High Level Architecture

Federation Development and Execution Process (FEDEP) Checklists

Version 1.5

December 1999

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
01-12-1999		xx-xx-1999 to xx-xx-1999

4. TITLE AND SUBTITLE
High Level Architecture Federation Development and Execution Process (FEDEP) Checklists
Unclassified

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
Defense Modeling and Simulation Office
1901 N. Beauregard St., Suite 500
Alexandria, VA22311-1705

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
United States Department of Defense
Defense Modeling and Simulation Office
1901 N. Beauregard St., Suite 500
Alexandria, VA22311-1705

10. SPONSOR/MONITOR'S ACRONYM(S)
11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The High Level Architecture (HLA) allows the assembly of different tools to address a requirement. The requirement may arise from the examination of an analysis problem; research and development explorations; test and evaluation of an object, component, or a process; or the provision of training to individuals or staffs. The HLA allows this requirement to be met by assembling an appropriate set of models, simulations, and other tools. Once identified, the challenge is to employ each model, simulation, or tool in a way that takes advantage of its strengths and complements the application of the other selected tools to meet the requirement. When assembled, the models, simulations and tools compose a federation; the individual components, called federates.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	Public Release	29	Fenster, Lynn lfenster@dtic.mil
Unclassified	Unclassified	Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007

FEDEP Checklists

Introduction

The High Level Architecture (HLA) allows the assembly of different tools to address a requirement. The requirement may arise from the examination of an analysis problem; research and development explorations; test and evaluation of an object, component, or a process; or the provision of training to individuals or staffs. The HLA allows this requirement to be met by assembling an appropriate set of models, simulations, and other tools. Once identified, the challenge is to employ each model, simulation, or tool in a way that takes advantage of its strengths and complements the application of the other selected tools to meet the requirement. When assembled, the models, simulations and tools compose a federation; the individual components, called federates.

The Checklists in this document identify many of the details that one must consider when assembling the federation. This document complements the Federation Development and Execution Process (FEDEP) Model (Version 1.5, December 1999) which offers a six step process for assembling federations. As with the FEDEP, note that the discussions, decisions, and activities in the checklists are grouped logically, but not necessarily temporally. That is, many of the items contained in these lists may be accomplished sequentially, iteratively, concurrently, or not at all. It is common for federation development activities from several FEDEP steps to be executed concurrently.

FEDEP Checklist Foundation

The checklists were developed based on experience gained through the development of several specific federation applications. To this extent, the checklists represent accumulated experience from several case studies. Each experience was unique in that it involved different application domains, different goals, different federates, and different participants. In general the items in the checklists are applicable to all federation efforts, it is however, expected that some amount of tailoring is required to meet specific federation constraints and objectives. Indeed, the checklists may not be complete, additional items may be needed.

Structure of Checklists

The checklists are organized along the six steps of the FEDEP model. The checklist for each FEDEP step begins with the definition of that step and includes the likely participants in the activities. Checklist items represent management and technical decisions and tasks that are acted upon by members of the federation team. Both the managerial and technical checklists may be composed of subcategories of related activities. The placement of these groupings within the checklist may indicate sequential activities, but more often represent activities being accomplished in parallel or perhaps in

a repeated or cyclic manner, as the teams understanding of the problem space is refined. Managerial activities for each step are in a grouping separate from the technical activities, Program Management, to aid management and technical team members in focusing on activities relevant to their responsibilities.

Within each FEDEP step, checklist items that generally apply to all federations are listed. Following the general checklist items are additional sets of items that are more closely aligned with a specific application area. These application areas are those in the case studies mentioned above: Experimentation and Analysis, Training, and Test and Evaluation.

The reader is encouraged to consider the checklist items as a touchstone and to tailor the items (add, modify, substitute, or ignore) as appropriate for the individual circumstances of the federation development project. The checklists are intended as an additional input to the systems engineering process. To further encourage the tailoring of the checklists, two columns follow the checklists. The columns are labeled "A" for applicable, and "C" for completed.

The last section of this document contains brief definitions of the application areas referenced as well as other terms and acronyms that appear in the checklists.

Federation Participants

For clarity of discussion, the participants in the federation development and execution process are identified. The terms used are intended to describe the role of the participant. The actual terms used for a specific federation implementation are likely to vary with each implementation and domain. Additionally, it is noted that the participants identified below are sometimes represented by an individual, and at other times are represented by teams within a single organization or built across multiple organizations.

Participants:

- Federation User/Sponsor: Person(s) that is applying the federation to meet an objective. The federation user and sponsor often have an organizational relationship.

- Federation Manager: Person(s) responsible for pulling the pieces of the federation together to meet the requirements of the federation user/sponsor. The federation manager works with the user/sponsor to identify requirements, schedules, resources, constraints. The federation manager works with the federate developers to identify a federation design and execution that meets the user's requirements.

- Federate Developer: Person(s) responsible for developing or modifying a federate to meet the federation objectives.

