Cybersecurity Transformation Applied through Enterprise Engine (E2)

Prepared for the OMG Cybersecurity Workshop
Jeff Smith, Chief Systems Engineer at Sierra Nevada Corp

March 21, 2017

Agenda

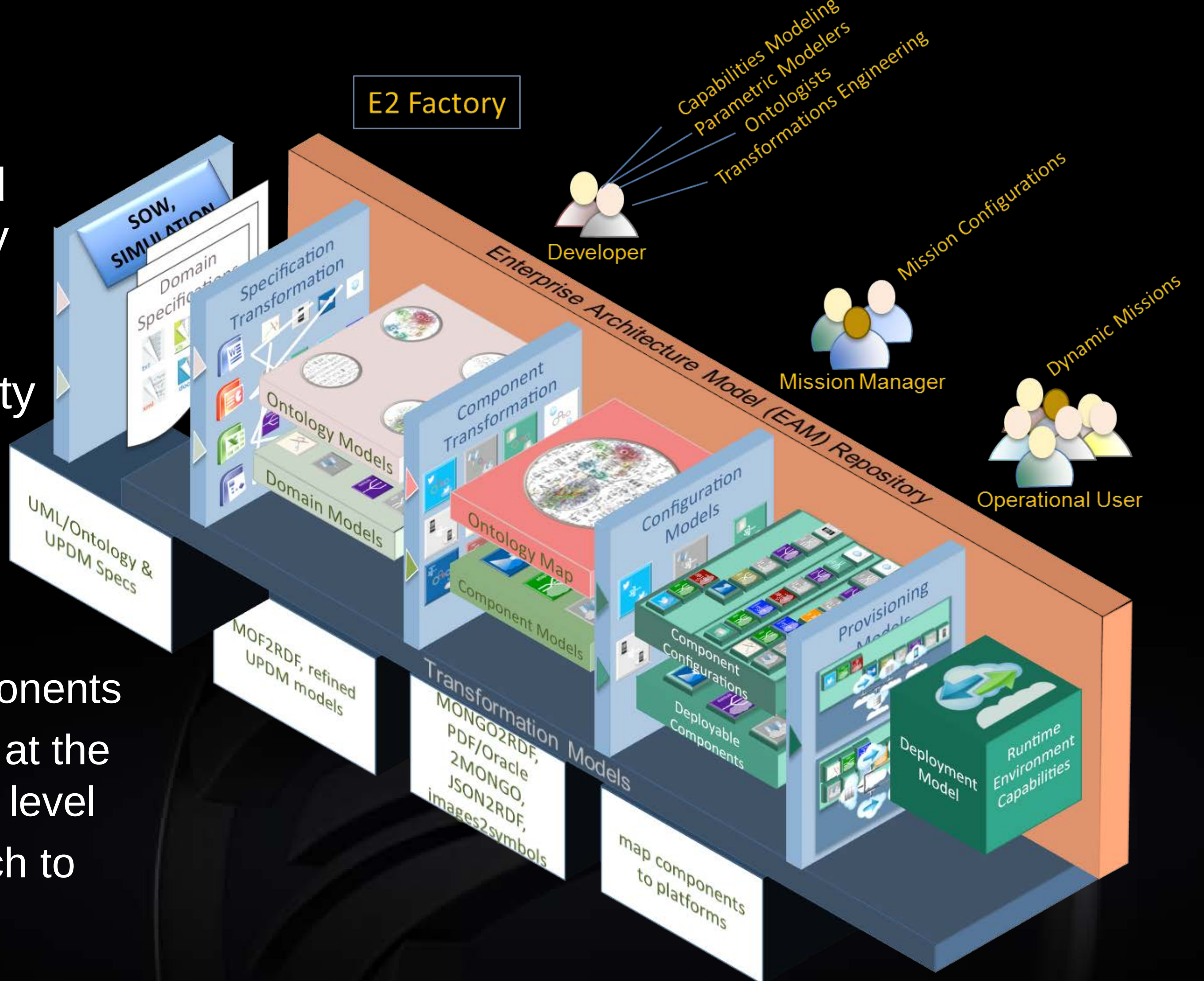
- Introduce the larger Enterprise Engine (E2) applications for:
  - Core standards and processes introduced by LCDR Wicks
  - E2 Model Oriented Development Environment (MODE) program
  - Department of Defense Use Cases

•Invitation to see demos and other cyber-related OMG activities

MODE

Demonstrate improved methodology to quickly develop systems cheaper & with improved maintainability

