Distributed Event Integration and Execution

Michael J. O'Connor, Trideum Corporation
Dr. Kenneth G. LeSueur, Redstone Test Center

TRIDEUM
Analyze. Integrate. Innovate.

UNITED STATES ARMY RTC REDSTONE TEST CENTER

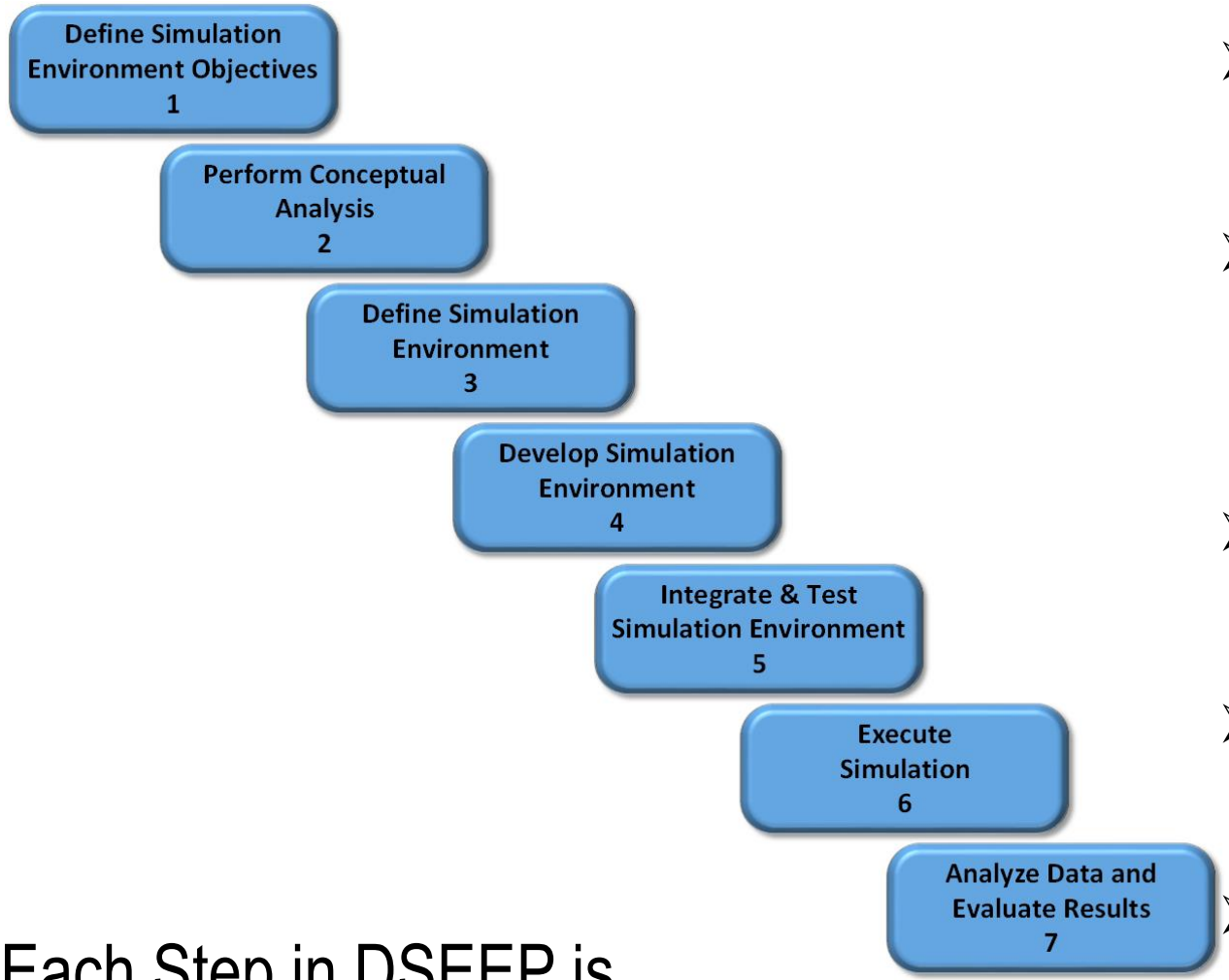
Learning Objectives

- At the end of this tutorial, students will be able to:
  - List the activities required to perform integration and execution of a distributed simulation event
  - Describe an event in the terms required to plan the integration
  - Select the integration activities required for an event
  - Develop an outline for an integration plan for a distributed simulation event
  - Describe the key roles in a distributed event integration and execution

Process Purpose

- Distributed Live Virtual Constructive (LVC) events are conducted to support training, testing, research & development, and mission rehearsal
- For many years, these environments were created by a small set of very experienced teams
  - Events with less skilled teams often failed, overran costs, or did not meet schedules
- A well-defined process allows for less reliance on highly skilled practitioners
- It is critical that the users of data from distributed LVC environments trust the results
  - An incorrectly created environment can lead to negative training, false test results, bad research, and failed missions

DSEEP



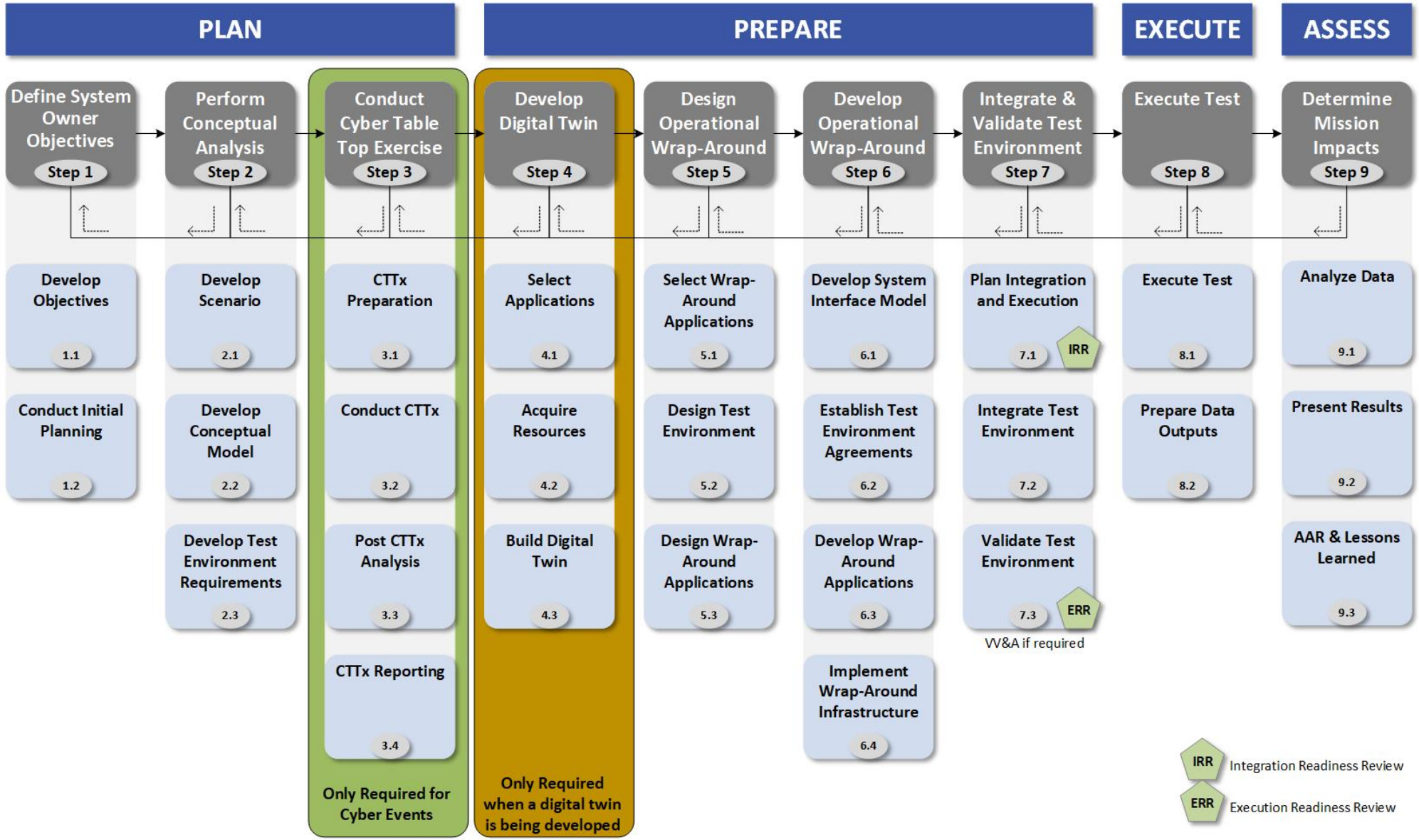
Each Step in DSEEP is divided into activities

- Distributed Simulation Engineering and Execution Process (DSEEP)
- IEEE Std 1730-2010, developed by Simulation Interoperability Standards Organization (SISO)
- Distributed simulation architecture independent
- Process model for the integration of distributed simulations
- The Process model has to be instantiated with a set of processes and supporting material

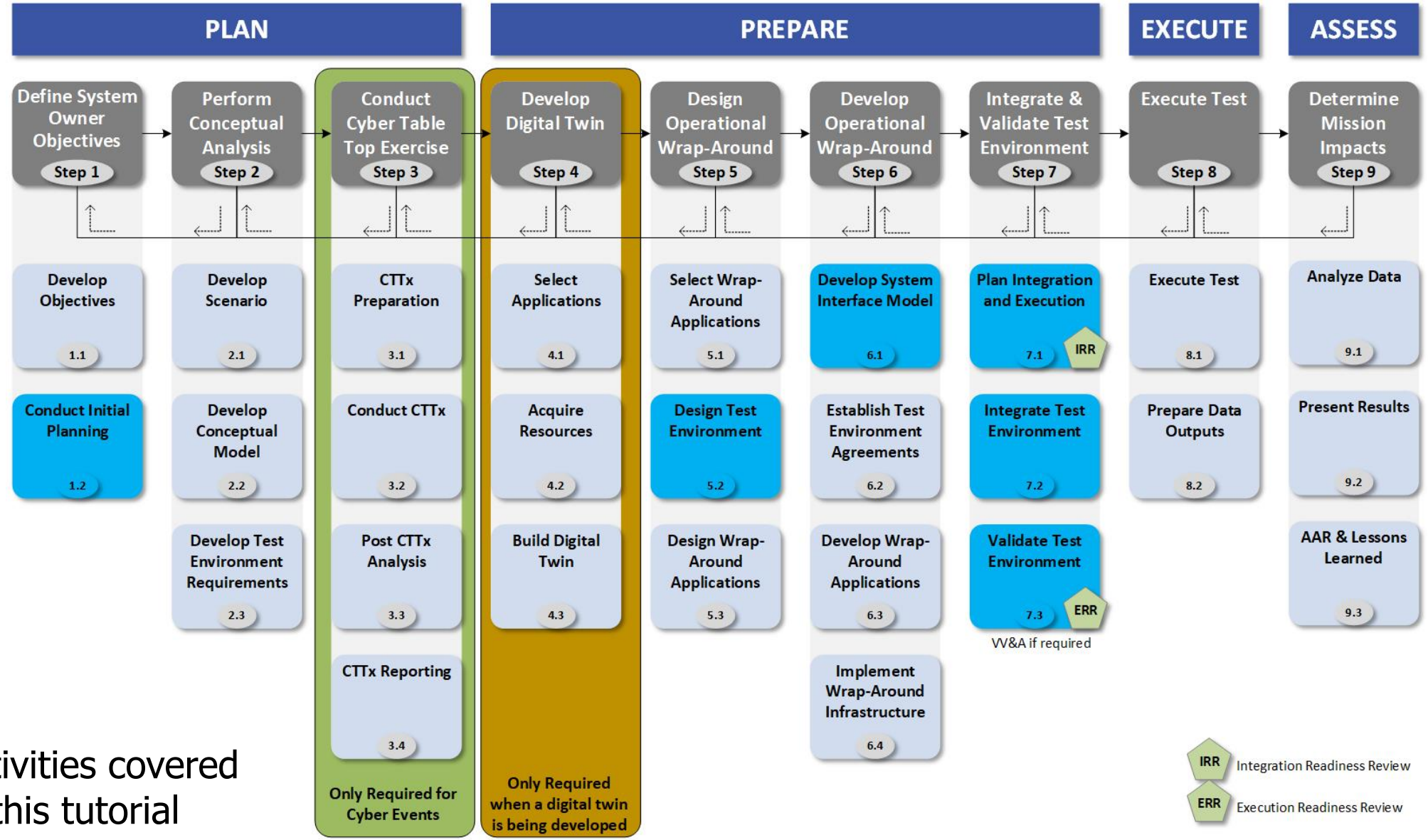
Process

- This process is based on the DSEEP model
- The processes documented here are based on years of experience integrating distributed LVC simulation events
- Distributed simulation events come in different sizes and have different objectives, but the same approach can be used for all of them with some tailoring
- This tutorial describes how to adjust based on the size and nature of the event being planned
- Today's tutorial only covers a limited part of the process

