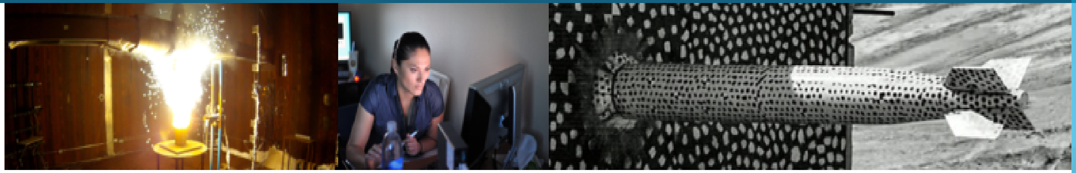
SAND2021-2310C

Investigating Operational Solutions for MBE Assurance



DoD/NNSA Software Assurance CoP Presentation
March 9, 2021

Team: April Suknot (PI), Crystal Cheung,
Michael Frank, Sarah Hale, Gary Huang, Brian Scott
Program Manager: Rick Moleres

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.
SAND____

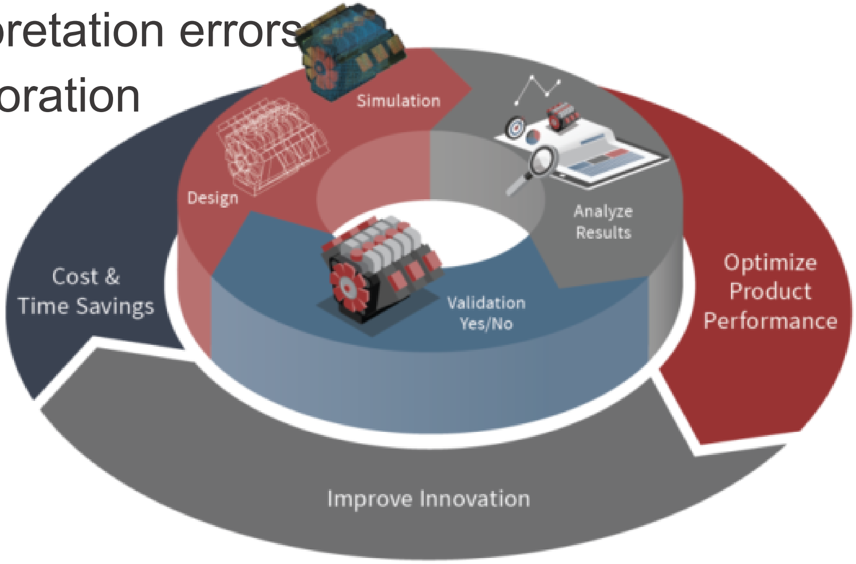
Presentation Outline

1. Introduction
   - What is MBE?
   - Background/Motivation
   - Project Goals
   - Use case and Hypotheses
   - Expected challenges
   - Innovation Opportunities
2. Research approach
3. Preliminary findings
4. Future work
5. Questions and Feedback?

