CONCEPTS GUIDE

SL 4E

USAREUR-AF

CONCEPTS GUIDE — SL 4E — MAVEN SMART SYSTEM (MSS): PROTECTION WARFIGHTING FUNCTION · CONCEPTUAL COMPANION FOR SENIOR LEADERS AND STAFF

Specialist Course Manual

HEADQUARTERS
UNITED STATES ARMY EUROPE AND AFRICA
(USAREUR-AF)
Wiesbaden, Germany

26 MARCH 2026

DRAFT — UNOFFICIAL — NOT FOR OPERATIONAL USE

CONCEPTS GUIDE — SL 4E — MAVEN SMART SYSTEM (MSS): PROTECTION WARFIGHTING FUNCTION · CONCEPTUAL COMPANION FOR SENIOR LEADERS AND STAFF

Prereqs: SL 1 (Maven User), SL 2 (Builder), and SL 3 (Advanced Builder) — all required as prerequisites (Go evaluations on file) before beginning SL 4E. Read this Concepts Guide after completing SL 3 and before beginning SL 4E task instruction. Builder skills are not exercised in this track — protection WFF practitioners operate pre-built products. *HQ USAREUR-AF · v1.0 · 2026 · DISTRIB: USG only*

FOREWORD

Protection is not a staff function — it is a command responsibility. Commanders preserve their forces and their freedom of action. Staffs provide the data, analysis, and coordination that enables commanders to execute that responsibility with knowledge rather than intuition.

In USAREUR-AF, the Maven Smart System provides the data integration platform that can connect the protection WFF's multiple functional cells — CBRN, AT, PMO, AMD, engineer, legal — into a single, visible protection picture. Whether that picture is useful depends entirely on the discipline of the practitioners who maintain it.

This guide explains the conceptual foundations that make that discipline worth pursuing. Read it with a focus on why the protection WFF needs integrated data — not what buttons to push in MSS. SL 4E covers the buttons. This guide covers the thinking behind them.

PURPOSE

This guide explains the conceptual foundations of protection WFF data management in MSS. It does not teach procedures — SL 4E covers those. It explains the why: why protection data management matters, how doctrine aligns to data practice, and where protection leaders most commonly fail in the MSS environment. Read this guide before beginning SL 4E. Return to it when protection data problems arise.

SECTION 1 — THE PROTECTION WFF AND DATA: DOCTRINE TRANSLATED TO DATA REQUIREMENTS

1-1. What ADP 3-37 Actually Requires from a Data Perspective

ADP 3-37 defines protection as the preservation of the force and its freedom of action. That single sentence contains a substantial data requirement. "Preservation" requires knowing the current state of the force — what threats exist, what vulnerabilities exist, what protective measures are in place, and whether those measures are working. "Freedom of action" requires knowing which threats, if not countered, would deny the commander options.

None of that knowledge is possible without data. Specifically, it requires data that is current, integrated across protection functions, accessible to decision-makers, and accurate enough to act on. Before MSS, protection practitioners in USAREUR-AF collected this data through separate, disconnected channels. CBRN threats were tracked by the CBRN cell using their own systems. AT assessments lived in local files that rarely synchronized with the threat picture the S2 was maintaining. MP incident data stayed in the PMO blotter. AMD warning data traveled by voice.

The result was a protection picture that was, at best, a staff officer's mental synthesis of information from multiple sources — not a shared, integrated picture that multiple leaders could see simultaneously. ADP 3-37 assumes integrated protection. Legacy data practices made integration structurally difficult. MSS is the platform change that makes integration operationally achievable.

1-2. Protection Tasks and Their Data Dependencies

Each of the twelve protection tasks in ADP 3-37 has a specific data dependency — information that must exist, be current, and be accessible for the task to be executed effectively.

The protection officer's job is not just to manage protection tasks. It is to ensure the data infrastructure that supports those tasks is sound. A CBRN contamination overlay that is 12 hours old during a dynamic CBRN event is not "CBRN defense" — it is navigating blind. A CAL/DAL that was last reviewed two months ago does not reflect the current mission. An FPCON level that has changed at the theater level but has not propagated to the unit's MSS workspace means subordinate elements are executing the wrong protective measures.

Data currency is a protection requirement. It should be treated with the same rigor that units apply to ammunition accountability, vehicle maintenance, or communications security.

1-2a. The Five Questions of the Integrated Protection Picture

Before the protection WFF can integrate data in MSS, practitioners must understand what an integrated protection picture is supposed to answer. ADP 3-37 does not define a specific set of products. But doctrinal logic produces five questions that the protection picture must be able to answer at all times:

Question 1: What threats are active in the AOR, and what is their assessed capability and intent? This is primarily an AT and S2 question. The threat picture drives FPCON, RAM, and AT countermeasure selection. Without current, specific threat data, the protection program is generic — applying the same measures to all environments regardless of actual threat context.

Question 2: What is the CBRN risk, and where are the hazards? This is the CBRN officer's domain. It requires current contamination overlays, detection coverage data, and decontamination capability status. In a CBRN-free environment, this question is answered quickly with "no active threat." In a contaminated environment, it requires real-time data.

Question 3: What is the physical security posture — are access points controlled, and is the perimeter sound? This is the PMO's domain. ECP status, perimeter integrity, and incident history collectively answer this question. A perimeter with a gap, an ECP with degraded access control, or a pattern of probing incidents changes the protection posture even if no breach has occurred.

Question 4: What AMD coverage exists, and what critical assets are not defended? This is the ADA officer's domain. The CAL/DAL status, AMD system readiness, and ADW level collectively answer this question. The protection officer needs to know not just what is on the DAL, but what is explicitly NOT on the DAL and why.