Process

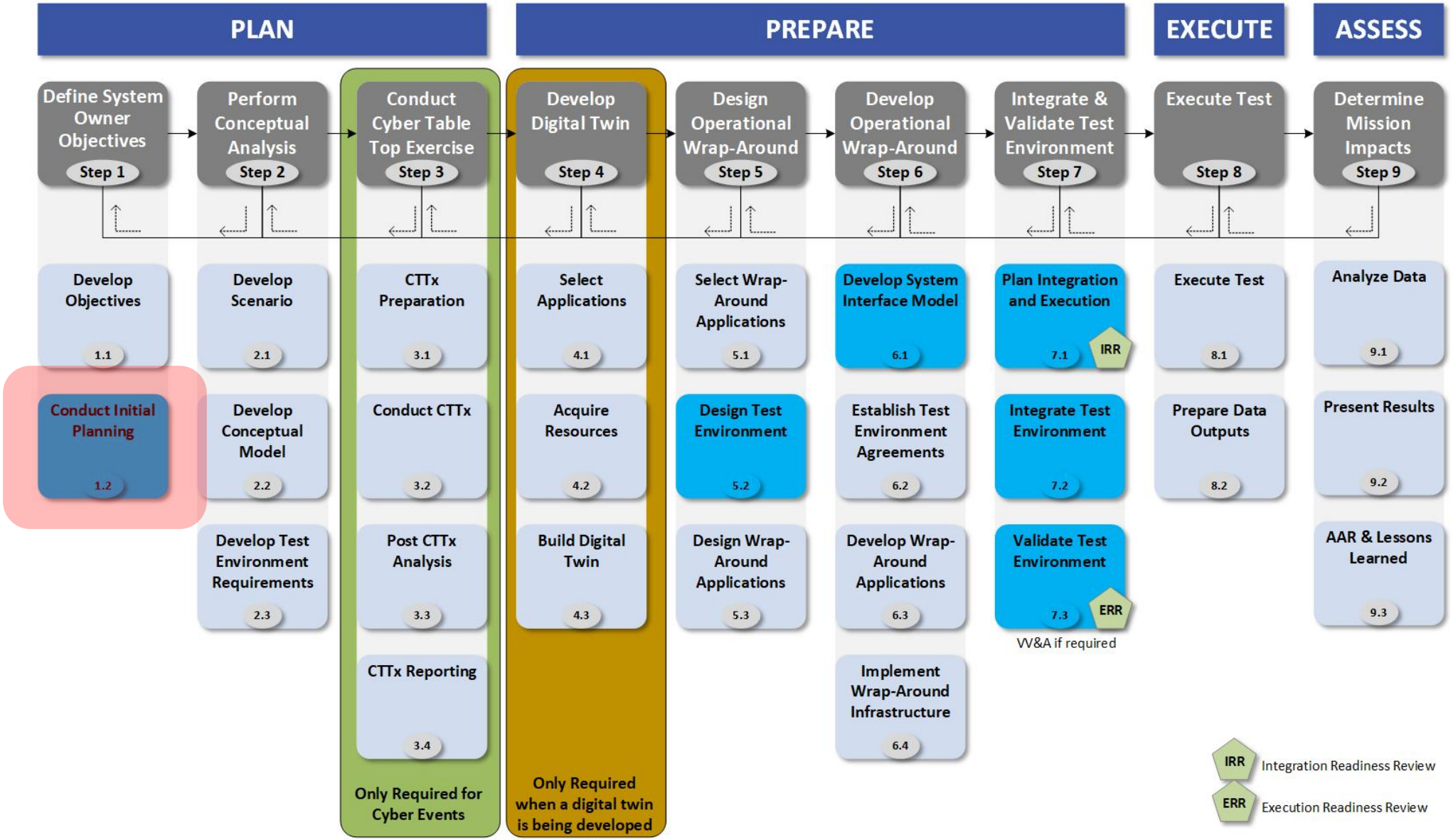

PLAN
PREPARE
EXECUTE
ASSESS
Define System Owner Objectives
Step 1
Perform Conceptual Analysis
Step 2
Conduct Cyber Table Top Exercise
Step 3
Develop Digital Twin
Step 4
Design Operational Wrap-Around
Step 5
Develop Operational Wrap-Around
Step 6
Integrate & Validate Test Environment
Step 7
Execute Test
Step 8
Determine Mission Impacts
Step 9
Develop Objectives
1.1
Conduct Initial Planning
1.2
Develop Scenario
2.1
Develop Conceptual Model
2.2
Develop Test Environment Requirements
2.3
CTTx Preparation
3.1
Conduct CTTx
3.2
Post CTTx Analysis
3.3
CTTx Reporting
3.4
Select Applications
4.1
Acquire Resources
4.2
Build Digital Twin
4.3
Select Wrap-Around Applications
5.1
Design Test Environment
5.2
Design Wrap-Around Applications
5.3
Develop System Interface Model
6.1
Establish Test Environment Agreements
6.2
Develop Wrap-Around Applications
6.3
Implement Wrap-Around Infrastructure
6.4
Plan Integration and Execution
7.1
IRR
Integrate Test Environment
7.2
Validate Test Environment
7.3
ERR
V&A if required
Execute Test
8.1
Prepare Data Outputs
8.2
Analyze Data
9.1
Present Results
9.2
AAR & Lessons Learned
9.3
Only Required for Cyber Events
Only Required when a digital twin is being developed
IRR
Integration Readiness Review
ERR
Execution Readiness Review

Today's Tutorial



Activities covered in this tutorial

Activity 1.2


PLAN
PREPARE
EXECUTE
ASSESS
Define System Owner Objectives
Step 1
Perform Conceptual Analysis
Step 2
Conduct Cyber Table Top Exercise
Step 3
Develop Digital Twin
Step 4
Design Operational Wrap-Around
Step 5
Develop Operational Wrap-Around
Step 6
Integrate & Validate Test Environment
Step 7
Execute Test
Step 8
Determine Mission Impacts
Step 9
Develop Objectives
1.1
Conduct Initial Planning
1.2
Develop Scenario
2.1
Develop Conceptual Model
2.2
Develop Test Environment Requirements
2.3
CTTx Preparation
3.1
Conduct CTTx
3.2
Post CTTx Analysis
3.3
CTTx Reporting
3.4
Only Required for Cyber Events
Select Applications
4.1
Acquire Resources
4.2
Build Digital Twin
4.3
Only Required when a digital twin is being developed
Select Wrap-Around Applications
5.1
Design Test Environment
5.2
Design Wrap-Around Applications
5.3
Develop System Interface Model
6.1
Establish Test Environment Agreements
6.2
Develop Wrap-Around Applications
6.3
Implement Wrap-Around Infrastructure
6.4
Plan Integration and Execution
7.1
IRR
Integrate Test Environment
7.2
Validate Test Environment
7.3
ERR
VV&A if required
Execute Test
8.1
Prepare Data Outputs
8.2
Analyze Data
9.1
Present Results
9.2
AAR & Lessons Learned
9.3
IRR Integration Readiness Review
ERR Execution Readiness Review

Organization/Roles

Conduct Initial Planning

1.2

- The Process defines a set of roles and working groups to execute the Process
  - Each activity is assigned to a role
  - Assigning a lead for each activity is done to ensure that no activities are skipped
- The exact organization varies based on the participants and the event
  - A single individual may have multiple roles
- Working Groups are established to plan and execute the process
  - Each working group is lead by one of the defined roles

Role Groups

Overall Roles: These roles direct the overall Process and participate from the beginning to end of each event. These roles participate heavily in Step 1 and contribute throughout the rest of the Process:

- **System Owner**
- **System Liaison Officer, Action Officer, or Point of Contact**
- **Test Director**
- **Test Lead**
- **Mission System Digital Twin Lead**
- **Analysis (Mission Impact) Lead**

Digital Twin Roles: These roles focus on the implementation and operation of the digital twin of the mission system. These roles participate throughout the process, lead Step 4, and contribute heavily in Steps 2, 3, 7, and 8:

- **Mission System Digital Twin Lead**
- **Digital Twin System Development Lead**
- **Digital Twin Network Lead**

Test Environment Roles: These roles focus on the implementation and operation of the wrap-around and integration of the Test Environment. These roles participate throughout the process and lead Steps 5, 6, 7, and 8:

- **Test Coordinator**
- **Battle-Master**
- **Site Lead**
- **Thread Lead**
- **Operators**
- **Role Players**

