Building Trust in Autonomous Systems: Opportunities for Modelling and Simulation

Thomas Mansfield[1(✉)], Pilar Caamaño[1], Sasha Blue Godfrey[1], Arnau Carrera[1], Alberto Tremori[1], Girish Nandakumar[2], Kevin Moberly[2], Jeremiah Cronin[2], and Serge Da Deppo[3]

[1] NATO STO Centre for Maritime Research and Experimentation, Viale San Bartolomeo 400, La Spezia, Italy
{thomas.mansfield,pilar.caamano,sasha.godfrey,arnau.carrera,alberto.tremori}@cmre.nato.int
[2] Old Dominion University, 5115 Hampton Blvd, Norfolk, VA, USA
{gnand002,kmoberly,jcronin}@odu.edu
[3] NATO ACT Innovation Hub, 4111 Monarch Way, Norfolk, VA, USA
serge.dadeppo@innovationhub-act.org

Abstract. Advances in artificial intelligence and robotics development are providing the technical abilities that will allow autonomous systems to perform complex tasks in uncertain situations. Despite these technical advances, a lack of human trust leads to inefficient system deployment, increases supervision workload and fails to remove humans from harm's way. Conversely, excessive trust in autonomous systems may lead to increased risks and potentially catastrophic mission failure. In response to this challenge, trusted autonomy is the emerging scientific field aiming at establishing the foundations and framework for developing trusted autonomous systems.

This paper investigates the use of modelling and simulation (M&S) to advance research into trusted autonomy. The work focuses on a comprehensive M&S-based synthetic environment to monitor operator inputs and provide outputs in a series of interactive, end-user driven events designed to better understand trust and autonomous systems.

As part of this analysis, a suite of prototype model-based planning, simulation and analysis tools have been designed, developed and tested in the first of a series of distributed interactive events. In each of these events, the applied M&S methodologies were assessed for their ability to answer the question; what are the key mechanisms that affect trust in autonomous systems?

The potential shown by M&S throughout this work paves the way for a wide range of future applications that can be used to better understand trust in autonomous systems and remove a key barrier to their wide-spread adoption in the future of defense.

Keywords: Modelling and simulation · Trusted autonomy · Model based systems engineering · Future of defense

© Springer Nature Switzerland AG 2022
J. Mazal et al. (Eds.): MESAS 2021, LNCS 13207, pp. 424–439, 2022.
https://doi.org/10.1007/978-3-030-98260-7_27

1 An Introduction to Trust and Autonomous Systems

Despite continued advances in artificial intelligence and robotics development that provide the technical abilities that will allow autonomous systems to perform complex tasks in uncertain situations, incorrect levels of trust are a key barrier preventing autonomous systems from fully achieving their potential. A lack of trust leads to inefficient system deployment, increases supervision workload and, under certain conditions, could lead to potentially catastrophic mission failure.

In response to this challenge, trusted autonomy is an emerging scientific field aiming at establishing the foundations and framework for developing trusted autonomous systems. One area of research within this field is working to identify the mechanisms that affect human trust in autonomous systems. The first line of research in this field is defining standard methods to measure changes in human trust while training, operating and making decisions based data obtained from of autonomous systems. A second research track is working to identify methods that allow humans to better understand autonomous system behaviors and the operation of emerging technologies in order to encourage the correct level of trust to be obtained. Despite these efforts, challenges stem from the rapid pace of system capability and complexity. As autonomous systems rapidly evolve, the opportunities for humans to interact with systems and manually understand data sets generated by their use is reduced. Further, the accelerating complexity of emerging technologies and sophistication of autonomous system decision making is placing pressure on the pace of progress in the field of trusted autonomy.

Building upon the recent successes of using model-based methodologies in the communication of emerging technologies and systems [1, 2], the focus of this paper is the design and test of the first iteration of a model based framework that, coupled with existing wargame approaches, promise to provide a powerful technology analysis capability. Utilizing standardized modelling and simulation (M&S) approaches, the framework provides two layers of support; the first allows users to interact with emerging technologies and to understand the behavior of autonomous systems. Secondly, the model-based framework supports the collection of actionable data to reveal changes to the player's level of trust throughout system operation.

The remainder of the paper provides a review of related work in Sect. 2 and a description of the framework's architectural design in Sect. 3 before discussing initial test results in Sect. 4 and highlighting the main conclusions in Sect. 5.