- Federation Team: Participants include the user/sponsor, federation manager, and the federate developers. Additional participants, such as subject matter experts, may be identified during the course of a federation effort.

The checklists in this document are presented from the federation manager's perspective. Other perspectives to consider are the federation user's perspective and the federate developer's perspective.

Related Documents

The following documents are related to federation development and may be useful sources of guidance during federation development efforts:

- “Department of Defense High Level Architecture Federation Development and Execution Process (FEDEP) Model”, Version 1.4, June 1999.

- “HLA FEDEP: VV&A Overlay” presented at the Architecture Management Group Meeting, 11 February, 1999.

- "Federation Security Process (Overlay for FEDEP)" presented at the Architecture Management Group Meeting, 11 February, 1999.

- "HLA Tools Update" presented at the Architecture Management Group Meeting, 13 October, 1999.

Checklist Development

The FEDEP Checklists are based on experience gained from the specific application of the FEDEP model to federation efforts in several domain areas. It is anticipated that as federation solutions are applied, more experience will be gained and the checklists will expand to capture that experience.

Step 1: Define Federation Objectives

The federation user and federation development team define and agree on a set of objectives, and document what must be accomplished to achieve those objectives.

Participants: The federation user/sponsor, and the federation manager work to accomplish this step. If a persistent federation[1] is applied, then federate developers may also participate. If a persistent federation is not in use, then federate developers have not yet been identified.

	A	C
Identify Needs		
1. Identify the purpose of the endeavor (experimentation, analysis, R&D, training, acquisition, other).		
2. Identify the mission area addressed by the project (JSEAD, JAO, naval operations, ground combat, logistics, etc.).		
3. Identify critical operational issues to be addressed. Identify the problem to be solved and the federation's role in addressing the problem.		
Develop Objectives		
• Identify the tools under consideration (one or more simulations, hardware-in-the-loop, C2 systems).		
• Identify the preferred location and method for development, integration, test, and execution (local, at a specific site, distributed, other).		
• Review applicable fidelity standards and referents. Identify high level fidelity objectives, including accuracy and capacity.		
• Identify VV&A participants, activities, and products. [VV&A]		
• Determine desired level of security required. Actual security level may depend on the data or federates. [Security]		
• Review Security constraints and requirements. These may impact timelines as well as cost (hardware, safes, procedures, etc.). [Security]		
• Identify security authority for federation. [Security]		
Program Management		
• Schedules and Budget		
1. Identify schedule drivers (federation user and sponsor milestones, complexity of implementation, availability of funds and other resources).		
2. Identify the overall funding profile and major milestones. Prepare a high-		

1 A persistent federation is one that is developed to meet multiple application goals from the outset, or alternatively, developed to meet a single application goal and then applied again after the end of the program which created it. The federation is re-used, possibly modified, and applied to a new objective.

	A	C
level Schedule and Budget. 3. Identify POCs for programmatic schedule and budget coordination. 4. Conduct feasibility and risk assessment. Identify decision criteria. Place decision points in schedule. 5. Consider HLA training for one or more members of team; identify training dates and locations.		

Federation Objectives Definition for Experimentation and Analysis	A	C
1. Identify user for experiment content. 2. Develop the essential elements of analysis. 3. Identify federation characteristics such as validity, repeatability, extractability of results, and speed; and methods for obtaining them. 4. Write the Experimentation Plan. Identify hypotheses. a Identify the type of excursions (varying one or multiple data points, varying behaviors or procedures, etc.). b Identify the number of runs per excursion. c Identify the MOEs/ MOPs. d Prepare federation documentation to capture critical elements of the experiment being simulated including the key events, objects, and behaviors.		

Federation Objectives Definition for Training	A	C
1. Identify training objectives, training audience, and tasks to be trained. 2. Define how the training will be conducted (concepts of operations). 3. Determine how the training will be evaluated. Identify data required to support the evaluation. 4. Identify how the training results will be presented to the training and evaluation audience (e.g., three dimensional view, side-by-side displays of simulation screens and C2 tactical displays, videos, tailored briefing packages, or other method). 5. Identify methods for training results to stimulate training improvements. 6. Identify security directives and requirements. [Security]		

Federation Objectives Definition for Test and Evaluation	**A**	**C**
1. Review relevant system Operation Requirements Documents (ORDs) and T&E Master Plans (TEMPs).		
2. Determine test objectives, high level scenarios, and conditions. Identify the performance parameters (MOEs) to be evaluated.		
3. Determine operational context constraints or preferences, including geographical regions, environmental conditions, threats and tactics.		
4. Decompose MOEs so that they are measurable. Identify MOE drivers. This will serve as a blueprint for conceptual model development.		
5. Document relationship between performance measures and their drivers.		
6. Select tools to support scenario development, conceptual analysis, VV&A and test activities, and configuration management.		
7. Develop an architecture and network development plan including approximate schedule and major milestones.		
8. Develop a configuration management plan.		
9. Develop initial verification, validation, and accreditation (VV&A) and test plans. [VV&A]		

Step 2: Develop Federation Conceptual Model

A representation of the real world domain that applies to the problem space is developed.