Conduct Initial Planning

1.2

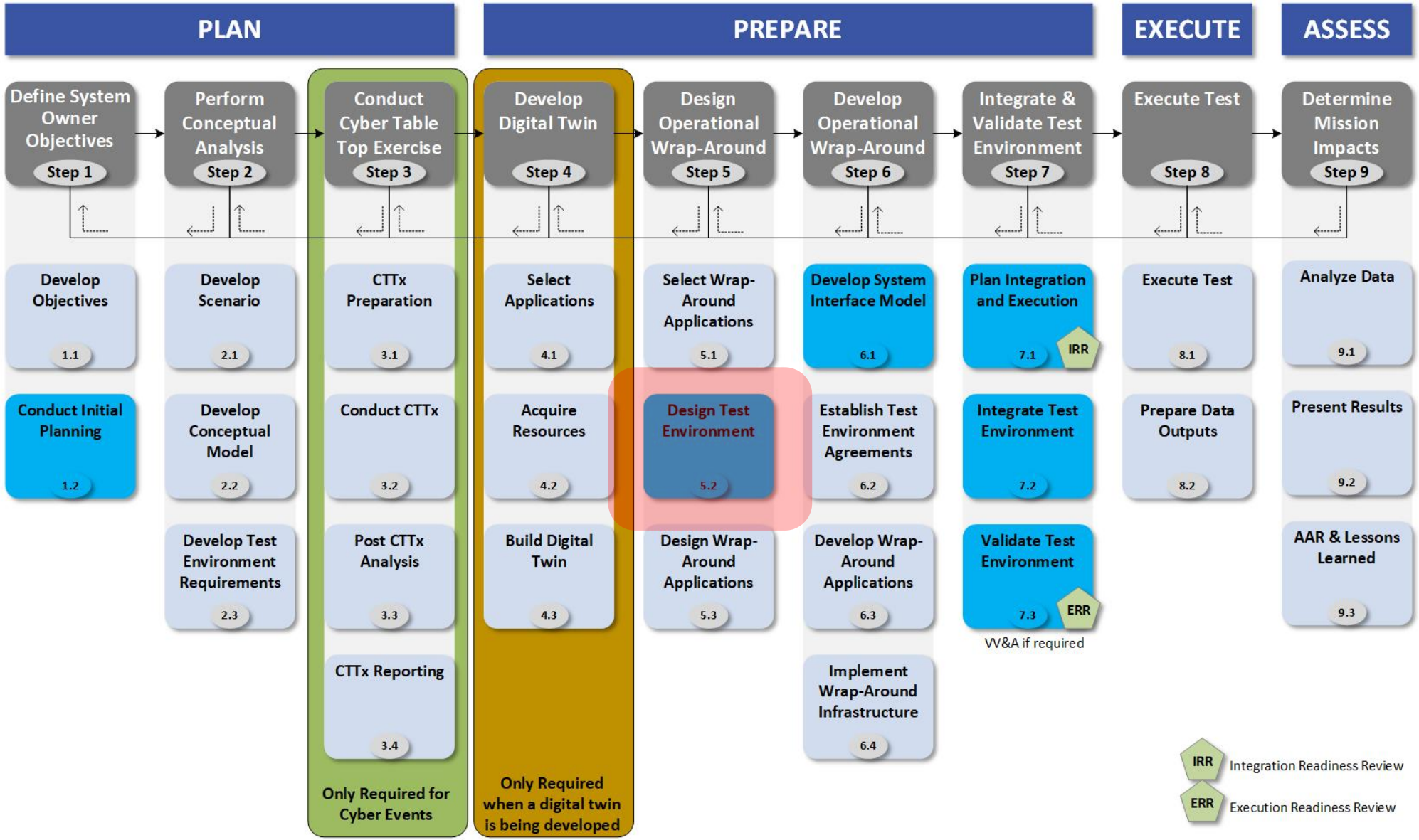
Working Groups

Conduct Initial Planning

1.2

- **Execution Control Group (EXCON):** Lead by the Test Lead, this team identifies and coordinates the plan of action and milestones for the event and produces the Test Plan.
- **Technical Working Group (TWG):** Lead by the Test Coordinator, this team develops the architecture products and builds the Test Environment
- **Scenario Working Group**. Lead by the Battle-Master, this team develops the scenarios, vignettes, and test threads and provides the operational context to the event.
- **Network Working Group**. Lead by the Test Coordinator, this team develops the network requirements and implements the test network infrastructure.
- **Analysis Working Group**. Lead by the Analyst (Mission Impact) Lead, this team develops the analysis plan and defines the data collection requirements, identifies the strategy for data collection, management, and analysis.
- **Security planning**. Lead by the Test Lead, this team identifies the level of security for the Test Environment.

Activity 5.2

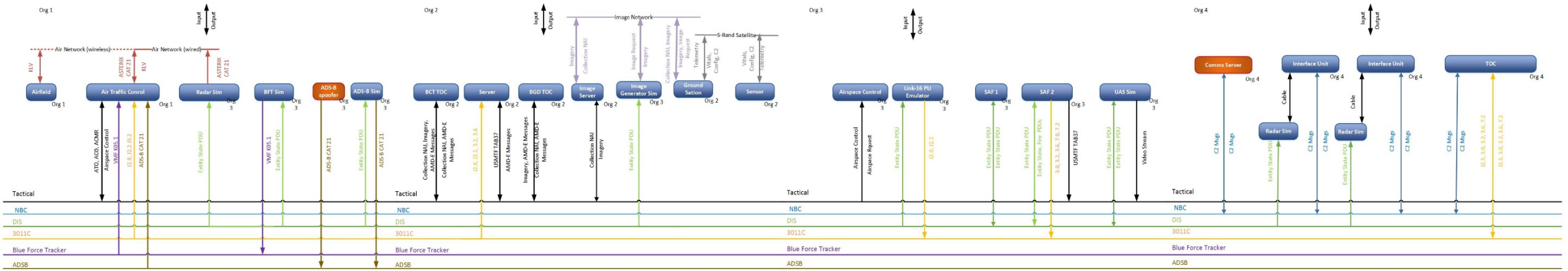

PLAN
PREPARE
EXECUTE
ASSESS
Define System Owner Objectives
Step 1
Perform Conceptual Analysis
Step 2
Conduct Cyber Table Top Exercise
Step 3
Develop Digital Twin
Step 4
Design Operational Wrap-Around
Step 5
Develop Operational Wrap-Around
Step 6
Integrate & Validate Test Environment
Step 7
Execute Test
Step 8
Determine Mission Impacts
Step 9
Develop Objectives
1.1
Conduct Initial Planning
1.2
Develop Scenario
2.1
Develop Conceptual Model
2.2
Develop Test Environment Requirements
2.3
CTTx Preparation
3.1
Conduct CTTx
3.2
Post CTTx Analysis
3.3
CTTx Reporting
3.4
Select Applications
4.1
Acquire Resources
4.2
Build Digital Twin
4.3
Select Wrap-Around Applications
5.1
Design Test Environment
5.2
Design Wrap-Around Applications
5.3
Develop System Interface Model
6.1
Establish Test Environment Agreements
6.2
Develop Wrap-Around Applications
6.3
Implement Wrap-Around Infrastructure
6.4
Plan Integration and Execution
7.1
IRR
Integrate Test Environment
7.2
Validate Test Environment
7.3
ERR
VV&A if required
Execute Test
8.1
Prepare Data Outputs
8.2
Analyze Data
9.1
Present Results
9.2
AAR & Lessons Learned
9.3
Only Required for Cyber Events
Only Required when a digital twin is being developed
IRR Integration Readiness Review
ERR Execution Readiness Review

Connectivity Diagram

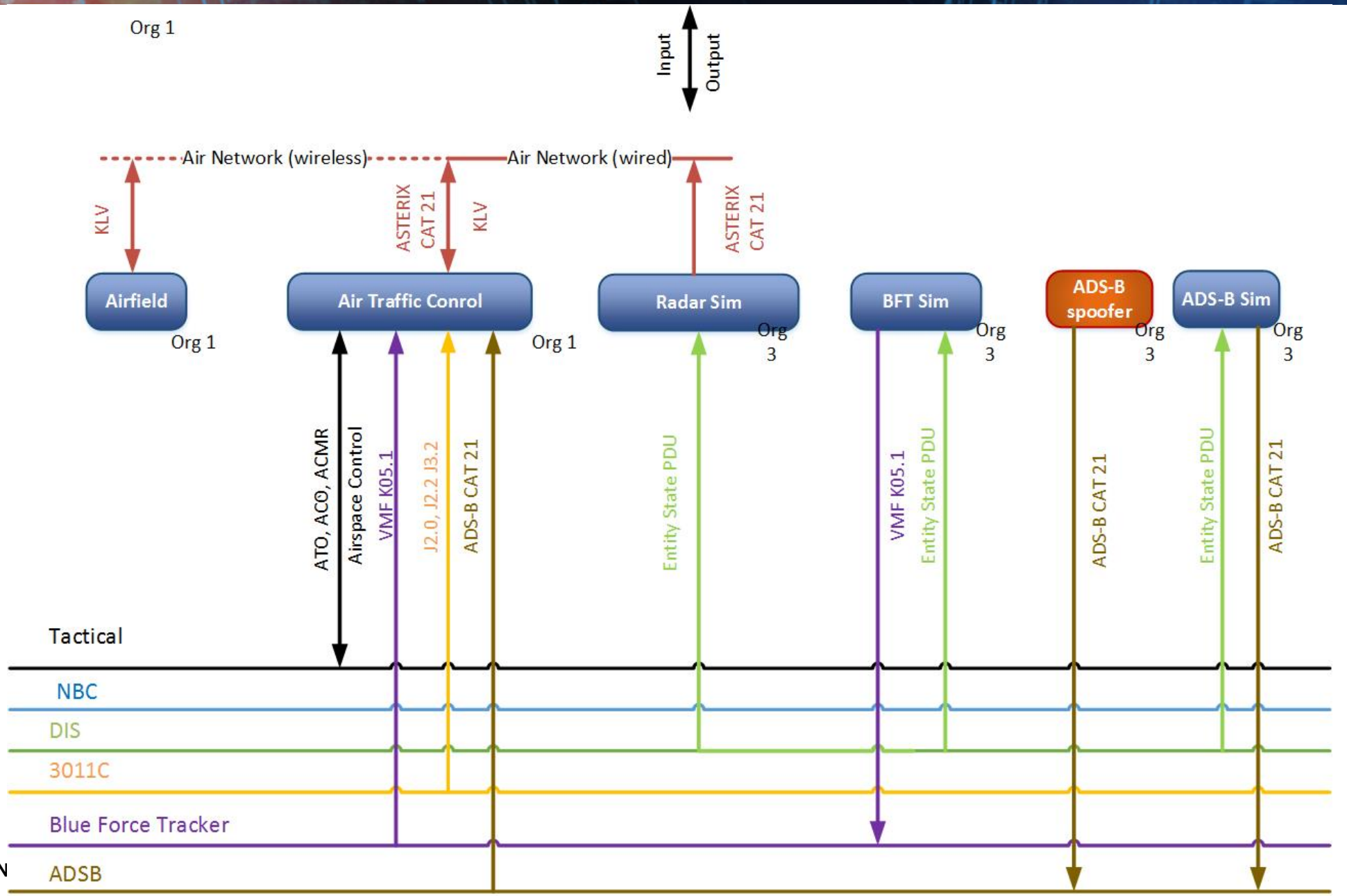
Design Test Environment

5.2

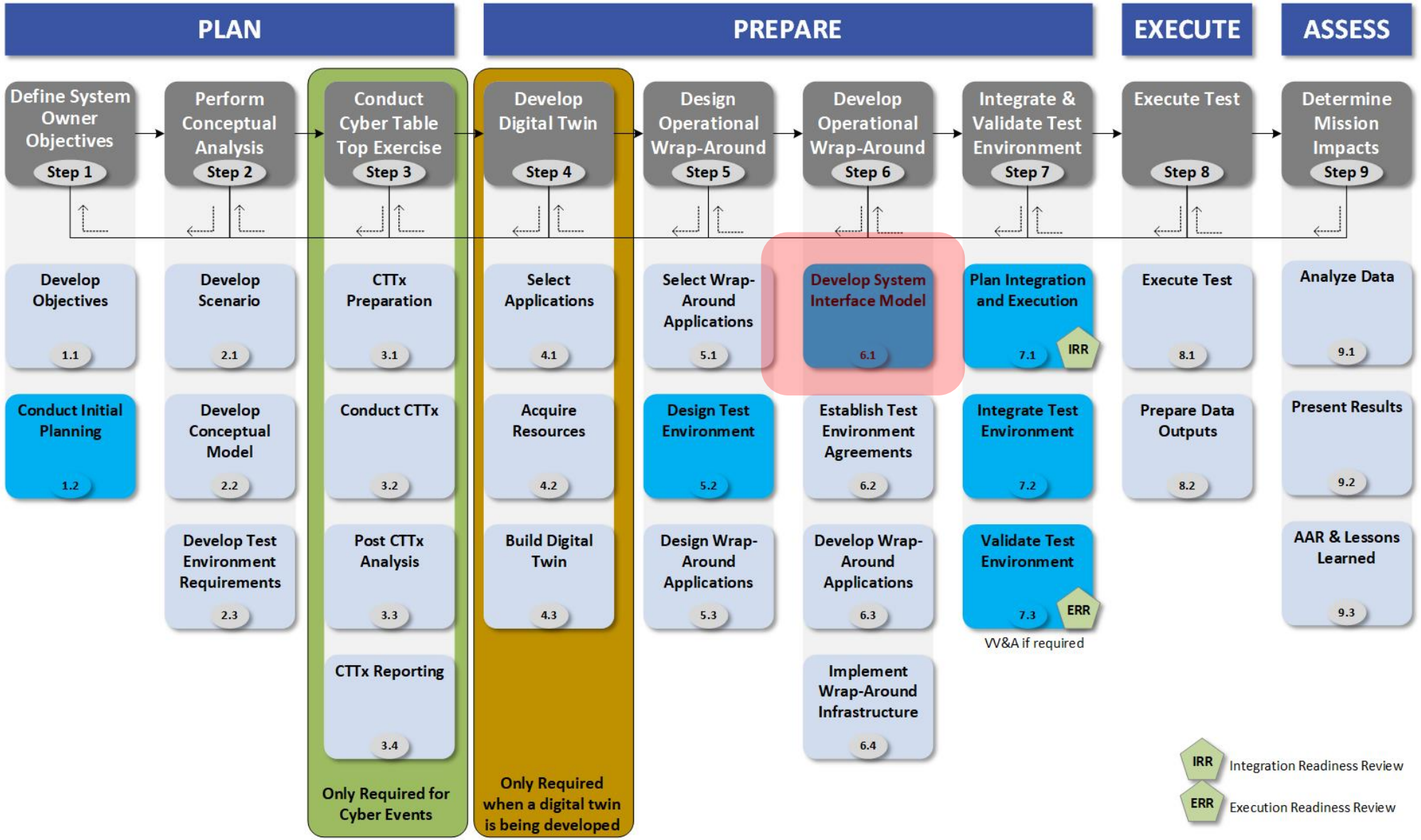
- The purpose of this diagram is to convey the connectivity between systems
- The representation and data vary by event
- Key data includes: Protocol, messages, and system names
- A key consideration in the selection of format is how well it can be briefed