2 Related Work: Trusted Autonomy and Measuring Trust

2.1 What is Trust?

In the field of Trusted Autonomy [3], a single definition of trust is emerging and beginning to be widely adopted. This definition of trust is:

> **"Trust is the attitude that an agent will help achieve an individual's goals in a situation characterized by uncertainty and vulnerability"** [4, 5]

Within this definition there are two important elements that must be present in any experiment investigating the concept of trust:

1. Uncertainty [6] – The problem is not simple or trivial, there must be an element within the scenario that the trustor does not fully control. However, the trustor must have an inherent understanding of the trustee's ability to achieve goals.
2. Vulnerability [6, 7] – The presence of vulnerability implies the trustor will be less likely to relinquish control in the presence of low trust. The need for there to be a 'loss' to the trustor is vital in order to test, understand and measure system trust. Without it, trust is not important and players will just play with interesting things.

While a single, common definition of trust is emerging in current literature, the field of trusted autonomy has not yet established a single, agreed and effective measure of trust. The primary challenge with the measurement of trust is that it is an abstract, human opinion that is difficult to record in a robust or reliable manner. A popular way to address this shortcoming in the field of trusted autonomy is to instead measure the reliance that a user has on a system, inferring trust based on the reliance the human has on the system under test [8]. In the process of inferring trust from reliance, other factors that contribute to reliance, such as perceived risk and self-confidence must also be considered [9, 10]. A typical causal flow, highlighting some of the key interrelations among human, machine and environmental factors in the context of user trust in depicted in Fig. 1.

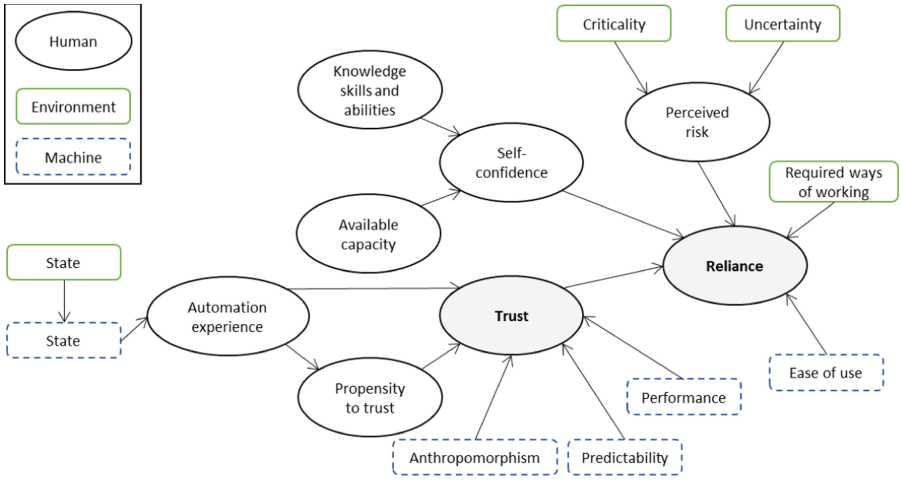

Fig. 1. A causal flow diagram summarizing the interactions that effect trust and reliance adapted from [8]

Based on this rationale, the investigation reported in this paper will focus on the measuring of autonomous system reliance and control the perceived risk and user self-confidence, allowing trust to be inferred.

2.2 How Can Reliance Be Measured?

While the measure of system reliance can be used to infer trust, measuring it still requires the consideration of challenging human aspects. Typical measures of reliance break down into three main methods; subjective surveys, measuring psychophysiological human characteristics and indirect assessment of behaviors influenced by trust.

Subjective surveys require humans to consciously report their level of trust. Difficulties exist with this measurement as not all humans can accurately characterize or understand their current trust attitudes or may not be willing to report their true attitude [11]. However, basic subjective surveys are often easy to implement in many military wargame settings and provide a source of actionable data.

To overcome the problems with subjective trust measurement, many researchers have tried to create objective measures of trust. One form of objective trust measures is to associate trust with different psychophysiological human characteristics, such as electroencephalography (EEG) [12] or galvanic skin response (GSR) [13]. Unfortunately, these measures need to be subsequently calibrated against some subjective measure of trust to ensure they provide a meaningful measure of trust. Additionally, the ability to measure psychophysiological human characteristics is significantly diminished due to practical barriers such as the common availability of technology and the extensive training required to operate it reliably.

