MSG-088 Data Farming in Support of NATO: Case Study Force Protection

Daniel Kallfass
CASSIDIAN/EADS Deutschland GmbH
Claude Dornier Straße, 88090 Immenstaad
GERMANY

Daniel.Kallfass@cassidian.com

Tobias Schlaak
CASSIDIAN/EADS Deutschland GmbH
Landshuterstraße 26, 85716 Unterschleißheim
GERMANY

Tobias.Schlaak@cassidian.com

Stephan Seichter
Bundeswehr Planning Office
Einsteinstraße 20, 85521 Ottobrunn
GERMANY

stephanseichter@bundeswehr.org

Sascha Mayer
Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support
Ferdinand-Sauerbruch-Straße 1, 56073 Koblenz
GERMANY

saschamayer@bundeswehr.org

ABSTRACT

The nature of scenarios that NATO forces are faced with in today's world are uncertain and complex. It is essential for the military decision maker to rapidly gain insight into questions of operational relevance and to more fully understand the landscape of possibilities including unexpected results and so called outliers. Data Farming as a question based approach is able to provide this ability in answering the basic question: What if?

The application of the power of Data Farming to our questions is essential to providing support to NATO decision makers not currently available. Data Farming has already successfully been applied to many questions including peace support operations, urban operations, anti-piracy operations, defeating improvised explosive devices, etc.

NATO Science and Technology Organization (STO, former RTO) started the three-year US / DEU co-lead Modeling and Simulation Task Group MSG-088 "Data Farming in Support of NATO" in 2010. The task group's objective has been to assess and document the Data Farming methodology to be used for NATO decision support. In course of the MSG-088 Program of Work two case studies have been performed as part of the proof-of-concept explorations to demonstrate the power and benefits of Data Farming.

This paper describes in detail the DEU lead case Study "Force Protection". Operational questions in the context of an effective protection of a Combat Outpost (COP) in a joint NATO environment, such as for example "Which COP configurations perform consistently well against a large variety of threats?", are examined by applying the Data Farming methodology. Conducting thousands of simulation runs several courses of actions are examined with thousands of alternatives by using an agent-based model, PAXSEM, developed on behalf of and currently in use by the German Armed Forces. In the same way threat analyses are performed in order to identify most dangerous threats against certain COP configurations.

After a short review of the Data Farming concept the paper describes the analysis approach, the development of the scenario, the used Design of Experiment (DOE) and presents parts of the analysis results. In summarizing the paper also discusses the merits and cautions to be considered when applying Data Farming in order to obtain valid results to support our decision makers in the future in more and more complex and uncertain operational environments.

1.0   INTRODUCTION

Data Farming, introduced by (Brandstein and Horne 1998 [1]), is not a new scientific term but a process that has been developed in order to support decision-makers in answering questions that are not addressed by traditional modeling and simulation processes (Horne and Meyer 2004 [3]). The Data Farming methodology will be described in a subsequence section.

Only few nations make use of the Data Farming methodology in conjunction with their simulation models yet to gain insights into the complexity of civil or military problems. Initiated by this interest group, an international community has been conducting common activities for about a decade now around the idea of Data Farming. International Data Farming Workshops (IDFW) have taken place twice a year under the direction of the Naval Postgraduate School (NPS) Monterey, California in order to exchange knowledge in the field of Data Farming, covering topics such as model development or experimental designs.

In 2010 the NATO Research and Technology Organization (RTO) has started the NMSG Task Group MSG-088 "Data Farming in Support of NATO" to evaluate and further develop the Data Farming methodology to be used for decision support within NATO. This task group deals with the six realms of Data Farming, each of which is represented in a corresponding subgroup of the MSG-088.

The simulations available to NATO analysts are often large and complex. Their current application methodology however does not manage to exploit them to the utmost. And even the smaller more abstract agent-based models are still too complex to be easily applied in order to create an added value. In addition, response surfaces of the model output can be highly non-linear. Thus efficient experimental designs and other methods have been integrated in the Data Farming process in order to encompass that kind of the questions not to be answered by other methods (Horne and Meyer 2004 [3]).

As part of the "Program of Work" of MSG-088, proof-of-concept explorations regarding questions and models of interest to NATO nations are to be conducted, with the objective of illustrating the power of Data Farming for decision support. The task group has set up two case studies. The first one being related to "Humanitarian Assistance and Disaster Relief (HA/DR)", whereas the second case study involves in the topic "Force Protection".

With the subsequence chapters this paper describes the results of the case study "Force Protection" where the Data Farming methodology was applied using the German agent based simulation system PAXSEM in order to answer military operational questions on how to protect a combat outpost (COP), possibly with the support of joint fire assets in an Afghan mission setting against strong and coordinated insurgent forces.