Question 5: Are there any uncontrolled risks that the commander needs to know about? This catches everything the other four questions miss — High-residual-risk CRM assessments, survivability deficiencies at critical facilities, AT incidents under investigation, recurring physical security failures. This question requires the protection officer to synthesize across all data domains, not just report each cell's status in isolation.

An MSS protection workspace that consistently answers all five questions with current, accurate data is a protection data program that is working. One that answers some and leaves others vague is a protection data program that is partially working — and the vague answers are the risk the commander is not seeing.

1-3. The Protection Working Group as a Data Synchronization Event

The PWG is, doctrinally, the forum where protection tasks are synchronized across WFFs. In practice, it is also the primary data quality event for the unit's protection picture. Every PWG should answer four data questions before addressing any operational agenda item:

1. Is the CBRN overlay current? When was it last updated, and what is the source?

2. Is the FPCON current and reflected accurately in MSS? When was it last changed, and who directed the change?
3. Are open AT incidents and SIRs current in MSS, or are there entries that have not been updated?
4. Is the survivability picture current, or have position status changes not been entered?

If the answer to any of these questions is "no" or "unknown," the PWG has a data quality problem before it has a protection problem. Fixing the data problem is the prerequisite to doing useful protection analysis.

BLUF: The PWG is where protection data quality is either enforced or neglected. A protection officer who accepts stale, incomplete, or unattributed data at the PWG is not running a protection program — they are running a theater.

SECTION 2 — RISK MANAGEMENT AS A DATA DISCIPLINE

2-0. The FM 5-19 Process as a Data Pipeline

Before examining risk management as a data discipline, it is useful to understand how FM 5-19's five-step CRM process maps to a data pipeline. Each step generates specific data, and the failure of any step degrades the quality of everything downstream.

Step 1 — Identify Hazards: Produces a hazard list. Data quality failures here: hazards are generic, incomplete, or not mission-specific. The downstream consequence is that all controls, risk scores, and acceptances are built on a flawed foundation.

Step 2 — Assess Hazards: Produces a risk score for each hazard. Data quality failures here: probability and severity scores are assigned without analysis, defaulting to low scores to speed approval. The downstream consequence is artificially low residual risk that does not reflect reality.

Step 3 — Develop Controls: Produces a control list. Data quality failures here: controls are generic ("drive carefully"), unverifiable, or unassigned. The downstream consequence is that residual risk scores are meaningless because the controls reducing risk cannot actually be verified.

Step 4 — Implement Controls: Produces execution. This step generates no MSS data unless the verification step is explicitly linked. The failure here is the most common — controls are entered in MSS but never actually implemented. MSS has no way to know.

Step 5 — Supervise and Evaluate: Produces verification data and lessons learned. Data quality failures here: controls are marked "verified" without actual verification, or lessons learned are never captured. The downstream consequence is that the formation cannot learn from its CRM experience.

The protection officer and safety officer who understand CRM as a data pipeline can identify where each unit's CRM program is failing and address it at the specific step — rather than demanding more paperwork or stricter compliance with a process that is already producing compliance-grade output

without safety-grade results.

2-1. CRM Is a Data Quality Problem in Disguise

FM 5-19 presents CRM as a five-step analytical process. In execution, CRM frequently becomes a compliance exercise: leaders fill out the form, the form gets signed, and the risk controls are not enforced or verified. MSS does not solve this problem by itself. But MSS makes the problem visible in a way that paper-based CRM systems cannot.

When CRM data lives in MSS and is aggregated across the formation, two things become apparent that were previously invisible:

First, the gap between "controls entered" and "controls verified" becomes measurable. If a unit consistently enters control measures but marks them as "not verified" after execution, that is a data signal that CRM is being done on paper but not in practice. Before MSS, this was impossible to see at any level above the individual leader. On MSS, it is visible to the battalion safety officer, the brigade safety officer, and the commander.

Second, recurring hazards become identifiable. If the same hazard — vehicle rollover on a specific route, heat injury risk during certain training tasks, electrical hazard at a specific facility — appears across multiple risk assessments over multiple months, the data reveals a systemic problem that was previously masked by the episodic nature of paper-based CRM. MSS makes the pattern visible so that commanders can address root causes rather than reacting to individual incidents.

2-2. Residual Risk Is a Decision, Not a Calculation

The Army risk matrix gives leaders a mechanistic tool for scoring risk. MSS automates that calculation. But residual risk acceptance is not a calculation — it is a command decision that reflects the commander's operational judgment about what level of risk is acceptable to accomplish the mission.

This distinction matters for how leaders should use MSS CRM data. When a subordinate unit submits a risk assessment in MSS with a High residual risk, that does not mean the task cannot be executed. It means the task requires commander-level acceptance of the residual risk, with the commander's full understanding of what that risk entails and why the mission requires it.

MSS can enforce the requirement that a High-risk assessment receive the appropriate approving authority signature before the task executes. What MSS cannot do is ensure that the approving authority's decision is based on genuine understanding rather than reflexive signature. Leaders must guard against CRM becoming a bureaucratic signature chain divorced from operational judgment.

2-3. Data Completeness as a Leading Indicator of Safety Culture

A unit's CRM data in MSS is a leading indicator of its safety culture. Units with high CRM data completeness — risk assessments that are fully populated, with controls verified after execution, and hazards that are specific rather than generic — consistently demonstrate better safety outcomes. Units where CRM data is sparse, uses generic hazard descriptions, or shows a pattern of "not verified" controls are exhibiting safety culture warning signs.