- Design and maintain systems at the conceptual level
- Provide reusable components
- Provide interoperability at the service and data object level
- Open Systems approach to software development

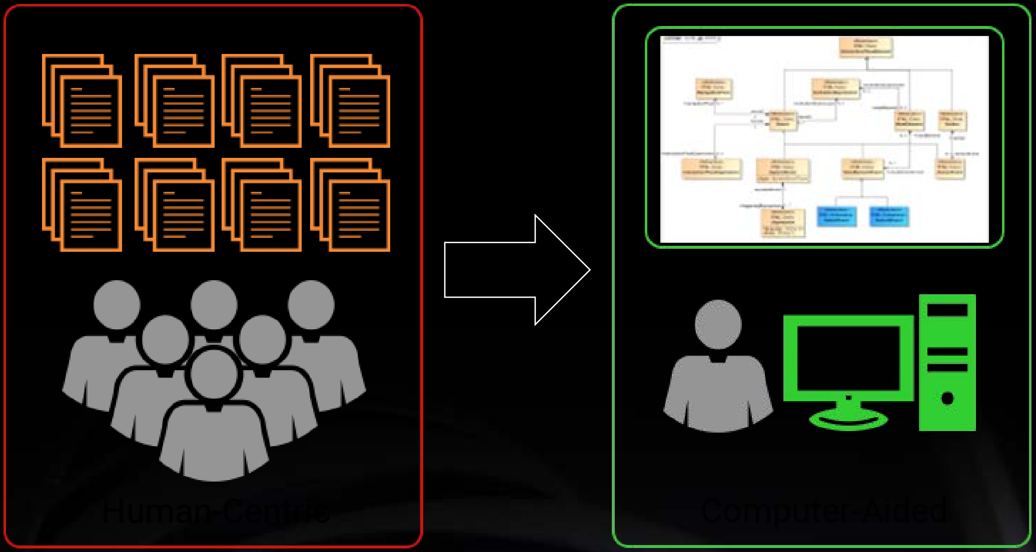


- E2 is a framework for agent-based systems that follow similar patterns
- MODE tools allow us to deliver framework for use-cases with security-first design
- E2 team actively contributes to OMG open standards and tools

E2 Use Case: MODE

Capabilities Review:

- Application of AI results 1-3 orders of magnitude speedup of the process
- Requires fewer people per process saving
- Improves quality and security of DoD IT systems
- Scales to the Enterprise
- DoD IT systems can be delivered better, faster, cheaper…



Performance Parameters (*14,000 errors)	Human-Centric	Computer-Aided
Analysis Time	1.5 person year x 3 people	1 person hour with 1 person
Correction Time	30 min. per error	~1-2 sec. per error
Document Generation	170 pages in 1.5 to 2 person months	170 pages in 5-10 mins.

Process reduces A&A timeline and cost by 1-3 orders of magnitude

E2 Use Case: Content Production (As-is vs. To-be)

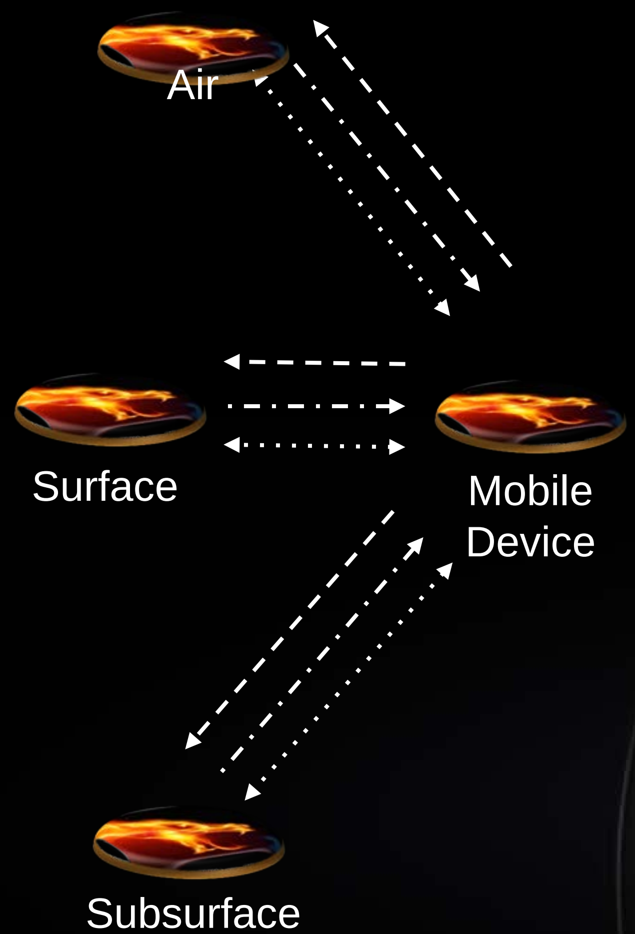
Information from many sources and languages	Information is reviewed and stored in a DB or file cabinet	Physical content is printed and pre-annotated	Team Leader distributes content to Analysts (assignment)	Analyst picks content	Analyst gathers supporting material	Analyst previews & writes a product	Checker Analyst reviews product	Section Reviewer reviews product	Post process/ publish