2.0   THE DATA FARMING METHODOLOGY

The Data Farming methodology applies a simulation-based, holistic and iterative approach to analyze complex systems. In general, the challenge of all simulation systems is the fact, that running *one* simulation only provides *one* singular result regarding just the *one* given situation and circumstances. In this case, no conclusions as to different circumstances - including (identification of) best / worst case scenarios - can finally be drawn. A wider description of the underlying system would be most valuable to obtain a deeper insight.

This awareness gave rise to the establishment of Data Farming, a simulation based analysis process that is:

   •   applicable for quantitative analysis of complex questions

   •   to enable "what if" analyses

   •   to gain robust results

   •   to compare results based on defined measurement categories.

The nucleus of Data Farming builds on myriad simulation runs, conducted on high-performance supercomputers, with numerous input parameters varied along a deliberately defined plan, measuring the output and finally examining the mutual interrelation as depicted in Figure 1.
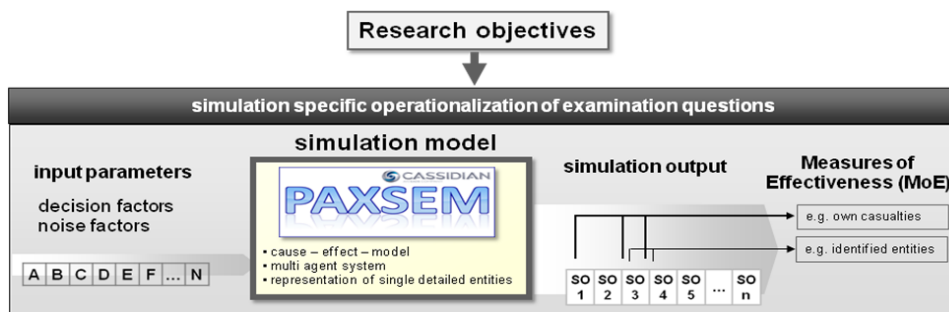

Figure 1: The concept of Data Farming

Within this scene, Data Farming enables to check assumptions, to gain new insights into relevant relationships and, last but not least, to obtain more robust statements on opportunities and risks of specific mission situations. Briefly, to obtain a more detailed insight into the properties of the examined complex system. This is achieved through a deliberate alternation of parameter values of decided input parameters that are depicted a priori, assuming them to be crucial as regards the measures of effectiveness. Data generated thusly can be of different nature. Dependant on its extent the following analysis can be exploratory or descriptive.

Data Farming is an iterative team process (Horne and Meyer 2004 [3]). Figure 2 presents the Data Farming process as a set of embedded loops that reflect the six realms of Data Farming (NATO STO 2013 [10]):