Protection officers and commanders should review CRM data quality as part of their routine MSS reviews — not just looking for open High-risk assessments, but assessing whether the data quality reflects a genuine engagement with risk management or a compliance check-box culture.

SECTION 3 — CBRN DEFENSE AS AN INFORMATION PROBLEM

3-1. The Criticality of Rapid, Accurate CBRN Data Dissemination

CBRN defense is, at its operational core, a race between information and effect. When a CBRN event occurs, the outcome for affected personnel is determined in minutes — by whether they have MOPP gear on, by whether they are upwind or downwind of the hazard area, by whether routes they are about to use cross contaminated terrain. The doctrinally required response times (MOPP alerts, NBC 3 report transmission, CCP establishment) reflect the urgency of that race.

In the pre-MSS environment, the CBRN information chain was as fast as the voice reporting net — and no faster. An NBC 3 report transmitted by voice was heard by the units monitoring that net in real time. But for units not monitoring that specific net, information had to propagate through intermediate echelons, which introduced delay.

MSS changes this by integrating CBRN data into the shared protection workspace that all units in the formation can access simultaneously. When a CBRN officer enters an NBC 3 data record in MSS and it triggers an automated alert to all workspace participants, the dissemination is near-simultaneous rather than sequential. This is a structural improvement in CBRN information speed — but only if the CBRN officer enters the data with sufficient accuracy and speed to make the dissemination meaningful.

The CBRN cell's data discipline — entering events promptly, using correct agent identifications, sourcing data accurately, and updating hazard predictions when meteorological conditions change — is not an administrative function. It is a life-safety function. Data errors in the CBRN workspace have physical consequences.

3-2. The Confirmed/Probable/Suspected Distinction

One of the most consequential data quality decisions a CBRN officer makes in MSS is the confidence level assigned to agent identification data. The three-tier scale — Confirmed, Probable, Suspected — carries significant operational weight.

A "Confirmed" agent identification in MSS will drive protective actions, route changes, and patient treatment protocols. Marking unconfirmed data as "Confirmed" because it feels certain creates downstream errors in the protection picture that are extremely difficult to correct. Conversely, marking confirmed detection data as "Suspected" out of excessive caution can cause delays in issuing protective guidance that cost lives.

The CBRN officer must resist two failure modes: premature certainty (marking Suspected as Confirmed before laboratory analysis) and excessive hedging (treating confirmed sensor data as Suspected because laboratory confirmation has not arrived). The confidence level in MSS must reflect the actual evidentiary basis for the assessment — and the CBRN officer must be willing to update that level as additional data arrives, even if the update reverses a prior entry.

3-3. CBRN Data Silos — A Common but Dangerous Failure

One of the most persistent CBRN data failures in MSS-equipped formations is the CBRN data silo: the CBRN cell manages CBRN data in isolation, without integration into the broader protection workspace or the COP. The contamination overlay exists in the CBRN specialist's local workspace but has not been shared with the S3, the S2, or the subordinate units. The decontamination site is tracked by the CBRN NCO on a personal spreadsheet but is not in MSS. The CCP exists in the unit's ground truth but not in the digital protection picture.

Data silos form for understandable reasons: the CBRN cell may not have received adequate MSS training, the protection workspace may not have been properly configured for CBRN data sharing, or the CBRN officer may not have had time to enter data during a fast-moving CBRN event. But the operational consequence of the silo is that commanders and subordinates are making movement, route, and medical decisions without access to CBRN data that exists — but is invisible.

The protection officer's job is to break silos. Specifically: ensure the CBRN workspace is accessible to S2, S3, and subordinate units; establish data entry standards that the CBRN cell can execute even during a CBRN event; and review CBRN data at the PWG to verify it reflects the CBRN cell's operational picture, not just their administrative record.

SECTION 4 — ANTITERRORISM INTELLIGENCE INTEGRATION: FUSING AT AND INTELLIGENCE DATA IN MSS

4-1. The AT Officer and S2 Relationship in Data Terms

Antiterrorism, as defined in ATP 3-37.2, requires the fusion of threat intelligence with vulnerability assessment to produce an AT risk picture. This is fundamentally an intelligence-protection data integration problem. The threat data lives with the S2. The vulnerability data lives with the AT officer. The fusion product — the AT risk assessment — must integrate both.

Before MSS, this fusion was achieved through staff coordination: the AT officer asked the S2 for current threat data, the S2 produced a summary, the AT officer incorporated it into the assessment. The data relationship was human-mediated and asynchronous. If the S2 received a threat update after the AT officer's last assessment, the AT picture was outdated until the next coordination cycle.

MSS creates the possibility of near-real-time threat-vulnerability integration because both data streams can exist in the same platform. When the S2 updates the threat assessment data and the AT officer's vulnerability data is already in the AT workspace, the AT risk picture can be recalculated quickly rather than through a days-long coordination cycle. This is a structural improvement — but it only functions if both the S2 and the AT officer are maintaining their data in MSS consistently.

4-2. What Makes an AT Assessment Actionable

An AT vulnerability assessment that lives in MSS but drives no protective action has consumed the AT officer's time without improving force protection. For an AT assessment to be actionable, it must meet three tests:

First, it must be current. An AT assessment based on threat data that is 6 months old is not an AT assessment — it is a historical document. The threat environment changes. Specific threat actors that did not operate in the AOR when the last assessment was conducted may be active now. The AT officer must maintain a continuous update cycle, not treat the annual assessment as a compliance event.