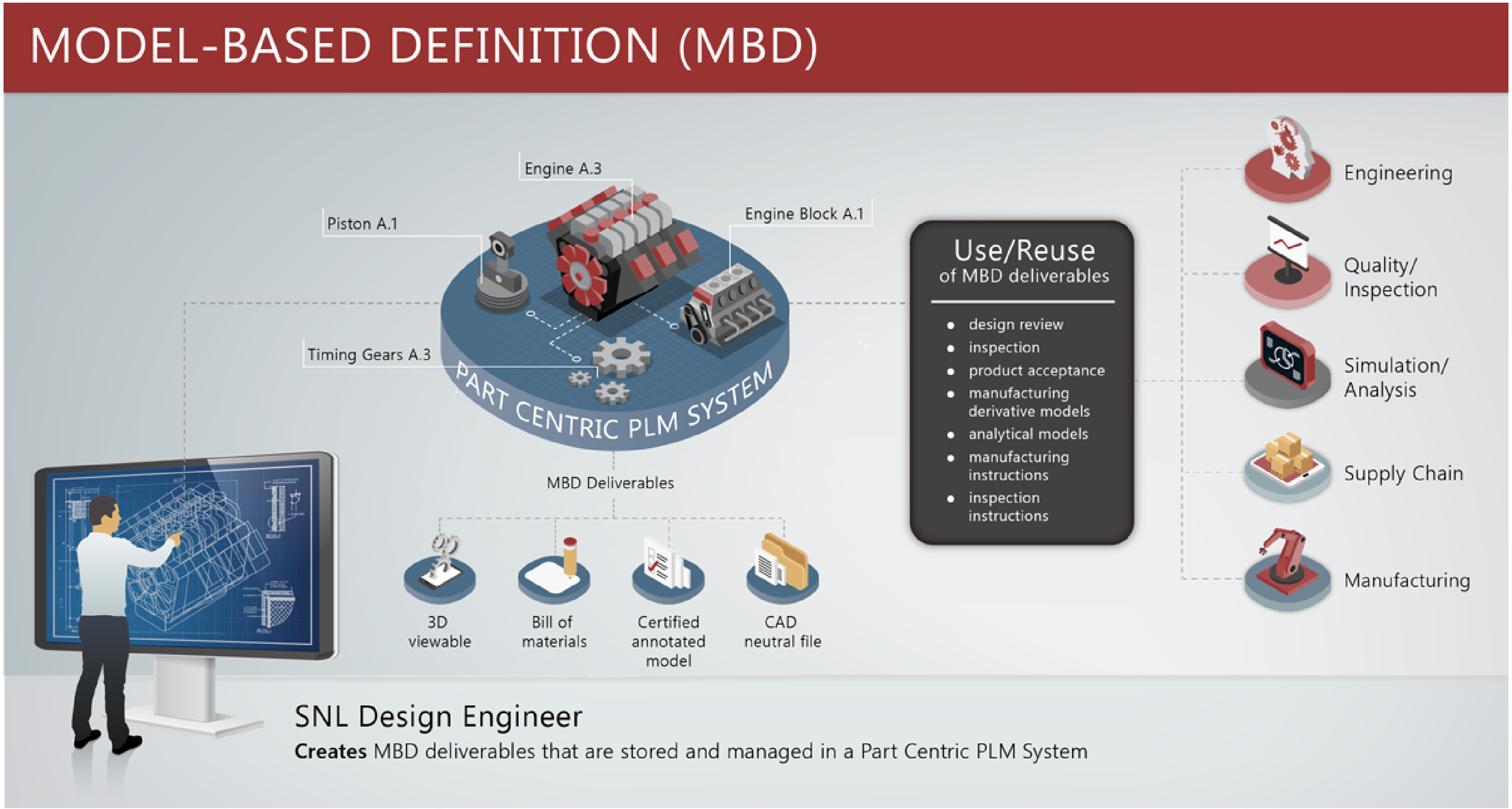
Introduction

What is model-based enterprise (MBE)?

- Fully integrated and collaborative environment founded on a 3D CAD model that contains complete product definition
- MBE supports rapid, seamless, and affordable deployment of products from concept to disposal.
- Sandia envisions using MBE concepts, processes, and tools throughout the product development lifecycle to realize these key benefits:
  - Shorten product development
  - Reduce interpretation errors
  - Enable collaboration



MBD Workflow



MODEL-BASED DEFINITION (MBD)

Use/Reuse of MBD deliverables

- design review
- inspection
- product acceptance
- manufacturing derivative models
- analytical models
- manufacturing instructions
- inspection instructions

SNL Design Engineer

Creates MBD deliverables that are stored and managed in a Part Centric PLM System

Introduction

Background and Motivation

- Enhance current model assurance capabilities to stay ahead of our adversaries
- Model-based Enterprise (MBE) requires adoption of digital product (CAD) models
- Problem: Ensure that a given CAD model, regardless of where it is found (e.g. PDM system, local hard drive), can be verified for authenticity and has not been intentionally altered from its origin
  - Need to provide assurance via secure model provenance:
    - Model authenticity
    - All changes to models are authorized – who changed it and why
  - Need risk mitigations to guard against:
    - Accidental undesirable changes
    - Cyber attacks
    - Malicious insider activities