   1.   Collaboration

   2.   Rapid prototyping of scenarios

   3.   Model development

   4.   Design of experiments

   5.   High performance computing

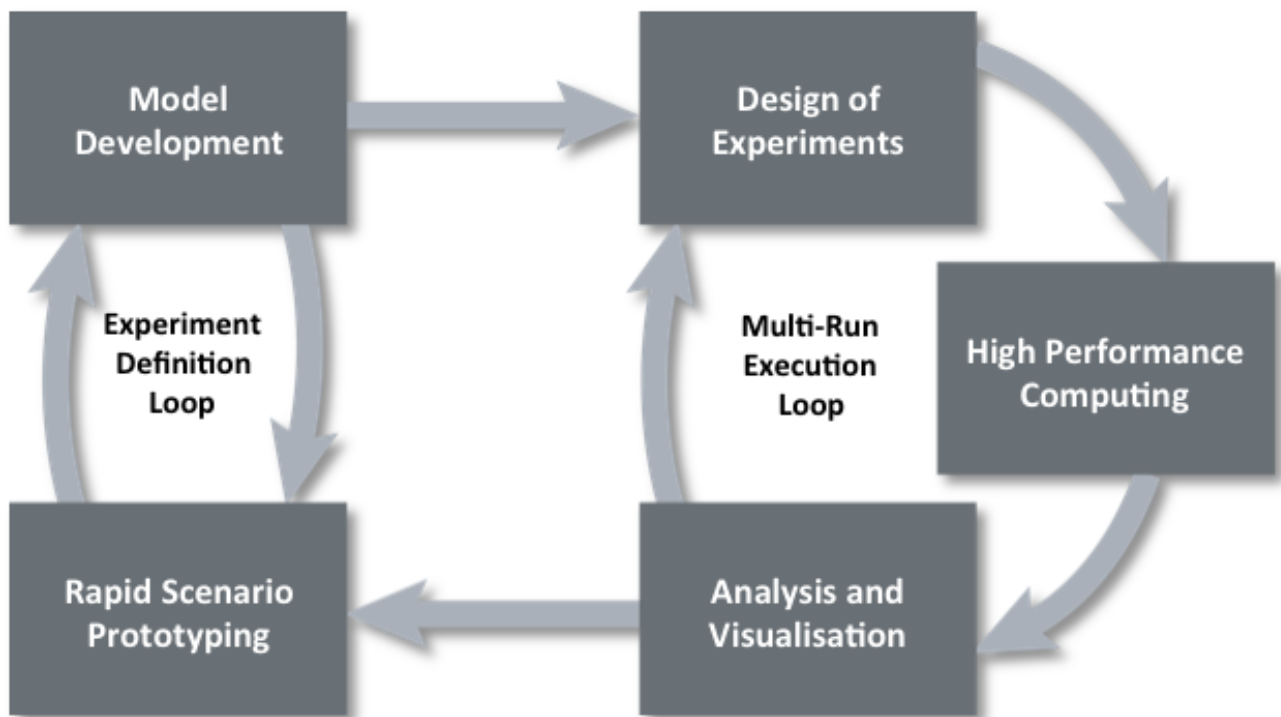   6.   Data analysis & visualization

Figure 2: The Data Farming Loop of Loops

Data Farming should be regarded question-centric at any stage. It engages an iterative process that scientifically and systematically refines an operational question from its initial raw version (commonly colloquially formulated) into a corresponding answer (at best in a most suitable jargon).

Once injected into the process the operational question sets the scene for the derivation of an overarching examination question serving as a central research objective. The replenishment with additional less aggregated questions is commonly necessary to describe the successive analysis activities more precisely. Within the boundaries set by this groundwork, a scenario is defined in close **collaboration with subject matter experts (SME) representing the first realm**. The scenario serves as a behaviour framework within which relevant environment-specific rules of behaviour are imposed upon the agents involved. Although lacking a commonly recognized definition, an agent may be described as an autonomously deciding system existing in a complex dynamic environment and conducting reasonable actions in order to pursue definite goals (Woolridge 2002 [9]). The modeled agents are part of a deliberate plot that represents the basis of examination.

The **second realm "Rapid Prototyping of Scenarios"** emphasizes the importance of scenarios as a crucial qualification to answer the initial questions. A rapidly generated scenario accelerates and drives the scenario discussion and its correct implementation into a specific simulation model. The resulting scenario should not only include the definition of the Measures of Effectiveness (MOEs) and the input parameters including corresponding value ranges varied through the Data Farming experiment. Also the expected interrelation of input parameters and command variable are to be formulated (ITIS 2011 [5]). The input parameters can be divided along their persuasibility into decision factors that a decision maker may influence (e.g., the number of soldiers within a COP) and noise factors that cannot be influenced (e.g., the size of an insurgent group). This represents the **third realm "Model Development"** where a model needs to be developed enabling to simulate the required scenario on the required level of detail with the given set of input parameters and MOEs. Verification of the scenario's electronically version by the involved subject matter experts is again crucial as to the final acceptance of all examination results.

The **fourth realm "Design of Experiments" (DoE)** comprises the statistical experiment planning. DoE can cut down the sampling requirements by orders of magnitude, yet make it possible and practical to develop a better understanding of a complex simulation model. As stated in (Sanchez 2006 [7]) a well-designed experiment allows the analyst to examine many more factors than would otherwise be possible, while providing insights that cannot be gleaned from trial-and-error approaches or by sampling factors one at a time.

The multiplicity of the numerous individual simulation runs manifests how Data Farming can bring its major advantages into play. The fifth realm "High Performance Computing" (HPC) copes with the techniques to efficiently run thousands of simulation runs on high performance computer clusters thus providing reasonable runtimes even for encompassing experiments.

Finally, the sixth realm is "Data Analysis and Visualization" which involves techniques and tools for data processing of huge datasets resulting from the Data Farming experiment. The concluding statistical analyses examine the comprising data upon anomalies, outliers, unexpected developments or simply the underlying interdependencies as described above.

3.0   SETUP OF THE CASE STUDY EXPERIMENT

This section gives some detailed insight into the setup and results of Data Farming activities within NATO's MSG-088.

3.1   Examination questions

The overall examination question has been defined as:

In order to effectively protect a COP, which tactics / equipment are most robust against different kinds of threats?

To answer that question, the following three sub-questions have been derived:

1. Is there a COP configuration that performs consistently well?
2. What is the most dangerous threat and how does the robust COP work for that threat?
3. Under which circumstances can joint fire support improve the survivability of the COP?

The overall examination question also implies the investigation of the chosen solution's robustness. Hence, to incorporate this aspect, the agreed approach was to run the different COP setups or strategies against different kinds of insurgent threats. From the resulting matrix the average performance of a specific COP setup was intended to be determined.

3.2   Scenario

A simulation-based analysis manifests best in the formulation of a scenario. However, in accordance with NATO's Code of Best Practice for C2 Assessment, it is only one part of a larger analytical methodology (NATO 2002 [6]). Beyond, Data Farming rather satisfies the general need for multiple scenarios when intending to cover the problem space through its indigenous variation of parameters. In that context, the first two realms of Data Farming go hand in hand with the above mentioned NATO document.

The following section gives an overview of the general scenario setup and plot.