2 weeks — **1-2 weeks** — **2+ weeks**

PDF and XML Ingest	Stores and validates for processing and archiving	*Not Needed Stored in DB*	Proposes assignment, only sign-off by Team Lead	Sorts and prioritizes source changes (rules given by Analysts)	Presents all supporting materials for selected production tasks	Presents suggested product; Analyst may change or just accept after assessing materials	Presents all source material used to write product automatically	Product prepared for review	Post process/ Publish

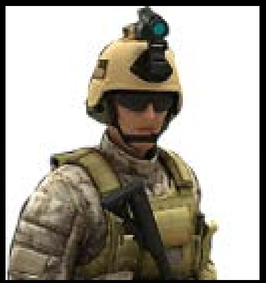
1-2 minutes — **3-8 minutes** — **1 week**

E2 Use Case: **Autonomous Systems (DRAGON)**



Nano decisions are made by DRAGONs.
Awareness usually takes milliseconds.

Delegated Autonomy



Macro decisions are made by people.
Awareness usually takes seconds.

Planning & Delegation
Monitoring
Control

- Human operator delegates most decisions to DRAGON(s)
- Human operator makes **<u>critical decisions</u>** while maintaining broader Mission awareness and performs other tasks
- Increases speed and effectiveness of operations by 1-3 orders of magnitude

E2 Programs follow same pattern/standards generalizable to many applications

E2 Program	Source	Ingest	Decode	Xform/Store	Services
Model Oriented Development Environment (MODE)	Requirements and design docs, knowledge bases e.g. CWE, CVE, …	Application software code	Models, patterns and AST discovered from code	Models supporting "bad" patterns; XML UML/MOF,... → RDF	Assign vulnerabilities to code; Recommend/ generate confidential fixes
Content Management	Geospatial Information	XML error detection and correction, image recognition and encoding, PDF	Glyph decoding, language translation from diverse sources	JSON, SGML,UML/MOF,... → RDF	User assessment, analyst assistant
Talent Management	Personnel history, awards, certificates, decorations	Image recognition and encoding, PDF	Decode information from diverse sources	JSON, XML UML/MOF,...→ RDF	Timeline of performance records; Upload/manage certificates; talent profile matching
Autonomous Systems	Mission development, autonomous navigation, and task execution	Radio messages with position, alerts, situations, damage assessments, …; image recognition and encoding, operator control	Decode messages and objects from diverse sensors and platforms	Message, images,… to test, control and monitoring; Eventually transform to RDF	Formation movement across land and sea; Observe obscured regions for threats; Enhanced map construction