Participants: The federation user/sponsor and the federation manager work to accomplish this step. If one or more federates have been selected or a persistent federation is in use, then federate developers may also participate.

	A	C
Develop Scenario		
1. Identify the real world military operations of interest (e.g., close air support provided by fixed wing aircraft to a mechanized ground force executing a deliberate attack mission).		
2. Identify the key event sequences and the number and types of objects needed.		
3. Identify the factors (doctrinal, operational, or natural) that impact events and behaviors).		
4. Identify the geographic location of interest.		
5. Identify natural and man-made features needed in the terrain and atmosphere (e.g., road networks, buildings, towers, railroads)		
6. Identify the size and nature of the threat forces (confirmed and unconfirmed) and the civilian component of the environment.		
7. Identify the length of time to be simulated (e.g., seconds, minutes, days, weeks).		
8. Identify the desired time period with respect to the timeline of hostilities (e.g., days 30-40 of a conflict after a 15-day build-up of forces in theater).		
9. Identify the starting locations and dispositions for all objects in the simulated environment (e.g., friendly, threat, and civilian equipment and personnel).		
Perform Conceptual Analysis		
1. Select a technique and format for recording the conceptual model (e.g., static process flow diagram, correlation tables of objects and behaviors, descriptive text)		
2. Describe (in the selected format) the objects and behaviors needed to carry out the scenario specified in the previous step.		
3. Where possible, reference authoritative sources for approved descriptions and explanations of battlefield processes and equipment features and behaviors. Doing this will reduce the uncertainty and effort associated with the validation, verification and accreditation activities.		
4. Determine the degree to which the federation can tolerate deviations from the desired fidelity.		
5. Verify that the conceptual model can be tested. [VV&A]		
6. Identify behaviors to be tested. [VV&A]		
7. Identify tests to measure influence of identified factors. [VV&A]		

	A	C
8. Review Security requirements of conceptual model.[Security]		

Develop Federation Requirements	A	C
1. Distill the results of conceptual analysis into a straightforward set of objects and behaviors that must be in the federation with emphasis on quantifiable characteristics that can be used to guide federate selection and testing.		
2. Assess the requirement for faster-than-, slower-than-, or real-time federates.		
3. Determine the need for futuristic objects (e.g., prototype weapons or sensors) or behaviors (e.g., experimental tactics, techniques or procedures) that are not currently defined in the domain reference literature.		
4. Determine the need for non-simulation components of the federation (e.g., C4I systems, hardware-in-the-loop, human-in-the-loop).		
5. Identify federation reporting requirements before, during, and after execution.		
6. Refine high level fidelity objectives to a measurable set of fidelity requirements.		
7. Identify test evaluation criteria. [VV&A]		
8. Assess security requirements with respect to hardware. [Security]		
9. Assess security requirements with respect to network, data, and software. [Security]		
Program Management		
• Schedules and Budgets		
1. Conduct feasibility and risk assessment. Review objectives and conceptual model. Is modeling and simulation the appropriate tool to apply? Can it reasonably be applied in the timeframe required?		
2. Review schedules and budgets in light of feasibility assessment. Adjust as appropriate.		
3. Begin dialog between any identified federate security representatives and federation's security authority. [Security]		

Conceptual Model Development for Experimentation and Analysis	**A**	**C**
1. Identify the key events and objects for each case (base and excursions). How many objects are anticipated per case? How many cases?		
2. Record all decisions and descriptions pertaining to the Conceptual Model. One or more techniques may be used: process flow diagrams for each case, correlation tables of entities (or objects) and activities, descriptive text, other.		
3. Identify factors that influence current and futuristic events or object behavior. For example, "Future imagery collection systems will not be impacted by cloud cover".		
4. Identify sources for knowledge acquisition with respect to future objects and behaviors.		
5. Identify performance data for new entities or objects and their behaviors.		
6. Refine MOEs and MOPs.		
7. Augment federation documentation developed in step 1 (Define Federation Objectives) with the Conceptual Model. Include objects, activities, and factors for each event.		
8. Verify that federation documentation and Experimentation Plan are consistent. [VV&A]		
9. Identify and record experiment assumptions. For example, "It is assumed that blue command and control aircraft are not targeted by the enemy because the aircraft operate at stand-off distances".		

Conceptual Model Development for Training	**A**	**C**
1. Identify key events and objects required to meet specific training requirements.		
2. Identify training instructor control/monitoring/recording functionality required to meet training objectives.		
3. Identify threat, image and environmental representation required to create appropriate training environment.		
4. Verify that federation documentation and Training Master Plan are consistent. [VV&A]		
5. Record all decisions and descriptions pertaining to the Conceptual Model for the training application.		