A COP is operational next to an Afghan village. Figure 3 visualizes the geographical deployment. It is equipped with various sensor and weapon systems which help to identify enemies and hence protect itself. Both sensors and effectors are installed inside and outside the COP.

Sensors inside the COP may be positioned e.g. on set-up watchtowers or placed on vehicles, whereas external sensors could be positioned at an observation point (OP) on a nearby hill to get a better overview over the area. Additionally, UAVs can be used to improve the recognized operational picture (ROP) temporarily and a Quick Reaction Team (QRT) at COP command allows instantaneous checks on potential enemies prior to their attack on the COP.

In terms of effectors, the COP has access to weapon systems stationed inside the COP, like the soldiers' rifles, mortars and mounted effectors on the vehicles. From outside the COP, joint fire support in form of helicopters, fixed wing aircrafts or artillery can be requested, once a suitable target has been identified.

Offensive activities initiated by the enemy forces have been defined twofold. Attack takes place either in the form of homogenous long distance attacks with the help of mortars or rocket launchers, or in the form of a force-on-force attack, seeking direct confrontation.
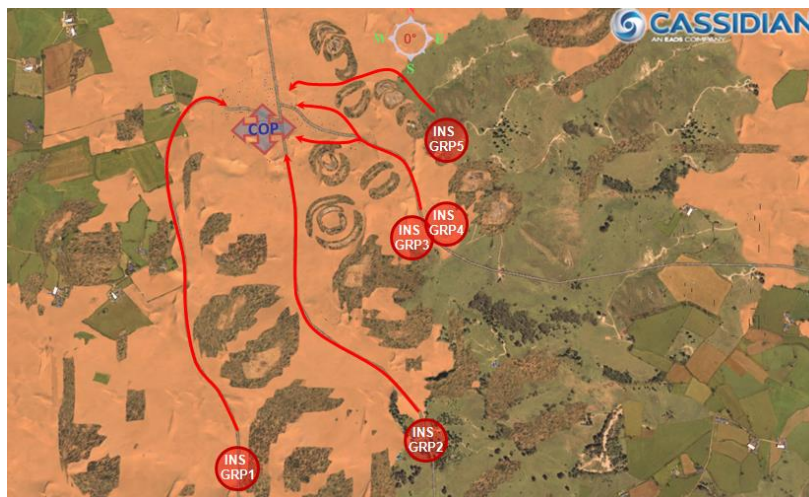
Figure 3: scenario force-on-force attack on COP

3.3   Simulation Model

Contemporary problems are coined by a rising complexity. Data Farming is applied in accordance with Ashby's law of requisite variety, postulating that complex problems need complex methods for their solutions.

Ideally, an examination is proceeded by the orchestration of a set of applicable tools (NATO 2002 [6]). However, this preparation too often rivals the time offered for problem solving (Bleicher 2004 [2]) and exploitation of existing technology is a valid compensator. In the depicted project, a compulsory initial question-centric comparison (ITIS 2011 [5]) of the needed simulation capabilities (TO BE) and the existing resources (AS IS) led to a further development of the German agent-based simulation system PAXSEM, which was used along with the German Data Farming environment for modeling the given scenario situation and analyzing the posed questions. The latter consists of a Data Farming management software offering a user friendly GUI for defining, executing and analyzing Data Farming experiments being run on the nationally hosted high performance computer clusters.

PAXSEM is an agent-based simulation model developed by CASSIDIAN since 2008 on behalf of the German Bundeswehr. PAXSEM enables a detailed, physically based representation of technical systems as regards the combined application of sensors (optical/infrared/radar) and effectors (point/area weapons, rockets/controlled missiles/fire-and-forget). All contained agents act according to their predefined complex rule sets just like in the real world. Within PAXSEM, as a multi-agent system, their individual behaviour is coined by mutual influences. Unlike their isolated behaviour, the collective behaviour of all agents cannot be accurately predicted. PAXSEM hence represents complex systems.

Furthermore, it allows the highly resolved 3D visualization of technical-tactical scenarios and plots. Within these, military units are represented as agents in a granularity from single entity to enforced company level. The simulation environment offers a flexible level of detail which is to be aligned with the examination subject. In order to generate even more added value, its expandability comprises the combination with third party models (e.g., weapon effect service), detailed modules (e.g., communication model), free-to-choose landscapes and real systems (e.g., in a testbed).

PAXSEM brings substantial support to operational activities through enhancing the formulation of standing operational procedures of technical systems in military scenarios or the pre-testing of potential, jointly provided solutions towards skill gaps. By definition, PAXSEM qualifies to address multiple-criteria evaluation problems with its overarching rationale of a known number of alternatives to be examined in broader width. Additionally, PAXSEM has provided support to military procurement through evaluation of performance of existing systems or systems in procuration (i.e., virtual prototyping), the analysis of different sensor / effector systems, all coming with the possibility to immediate, transparent and reproducible examination of systems alternatives.