Connectivity Diagram Detail



Activity 6.1


PLAN
PREPARE
EXECUTE
ASSESS
Define System Owner Objectives
Step 1
Perform Conceptual Analysis
Step 2
Conduct Cyber Table Top Exercise
Step 3
Develop Digital Twin
Step 4
Design Operational Wrap-Around
Step 5
Develop Operational Wrap-Around
Step 6
Integrate & Validate Test Environment
Step 7
Execute Test
Step 8
Determine Mission Impacts
Step 9
Develop Objectives
1.1
Conduct Initial Planning
1.2
Develop Scenario
2.1
Develop Conceptual Model
2.2
Develop Test Environment Requirements
2.3
CTTx Preparation
3.1
Conduct CTTx
3.2
Post CTTx Analysis
3.3
CTTx Reporting
3.4
Select Applications
4.1
Acquire Resources
4.2
Build Digital Twin
4.3
Select Wrap-Around Applications
5.1
Design Test Environment
5.2
Design Wrap-Around Applications
5.3
Develop System Interface Model
6.1
Establish Test Environment Agreements
6.2
Develop Wrap-Around Applications
6.3
Implement Wrap-Around Infrastructure
6.4
Plan Integration and Execution
7.1
IRR
Integrate Test Environment
7.2
Validate Test Environment
7.3
ERR
VV&A if required
Execute Test
8.1
Prepare Data Outputs
8.2
Analyze Data
9.1
Present Results
9.2
AAR & Lessons Learned
9.3
Only Required for Cyber Events
Only Required when a digital twin is being developed
IRR Integration Readiness Review
ERR Execution Readiness Review

Interface Matrix

Develop System Interface Model

6.1

- One row for each data message by source and target
- Columns for all information required to configure and test the systems

Source System	Source Instance	Target	Target Instance	Logged By	Source Protocol	Source Message	Source Transport	Source send to Address	Source send to Port	Target Protocol	Target Message	Target Transport	Target receive from Address	Target receive from Port	Description	Event Purpose	Update Condition	Tested
UAS Sim	Org 4	EADSIM	Org 4	MAK DIS Logger	DIS	Entity State PDU	UDP Multicast	225.10.27.72	3000	DIS	Entity State PDU	UDP Multicast	225.10.27.72	3000	Ground Truth Entity state	Position of UAS	DIS Dead Reckoning	
OneSAF	Org 4	EADSIM	Org 4	MAK DIS Logger	DIS	Entity State PDU	UDP Multicast	225.10.27.72	3000	DIS	Entity State PDU	UDP Multicast	225.10.27.72	3000	Ground Truth Entity state	Position of ground entitles and RWA	DIS Dead Reckoning	
OneSAF	Org 4	Radar Sim	Org 2	MAK DIS Logger	DIS	Entity State PDU	UDP Multicast	225.10.27.72	3000	DIS	Entity State PDU	UDP Multicast	225.10.27.72	3000	Ground Truth Entity state	Position of RWAs	DIS Dead Reckoning	
EADSIM	Org 4	OneSAF	Org 4	MAK DIS Logger	DIS	Entity State PDU	UDP Multicast	225.10.27.72	3000	DIS	Entity State PDU	UDP Multicast	225.10.27.72	3000	Ground Truth Entity state	Position of FWA. TELs, and TBMs	DIS Dead Reckoning	
EADSIM	Org 4	Radar Sim	Org 4	MAK DIS Logger	DIS	Entity State PDU	UDP Multicast	225.10.27.72	3000	DIS	Entity State PDU	UDP Multicast	225.10.27.72	3000	Ground Truth Entity state	Position of FWA. TELs, and TBMs	DIS Dead Reckoning	
EADSIM	Org 4	Link-16 PLI Emulator	Org 4	MAK DIS Logger	DIS	Entity State PDU	UDP Multicast	225.10.27.73	3000	DIS	Entity State PDU	UDP Multicast	225.10.27.73	3000	Ground Truth Entity state	Position of Blue FWA	DIS Dead Reckoning	
EADSIM	Org 4	UAS Sim	Org 4	MAK DIS Logger	DIS	Entity State PDU	UDP Multicast	225.10.27.73	3000	DIS	Entity State PDU	UDP Multicast	225.10.27.73	3000	Ground Truth Entity state	Position TELs	DIS Dead Reckoning	
EADSIM	Org 4	Sat Sim	Org 4	MAK DIS Logger	DIS	Fire PDU	UDP Multicast	225.10.27.74	3000	DIS	Fire PDU	UDP Multicast	225.10.27.74	3000	Weapon fire	Represent TBM fire	Launch	
EADSIM	Org 4	EOC Lite	Org 2	NSITE	30111-C	J 3.0	UDP Multicast	225.10.2.2	3100	30111-C	J 3.0	UDP Multicast	225.10.2.2	3100	Surveillance - Referance Point	TBM Laucnh point	N/A	
EADSIM	Org 4	ATC	Org 5	NSITE	30111-C	J 3.2	UDP Multicast	225.10.2.2	3100	30111-C	J 3.2	UDP Multicast	225.10.2.2	3100	Surveillance - Air Track	Air track from radar	N/A	
Link-16 PLI Emulator	Org 4	ATC	Org 5	NSITE	3011-C	J 2.0	UDP Multicast	225.10.2.2	3100	3011-C	J 2.0	UDP Multicast	225.10.2.2	3100	PPLI - Indirect Interface Unit	Forwarded postion message from FWA		
ADS-B Sim	Org 4	ATC	Org 5	Wireshark	ASTERIX	CAT 21	UDP Multicast	225.10.2.3	TBD	ASTERIX	CAT 21	UDP Multicast	225.10.2.3	TBD	Aircraft Position	Position of FWA		
ADS-B Spoofer	Org 4	ATC	Org 5	Wireshark	ASTERIX	CAT 21	UDP Multicast	225.10.2.3	TBD	ASTERIX	CAT 21	UDP Multicast	225.10.2.3	TBD	Aircraft Position	Fake postions fo FWA		
JSTEN	Org 4	ATC	Org 5	NSITE	VMF	K05.1	UDP Multicast	TBD	TBD	VMF	K05.1	UDP Multicast	TBD	TBD	Entity Position	Emulation of Blue Force Tracker	BFT publishing rules	
Radar Sim	Org 4	ATC	Org 5	TBD	ASTERIX	CAT 1/2	UDP Multicast	TBD	TBD	ASTERIX	CAT 1/2	UDP Multicast	TBD	TBD	Aircraft Position	Output of ATNAVICS Radar		

All addresses are notional

Interface Matrix Detail

System that is the source of the message

System that is the Target of the message

There is a line for every source/target pair even if it is the same message

Source System	Source Instance	Target	Target Instance	Logged By	Pr
UAS Sim	Org 4	EADSIM	Org 4	MAK DIS Logger	
OneSAF	Org 4	EADSIM	Org 4	MAK DIS Logger	
OneSAF	Org 4	Radar Sim	Org 2	MAK DIS Logger	
EADSIM	Org 4	OneSAF	Org 4	MAK DIS Logger	
EADSIM	Org 4	Radar Sim	Org 4	MAK DIS Logger	
EADSIM	Org 4	Link-16 PLI Emulator	Org 4	MAK DIS Logger	
EADSIM	Org 4	UAS Sim	Org 4	MAK DIS Logger	
EADSIM	Org 4	Sat Sim	Org 4	MAK DIS Logger	
EADSIM	Org 4	EOC Lite	Org 2	NSITE	

It is critical to list how the message is logged

There may be more than one instance of the system potentially at different sites

Interface Matrix Detail

Develop System Interface Model

6.1

Protocol can be distributed sim or tactical

The actual message being sent

Transport Examples: UDP Multicast, UDP Broadcast, TCP Unicast

Address the message is sent to

Port the message is sent to

Source Protocol	Source Message	Source Transport	Source send to Address	Source send to Port	Target Protocol	Target Message	Target Transport	Target receive from Address	Target receive from Port	De
DIS	Entity State PDU	UDP Multicast	225.10.27.72	3000	DIS	Entity State PDU	UDP Multicast	225.10.27.72	3000	Gr E
DIS	Entity State PDU	UDP Multicast	225.10.27.72	3000	DIS	Entity State PDU	UDP Multicast	225.10.27.72	3000	Gr
DIS	Entity State PDU	UDP Multicast	225.10.27.72	3000	DIS	Entity PDU				
DIS	Entity State PDU	UDP Multicast	225.10.27.72	3000	DIS	Entity PDU				
DIS	Entity State PDU	UDP Multicast	225.10.27.72	3000	DIS	Entity PDU				
DIS	Entity State PDU	UDP Multicast	225.10.27.73	3000	DIS	Entity PDU				
DIS	Entity State PDU	UDP Multicast	225.10.27.73	3000	DIS	Entity PDU				
DIS	Fire PDU	UDP Multicast	225.10.27.74	3000	DIS	Fire P				
30111-C	J 3.0	UDP Multicast	225.10.2.2	3100	30111-C	J 3.0				
30111-C	J 3.2	UDP Multicast	225.10.2.2	3100	30111-C	J 3.2				
3011-C	J 2.0	UDP Multicast	225.10.2.2	3100	3011-C	J 2.0	UDP Multicast	225.10.2.2	3100	In
ASTERIX	CAT 21	UDP Multicast	225.10.2.3	TBD	ASTERIX	CAT 21	UDP Multicast	225.10.2.3	TBD	Airc
ASTERIX	CAT 21	UDP Multicast	225.10.2.3	TBD	ASTERIX	CAT 21	UDP Multicast	225.10.2.3	TBD	Airc
VMF	K05.1	UDP Multicast	TBD	TBD	VMF	K05.1	UDP Multicast	TBD	TBD	En
ASTERIX	CAT 1/2	UDP Multicast	TBD	TBD	ASTERIX	CAT 1/2	UDP Multicast	TBD	TBD	Airc

- There may be a “middle-man” between the sending and receiving applications
- Therefore the address the message is sent to may not be the one the target application receives it on
- The most common example of this is distributed simulation gateways, but is also used for some tactical systems as well