Finally, a third form of trust measurement involves indirect assessment by measuring behaviors influenced by trust. This includes the ability to monitor and assess behaviors via the user's interaction with software [14]. This approach may be of particular value in projects based on the use of modelling and simulation methodologies which may result in the creation of interactive and immersive software applications.

2.3 When Can Reliance Be Measured?

Most experiments, games or events that focus on automation may be broken into three distinct sections; before, during and after the application of automation [5]. At each stage of the event, any direct or indirect measure of trust may be applied. Further, it is assumed that throughout this work the user will iteratively cycle through repeated stages, as shown in Fig. 2.

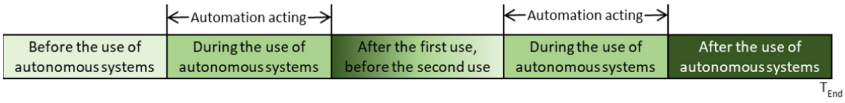

Fig. 2. Non-operational time may be before or after an automated event.

One clear example of an iterative approach [7], allowed players under pressure (money or a timer) to escape from a maze with the assistance of an autonomous, robotic guide. In the first iteration, the autonomous guide exhibited behaviors associated with the technology under test. The key aspects were also explained to the subjects using videos, images, or text and providing information that allowed the participant to evaluate the

risk associated with choosing to follow the robot. In a second iteration, the players were then asked to play a second time, with the option of not using the robotic guide. This selection was used to infer trust for each of the technologies under test.

Monitoring when the human takes action to activate the automation, as well as instances where the user does not take action, provide a good indication of the reliance the user has in the system [15]. It may also be noted that the underlying trust once the mission is complete is manifested differently when the human has authority to activate the automation rather than when the machine activates automation as the positive or negative response to their action is likely to strongly affect both the self-confidence and perceived risk of subsequent interactions with the autonomous system.

Once an automation has begun to act, the authority to turn an automation off will influence the way trust behaviors are expressed. When an automation is running, if the human can override the machine, an act of reliance will constitute inaction (i.e. he or she will choose to not turn it off). In this case, an act of non-reliance will look like turning the automation off. Once the automation has finished, another type of authority that could be monitored is the human decision to repeat or re-run the activity taken by the autonomous system. Authority for the human to repeat or re-run only pertains once the automation has completed its action.

2.4 NATO Investigation Frameworks

In order to investigate future technologies and their impact on future military missions, NATO typically utilizes a wargame framework known as the Disruptive Technology Assessment Game (DTAG) [16]. The DTAG flow, shown in Fig. 3, allows opposing blue and red teams to build upon a starting vignette, allowing likely confrontations to be played and understood.

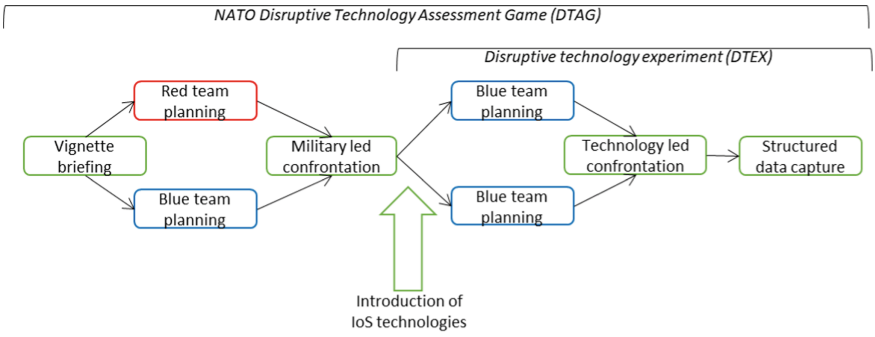

Fig. 3. DTAG framework, adapted from [16] (Color figure online)

Once this baseline has been set, new and emerging technologies are added into the wargame in the form of Ideas of Systems (IoSs). These ideas of systems briefly describe the key technologies, operational benefits and drawbacks of future technologies. Once understood by the game players, competing blue teams try to identify the best combined use of the technologies to achieve the vignette aims. Initially based on the DTAG model,

DTEX improves it and expands its range of application, through computer assisted processes, and distributed participation. The Disruptive Technology Experiment (DTEX) approach was created by the NATO Innovation Hub in Norfolk, Virginia, USA in partnership with Old Dominion University's Institute for Innovation and Entrepreneurship (IIE) and the NATO STO's Center for Maritime Research and Experimentation (CMRE) to reduce the time required to evaluate technologies, increase the level of input into the evaluation by leveraging virtual/distance methods, and employ synthetic environments (SENs), in addition to subject matter experts, to quickly provide outcomes based upon participants choices of ideas of systems. The objective was to create an approach that would allow the Innovation Hub to quickly and regularly test new ideas, concepts, and solutions sourced through its open innovation efforts such as the NATO Innovation Challenge.