3.4   Measures of Effectiveness

For the purpose of simplification, only two Measures of Effectiveness (MOEs) will be depicted within this paper. The following MOEs have been identified as being suitable to actually identify the performance of the course of action in terms of the initially formulated overall question:

- The total number of own casualties
- The percentage of own casualties

The robustness of the COP can be defined as a steady success against varying strength / capabilities / tactics of enemy forces. Therefore the above MOEs may also be incorporated into a quadratic loss function that does not only take into account the average performance of a COP (mainly the mean value of total/percentage of casualties) but also the deviation of the results.

3.5   Design Of Experiment

For the described scenario, various input factors have been defined that are deemed likely to have an influence on the course of the scenario and the outcome in terms of the defined MOEs. As described in chapter 2, the input parameters may commonly be divided into "decision factors" that a decision maker may influence and "noise factors" that may not be influenced. In this scenario all factors that define the properties of the own forces of the COP are treated as decision factors and all factors that define type and threat of the enemy forces are treated as noise factors.

The 21 decision factors of the own forces listed in Table 1 consist of 13 discrete, 1 continuous and 7 categorical decision factors. They may be further divided in factors that make up the weapon systems within the COP (e.g., number of rifles, number of snipers) and indirectly define the number of required soldiers within the COP. Each weapon system's effectiveness is defined by the factors "available ammunition factor" and "marksmen proficiency level". The following factors influence the sensor systems (e.g., #UAVs,

#Observation Points). Finally the last two decision factors define the availability of a joint fire asset and its latency once fire support is requested.

Table 1: 21 decision factors

Decision factor	Scale	Value Range
#rifles (5,56mm)	discrete	[0;49]
#medium MG (7,62mm)	discrete	[0;9]
#guided rockets	discrete	[0;9]
#unguided rockets	discrete	[0;9]
#sniper	discrete	[0;4]
mortar and mortar tactics	categorical	none / 1 in COP / 1 in OP / 1COP+1OP / 2 in COP /2 in OP
#heavy armed vehicles	discrete	[0;8]
heavy armed vehicle weapon system	categorical	machine canon (20mm) / grenade launcher
#medium armed vehicles	discrete	[0;8]
medium vehicle weapon system	categorical	medium MG (7,62mm) / grenade launcher
#unprotected vehicles	discrete	[0;8]
unprotected vehicle weapon system	categorical	medium MG (7,62mm) / grenade launcher
available overall ammunition factor	discrete	[1;5]
marksmen proficiency level	categorical	low / medium / high
#QRT (Quick Reaction Teams)	discrete	[0;1]
#UAV	discrete	[0;2]
type of UAV	categorical	small / medium
#OP towers within COP	discrete	[0;1]
#OP towers outside COP	discrete	[0;1]
type of fire support	categorical	none / fixed wing / helicopter / artillery
latency factor joint fire support	continuous	[0;100%]

The 13 noise factors of the enemy forces' configuration listed in Table 2 consist of 6 discrete, 4 continuous and 3 categorical noise factors. The first noise factor is the marksmen proficiency level, corresponding to the decision factor above. The second factor defines the type of INS attack on the COP. This may either be a long distance attack (LDA) or a force on force attack (FOF). The FOF attack can further be divided in a FOF attack with one single large and well-coordinated group (FOF LARGE GRP) or multiple distributed small groups (FOF DISTRIBUTED). For each type of attack different noise factors are taken into account (e.g., the third factor "LDA:#INS" which defines the number of INS for a long distance attack).

Table 2: 13 noise factors

Noise factor	Scale	Value Range
Marksmen proficiency level	categorical	LOW / MEDIUM / HIGH
INS Tactics	categorical	LDA / FOF LARGE GRP / DISTRIBUTED
LDA: #INS	discrete	[1;5]
LDA: #EMPLACEMENTS	discrete	[1;5]
LDA: INS SPEED	categorical	running / walking / crawling / motorized
LDA: %RPG	continuous	[0-100%]
FOF DISTRIB: #GROUPS	discrete	[3;5]
FOF DISTRIB: #INS PER GROUP	discrete	[5;10]
FOF LARGE GRP: #INS	discrete	[50;100]
FOF: %RPG within group	continuous	[0%;20%]
FOF: %HMG within group	continuous	[0%;20%]
FOF: %MORTAR within group	continuous	[0%;10%]
FOF: #improvised rocket launcher	discrete	[0;2]

With the given large number of factor and ranges, a fully gridded design, combining all possible values of all factors, is not appropriate. The number of required design points and the tantamount number of required simulation runs (without replications) would be around 2,5 * 1027. Therefore choosing an appropriate DoE is essential for this case.

In contemporary literature, many designs of experiments can be identified. A broad overview may be found at (Sanchez 2006 [7]). The problem that most design of experiments have is coping with categorical factors.