All addresses are notional

Interface Matrix Detail

Develop System Interface Model

6.1

Description of the message

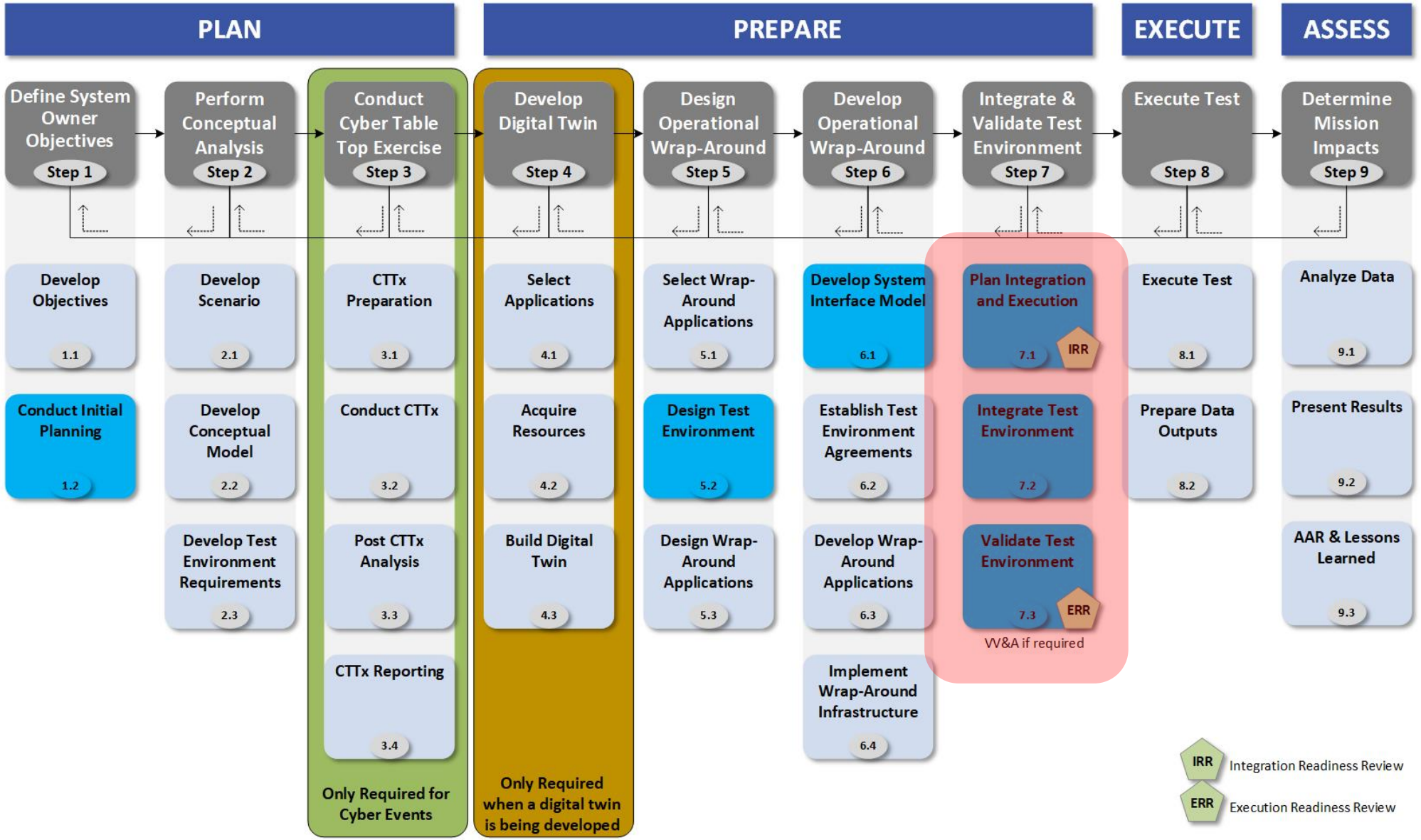
The specific purpose of the message for the event, the same message may have different purposes based on the source/target pair

t	Description	Event Purpose	Update Condition	Tested
	Ground Truth Entity state	Position of UAS	DIS Dead Reckoning	
	Ground Truth Entity state	Position of ground entitles and RWA	DIS Dead Reckoning	
	Ground Truth Entity state	Position of RWAs	DIS Dead Reckoning	
	Ground Truth Entity state	Position of FWA. TELs, and TBMs	DIS Dead Reckoning	
	Ground Truth Entity state	Position of FWA. TELs, and TBMs	DIS Dead Reckoning	
	Ground Truth Entity state	Position of Blue FWA	DIS Dead Reckoning	
	Ground Truth Entity state	Position TELs	DIS Dead Reckoning	
	Weapon fire	Represent TBM fire	Launch	
	Surveillance - Referance Point	TBM Laucnh point	N/A	
	Surveillance - Air Track	Air track from radar	N/A	
	PPLI - Indirect	Forwarded postion		

Used to indicate that the receipt of the message by the target has been confirmed

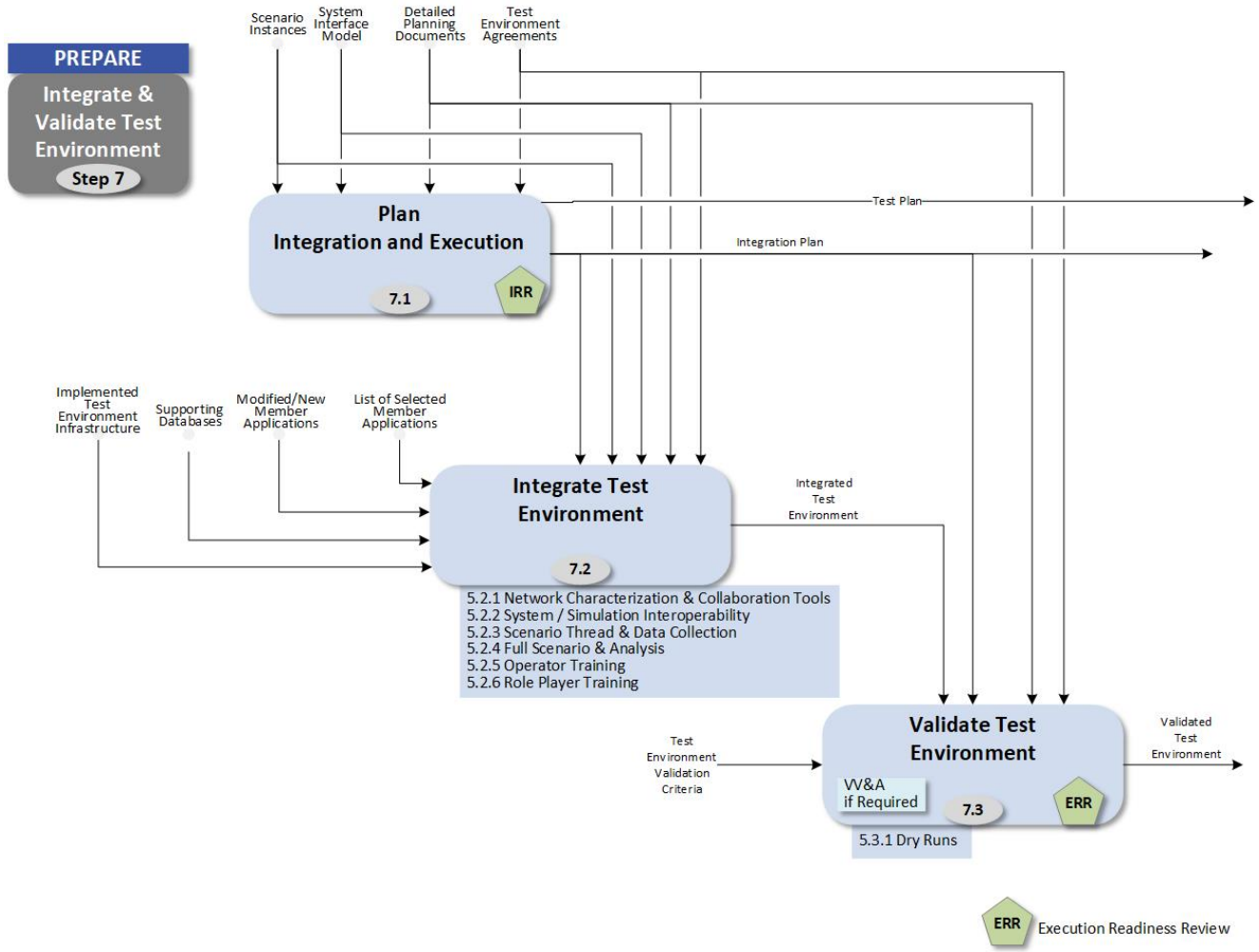
Update condition may be trigger based or rate based

Activities 7.1, 7.2, & 7.3



Integration Planning and Execution

- Step 7 Plans the integration of the distributed LVC environment
- A key part of the integration is the execution of the 7 integration blocks
- The plan is created in activity 7.1
- Blocks 1 through 6 are performed in activity 7.2
- Block 7 is performed in activity 7.3



Integration Planning

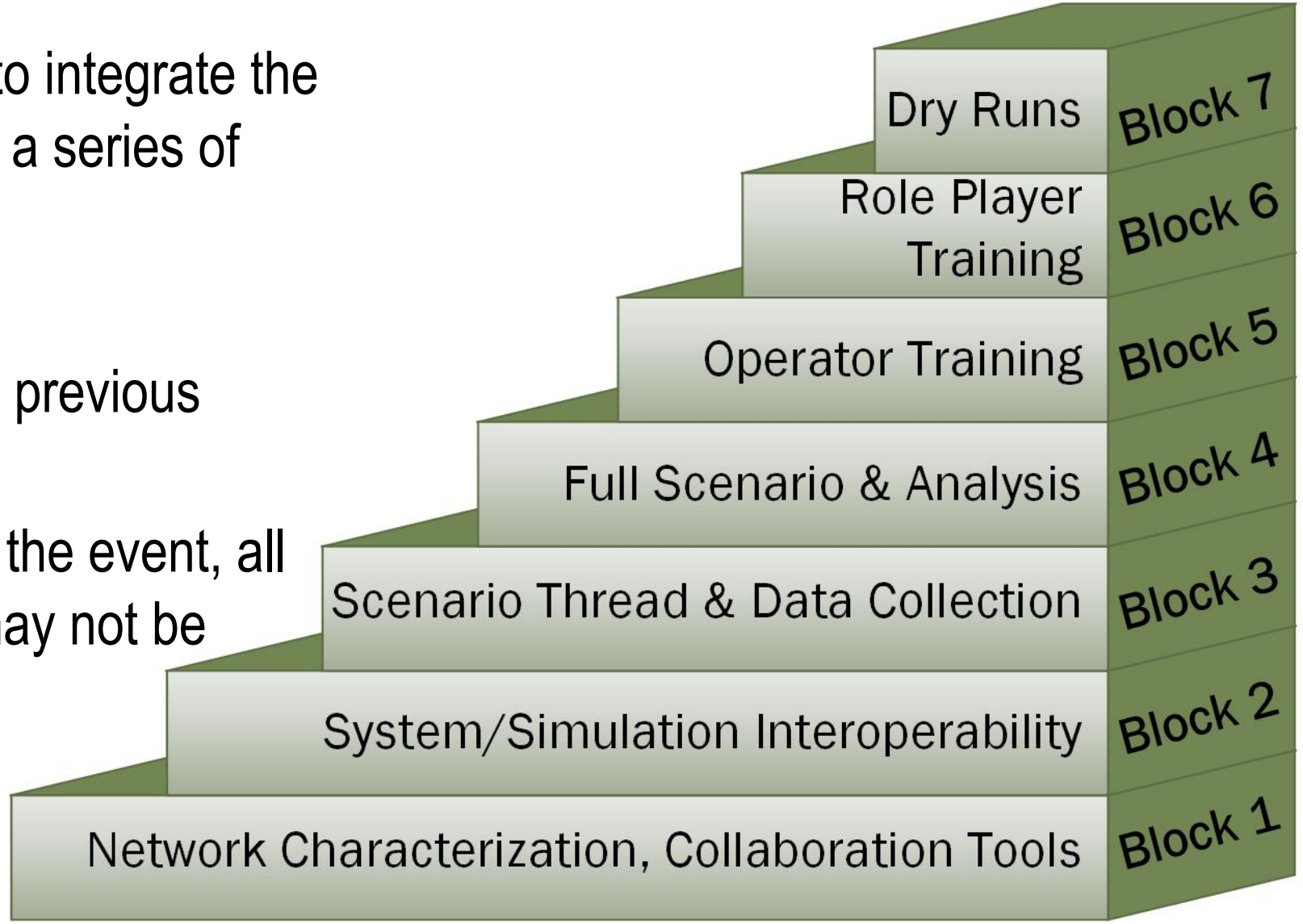
Plan Integration and Execution

7.1

- Integration Plan
- Integration Blocks
  - Set of activity blocks to integrate a distributed simulation system
- Integration Planning
  - Mapping activity blocks to integration spirals
  - Scheduling integration spirals
  - Integration Plan development
- Spiral Planning
  - Expanding Integration Plan
  - Developing detailed integration spiral plan