Conceptual Model Development for Test and Evaluation	**A**	**C**
1. Identify major objects that must be represented to satisfy the performance measures defined in step 1 (Define Federation Objectives).		
2. Describe capabilities, behavior and relationships between major objects over time to satisfy the performance measures defined in step 1 (Define Federation Objectives).		
3. Specify relevant environmental conditions which impact or are impacted by the objects.		
4. Determine requirement for data time stamp accuracy.		
5. Identify acceptable latency and latency variations, especially when closed loop interactions are involved.		
6. Identify acceptable level of induced errors (e.g. dropout rate, missing data).		
7. Refine post-test data management, processing, and analysis requirements defined in step 1 (Define Federation Objectives).		
8. Identify network requirements including the protocols to be used.		
9. Develop test control and monitoring requirements.		
10. Determine display and monitoring requirements.		
11. Determine voice communications requirements.		

Step 3: Design Federation

Federation participants (federates) are determined, and required functionalities are allocated to the federates.

Participants: The federation user/sponsor and federation manager are the participants at the beginning of this step. As the step progresses, and federates are selected, the federate developers also participate. The user/sponsor monitors progress periodically.

	A	C
Select Federates		
1. Identify candidate federates. Sources for review include: the Object Model Library (OML), the DOD and Service specific Modeling and Simulation Resource Repositories (MSRRs), user preference, federation manager experience, and federation sponsor required federates (if any).		
2. Survey candidate federates; select federates based upon criteria listed below; identify additional criteria as applicable.		
3. Review goals for federation application with respect to selected federates and availability of resources.		
• Survey Candidate Federates - Operational Characteristics		
1. Does the candidate simulation support some or all of the Conceptual Model?		
2. Can the simulation represent desired object behaviors?		
3. Has the simulation been accredited for use in similar applications? [VV&A]		
4. Can the simulation be modified (if required) to meet requirements defined in FEDEP steps 1 and 2?		
5. Can this simulation, coupled with one or more other simulations, meet requirements?		
• Survey Candidate Federates - Technical Characteristics		
1. How many objects can the simulation represent? How is object count related to performance?		
2. In a typical simulation run, what period of time is represented? How long (wall clock time) does it take to simulate that period of time?		
3. What time evolution mechanism does the simulation employ?		
4. Does the simulation have interfaces to other models or systems? What type of interfaces? What models? What systems?		
5. Has the simulation completed HLA compliance testing? What version of the Specification?		
• Survey Candidate Federates - Logistical Characteristics		
1. If necessary, is the simulation portable? What type of computer(s) are		

	A	C
required to host the simulation? Are secure computer(s) required to host the simulation? [Security]		
2. Where does/can simulation development occur?		
3. What scenarios are available?		
4. Is a human in the loop required? Is a human in the loop supportable?		
5. Is the federate available during the anticipated federation execution?		
6. If a live federate, will asset be available?		
7. Will the selected federates be able to support the security requirements of any newly identified functionality. [Security]		
Allocate Functionality		
1. Of the selected federates, identify the simulation that provides the most credible representation of the desired functionality.		
2. Identify the desired level of detail for specific functionality required by the federation application. Verify that the simulation can provide that level of detail.		
3. Determine if the representation of an object in a particular simulation provides the appropriate doctrinal representation.		
4. Review federate functional allocations from a performance perspective. Will the allocated functions prevent the simulation from achieving the desired performance?		
5. Assess the flexibility of the simulations to model future and alternative events, objects, and behaviors against the requirements of the federation application.		
6. Assess the cost and impact of modifications to simulations required by the federation application.		
7. Assess availability of security mechanisms and processes to support desired level of security within the federation (i.e., is the federation implementation feasible from a security perspective?). [Security]		
8. Verify that Federation Design appropriately represents the Conceptual Model. [VV&A]		
Prepare Plan		
1. Develop a coordinated plan to guide the development, test, and execution of the federation.		
2. Draft Verification and Validation Plan based on functional design. Verify tests will measure influence of identified factors. [VV&A]		
3. Focus V&V efforts placing the greatest attention and focus on the most critical federation objectives. [VV&A]		
4. Develop Security Test Plan. Review federation test and integration plan for overlap, so that security data can be gathered as federation test and integration is accomplished. [Security]		

	A	C
Program Management		
• Federation Startup		
1. Establish contractual relationships.		
2. Host a kickoff meeting to introduce participants, review federation objectives, functional allocation, and discuss schedule and milestones.		
• Federation Coordination		
1. Put contract vehicles in place for federate developers as they come on board.		
2. Verify existence of developer resources to support effort.		
3. Identify required agreements between federate sponsor and federation sponsor. Put in place as needed.		
4. Identify locations of federate development activities (single site or distributed).		
5. Determine locations for integration, test, and execution activities (single site or distributed).		
6. Plan location and frequency of federation team meetings.		
7. Organize administrative lists: email, phone, unclassified mailing addresses, classified mailing addresses.		
8. Identify strategy for incorporating expanding staff as federate developers join effort.		
9. Identify strategy for identifying problems and solutions as the federation effort gets underway.		
• Schedules and Budgets		
1. Expand high-level schedules to identify major milestones and decision points.		
2. Recognize schedule drivers. End dates may be driven by: federation sponsor requirements, complexity of implementation, and resource availability.		
3. Review schedule drivers with user/sponsor.		
4. Record detailed plans and schedules for the whole federation and the individual federates in a Federation Development Plan.		
5. Compare schedules and available resources to federation design and development plan.		
6. Review estimated hardware, software and network requirements. Adjust funding, schedule, and project scope as required.		
7. Assess impact of any changes in security classification level on timelines. [Security]		