Due to the mixture and combination of the chosen input factors, of which some are numerical and others categorical, the *Nearly Balanced Nearly Orthogonal Mixed Design* which was developed at the Naval Postgraduate School in Monterey, California (Vieira Jr. et al. 2011 [8]) was chosen. This design offers the following characteristics (for the purpose of simplification the measures like variance inflation factors (VIF) are not explicitly depicted for this paper):

- The design is mixed as at it supports different factor types (categorical, discrete and continuous) and/or different factor levels.

- The design is balanced as the number of objects in each of the levels of each column is almost equal (an imbalance less than 20% is guaranteed).

- The design is nearly orthogonal (maximum absolute pair wise correlation between any two factors (columns) is below 0.05).

- Finally, the design is characterized as efficient as the number of resulting design points is acceptable.

As the asked questions require to run different COP setups against different INS configurations it was decided to combine two sub-designs:

- Sub-design 1: 168 design points for all 21 decision factors and

- Sub-design 2: 72 design points for all 13 noise factors.

Both designs are finally crossed. With this resulting design, the initially calculated number of $2.5 * 10^{27}$ design points was finally reduced to a total number of 12.096 design points. To handle stochastic processes within each simulation run, the number of replications of each design point was set to 20. This leads to a total number of simulation runs of 241.920.

4.0 RESULTS

The scenario was implemented using the German PAXSEM simulation model and the design of experiment was processed using the German Data Farming environment. All 241.920 simulation runs have been computed on a German HPC with 512 nodes which took around 20 hours to compute the entire experiment.

In an initial analytic step all input parameters have been verified to be in the correct range, full spacing and nearly orthogonal. The distribution of the two MOEs is as follows: the average number of own casualties has a mean of 2.2 and a standard deviation (SD) of 3.4, which is described in percentage a value of 5,2% with a standard deviation of 9.1%. The 25% quartile with 0 casualties indicates, that throughout all simulation runs at least 25% have no own casualties. 75% of all runs have 3 or less casualties.

4.1   1st sub-question: finding most robust COP configurations

To demonstrate the various possibilities in doing Data Farming analyses, two different analysis approaches have been used.

MOE1 "percentage of blue casualties" was used in conjunction with a quadratic loss function (LossFnk = %blueCasualties²) to take into account both the mean value and the deviation. If both values are low, the COP configuration is robust and therefore should perform consistently well.

The partition tree of the LossFnk in Figure 4 depicts that the major critical success factor to minimize the loss function is the number of dismounted soldiers within the COP (represented as #light MG & #rifles). If a relatively high number of dismounted soldiers are available, then the targeting precision becomes the second most important factor. This is achieved either through a larger number of precise guided rockets (>=3) or, if this is not possible, through a medium/high soldier proficiency level. Further splits in the partition tree did not significantly improve the coefficient of determination (R^2) which is at 28%. This implies that all other factors – especially additional sensor systems like UAVs or OPs and joint fire support assets do not have a significant influence on the MOE in the given setup. Additionally regression models were deployed but they did not provide further insights.

Sub-question 1 can be answered as follows: A robust COP configuration is a large COP with at least 40 well trained soldiers well equipped with guided rockets.

Regarding MOE2 (total number of own casualties) the data set was handled with the following restrictions: Only data points are used where the MOE2 has zero losses (any loss of soldiers was declared to be unacceptable and the COP size does not exceed 40 dismounted soldiers.
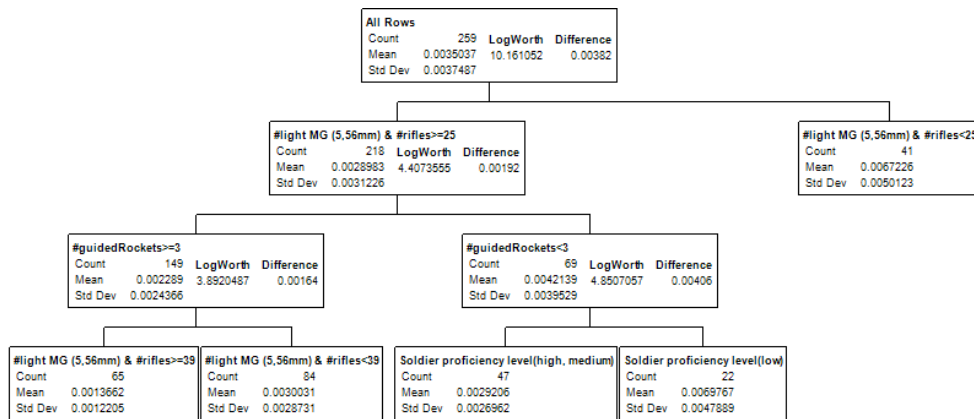
Figure 4: Regression tree for LossFnk(%blueCasualties)

These restrictions imply a data subset which was then analyzed. This effect-based approach identified the following requirements for a mid-size COP to perform consistently well, which were derived from the extant values of the decision factors:

