorado State University. He is an INCOSE Certified Systems Engineering Professional (CSEP), and is an active member of the INCOSE International Product Line Working Group. James joined Raytheon in 2016 and is assisting the organization with the continued rollout of feature-based systems and software product line engineering and management.

Dr. Bobbi Young is a systems engineer and certified architect at Raytheon. She currently leads an Internal Research and Development Project focusing on adoption of PLE across the business. She is regarded throughout Raytheon as an expert in MBSE and co-chairs an MBSE Technical Interchange Group. Bobbi is also a faculty member of Worcester Polytechnic Institute as an MBSE instructor and has co-authored a book on object oriented analysis and design. She is a US Navy Commander (ret).

Dr. Paul Clements is the Vice President of Customer Success at BigLever Software, Inc., where he works to spread the adoption of systems and software product line engineering. Prior to this, he was a senior member of the technical staff at Carnegie Mellon University's Software Engineering Institute, where for 17 years he worked leading or co-leading projects in software product line engineering and software architecture documentation and analysis. Prior to the SEI, Paul was a computer scientist with the U.S. Naval Research Laboratory in Washington, D. C.

This document does not contain technology or Technical Data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.