Project Goals

- Investigate solutions for model assurance, including but not limited to:
  - Blockchains for model integrity, provenance, and non-repudiation
  - Effectiveness of leveraging machine learning to identify potentially abnormal activities
- Identify operational solutions for potential security weaknesses

Introduction

Use Case

- Knowing how a model has changed, and by whom, with assurances that these changes are legitimate (i.e., not malicious or accidental) is critical to establish trust in the model

Hypotheses

- Models follow a natural “pattern of life”
- A privileged insider can make a seemingly normal change that is malicious, but such changes can be detected via analytical methods that identify changes violating the “pattern of life”
- Blockchain-like technologies can provide an open, decentralized ledger of cryptographically secure change records
- Evaluating algorithms for the following will result in a system that can bolster MBE model assurance:
  - Model change detection
  - Provenance tracking for tamper detection
  - Approaches that combine multiple solutions

Introduction

Expected Challenges

- ➢ Simulating adversarial behavior is difficult and must be done elegantly enough that the algorithm does not become biased toward specific behaviors
- ➢ Adversarial behaviors can occur over various windows of time
  - Having an exhaustive set of simulated examples for all possible adversarial actions is not feasible
- ➢ Challenge mitigations: Solicit SME input to create a wide enough range of scenarios to create an effective system

Innovation Opportunities

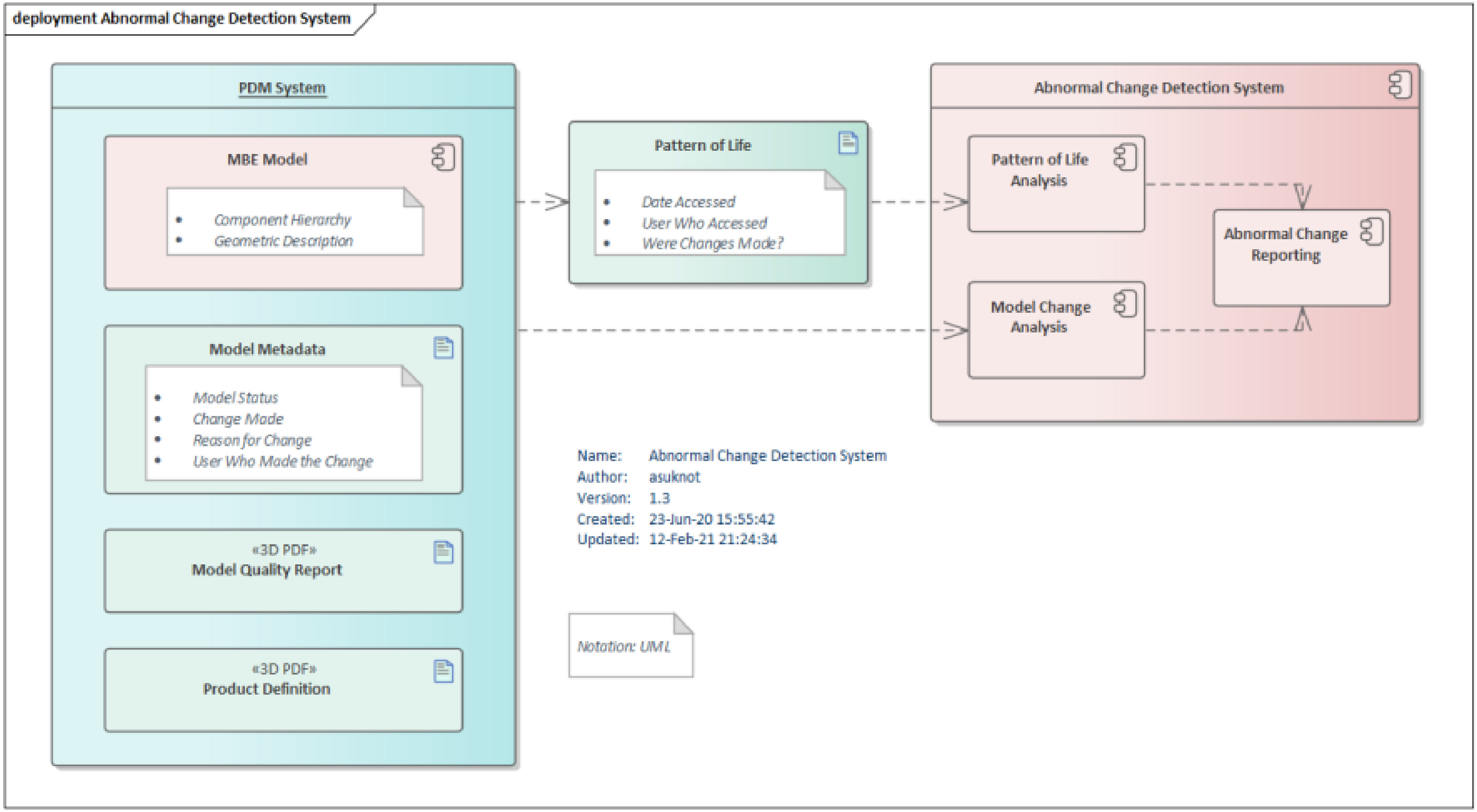
- ➢ Discovery of effective and scalable solutions for effectively establishing model provenance, which is almost certainly a requirement for MBE
- ➢ Identification of novel techniques for detecting both adversarial behavior and unintended model changes
- ➢ Novel approaches and lessons learned could be potentially applied to any manufacturing process utilizing MBE