- Ammunition factor of own forces >= 2 and number of guided rockets >= 2

- 1 medium UAV or 2 small UAVs

- Mortar tactics: 1 inside COP & 1 outside COP with at least one observation tower outside COP

- 1 QRT

- fixed wing or artillery joint fire support available

- Low latency for joint fire assets (i.e., less than 18 minutes for artillery)

4.2   2nd sub-question: performance of the most robust COP against the most dangerous threat

In order to determine the most dangerous threat, the above described approach was repeated, but this time focusing on the noise factors that have the most critical influence on the value of own casualties. The right splits of the partition tree in Figure 5 show those main influencing noise factors (R^2 is 90%). Casualties are more likely when opposed to a large enemy group (>60) at a high proficiency level. Another insight could be won as large enemy groups imperatively coincide with the tactics "Force on Force Large Group". Thus, force on force combat should be avoided when facing large groups.
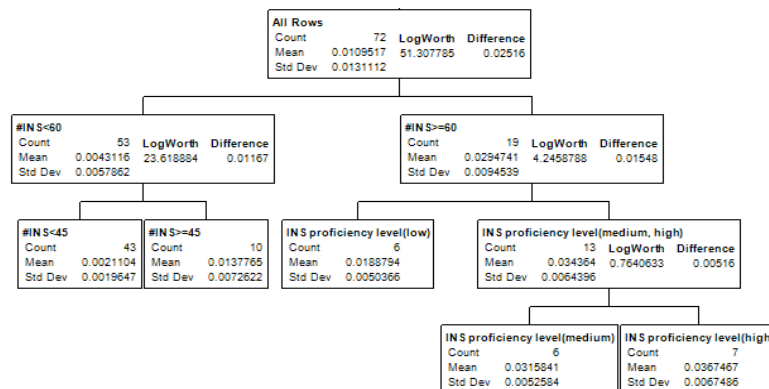

Figure 5: partition tree for the loss function (%own asualties²) by noise factors

To calculate the performance of the most robust COP configuration against the most dangerous threat the data sample was again limited. Here the advantage of crossing the decision factor design with the noise factor design allows to directly build this subset without the need to rerun a new Data Farming experiment using a new design with adjusted factor ranges. From the resulting subset, comprising only those simulations runs leading to the desired end state, the values of the relevant MOEs were then compared to those of the overall data.

Figure 6 shows the results of this comparison: the most robust COP can significantly reduce the mean of the total number of blue casualties compared to the average of all possible blue configurations to almost half from (nominal) 6.44 to 3.3 which represents a reduction of 68% (14.5% to 4.6%).
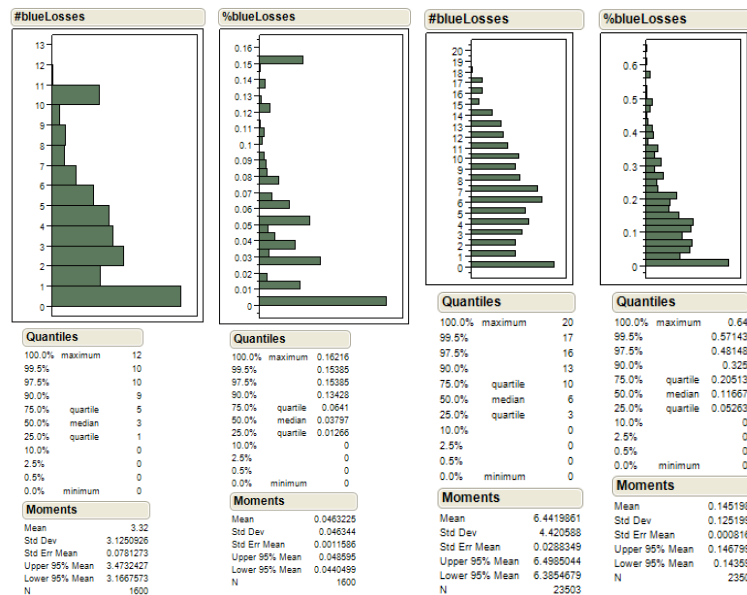
Figure 6: Performance of the most robust COP configuration (left) and all COP configurations
(right) against the most dangerous threat

4.3 3rd sub-question: find circumstances where joint fire support can improve the survivability of the COP

The 3rd sub-question was basically co-answered with the 1st sub-question. If there is a large size COP the joint fire support does not have an influence on the outcome. The COP can autonomously defeat all types of enemy attacks. But if there is only a mid-size COP, the joint fire support does have a significant impact on the outcome. Then early detection of the enemy forces (i.e., UAVs and OPs are required), an early identification through the QRT and low latency times until the joint fire support is available are most decisive and hence most valuable.