Second, it must be specific. Generic threat descriptions ("general criminal threat") and generic vulnerability findings ("perimeter security could be improved") produce generic countermeasures ("improve perimeter security"). Specific AT assessments — naming specific threat vectors, identifying specific physical vulnerabilities, linking them to specific recommended countermeasures with responsible parties and timelines — produce protection improvements that can be implemented and verified.

Third, countermeasures must be tracked to execution. An AT assessment in MSS with a list of recommended countermeasures and a field of "not yet implemented" entries is a liability assessment, not a force protection improvement. The AT officer's job is to ensure that countermeasures listed in MSS are assigned to responsible parties, tracked to implementation, and verified as effective.

4-3. FPCON as an Information Product, Not Just a Status

FPCON is frequently treated as an administrative status: the theater sets the FPCON level, the unit records it, and personnel execute the measures. This misses what FPCON is as an information product.

FPCON is the distillation of a large body of threat intelligence into a single actionable guidance level. When USAREUR-AF moves from ALPHA to BRAVO, that change reflects a change in assessed threat probability — usually based on specific intelligence that may or may not have been disseminated to all echelons. The FPCON change is both a measure implementation directive and a threat indicator.

The AT officer's job in the MSS context is not just to record the FPCON change and trigger the measures checklist. It is to understand the threat context behind the change, update the unit's AT vulnerability assessment to reflect the new threat environment, and ensure subordinate leaders understand why the FPCON changed — not just that it changed. FPCON changes that arrive in MSS without explanation produce mechanical compliance. FPCON changes that arrive with threat context produce understanding and initiative.

SECTION 5 — AMD AND THE AIR PICTURE: SHARED DATA RESPONSIBILITY BETWEEN PROTECTION AND FIRES

5-1. Why AMD Sits at the Protection-Fires Intersection

Air and missile defense appears in both the protection WFF (ADP 3-37) and the fires WFF (ADP 3-19). This is not doctrinal ambiguity — it reflects the actual operational nature of AMD. AMD protects the force from aerial threats (a protection function) through weapons fire (a fires function). The data requirements of AMD thus span both WFFs, and both the protection officer and the fires officer have AMD data responsibilities.

The practical implication for MSS is that AMD data must be visible in both the protection workspace and the fires workspace. The air threat picture maintained by the ADA officer is relevant to the protection officer's air defense warning status and CAL/DAL management. It is equally relevant to the fires officer's airspace management and engagement coordination. If AMD data lives only in the protection workspace, the fires officer cannot execute airspace deconfliction effectively. If it lives only in the fires workspace, the protection officer cannot maintain an accurate CAL/DAL picture.

USAREUR-AF MSS architecture addresses this by maintaining AMD data as a shared layer accessible from both workspaces. The ADA officer owns the data — enters, updates, and validates it. Both protection and fires staff consume it. When there is disagreement between what the protection officer believes the CAL/DAL status is and what the ADA officer has entered, that is a coordination failure, not an MSS failure.

5-2. The CAL/DAL Gap as an Accepted Risk Statement

The gap between the critical asset list and the defended asset list is not a planning failure — it is a resource reality. No AMD formation has sufficient assets to defend every critical asset against every air and missile threat. The commander accepts risk on the assets not on the DAL. That accepted risk should be an explicit decision, documented in MSS, not an implicit omission.

Protection officers should ensure that for every CAL asset not on the DAL, the MSS entry includes: - The reason the asset is not on the DAL (insufficient AMD assets, asset is low probability of attack given the threat, asset has alternative protection measures) - Who accepted the risk (commander name and DTG of acceptance) - Any compensatory measures in place (dispersion, camouflage, alternate site, redundancy)

A CAL/DAL gap that is documented as an accepted risk with compensating measures is sound protection planning. A CAL/DAL gap that exists as a blank field in MSS because the AT officer never filled it in is a planning failure.

5-3. ADW as a Shared Awareness Trigger

Air Defense Warning (WHITE/YELLOW/RED) functions as a shared awareness product. When ADW changes in the formation's MSS workspace, it is not just an AMD status update — it is relevant to every element of the formation. Convoys on MSRs need to know if the ADW is RED before departing. Ground commanders at exposed positions need to know. Aircraft operating in the AOR need to know.

MSS makes ADW dissemination faster than voice-only reporting. But faster dissemination only improves protection if recipients understand what the ADW level means for their specific protective actions. Units that receive an automated ADW alert in MSS and do not know what protective actions to take have been informed but not protected. The protection officer's training responsibility includes ensuring every element understands what each ADW level requires — before the ADW changes to YELLOW or RED.

SECTION 6 — COUNTER-UAS AS AN EMERGING DATA DOMAIN

6-1. The C-UAS Data Challenge

Counter-UAS is one of the most rapidly evolving protection domains, and its data management requirements are correspondingly immature. Unlike CBRN defense, which has decades of doctrine and established reporting formats, C-UAS operations in MSS are being designed and refined in near-real time as threats evolve and defeat systems are fielded.

The fundamental C-UAS data problem is correlation: multiple sensors may detect the same UAS from different positions and report it as multiple tracks. Without correlation, the protection picture shows five separate UAS threats when there is actually one. This is not merely a nuisance — it can trigger disproportionate response, drain engagement resources, or create coordination failures with aviation.

MSS does not automatically correlate UAS tracks. Correlation is an analyst function — the AMD officer or C-UAS operator reviews incoming detections, assesses whether multiple reports describe the same object, and produces a correlated picture. Building this discipline into the C-UAS data workflow — requiring entries to note whether a new detection is correlated to an existing track or represents a new object — is a foundational data quality requirement.