Federation Design for Experimentation and Analysis	**A**	**C**
• Federate Survey		
1. Assess ability of candidate simulation to generate MOEs and MOPs in support of experiment.		
• Functional Allocation		
1. Once federates have been chosen, each federate provides information about key algorithms, data requirements, and known data sources.		

Federation Design for Training	**A**	**C**
1. Assess candidate simulations ability to support training requirements. Do the candidate simulations provide the desired battlespace functionality at the resolution and accuracy required to meet training objectives and plans?		
2. If the number and type of simulations and simulators will change during the course of a training event, identify the configuration required for each phase of the training event and identify the resources required to facilitate those changes.		
3. Assess candidate simulations ability to support instructor, security, and facility requirements. [Security]		
4. Assess ability of candidate simulations to generate MOEs and MOPs in support of the training data collection requirements.		
5. Identify the data collection approach, including what data will be collected, how that data will be collected, and how the data will be applied to meet federation objectives.		
6. Identify federation requirements for environment, threat and image database correlation and methods for obtaining them.		
7. Verify that federates participating in the federation can support "fair-fight" requirements. [VV&A]		
8. Determine availability of simulations for use in particular training exercise. Deconflict simulation and support team schedules.		

Federation Design for Test and Evaluation	**A**	**C**
1. If distributed, conduct federate surveys for security, operating parameters, and network concerns. [Security]		
2. Select test control hardware and software.		
3. List any data deficiencies and resultant requirements for new model development and plans to accomplish.		
4. Draft data collection plan.		

Step 4: Develop Federation

The Federation Object Model (FOM) is developed, federate agreements on consistent databases/ algorithms are established, and modifications to federates are implemented (as required).

Participants: The federation manager and federate developers are the primary participants of this step. The user/sponsor monitors progress and participates based on availability.

	A	C
Develop FOM		
• FOM Design		
1. Design FOM from Conceptual Model.		
2. Select a FOM development approach, for example: merging individual federate SOMs, starting from a primary federate SOM and adding objects and interactions, selecting a reference FOM and modifying it.		
3. Examine the Object Model Data Dictionary System (OMDDS). Look for common labels and enumerations for objects, attributes, interactions, and parameters. Where appropriate, use terms from the OMDDS.		
4. Trim the FOM to reflect the public and private objects required by the federation publication/subscription agreements.		
5. Check the FOM to ensure that object and interaction publications and subscriptions are correct.		
6. Ensure that FOM supports the federation's data collection requirements.		
7. Review security agreements with respect to the ability of the federates to share data. Establish memorandums of agreement (MOA) between federates to enable classified information sharing. [Security]		
8. Verify that the FOM reflects federate selection, functional allocation, federation agreements, and data collection agreements. [VV&A]		
• Publication/Subscription Agreements		
1. Discuss public and private objects (are all objects public, or only objects required for reflection?).		
2. Discuss and decide on an object update practice: update objects when attributes change, update objects on a periodic basis as long as object exists, or other?		
Establish Federation Agreements		
• Scenario		
1. Confirm availability of desired location and terrain data files.		
2. Determine availability of data for year being simulated (for example, aircraft in the year 2010).		

	A	C
3. Confirm federates' ability to support desired simulation duration (3 hours, 48 hours, two weeks, etc.).		
4. Identify authoritative data sources whenever possible; obtain and review data.		
5. Build federate databases.		
6. Review security agreements. [Security]		
• Time		
1. Discuss and decide on a measurement unit for federation time.		
2. Identify whether the federation should employ real-time or logical time.		
3. If logical time, discuss time-evolution mechanisms (next event, periodic advances).		
4. Determine each federate's update frequency and lookahead. Different types of objects may have different update frequency requirements.		
a Synchronization		
1. Discuss the need for federation synchronization points.		
2. Determine implementation strategy.		
• Save & Restore		
a Discuss the need for federation save and restore.		
b Determine implementation strategy.		
• Data Distribution Management		
1. Discuss the need for data distribution management.		
• Federation Algorithms		
1. Identify key algorithms (such as line-of-sight, detection, probability of kill, etc.) and establish federation method.		
2. Determine which federate computes attrition, for example, the federate owning the target object computes attrition.		
3. Determine which federate computes communication delays; for example, the federate sending the message, or a communications server federate.		
4. Discuss dead-reckoning algorithms and applicability.		
5. Determine the conditions under which federation algorithms will meet fidelity requirements.		
• Physical Representations		
1. Determine earth projection (flat earth, spherical earth, other).		
2. Determine location coordinate system (2 or 3 dimensional, UTM, latitude and longitude (degrees, minutes, seconds, or decimal degrees and number of decimal places)).		
3. Determine units of measure: speed, altitude, depth, etc.		
4. Describe unit placement (dimensions relative to orientation described as degrees from north).		