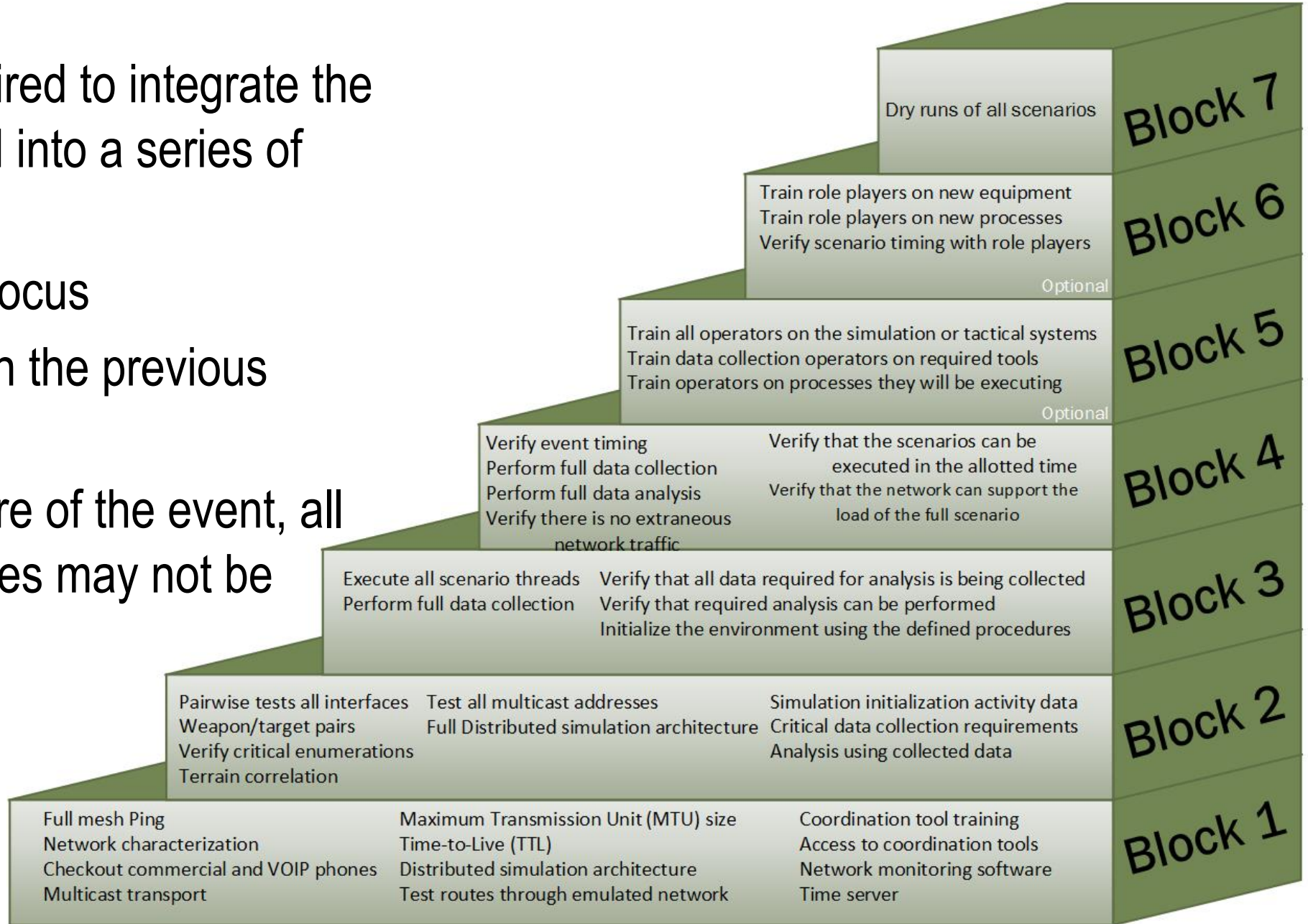
Integration Activity Blocks

- The activities required to integrate the system are divided into a series of seven blocks
- Each block has a focus
- The block builds on the previous blocks
- Based on the nature of the event, all of the block activities may not be required



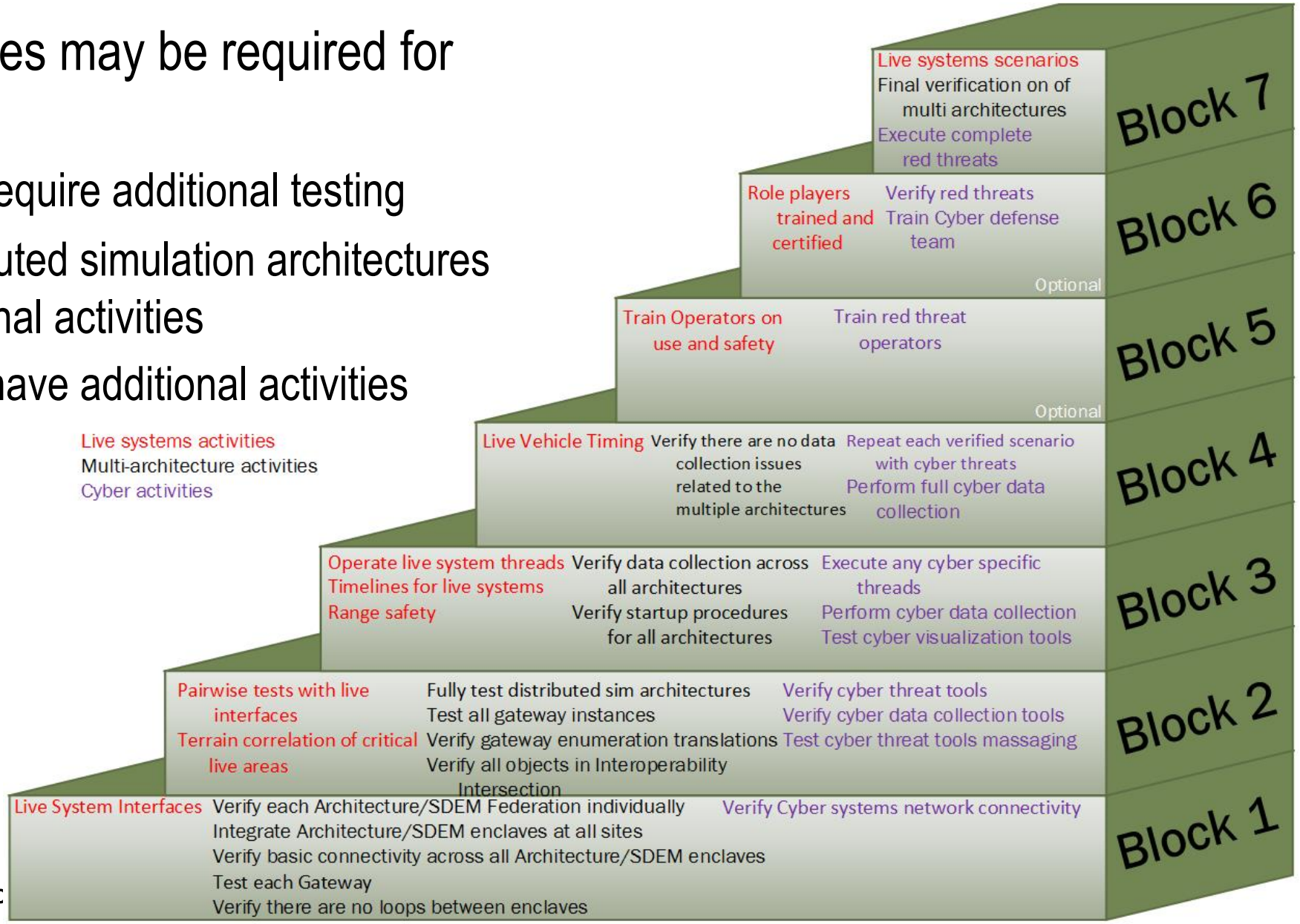
Integration Activity Blocks

- The activities required to integrate the system are divided into a series of seven blocks
- Each block has a focus
- The block builds on the previous blocks
- Based on the nature of the event, all of the block activities may not be required



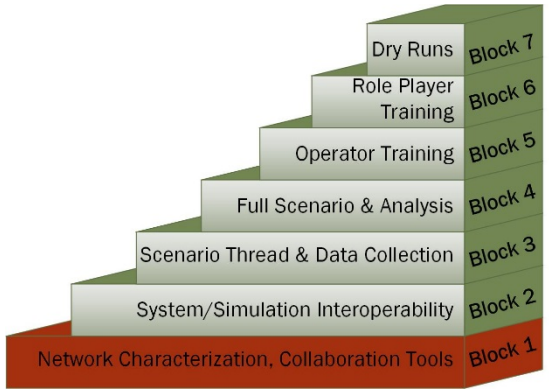
Integration Activity Blocks – Cyber, Live, & Multi Architecture

- Additional activities may be required for some events
  - Live systems require additional testing
  - Multiple distributed simulation architectures require additional activities
  - Cyber events have additional activities



Block 1: Network Characterization, Collaboration Tools

- Block 1 activities focuses on establishing:
  - the network
  - infrastructure tools
- The minimum entrance requirements for this block are:
  - all sites on the network
  - infrastructure tools installed



Block 1 Activities: Network Characterization, Collaboration Tools

General

- Ping all sites from all other sites to verify full mesh connectivity
- Perform full mesh network characterization to determine network latencies, jitter, and bandwidth
- Checkout voice coordination lines, commercial and VOIP as required
- If multicast transport is required, verify at least one multicast address is working to make sure the rendezvous point is correctly configured
- Determine the correct Maximum Transmission Unit (MTU) size for the network, and make sure all computers have correctly set the MTU
  - MTU size is critical when tunnels or encryptors are used
- Verify systems have Time-to-Live (TTL) set based on network configuration

Block 1 Activities: Network Characterization, Collaboration Tools

General

- Check out connectivity using the selected distributed simulation architecture(s)
- Verify all sites have access to coordination/collaboration tools
- Provide training for coordination tools including chat, file share, Time Ordered Event List (TOEL) server, visualization, and VTC
- Implement and test network monitoring system
- Verify all sites have access to a time server (need to determine if a single or multiple time servers will be used)
- If emulated networks are being used – verify routes through the emulated network

Live

- Test connectivity to software and systems used to convert live data to simulation