6-2. The Legal Dimension of C-UAS Data

C-UAS operations have a legal dimension that most other protection domains do not. Engagement of UAS systems — particularly through electronic means — may affect civilian and commercial UAS operations, commercial communications, and the EM spectrum. The AT officer and the unit judge advocate (27A) must be involved in C-UAS data management at the planning level to ensure that engagement records are maintained in a manner that supports legal review.

In MSS, C-UAS engagement records should include: - The basis for the threat classification (why the UAS was assessed as hostile rather than civilian or friendly) - The engagement authority who authorized defeat action - The defeat method employed - The result

This record exists not to create administrative burden but to enable post-engagement review — confirming that engagements were lawful, identifying equipment performance against specific threat types, and providing data for after-action review and TTP development. The judge advocate's review of C-UAS data is a risk management measure, not a bureaucratic obstacle.

6-3. C-UAS Data Maturation in the Formation

Protection officers in USAREUR-AF should treat C-UAS data management as a developing capability, not a mature one. The naming conventions, data fields, and workflow procedures for C-UAS in MSS are being refined based on operational experience. Units that identify gaps in the C-UAS data structure should report them to the C2DAO through the protection officer channel — this is how the platform improves.

What should not change, regardless of how the specific fields and workflows evolve, are the foundational principles: record what actually happened, attribute data to its source, maintain the confirmed/probable/suspected distinction for threat assessments, and document engagement authority for all defeat actions.

SECTION 7 — PROTECTION FAILURE MODES IN MSS

7-1. Overview

The following eight failure modes represent the most common ways USAREUR-AF protection units misuse or underuse MSS. They are presented not to assign blame but to help protection officers and commanders recognize and correct these patterns before they produce operational consequences.

Failure Mode 1: FPCON Drift

What it looks like: The theater or installation AT authority changes FPCON. The unit's MSS entry is not updated for days, or is updated but subordinate units' entries are not. The formation is executing different FPCON levels across echelons.

Why it happens: FPCON changes are received through voice or digital reporting chains. The AT officer who receives the change is at a different echelon from the person responsible for updating MSS. The handoff between "change received" and "change entered in MSS" breaks down.

The consequence: Subordinate units executing the wrong FPCON level. Units at lower FPCON than required are under-protected. Units that learn a FPCON change happened but never received it lose trust in MSS as an authoritative source.

The fix: Assign explicit MSS update responsibility at each FPCON change. The unit that receives the FPCON change direction is responsible for updating MSS within 15 minutes and verifying the change propagated to all subordinate workspaces.

Failure Mode 2: Stale AT Assessments

What it looks like: AT vulnerability assessments in MSS were last updated 8–12 months ago. Threat data referenced in the assessment is no longer current. The assessment's countermeasure section has entries marked "planned" that are either complete or no longer being pursued.

Why it happens: AT assessments are perceived as annual events, not living documents. The AT officer completed the assessment for compliance purposes and has not revisited it since.

The consequence: AT risk picture does not reflect the actual threat environment. Countermeasures that should be implemented are not tracked. Resources may be allocated to countermeasures for threats that no longer exist at the assessed level.

The fix: Treat the 180-day review cycle as a maximum, not a schedule. After any significant threat change, FPCON change, or force structure change, the AT officer initiates an assessment review. Use the MSS review date field as a forcing function — not just a compliance date.

Failure Mode 3: CBRN Data Silos

What it looks like: The CBRN cell maintains CBRN data in the CBRN workspace, but the contamination overlay is not shared with the S3, S2, or subordinate units. The CCP location is in the CBRN cell's local view but not visible on the protection workspace shared with others. CBRN data exists but is invisible to most of the formation.

Why it happens: The CBRN workspace was not properly configured for data sharing during initial MSS setup. The CBRN cell was not trained on workspace sharing protocols. The protection officer did not verify data sharing as part of workspace configuration.

The consequence: Subordinate commanders making route, movement, and medical decisions without access to CBRN data that exists in the formation. If a CBRN event occurs, the contamination overlay will not reach units that need it through MSS — they will depend on voice reporting alone.

The fix: The protection officer conducts a data sharing audit for the CBRN workspace before every exercise and deployment. Verify that the contamination overlay, CCP data, and detection equipment status are visible to S2, S3, and subordinate unit workspaces.

Failure Mode 4: C-UAS Track Flooding

What it looks like: MSS C-UAS detection data shows dozens of tracks over a 24-hour period. Many of these are duplicate reports of the same object from different sensors. The AMD officer cannot determine how many actual UAS have been observed. Engagement logs reference track numbers that do not correspond to any correlated object.

Why it happens: Multiple sensors report independently to MSS without a correlation step. Each sensor report creates a new track entry. No one has been assigned to correlate tracks before they are entered as separate threats.

The consequence: The C-UAS picture is unreliable. Engagement decisions may be based on the belief that multiple threats exist when there is one. Resources are expended tracking phantom tracks.

The fix: Establish a C-UAS track correlation discipline before data entry — designated by the AMD officer. Sensor reports are correlated against existing tracks before a new track entry is created. Training on this correlation procedure is included in pre-deployment MSS certification for AMD personnel.

Failure Mode 5: CRM as a Signature Event

What it looks like: CRM data in MSS is consistently complete on paper — every entry has all required fields, every hazard has control measures, every assessment has the required approving authority signature. But control verification data is uniformly blank or marked "verified" without detail. The data shows a formation executing CRM perfectly by the numbers but not engaging with the process substantively.