	A	C
5. Discuss terrain and environmental details described in Conceptual Model step. Ensure that the desired level of representation is obtained across the federation.		
• Federate-to-Federate Agreements		
1. Determine byte ordering scheme for public data.		
3. Determine encoding and decoding scheme for data elements including how element counts are identified for lists.		
4. Determine approach for byte boundary alignment within complex datatypes.		
5. Determine approach for object attribute consistency for late joining federates.		
• System Preparation		
1. Identify the version of the HLA Specification to be used and the version of supporting tools (RTI, OMDT, FEPW, etc.).		
2. Decide whether a federation management tool will be used.		
3. Determine whether a logging federate will be used or if each federate will log its own data.		
4. Determine if a viewer federate will be used.		
5. If integration and execution will be distributed, identify the requirements (this item gets more attention in the Step 5 Checklists):		
• identify the locations to host federates		
• identify bandwidth requirements		
• identify the security level of communications [Security]		
• establish communication links between site for people conducting integration, test, and execution.		
6. Assess security requirements with respect to hardware. [Security]		
7. Assess availability of security mechanisms and processes to support desired level of security within the federation (i.e., is the federation implementation feasible from a security perspective?). [Security]		
Implement Federate Modifications		
1. Implement internal modifications to the federates to support assigned domain elements.		
2. Implement modifications or extensions to the federates' HLA interfaces to support new FOM data structures or HLA services that were not supported in the past.		
3. Develop HLA interface for non-HLA-compliant federates.		
Program Management		
• Schedules and Budgets		
1. Expand high-level schedules to identify major milestones and decision points.		
2. Build detailed schedules:		

	A	C
• include roles and responsibilities for each product, • permit review and comment on all draft products, • obtain schedule concurrence with all participants, and • monitor continually. 3. Record detailed plans and schedules for the whole federation and the individual federates in a Federation Development Plan. 4. Compare schedules and available resources to federation design and development plan. 5. Ensure that all team members have access to report problems and offer solutions.		

Federation Development for Experimentation and Analysis	A	C
• FOM Design 1. Verify that the objects and interactions in the FOM reflect the Experimentation Plan. [VV&A] • Data Collection 1. Determine data collection approach: designate a logger federate, have each federate log data, or use a combination of these logging strategies. 2. Draft the Data Collection Plan. 3. Identify supporting calculations of the MOEs and MOPs. 4. Detail data elements to be collected to support MOE and MOP computations. 5. Specify data recording format and data recording frequency or triggers. 6. Establish file naming conventions. 7. Identify and record any agreements specific to data collection and interpretation.		

Federation Development for Training	**A**	**C**
1. Verify that the objects and interactions in the FOM reflect the master training plan. [VV&A]		
2. Verify that federates participating in the federation can support "fair-fight" requirements. [VV&A]		
3. Verify that federation documentation and the training master plan are consistent. [VV&A]		
4. Determine availability of simulations for use in particular training exercise. Deconflict simulation and support team schedules.		
5. Identify exercise participants (e.g. who will pilot the aircraft simulator?)		

Federation Design and Development for Test and Evaluation	**A**	**C**
1. Refine MOEs and their potential drivers.		
2. Verify that data required to support the MOEs is represented in the FOM. [VV&A]		
3. Determine coordinate transformations requirements, dead reckoning requirements.		
4. Determine data collection/instrumentation requirements.		
5. Determine and implement federate modifications		
6. Develop a document, such as an interface control document, to record the "who, what, when, where, and how" of each federation interface. This document, or a supplemental document, should also record all federation agreements.		
7. Perform "quick look" data collection and analysis.		

Step 5: Integrate and Test Federation

All necessary federation implementation activities are performed, and testing is conducted to ensure interoperability requirements are being met.

Participants: During this step, the federation manager works closely with the federate developers. The participation of the user is particularly important as new (future) objects and behaviors are developed and as data is obtained, input, and tested.