E2 MODE is part of comprehensive SNC/MACE Cyber Suite

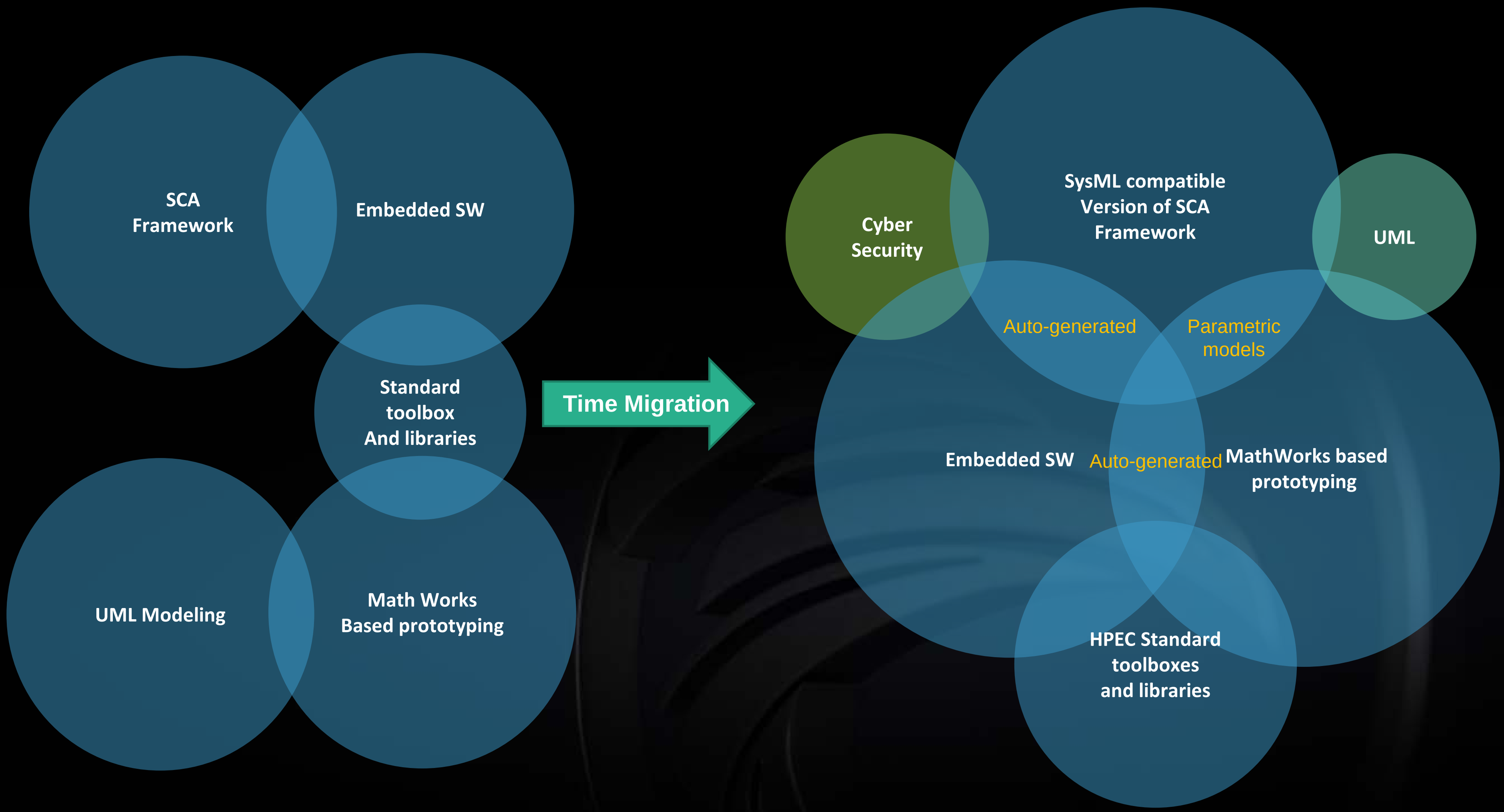
Program Name	Cyber Contribution
Model Oriented Development Environment (MODE)	Discover and evaluate code vulnerabilities based on open and custom standards. Generate security analysis and risk assessment reports. Recommend / generate code fixes. Production of secure and reliable code directly from executable UML models.
Critical Systems Resiliency (CSR)	A structured, flexible method for assessing and measuring the criticality and resiliency of federal systems to ensure prioritization of cyber security investments across the entire government. CSR extends NIST standards and produces granular reporting metrics to be used to drive security decisions.
Special Events Assessment Rating (SEAR) System	Using a risk-based methodology, SEAR ranks annual events (up to 10,000 a year) to advise allocation of federal support. Includes Risk Model functionality to calculate score using multiple attack types.
Defense Security Service (DSS)	Detects Cyber Security events across 3rd party companies; allows prioritization of cyber risk across companies and enables signatures to be identified and matched between companies, utilizing advanced analytics.
Infrastructure Information Collection Division (IICD)	Gathers, manages and protects CII (Critical Infrastructure Information). Submits CII of publically exposed sites to management systems for workflow and user management for User registration, profile management, training courses, and access to content.
LinkScraper	Collects risk data associated with a Vendor, allowing risk analysts to define categories and associated keywords and vendor data dashboard to automate the process.

Thank you for your time

- E2 MODE will be part of OMG demonstrations
- Videos of selected E2 programs can be given upon request
- MACE tour and introduction
- Resurrection of OMG's Software-Based Communications group to consolidate into an embedded, composable, networked, cyber security conscientious SysML model – further defined in the MARS Task Force (see next page if time)

Questions?

OMG's Recommended Vision To WInn-F March 2016



A highly effective Integration Systems Engineering Model – Lower Cost, Higher Quality, Reduce Delivery Times.