Why it happens: Leaders perceive CRM as a compliance requirement. The goal becomes completing the form and getting the signature, not identifying and controlling actual risk. MSS makes the form easy to complete — which can accelerate the compliance check-box dynamic.

The consequence: Risk that was identified but not actually controlled. When an accident or incident occurs, the CRM record shows it was "controlled" — but the control was never implemented. The data provides false assurance.

The fix: The brigade safety officer conducts quarterly audits of CRM control verification data. Units that show a high "not verified" rate, or that have identical generic control measures across multiple assessments, are flagged for command attention — not for a new form, but for a conversation about whether CRM is actually being executed.

Failure Mode 6: Protection Picture at the Wrong Classification Level

What it looks like: Protection data in MSS — particularly AT vulnerability assessments, C-UAS engagement records, and survivability position data — is entered at a lower classification level than the content warrants. Alternatively, CBRN threat data is entered at a higher classification level than required, making it inaccessible to units that need it at lower echelons.

Why it happens: Classification of protection data is ambiguous. AT vulnerability assessments may describe specific vulnerabilities that are sensitive but not classifiable as SECRET. CBRN threat data at the unclassified level is shareable widely, but at SECRET, dissemination slows dramatically. Leaders default to one extreme or the other without careful analysis.

The consequence: Underclassified sensitive data creates OPSEC risk. Overclassified data creates access problems — units that need the data to execute protection tasks cannot access it at their available classification level.

The fix: The unit IMO and S2 establish classification guidance for each protection data category at the beginning of an exercise or deployment. This guidance is briefed to all protection workspace contributors as part of MSS onboarding. The AT officer and CBRN officer are the primary authorities on classification for their data domains.

Failure Mode 7: The Missing Accepted Risk Entry

What it looks like: The CAL/DAL shows assets on the CAL that are not on the DAL. The MSS entries for those assets have no accepted risk documentation — no commander's name, no rationale, no compensating measures. The gap exists as a data null rather than a documented command decision.

Why it happens: The ADA officer and protection officer know which assets are not defended and why. But documenting accepted risk in MSS feels like extra administrative work when the command understands the situation.

The consequence: When the decision-maker rotates (as happens regularly), their replacement sees a CAL/DAL gap with no context. The new commander does not know whether the gap was accepted as a calculated risk with compensating measures or whether it represents an oversight. Decisions made in the absence of this context are structurally uninformed.

The fix: Make accepted risk documentation a mandatory field for every CAL asset not on the DAL. The protection officer enforces this at the PWG. Entries without accepted risk documentation are flagged as incomplete, not just entries with missing data.

Failure Mode 8: Post-Incident Data Neglect

What it looks like: An AT incident, CBRN event, or physical security breach occurs. The initial MSS entry is made. But follow-on updates — investigation results, after-action findings, corrective actions taken, lessons learned — are never entered. The MSS record shows an open incident with no resolution.

Why it happens: Attention shifts to the immediate response and then to the next priority. Retroactive data entry feels low-value once the event has passed. The MSS entry sits open indefinitely.

The consequence: The formation loses the institutional value of the event data. Lessons that could improve AT assessments, CBRN procedures, or physical security planning remain un-extracted. If the same type of incident recurs, there is no MSS record connecting it to a prior event that should have produced corrective action.

The fix: The AT officer or protection officer owns the follow-up data discipline. Every open incident in MSS has a 72-hour follow-up requirement: status, immediate corrective action taken, and whether a formal after-action review is planned. Formal AAR findings are entered as a linked record. No incident is closed without lessons learned documented or explicitly noted as "none identified."

SECTION 8 — PROTECTION DATA STANDARDS: WHAT "GOOD" LOOKS LIKE

8-1. The Integrated Protection Picture Test

A formation's protection data in MSS passes the integrated protection picture test if a senior leader — arriving at the unit without prior context — can open the protection workspace and answer the following six questions accurately from MSS data alone, without asking staff:

1. What is the current FPCON and when did it last change?
2. What CBRN threats are active in the AOR, and what areas are contaminated or at risk?
3. What is the current AT risk at the primary installation?
4. Are all ECPs operational, and have there been any incidents in the past 48 hours?
5. What is the AMD picture — what assets are defending what critical assets, and are there coverage gaps?
6. Are there any outstanding High-risk CRM assessments awaiting commander acceptance?

If the protection workspace cannot answer these questions, the protection data program has failed — regardless of how much data is technically in the system. Data quality is measured by the quality of the answers it enables, not by the quantity of records entered.

8-2. Protection Data Standards by Time Category

Protection data has different required currency depending on its operational relevance. Table 8-1 provides a summary standard for protection officers and data managers.

Table 8-1. Protection Data Currency Standards

Data Element	Event-Triggered Freshness	Routine Update Frequency	Consequence of Staleness
CBRN contamination overlay	Update within 1 hour of met change (>10°/3kts)	Review at every PWG	Soldiers move into contaminated areas without warning
FPCON level	Update within 15 min of command direction	Review weekly	Units execute wrong protective measures
AT vulnerability assessment	Review after any significant threat change	Every 180 days minimum	AT risk picture does not match actual threat
RAM execution status	Mark after each execution window	Weekly summary review	Cannot verify AT program effectiveness

Data Element	Event-Triggered Freshness	Routine Update Frequency	Consequence of Staleness
AT incident status	Update within 72 hours of any development	At each PWG	Open incidents fade without resolution
ECP status	Update at every shift change	8-hour maximum	COP does not reflect actual access control posture
AMD/ADW status	Update within 10 min of command direction	Daily system status review	Units do not implement correct air threat response
CAL/DAL	Update after any AMD asset change	Monthly	Commander unaware of coverage gaps
Survivability position status	Update within 24 hours of construction completion	Weekly review	COP shows planned positions as complete when they are not
CRM risk assessment	Submit before task execution	Task-cycle based	Task executes without approved risk acceptance

8-3a. Data Quality Standards for Specific Protection Data Types

Not all protection data has equal operational consequence if it degrades in quality. Table 8-2 ranks the protection data types by consequence of quality failure — this helps protection officers prioritize data quality enforcement when time is constrained.