	A	C
Plan Execution		
• Begin Incremental Integration		
1. Test individual federates to ensure that HLA functionality has been implemented correctly.		
2. Perform incremental federation integration as a series of integration events.		
3. Schedule and complete federate compliance testing		
4. Perform federation testing encompassing scenario inputs and initialization, all functionality required by the conceptual model, and data collection, correlation and reduction.		
5. Verify that security procedures are in place wherever federation integration, test, and execution will occur. [Security]		
• Plan Federation Execution		
1. Select methodology or tool to complete federation execution planning.		
2. Identify available computer resources for federation execution and record them in the FEPW. Compare to estimated required computer resources identified in System Preparation items noted previously (in Step 3).		
3. Record network characteristics of available network in the FEPW. Compare to estimated required network resources.		
4. Record each federate's basic operating characteristics (tick parameters, time management scheme, etc.)		
5. Assign host machines for each federation component.		
6. Indicate RTI services used by each federate.		
• Prepare Facility		
1. Verify that all facilities are ready.		
2. Ensure that the appropriate hardware is in each facility.		
3. Ensure that all necessary software, including the RTI, is installed on each host.		
4. Establish appropriate user accounts.		
5. Ensure network connectivity exists between sites and between hosts.		
6. Work system administration details (system administrator, back up schedule, procedures for receiving classified materials, procedures for		

	A	C
writing classified materials, etc.).		
7. Ensure that dedicated lines are available with the appropriate modems and encryption devices. [Security]		
8. Verify that secure network connections are in place where required. [Security]		
• Test Federates		
Note: This testing is in addition to federate development and testing conducted by the federate developer.		
1. Plan individual federate testing with test federate, test harness, FVT , or other tools as instrumental.		
2. Ensure federate can join and resign.		
3. Test federate's declaration management by viewing its publication and subscription sets. One way this can be done is with a federation management tool.		
4. Ensure that federate can register and update objects, as appropriate for federate.		
5. Ensure that federate can send interactions as appropriate for federate.		
6. Use test federate or FVT to cause reflections to be sent to federate, as appropriate.		
7. Use test federate or FVT to cause interactions to be sent to federate, as appropriate.		
Integrate Federation		
b Integrate Federates		
1. Review FOM and federation execution planning prior to integration event. Ensure the FOM and the execution plan are consistent and complete.		
2. Write (if not already written) and review Test Plan. Verify that it tests the individual federate capabilities as well as federation modeling and data collection capabilities and constraints. Encourage federate developers to participate in Test Plan drafting and review. [VV&A]		
3. Schedule incremental integration events (subsets of functionality, data, federates, etc.). Make sure that federate development schedules are coordinated to permit incremental testing.		
4. Build and test scenario files incrementally. It may be helpful to test functionality using a small number of objects, then increase the number of objects to the number required. This technique may also be applied to behaviors.		
5. Schedule should include time for software and data debugging, coding, re-testing, and network performance tuning.		
6. Establish mechanism for recording known software problems and workarounds.		
7. Contact Help Desk for the RTI supplier if anomalies are suspected.		

	A	C
• Perform Compliance Testing		
1. All federates have to complete compliance testing. Federates should decide if compliance testing (if not previously accomplished) is to be completed as federates within a federation or independently. If compliance testing is to occur as a federation, it needs to be scheduled with the compliance testers and time allotted for this task. (Refer to compliance checklist on HLA web page for detailed compliance testing procedures.)		
Test Federation		
1. Review scenario inputs for each planned execution.		
2. Review all objects and behaviors identified in the conceptual model:		
• Is the simulation representation accurate?		
• Is it consistent across the federation?		
• Has a level playing field been achieved?		
3. Execute all tests in the Test Plan.		
4. Collect, reduce and analyze data for each test.		
5. Review each planned excursion with the user.		
6. To the extent possible, stress the federation by simulating the expected federation loads during execution from federation initialization through expected completion point.		
7. Conduct federation V&V. [VV&A]		
8. Review V&V results with user. [VV&A]		
9. Implement changes as required. [VV&A]		
10. Enable user to make accreditation decision. [VV&A]		
11. Implement any security tests as required to reach a positive certification and accreditation decision. [Security]		
Program Management		
• Schedules and Budgets		
1. Monitor management and technical problem reporting and solutions.		
2. Monitor schedules and budgets. Focus solutions on high priority elements of federation application.		

Federation Integration and Test for Experimentation and Analysis	**A**	**C**
1. Review the Experimentation Plan. Ensure that all critical elements of the Experimentation Plan are simulated in the federation.		
2. Review Data Collection Plan. Verify that all data elements required to support the experiment have been identified, and that a federate is responsible for collecting each data element. Review data reduction and correlation strategy for completeness and ease of institution. [VV&A]		
3. Review data delivery dates. (Have all data requirements been identified? Has data been delivered?)		
4. Test data collection and reduction.		
5. Schedule data reviews (input, output, and reduced data) with the user.		
6. Test each case (base and all alternatives) through data reduction. User participation is important!		
7. Consider batch processing or automated procedures for conducting multiple executions of each case. Conduct thorough end-to-end testing of each case (including data collection, correlation, and reduction) and operating procedures for multiple executions.		