Block 1 Activities: Network Characterization, Collaboration Tools

Multi-Architecture

- Verify each Architecture/SDEM Federation individually that is used for the test
- Integrate Architecture/SDEM enclaves at all sites
- Verify basic connectivity across all Architecture/SDEM enclaves
- Test an instance of each Gateway
- Verify there are no loops between enclaves

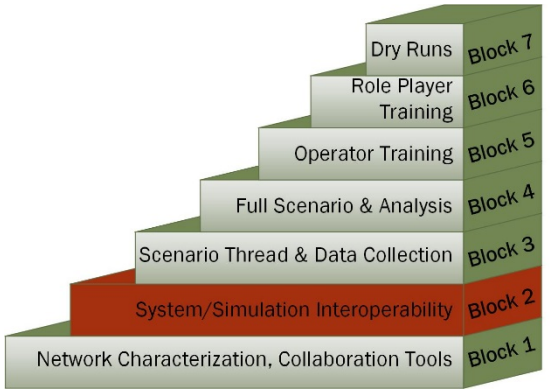
Cyber

- Verify Cyber systems network connectivity

SDEM: Simulation Data Exchange Model

Block 2: System/Simulation Interoperability

- Block 2 Activities are focused on data interchanges between systems
- The minimum entrance requirement for this block is an interface matrix showing all data exchanged between systems
- It may be necessary to develop temporary data files, configurations, or stimulations to test pair-wise messaging between simulations/systems



Block 2 Activities System/Simulation Interoperability

General

- Perform pairwise tests of all defined interfaces
- Verify that all weapon/target pairs work as expected
- Verify that critical enumerations are processed correctly
- Perform terrain correlation to the level required for the event
- Test all multicast addresses required for the event
- Fully test distributed simulation architecture
- Collect data for simulation initialization activities
- Check critical data collection requirements
- Perform limited analysis using collected data

Block 2 Activities: System/Simulation Interoperability

Live

- Perform pairwise tests with live interface systems using surrogates if the live systems are not available
- Verify terrain correlation with live systems in critical areas

Multi-Architecture

- Fully test distributed sim architectures across all sites
- Test all gateway instances
- Verify gateway enumeration translations
- Verify all objects in Interoperability Intersection

Block 2 Activities: System/Simulation Interoperability

Cyber

- Verify cyber threat tools
- Verify cyber data collection tools
- If cyber threat tools send messages to other systems, include the cyber tools in pair-wise testing

Scenario Testing Concept

- Avoid the “Big-Bang” approach where the scenario is run full up the first time
- Review the scenario to look for:
  - Activities that are repeated multiple times
  - Critical activities that are key to the scenario
  - Activities that have not been performed before
  - Very complex activities
  - Activities that involve a large number of participants
- Document the message flows and actions required for each of the identified threads
- GOAL: eliminate issues at a small scale before attempting the full scenario

Definitions

- Scenario: The scenario is the overall set of simulation and tactical activities required to create an operationally relevant LVC environment
  - Contains multiple similar activities that occur simultaneously
  - Contains multiple different activities that occur simultaneously
  - Involves all participants in the event
  - Is long in duration
  - Includes initial conditions for all entities (i.e. starting location, fuel state, etc.)
- Thread: A thread is a single chain of events that include simulation and tactical activities that are a part of an operationally relevant LVC environment
  - Is a single activity
  - Involves a subset of participants in the event
  - Is short in duration
  - Includes the conditions for the entities involved in the thread at start of the thread

Block 3: Scenario Thread & Data Collection

- Block 3 Activities are focused on testing scenario threads
- The minimum entrance requirement is having all scenarios defined
- A set of configuration files may have to be developed in advance to allow the threads to be executed
- Issues found in thread testing include
  - Timing issues: The activities can not be performed in the time specified
  - Message issues: The simulations or tactical systems do not generated the expected output from the inputs
  - Capability issues: The simulations or tactical systems can not or do not perform the activities
- Resolution of issues may require:
  - Changes to the simulations
  - Change in tactics
  - Modification of the scenario

Block 3 Activities: Scenario Thread & Data Collection

General

- Execute all scenario threads and verify correct execution
- Perform full data collection for each thread
- Verify that all data required for analysis is being collected for each thread
- Verify that required analysis can be performed
- Initialize the environment using the defined procedures

Live

- Operate live systems as part of threads
- Determine timelines to get live vehicles on station
- Ensure threads do not violate range safety constraints

Block 3 Activities: Scenario Thread & Data Collection

Multi-Architecture

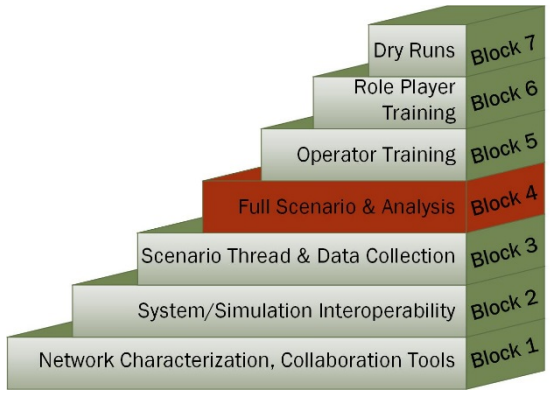
- Verify data collection across multiple architectures
- Verify startup procedures are correct for the multi-architectures

Cyber

- Execute cyber specific threads
- Perform cyber data collection
- Test cyber visualization tools

Block 4: Full Scenario & Analysis

- Block 4 Activities are focused on executing full scenarios
- The minimum entrance requirement is that all scenario threads have been verified



Block 4 Activities: Full Scenario & Analysis

General

- Execute each scenario to verify event timing
- Perform full data collection for each scenario
- Perform full data analysis for each scenario
- Verify that the required number of scenarios can be executed in the allotted time
- Verify that the network can support the load of the full scenario
- Verify there is no extraneous network traffic

Live

- Verify timing of live vehicles as part of the scenario

Block 4 Activities: Full Scenario & Analysis

Multi-Architecture

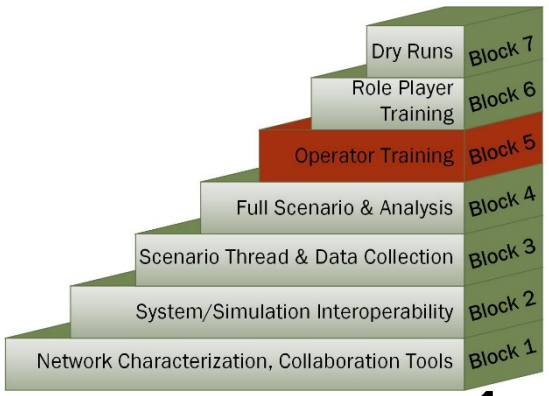
- Verify there are no data collection issues across the multiple architectures

Cyber

- Repeat each verified scenario with cyber threats
- Perform full cyber data collection
- Perform full cyber analysis for each scenario

Block 5: Operator Training

- Block 5 activities are focused on training simulation operators on the systems and tools required for the event
- Depending on the requirements for the event, this set of activities may have been met in the performance of the previous activities



Block 5 Activities: Operator Training

General

- Train all operators on the simulation or tactical system they will be using
- Train data collection operators on required tools including digital and manual collection
- Train operators on processes they will be executing

Live

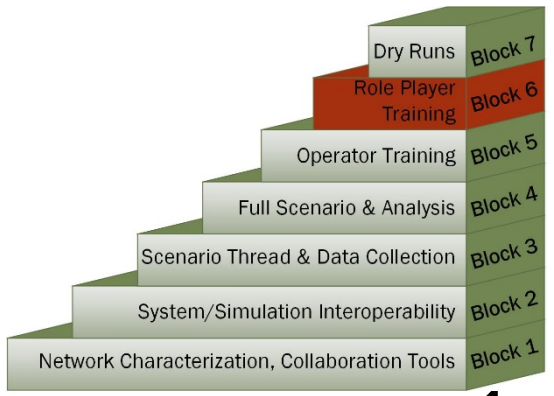
- Train all operators on the use and safety requirements of live systems

Cyber

- Train red threat operators

Block 6: Role Player Training

- Block 6 activities are focused on training role players that will be used during the event
- If role players are not being used in the event this block of activities can be omitted
- This set of activities is required if the equipment being used is new to the role players or the processes being used are different than the ones the role players normally use
- Cyber threat introduction if applicable to the event



Block 6 Activities: Role Player Training

General

- Train role players on new equipment
- Train role players on new processes
- Verify scenario timing with role players
- Verify cyber threats can be performed

Live

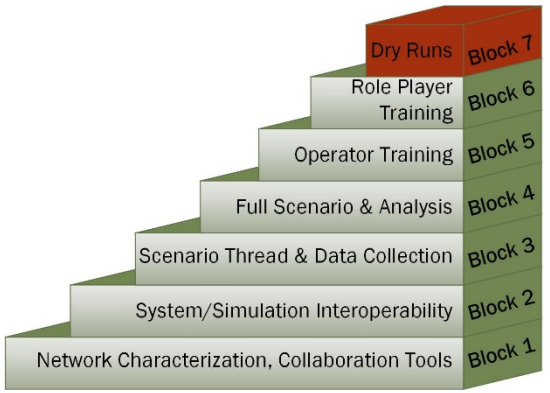
- Verify roles players are properly trained and certified to operate the live systems

Cyber

- Verify red threats
- Cyber defense team training

Block 7: Dry Runs

- Block 7 activities are Focused on conducting dry-runs of scenarios to be executed during the event
- This set of activities is required when data collection, test, or training requirements are dependent on an exact scenario execution



Block 7 Activities: Dry Runs

General

- Run each scenario with full data collection and role players

Live

- For each of the scenarios, conduct at least one dry run with all live systems

Multi-Architecture

- Final verification of distributed simulation architectures used in the event

Cyber

- Execute complete red threats

Integration Planning - Spiral Scheduling

Plan Integration and Execution

7.1

- The number, duration, and schedule of the integration spirals is dependent on the nature of the event and the participating sites
- In general a spiral lasts one week
- A nominal schedule for a medium sized event is three integration spirals over three months with the following assumptions:
  - Medium sized event with experienced sites
  - Neither dedicated operator nor role play training is required
  - The number and complexity of the scenarios is such that Block 3 and 4 activities can be performed in a single spiral
  - Dry runs can be performed if required

Nominal Spiral Schedule

Plan Integration and Execution

7.1

Spiral	Activities	Week
Spiral 1	Block 1	Week 1
Spiral 2	Block 2	Week 4
Spiral 3	Block 3 & Block 4	Week 7
Spiral 4 (optional)	Block 7	Week 10
Execution		Week 11 (week 10 if dry runs are not required)

Scheduling Considerations

Plan Integration and Execution

7.1

- One key issue that is not always understood is that the time between the spirals is as important as the spiral
- If spirals are performed too close together there will not be time to address issues that arise in a previous spiral or prepare for the next spiral
- In general at least two weeks should be planned between integration spirals
- The exception would be spirals for Block 5 and 6 activities that can be performed back-to-back
- The amount of time between spirals is also dependent on the confidence level that the activities can be performed in the time scheduled for the spiral

Add-in Spirals

Plan Integration and Execution

7.1

- The status of all objectives is tracked during each spiral
- If a few objectives are not met they can be pushed to the next spiral
- If a large number of objectives are not met, another spiral may be required
- It would be difficult to schedule an additional spiral if there are only two weeks separating planned spirals
- If the complexity of the event is such, scheduling more than two weeks between spirals allows make-up spirals to be added