Research Approach

- ➢ Investigate technical solutions for model assurance
  - Explore and evaluate blockchain solutions and analytical methods that seem viable for this use case
  - Identify additional technologies that may be applicable
  - Consider combinations of algorithms or technologies that could exist in a hybrid or hierarchical system
- ➢ Identify and gain access to robust datasets to leverage for simulation
- ➢ Identify and simulate abnormal change scenarios with which to test candidate solutions for accuracy and effectiveness
- ➢ Run simulations to gauge effectiveness, integration effort, and ability to enforce nonrepudiation
- ➢ Review findings with SMEs, document, and identify follow-on plan

Research Approach

High-Level Hypothetical System



Name: Abnormal Change Detection System
Author: asuknot
Version: 1.3
Created: 23-Jun-20 15:55:42
Updated: 12-Feb-21 21:24:34

Current progress

Accomplished Work to Date

- Collaborated with our MBE team to ensure that our team has access to appropriate CAD-related data, software, and training
  - This is the first step in being able to evaluate the data band begin surveying technology and methods that will be appropriate for that data
- Started data evaluation to identify how analytical methods can be used with the CAD data itself, along with output from quality control tools
- Began surveying how other teams, both internal and external, are leveraging blockchain technology to gain additional perspectives on how this technology could be leveraged
- Initial high-level design of hypothetical systems

Current progress

Preliminary Findings

- Key aspects of blockchain and blockchain-like tech that apply to our use case:
  - Provides to validate and audit file history.
    - Blockchain design ensures that the file records are immutable.
    - One viable and scalable option is to store file changes and version history directly on the blockchain, while storing the model files themselves on a centralized database off the blockchain.
  - Facilitates decentralization of file validation
    - Verification of provenance can be distributed across multiple nodes without a server to act as central authority
  - Resistant to insider attacks, (e.g. nefarious file or file record changes), due to blockchain design
    - Since provenance info is stored on the blockchain, an insider is unable to single-handedly make malicious changes simply by modifying files in the database. Corrupting provenance would require an unlikely collusion such that the number of malicious insiders is greater than the number of honest users.
  - Good potential to mix and match blockchain designs – many alternate design options have already been proven in industry