Federation Integration and Test for Training	**A**	**C**
1. Develop and execute an Integration and Test Plan to ensure that all critical elements of the master training plan are simulated in the federation and that the concept of operations is executable. This plan should include security planning. User and training command participation is critical. [Security]		
2. If different simulations and simulators are required by different phases of the training event, test the procedures identified to accomplish those changes. How quickly can the computer resources be reconfigured to support this requirement? Can the scenario be maintained? Is a level-playing field maintained?		
3. Verify that environment, threat and image database accuracy, format and presentation requirements are satisfied by the federation. [VV&A]		
4. Verify that environment, threat and image databases are correlated correctly across the federation. [VV&A]		
5. Verify that all data elements required to support the training have been identified, and that data collection responsibilities for each data element are clear. Review data reduction and correlation strategy for completeness and ease of institution. Test data collection and reduction. [VV&A]		

Federation Integration and Test for Test and Evaluation	**A**	**C**
1. Develop test scenarios to support integration.		
2. Develop test control procedures.		
3. Develop detailed execution plans.		
4. Install network hardware and software.		
5. Perform compliance testing.		
6. Execute integration plan.		
7. Identify and practice risk reduction measures if live players involved.		

Step 6: Execute Federation and Prepare Results

The federation is executed, outputs are generated and results provided.

Participants: Depending on the degree of automation that has been implemented, participants in this step will vary.

	A	C
Execute Federation		
1. Execute the desired runs.		
2. Review results, take appropriate action.		
3. Archive FOM in Object Model Library.		
4. Provide data recommendation entries to OMDDS.		
5. Archive federation products for future review or use.		
6. Ensure continued secure operation in accordance with certification and accreditation decisions and requirements. [Security]		
Process Outputs		
1. Apply appropriate statistical measures and other data reduction methods to transform raw data into derived results.		
Prepare Results		
1. Evaluate the derived results from the previous activity to determine if all federation objectives have been met.		
2. If all federation objectives have been achieved, store all reusable federation products in an appropriate archive and, if appropriate, make them available through systems such as the Modeling and Simulation Resource Repository (MSRR).		
3. Verify that each excursion meets VV&A expectations. [VV&A]		
4. Prepare an Accreditation Report. [VV&A]		
Program Management		
• Schedules and Budgets		
1. Complete scheduled executions and products.		
2. Complete contractual obligations.		

Federation Execution and Analysis for Experimentation and Analysis	A	C
1. Collect and reduce data.		
2. Analyze data and make results available to user (analyst) and subject matter experts for review.		
3. Make additional runs, as required by analysis.		

Federation Execution for Training	**A**	**C**
1. Manage federation simulation/simulator execution in accordance with the master training plan and conops, including training scenarios, initial simulation/simulator conditions, and mid-event transitions to different simulations and simulators as required.		
2. Populate environment, threat and image databases, and ensure correlation across the federation.		
3. Execute federation and collect training results data for federation sponsors and users.		
4. Detect and report problems with federation execution, including federate modeling capabilities, scenarios, databases, etc.		

Federation Execution and Analysis for Test and Evaluation	**A**	**C**
1. Develop test matrix based on test objectives.		
2. Execute test matrix.		
3. Exercise test control/management.		
4. Collect data.		
5. Analyze execution outputs with analysis team. Runs may need to be repeated if questionable data is gathered.		
6. Provide feedback.		
7. Document changes in code, scenarios, data collection plans, etc.		

Terms

Experimentation - federations used to support experimentation involve iterative exploration of hypotheses; and the quantification and assessment of results proving or disproving the hypothesis. Experiments are repeatable, credible, and include quantifiable measures. Experiments are a subset of Analysis which may employ a variety of different analytical methods.

Persistent Federation - a federation that is developed to meet multiple application goals from the outset, or alternatively, developed to meet a single application goal and then applied again after the end of the program which created it. The federation is re-used, possibly modified, and applied to a new objective

T&E - an activity whose purpose is to interactively evaluate and improve the design, performance, joint military worth, survivability, suitability, and effectiveness of systems to be acquired, and to improve on how those systems will be used. Both formal and less formal methods are used.

Acronyms

C2	Command and Control
C4I	Command, Control, Communications, Computers, and Intelligence
DMSO	Defense Modeling and Simulation Office
DOD	Department of Defense
FEDEP	Federation Development and Execution Process
FEPW	Federation Execution Planner's Workbook
FOM	Federation Object Model
HLA	High Level Architecture
JAO	Joint Attack Operations
JSEAD	Joint Suppression of Enemy Air Defenses
MOE	Measure of Effectiveness
MOP	Measure of Performance
MSRR	Modeling and Simulation Resource Repository
OMDDS	Object Model Data Dictionary System
OMDT	Object Model Development Tool
OML	Object Model Library
ORD	Operation Requirements Documents
POC	Point of Contact

R&D	Research and Development
RTI	Run Time Infrastructure
SOM	Simulation Object Model
T&E	Test and Evaluation
TEMP	T&E Master Plan
UTM	Universal Transverse Mercator
VV&A	Verification, Validation, and Accreditation