Block 1 Planning Considerations

Plan Integration and Execution

7.1

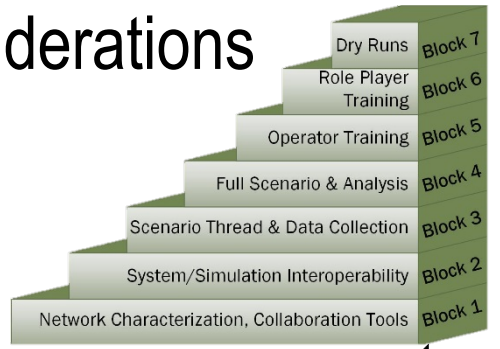
- In general Block 1 activities can be performed in a single integration spiral
- An event with a very large number of participants or an event with a large number of inexperienced participants could require more than one spiral to complete Block 1 activities
- Another option is to schedule a single two-week spiral

Block 2 Planning Considerations

Plan Integration and Execution

7.1

- Block 2 activities can generally be performed in a single spiral
- If there are a large number pairwise interfaces, hardware-in-the-loop (WHIL) systems, or live elements, more than one spiral may be required to complete all of the Block 2 activities
- If more than one spiral is required to complete Block 2 activities the systems and sites should be grouped by common interfaces
- If more than one spiral is required to complete Block 2 activities, these may be scheduled with only one week in between
- HWIL systems and live systems often require special scheduling considerations

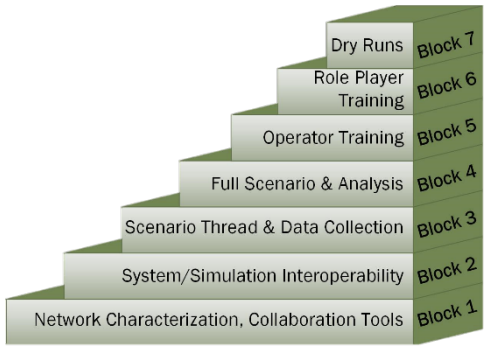


Block 3 & 4 Planning Considerations

Plan Integration and Execution

7.1

- For medium sized events Block 3 and 4 activities can generally be combined into a single spiral
- If there are a large number of threads, Block 3 and 4 activities may have to be assigned to separate spirals
- A large number of scenarios may also require scheduling separate spirals for Block 3 and 4 activities
- The duration of the scenarios is also a factor

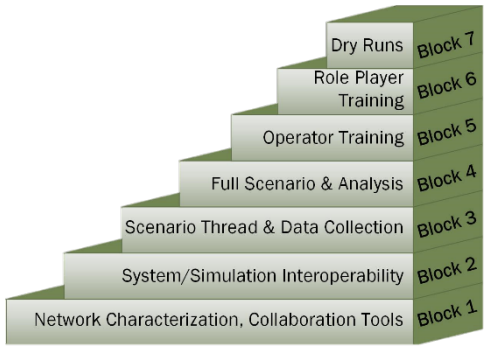


Block 5 & 6 Considerations

Plan Integration and Execution

7.1

- Block 5 and 6 activities are only performed if they are required
- Depending on the level of training required, a single spiral may be used perform both activities
- If Block 5 and 6 activities are performed in a single spiral, the week should be divided so the operator training is performed in the first half of the week and the role player training in the second half of the week
- Depending on the source of the role players, scheduling them is generally a long lead time item
  - Planning is required to make sure that role player time is used wisely

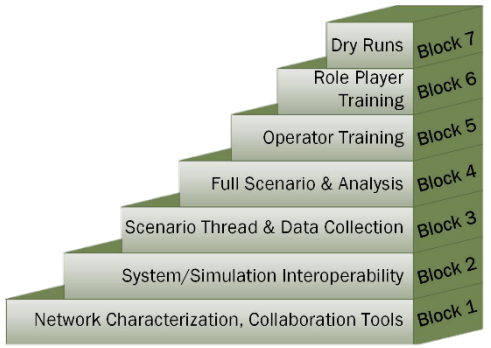


Block 7 Considerations

Plan Integration and Execution

7.1

- The amount of time required for Block 7 activities depends on the number of scenarios, the length of each scenario, and the number of iterations required
- If completing the block 7 activities requires more than one week, the spiral should be scheduled for consecutive weeks
- Block 7 activities and the event execution can be performed in consecutive weeks



Integration Plan Development

Plan Integration and Execution

7.1

- An Integration Plan is created to communicate with the full team the objectives, schedule, and mechanisms for the integration
- This document is developed and published prior to the start of integration
- In general this document is not updated after the Test Readiness Review
- Changes after that are described in the individual Spiral Plans
- The format of this document can vary, but there are several sections that should be included

Integration Plan Sections

Plan Integration and Execution

7.1

- Introduction: General information, overall schedule
- Communication Plan: Phone numbers, data stores
- Distributed Simulation: Architectures/Simulation Data Exchange Models (SDEMs), network configurations
- Scenario/Operational: Terrain databases, scenarios, systems under test
- Spiral Overview: Dates, objectives, participating sites, entrance & exit criteria
- Documentation Plans: Spiral plans, spiral reports, problem reports

Example Objectives

Plan Integration and Execution

7.1

ID	Objective
1	Establish network connectivity between DTCC and JOIN Lab
2	Characterize network performance over several days and times of day
3	RTC users log-in to Confluence using accounts on Active Directory
4	JOIN Lab users log-in to Confluence using accounts on Active Directory
5	Have a TENA application (Canary) join TENA EM at DTCC
6	Pass TENA platform data from DTCC to SIMDIS located at JOIN Lab
7	Test VOIP call manager

Example Entrance Criteria

Plan Integration and Execution

7.1

Site	Entrance Criteria
All	Verify site is available to participate in spiral
All	ISA signed and approved
All	User accounts created for at least one person at each NLT Friday 13 November 2015
Org1	JMN in place
NOC	JMN in place
DTCC	JMN in place
NOC	Verify all CSTB PoC Sites connected on JMN
Org1	Network check (ping test)
Org2	Network check (ping test)
NOC	Establish multicast Rendezvous Point (RP)
DTCC	Distribute VoSIP phone information to all sites
NOC	VoSIP call manager operational
NOC	Chat server operational
DTCC	Confluence site created
DTCC	Adobe site created
All	Download network characterization tools from Confluence
Org1	Have Linux computer on the network for network characterization tool
Org2	Have Linux computer on the network for network characterization tool
NOC	Have Linux computer on the network for network characterization tool
DTCC	Have Linux computer on the network for network characterization tool
All	IP addresses for local machines NLT Friday 13 November 2015
DTCC	Configure collaboration tools to use event LDAP

Exit Criteria Example

Site	Exit Criteria
Org1	All user accounts for the distributed sites have been verified
All	Network performance is sufficient for event requirements
All	VoSIP, chat, and Confluence between participating sites verified
All	Verified All sites connected to JMN
DTCC	Verified multicast group functionality
DTCC	Verified network monitoring approach
All	Infrastructure training complete: Confluence, Adobe Connect, Chat, and EventMan

Detailed Spiral Planning

Plan Integration and Execution

7.1

- A Spiral Plan is created for each integration spiral
  - The initial input for the plan is drawn from the Integration Plan
  - The list of objectives, entrance criteria, and exit criteria may be extended and refined from what is listed in the Integration Plan
- Any unmet exit criteria or other issues from the previous spiral are also input to the Spiral Plan
  - If a large number of objectives were not met in the previous spiral, the addition of interim spirals may be required
- The Spiral Plan is based on a template that can be modified to meet the needs of a specific program

Spiral Plan Content

Plan Integration and Execution

7.1

- Overview of the spiral
- List of participating sites
- Communication Plan: primary and backup phone lines
- Objectives
- Terrain databases
- Entrance Criteria
- Exit Criteria
- Detailed schedule of the spiral

Detailed Schedule Example

Plan Integration and Execution

7.1

Tuesday February 4

9:00 AM	Coordination teleconference
9:30 AM	Conduct network testing
10:00 AM	Verify Confluence/Active Directory interface
11:00 AM	Lunch
12:00 PM	Conduct network testing
1:00 PM	Have TENA Canary at JOIN connect to TENA EM at RTC
3:00 PM	Daily hotwash

Wednesday February 5

9:00 AM	Coordination teleconference
9:30 AM	Conduct network testing
10:00 AM	Publish TENA Platforms at RTC view on SIMDIS at JOIN
11:00 AM	Lunch
12:00 PM	Conduct network testing
1:00 PM	Setup and Test VOIP phones
3:00 PM	Daily hotwash

Wrap-Up

- A successful distributed LVC event depends on the completeness of the environment created
- A well-defined process provides the structure for a valid environment by ensuring that all required products and procedures are followed.
- DSEEP provides a good process model for distributed simulation event integration
- Todays tutorial focused on defining Integration Blocks and the planning process for them
  - Not completing all the preceding blocks adds risk to the following blocks

Integration Blocks Summary

Blocks	Block Name	All Events	Live Event	Multi-Architecture Events	Cyber Events
Block 1	Network Characterization, Collaboration Tools	• Full Mesh Ping • Network Characterization • Phone Checkout • Multicast transport • Maximum Transmission Unit size • Time-to-Live • Distributed Simulation Architecture • Coordination tool Training • Access to coordination tools • Network Monitoring Software • Time Server • Test routes through emulated network	• Live system Interfaces	• Verify each Architecture/SDEM Federation individually • Integrate Architecture/SDEM enclaves at all sites • Verify basic connectivity across all Architecture/SDEM enclaves • Test each Gateway • Verify there are no loops between enclaves	• Verify Cyber systems network connectivity •
Block 2	System/Simulation Interoperability	• Pairwise test all interfaces • Weapon/target Pairs • Verify Critical Enumerations • Terrain Correlation • Test all multicast addresses • Full distributed Simulation Architecture • Simulation initialization activity data • Critical data collection requirements • Limited analysis using collected data	• Pairwise tests with live interfaces • Terrain correlation of critical live areas	• Fully test distributed sim architectures • Test all gateway instances • Verify gateway enumeration translations • Verify all objects in Interoperability Intersection	• Verify cyber threat tools • Verify cyber data collection tools • Test cyber threat tool messaging
Block 3	Scenario Thread & Data Collection	• Execute all scenario threads • Perform full data collection • Verify that all data required for any analysis is being collected • Verify that required analysis can be performed • Initialize the environment using the defined procedures	• Operate live system threads • Timelines for live systems • Range safety	• Verify data collection across all architectures • Verify startup procedures for all architectures	• Execute any cyber specific threads • Perform cyber data collection • Test cyber visualization tools
Block 4	Full Scenario & Analysis	• Execute each scenario to verify event timing • Perform full data collection for each scenario • Perform full data analysis for each scenario • Verify that the scenarios can be executed in the allotted time • Verify that the network can support the load of the full scenario • Verify there is no extraneous network traffic	• Live Vehicle Timing	• Verify there are no data collection issues related to the multiple architectures	• Repeat each verified scenario with cyber threats • Perform full cyber data collection
Block 5	Operator Training	• Train all operators on the simulation or tactical systems • Train data collection operators on required tools • Train operators on processes they will be executing	• Train Operators on use and safety	•	• Train red threat operators
Block 6	Role Player Training	• Train role players on new equipment • Train role players on new processes • Verify scenario timing with role players	• Role players trained and certified	•	• Verify red threats • Train Cyber defense team
Block 7	Dry Runs	• Dry runs of all scenarios	• Live systems scenarios	• Final verification on of multi architectures	• Execute complete red threats

Learning Objectives

- You should now be able to:
  - List the activities required to perform integration and execution of a distributed simulation event
  - Describe an event in the terms required to plan the integration
  - Select the integration activities required for an event
  - Develop an outline for an integration plan for a distributed simulation event
  - Describe the key roles in a distributed event integration and execution

Distributed Event Integration and Execution

Michael J. O'Connor, Trideum Corporation
Dr. Kenneth G. LeSueur, Redstone Test Center

Questions?