Table 8-2. Protection Data Quality Risk Priority

Priority	Data Type	Quality Failure Consequence	Acceptable Degradation Window
1 (Highest)	CBRN contamination overlay	Soldiers enter contaminated areas; casualties	None — any staleness is unacceptable during active events
1	NBC 3 warning — geospatial accuracy	Warning covers wrong area; units in actual hazard not warned	None
2	FPCON level	Wrong protective measures executed across formation	15 minutes maximum from command direction
2	ADW status	Units do not execute appropriate air threat protective actions	10 minutes maximum from command direction
3	C-UAS detection track correlation	False threat picture; possible erroneous engagement	As rapid as possible; corruption cannot persist through a PWG
3	ECP operational status	COP does not reflect actual access control posture	One shift change maximum (8 hours)

Priority	Data Type	Quality Failure Consequence	Acceptable Degradation Window
4	AT vulnerability assessment currency	AT risk picture does not match threat environment	180 days before assessment is operationally stale
4	CAL/DAL	Commander unaware of AMD coverage gaps	30 days maximum; immediately on AMD asset status change
5	CRM verification data	Cannot identify compliance gap trends	End of each task cycle
5	Survivability position construction status	COP shows incorrect defensive posture	24 hours maximum

8-3. The Protection Officer as Data Quality Officer

The protection officer has two roles in MSS. The first is the operational role: running the PWG, coordinating protection tasks, advising the commander. The second is a role many protection officers undervalue — the data quality officer for the protection workspace.

Data quality officer responsibilities include: - Establishing and enforcing naming conventions (Appendix A of SL 4E) - Conducting weekly data quality reviews (Appendix H of SL 4E) - Resolving workspace access issues before they cause data silos - Identifying data entries that are technically present but operationally useless (generic hazard descriptions, unsigned risk assessments, incidents with no status updates) - Holding workspace contributors accountable for data currency at the PWG

This is not glamorous work. It does not feel like leading a protection WFF. But a protection officer who lets data quality degrade is, in effect, choosing to fly blind — and asking the commander to make protection decisions based on information that may not reflect reality. In the protection domain, that choice has consequences measured in casualties.

SECTION 9 — THE PROTECTION OFFICER'S MENTAL MODEL FOR MSS

9-1. Three Layers of Protection Data in MSS

Protection officers who struggle to get value from MSS often treat it as a single system with multiple tabs. A more useful mental model has three layers, each serving a different leadership function.

Layer 1 — The Operational Layer (real time): CBRN events, FPCON changes, ADW status, C-UAS detections, active incidents. This layer answers: "What is happening right now that affects force protection?" It must be current to hours, not days.

Layer 2 — The Posture Layer (days to weeks): AT vulnerability assessments, CAL/DAL status, survivability position construction status, RAM execution rates, physical security inspection findings. This layer answers: "What is the current state of the unit's protection program?" It drives PWG action items and commander advisories.

Layer 3 — The Trend Layer (weeks to months): CRM trend data, AT incident patterns, recurring hazards, recurring security deficiencies. This layer answers: "What systemic protection problems exist that require command intervention?" It informs training priorities, resource requests, and command emphasis.

Most protection officers are comfortable in Layer 1. Layer 2 requires discipline to maintain. Layer 3 is where MSS provides value that was structurally unavailable before digital data integration — and most units never get there because they are too busy maintaining Layers 1 and 2. The goal is to build Layer 1 and 2 data quality to the point where Layer 3 becomes accessible and regularly used.

9-2. Questions to Ask Before Every Commander's Brief

Before any brief that includes protection WFF data, the protection officer should be able to answer:

1. When was the CBRN overlay last updated, and what is the source?
2. Is the FPCON in MSS the current command-directed level, and who directed it?
3. Have all AT incidents in the past 72 hours been entered and updated?
4. Is there any protection data that exists in a cell's local files but has not been entered in the shared MSS workspace?
5. Are there any open action items from the last PWG that are past due?

If the answer to any question is "I'm not sure," the brief is not ready. The protection officer's credibility with the commander depends on the accuracy of the data behind every protection product. That accuracy is the product of daily data discipline — not pre-brief heroics.

9-2a. Using MSS to Identify Protection Gaps Before They Become Failures

One of MSS's most underused capabilities in the protection WFF is gap identification. The platform aggregates protection data from multiple cells — and in that aggregation, gaps become visible that are invisible to any single practitioner.

Common gap identification uses in MSS: - **Coverage gap:** CAL assets without DAL coverage, visible in the AMD workspace. If no one has documented the accepted risk rationale, the gap is invisible at the command level. - **Temporal gap:** CBRN data that has not been updated in 24+ hours during an active threat period. Visible in the CBRN workspace data-as-of timestamps. - **Geographic gap:** Survivability positions that exist in some areas of the AOR but not others, visible in the geospatial layer. Are there approaches to the base camp without fighting position coverage? - **Compliance gap:** AT assessments that are within 30 days of their 180-day review deadline. The MSS review date field enables this to be

surfaced as a predictive warning, not a reactive failure. - **Pattern gap:** AT incidents that cluster by location, time of day, or incident type but have not been identified as a trend because the data has never been reviewed in aggregate.