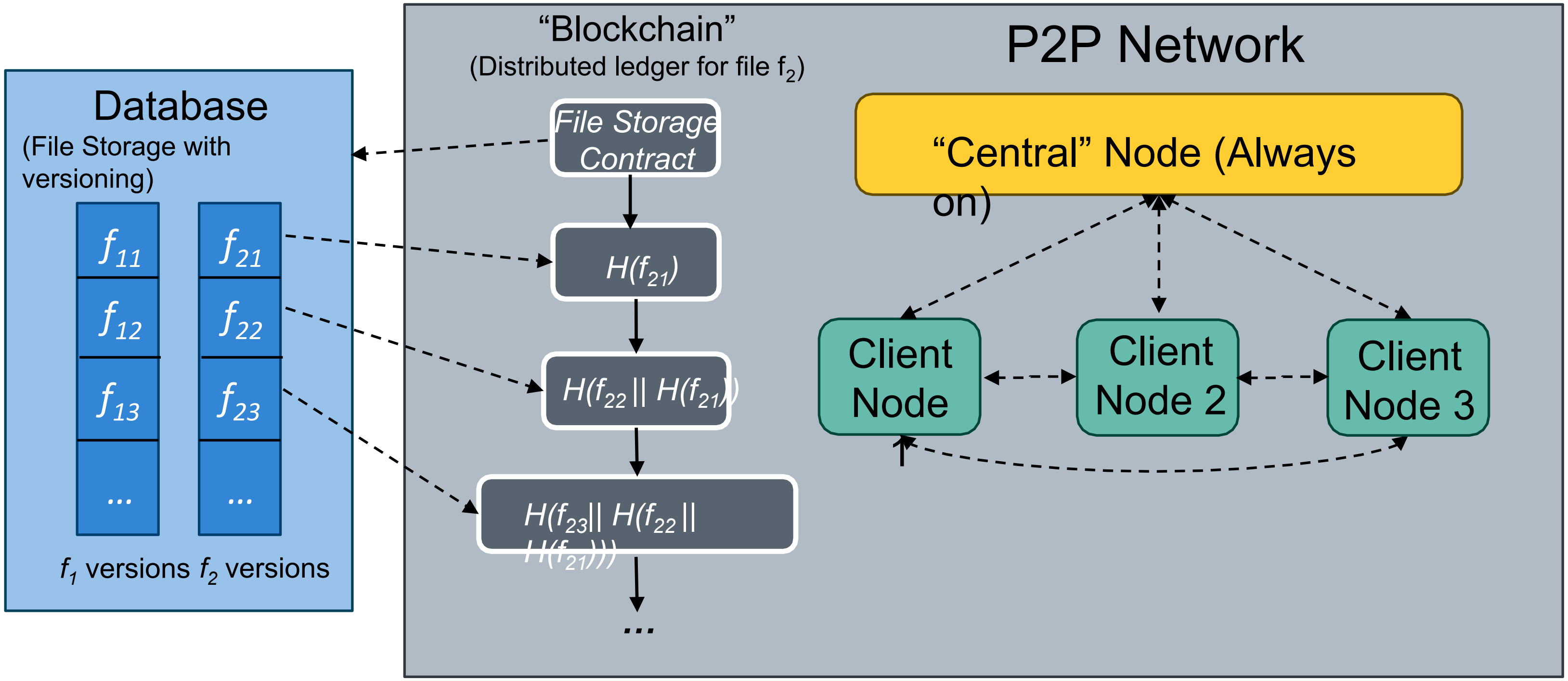
Current progress

Preliminary Findings cont’d

- ➢ Anomalous Behavior Analysis: Build Versus Buy
  - Commercial User and Entity Behavior Analytics tools
    - Uses: Can track data movement and detect suspicious behavior
    - Potential challenges and limitations:
      - Configuration difficulty
      - On-premises options
      - Scalability versus cost
      - Support options from vendors
  - Custom Anomaly Detection
    - Involves artificial intelligence methods that leverage
      - Graph theory/graph analysis
      - Probabilistic models
      - Clustering techniques (distance metrics)
    - Potential challenges and limitations:
      - Substantial research effort required
      - In-house development—implementation and maintenance cost

Current progress

- High-level system design drafting
  - In the process of developing high-level system designs for potential elaboration and usage in tabletop simulations.
- System design goals:
  - Immutable file records -- the ability to validate and audit file history
  - Decentralization of file validation
  - Resistance to insider attacks, e.g. nefarious file or file record changes



Future work

- Continue to research and identify potential algorithms, provenance tracking technologies, and additional solutions
- Create simulated data of abnormal model change scenarios with Data Security and Model-Based engineering SME input
- Down select to a few candidate solutions for further evaluation
- Develop simulations and design tabletop exercises for candidate solutions
- Run simulations and tabletop exercises on prepared data
- Pursue follow-on work as applicable
- Peer review the simulation results with SMEs
- Publish a report on the evaluation and results

Questions and Feedback?