4.4 Discussion about the validity of the results

The simulation model PAXSEM uses several methods to ensure that the model is verified, starting from simple unit tests to automated test procedures of complex scenarios. Besides that, many technical system models like the PAXSEM electro-optical sensor model are either validated or at least calibrated using real performance data. Nonetheless the validation of a whole system as agent based models is not trivial if possible at all. In this case study, a face validation of single scenario configurations was performed by military subject of matter experts (SMEs) to ensure that the scenario matches to realistic behaviours e.g., threat scenarios and behaviours that are known from current missions (NATO 2002 [6]). This approach allows to robustly generate qualitative results whereas quantitative results need to be deliberately treated.

5.0 CONCLUSIONS

Through the "Force Protection" case study of NATO's MSG-088 a Data Farming experiment based on an operational military question could be successfully set up and conducted in a combined NATO environment as described in this paper. All six realms of Data Farming have been integrated as compulsory elements to all Data Farming activities. Due to all the valuable inputs from experts in the military, DoE and M&S fields, it has been possible to develop and implement a realistic scenario, to define an appropriate Design of Experiment, to compute the simulation runs on an HPC and to conduct the analysis on the Data Farming results in order to finally answer the overall research question and the three subquestions of this case study.

From an operational perspective, this project has made valuable use of the advantages of simulation applications when examining situations that are undoable in the real world due to

- safety reasons (e.g., duel situation)

- the scarcity of budgetary resources and the scarcity of materialized resources (e.g., availability of personnel / equipment for experiment purposes)

- feasibility (e.g., two party combat based on attrition)

- sense making (time-consumption to traverse all possible parameter combinations).

The results have provided answers to the operational questions at the desired level of detail. Justified by any existing interest of operational NATO entities, an in-depth experiment along specific situations and settings would be a valid consequent step. This approach might as well involve the examination of geo-specific data of on-going NATO missions.

The execution of this project has offered all participating nations (irrespective their individual background) the occasion to gain insights, witness the modus operandi as regards Data Farming and evaluate the potential benefits thereof for their national type of operational problems. An outstanding benefit is related with the lowering of the barriers of entry as for participating nations with scarce resources for identification and exploitation of modern technologies. MSG-088 therefore has proved to be a valuable mediation of a complex technology undertaken in a combined and comprehensive approach.

For all military leaders, this project represents an invitation to consider the support of simulation-based analyses for their decisions. The deeper the experimentation group can dig into the parameters of the underlying problem, the more distinct the recommendations can be. In other words: Data Farming needs serious input (i.e., assumptions, mission-specific knowledge, technical system data) in order to generate highly dependable output.

This might turn out to be a vicious cycle. Hence, one is well advised to permanently work on both sides: the quality of the input and the quality of the output.

6.0 ACKNOWLEDGEMENTS

7.0 REFERENCES

[1] Brandstein, A. and Horne, G. 1998. "Data Farming: A metatechnique for research in the 21st century." Maneuver Warfare Science 1998, Marine Corps Combat Development Command Publication, Quantico, Virginia.

[2] Bleicher, K. 2004. "Konzept Integriertes Management." Campus : Frankfurt.

[3] Horne, G. and Meyer, T. 2004. "Data Farming: Discovering Surprise." In: Ingalls, R, Rossetti, M.D., Smith, J. S. and Peters, B. A. (eds.) Proceedings of the 2004 Winter Simulation Conference, p. 171-180. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

[4] Horne, G. and Meyer, T. 2010. "Data Farming and Defense Applications." Proceedings of the MODSIM World 2010 Conference, Hampton Roads, Virginia. (Awarded Best Paper Overall.)

[5] ITIS 2011. "Leitfaden simulationsgestützte Analysen in der Bundeswehr." Code of best practice of simulation based analyses in the German Armed Forces.

[6] NATO 2002. "NATO Code of Best Practice for C2 Assessment." Accessed June 12th, 2012. http://www.dodccrp.org/files/NATO_COBP.pdf.

[7] Sanchez, S. M. 2006. "Work smarter, not harder: guidelines for designing simulation experiments." In: Perrone, L.F., Wieland, F.P., Liu, J., Lawson, B.G., Nicol, D.M. and Fujimoto, R.M., (eds.) Proceedings of the 2006 Winter Simulation Conference, p. 47-57. Piscataway, NJ: Institute of Electrical and Electronic Engineers, Inc.

[8] Vieira Jr., H., Sanchez, S.M. Kienitz, K.H. and Belderrain, M.C.N. 2011. "Improved efficient, nearly orthogonal, nearly balanced mixed designs." Jain, S., Creasey, R. R., Himmelspach, J., White, K. P. and M. Fu., M. (eds.) Proceedings of the 2006 Winter Simulation Conference, Piscataway, NJ: Institute of Electrical and Electronics Engineers, Inc.

[9] Woolridge, M. 2002. "Intelligent Agents: The Key Concepts." In: Woolridge, M. (ed.) Multi-Agent Systems and Applications II, p. 151-190, Berlin, Heidelberg: Springer.

[10] NATO STO 2013. MSG-088 "Data Farming in Support of NATO". Technical Report.