The protection officer who uses MSS for gap identification is operating proactively — finding and addressing protection deficiencies before they produce casualties or security failures. This is the highest-value use of the integrated protection picture. It requires the same data quality discipline as reactive use — but the payoff is prevention rather than response.

9-3. A Note on Platform Limitations

MSS is a powerful data integration platform. It is not omniscient. The following limitations are inherent to any data platform and should inform how protection officers use MSS data:

- **MSS shows what has been reported, not what has occurred.** An incident that was not entered did not happen as far as MSS is concerned. Gaps in reporting chains create gaps in the protection picture.
- **MSS is as accurate as the data entered.** A contamination overlay that was calculated using incorrect meteorological data produces a geographic error in the hazard picture. The platform has no way to know the input was wrong.
- **MSS time stamps show when data was entered, not always when events occurred.** For events entered retroactively, the protection officer must verify that the DTG fields reflect the actual event time, not the entry time.
- **MSS access controls define what users can see, not what they should know.** A unit that lacks access to an adjacent unit's CBRN data in MSS may be operating in the same contaminated area. Access control architecture must be deliberately designed for interoperability, not just security.

These limitations do not reduce MSS's value — they define the boundaries within which the platform operates. The protection officer who understands these limitations can compensate for them through verification, coordination, and physical confirmation. The protection officer who forgets them treats MSS data as ground truth and is eventually surprised by the gap.

CLOSING NOTE FOR SENIOR LEADERS

The protection WFF requires integrated information to function. ADP 3-37 assumes it. MSS enables it. But the platform only produces an integrated protection picture if the practitioners — CBRN officers, AT officers, PMO, ADA officers, engineers, and legal advisors — maintain their data with the same discipline they bring to the physical tasks of protection.

The eight failure modes in Section 7 are not hypothetical. They represent observed patterns from formation-level MSS use in USAREUR-AF. Commanders and protection officers who recognize these patterns early and correct them produce formations where MSS is a genuine force multiplier for

protection. Those who tolerate them produce formations where MSS adds administrative burden without adding protection capability.

The protection officer's most important MSS role is not data entry. It is data quality enforcement — ensuring that the protection picture in MSS is accurate enough that a commander can look at it and make decisions. That standard, applied consistently, is what makes MSS a protection asset rather than a protection liability.

RELATED TRACKS AND PUBLICATIONS

WFF Peer Tracks

All six WFF tracks are at the same tier. All six WFF tracks require SL 1, SL 2, and SL 3 as prerequisites.

Track	Title	Prereq	Relationship to Protection WFF
SL 4A	Intelligence WFF	SL 1 + SL 2 + SL 3	AT intelligence integration; threat data for AT assessments
SL 4B	Fires WFF	SL 1 + SL 2 + SL 3	AMD coordination — fires and protection share AMD data domain
SL 4C	Movement and Maneuver WFF	SL 1 + SL 2 + SL 3	Physical security integration with maneuver operations
SL 4D	Sustainment WFF	SL 1 + SL 2 + SL 3	CBRN resupply coordination; medical tracking for CBRN casualties
SL 4E	Protection WFF	SL 1 + SL 2 + SL 3	This track
SL 4F	Mission Command WFF	SL 1 + SL 2 + SL 3	COP integration; CCIR products consuming protection data

Specialist Tracks (Prerequisite: SL 3)

For personnel pursuing technical depth, specialist tracks (SL 4G–O, prereq SL 3) are available. Not required for protection WFF employment.

Track	Title
SL 4G	ORSA (→ SL 5G)
SL 4H	AI Engineer (→ SL 5H)

Track	Title
SL 4M	ML Engineer (→ SL 5M)
SL 4J	Program Manager (→ SL 5J)
SL 4K	Knowledge Manager (→ SL 5K)
SL 4L	Software Engineer (→ SL 5L)
SL 4N	UI/UX Designer (→ SL 5N)
SL 4O	Platform Engineer (→ SL 5O)

CONCEPTS GUIDE — SL 4E: Maven Smart System, Protection Warfighting Function Headquarters, United States Army Europe and Africa Wiesbaden, Germany — 2026

Next scheduled review: March 2027 Submit corrections or recommendations to: USAREUR-AF C2DAO, Wiesbaden, Germany

QUICK REFERENCE: SECTION-TO-CHAPTER MAPPING

Concepts Guide Section	SL 4E Chapter(s)
Section 1 — Protection WFF and Data	Chapter 1
Section 2 — Risk Management as a Data Discipline	Chapter 2
Section 3 — CBRN Defense as an Information Problem	Chapter 3
Section 4 — Antiterrorism Intelligence Integration	Chapter 4
Section 5 — AMD and the Air Picture	Chapter 6
Section 6 — Counter-UAS as an Emerging Data Domain	Chapter 7
Section 7 — Protection Failure Modes in MSS	All chapters
Section 8 — Protection Data Standards	Appendices G and H

NOTE — New Doctrine Content in SL 4E: SL 4E now includes CVP (Criticality-Vulnerability-Probability) analysis from ADP 3-37 with a 5-step MSS procedure and data currency WARNING (section 4-2a), OPSEC 5-step process mapped to data security analogs (section 4-7), and the GMAD (Generate-Manage-Analyze-Disseminate) framework from FM 3-34 as a data lifecycle NOTE (Ch 8). These sections ground protection data management in their authoritative doctrinal sources. | Section 9 — Protection Officer's Mental Model | Chapters 9–10 |