3 Methodology: A DTEX Framework Based on Modelling and Simulation Approaches

This paper investigates the design and test of a framework that, based on the use of modelling and simulation methodologies, supports geographically distributed DTEX event which immerse the player into a scenario and collect data via subjective surveys and the indirect assessment of their decisions and software interactions. In this paper, the framework will be utilized to extract information about the level of trust users have during a scenario that relies on the successful operation of autonomous systems.

The design of the DTEX framework uses a model based approach to progress the design in three parallel and complementing streams: a gameplay stream, a human stream and a technology stream. Key attributes within each stream are listed in Fig. 4.

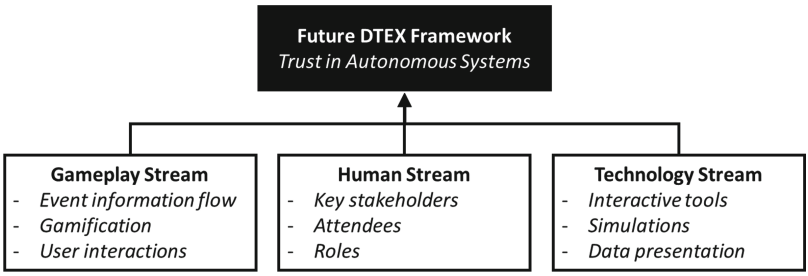

Fig. 4. Three areas of investigation

3.1 Gameplay Stream

A key principle of NATO's DTEX is to use a wargame to structure the interaction between competing blue teams. Within each team, gamification techniques provide the structure, rules and motivation to identify innovative solutions to challenging scenarios and record

the discussion points and rationale behind the decisions made. With a focus on investigating trust in autonomous systems, a series of key gameplay design decisions have been made and implemented. These design decisions focus largely on the flow of information provided to the players during the event along with managing their interactions with the supporting game tools.

Before the event, the pre-existing bias each player has with respect to their trust in autonomous systems is recorded via a subjective survey. The results of this survey are kept for later analysis following the completion of the gameplay activities. A description of the event objectives are then shared following this survey, allowing the event players to understand the topics to be addressed for the first time.

The first significant and tangible set of information provided to the players is a description of the scenario. The scenario describes how autonomous systems are currently used to survey a harbour following reports of suspicious behaviour by a terrorist organisation. The scenario also contains several motivating aspects for the timely and reliable completion of the mission with economic consequences of the harbour being closed coupled with a second concern about disrupting military peace keeping operations. Model based approaches were utilised to communicate the scenario in two specific ways; first the overall scenario was communicated in a view that forms part of the NATO Architectural Framework (NAF) guidance [17]. Secondly, specific technologies and interactions within the scenario need to be communicated within focus areas, such as operating behaviour and limits of autonomous underwater vehicles. The main advantages of using a model based approach to communicate the scenario content is the ability to quickly and effectively brief players with a varied range of skills and previous experiences with the key scenario elements in an intuitive and understandable way. Further, the approach provides the tools required to monitor player interactions at this stage of the event, highlighting areas in which users may have limited or differing experience (Fig. 5).

Following the explanation of the scenario, the players move into a series of three iterating confrontation stages. Implementing the iterative autonomy approach described in Sect. 2.3 of this paper, the approach provides multiple opportunities for the players to engage the autonomous systems, allowing each team member's self-confidence and perceived risk of the system to change and be monitored depending on the success of pervious events.

The first execution of the scenario is contained within a Baseline Confrontation in which none of the IoS technologies are incorporated. The main motivations for this baseline confrontation are to reinforce and further illustrate the key events of the scenario and allow the players to better understand the current operation and limitations of autonomous systems while beginning to build momentum and an understanding of the DTEX event stages. At the end of the baseline confrontation, the outputs of the autonomous systems are presented and the players are asked if they trust the results enough to reopen the harbour to traffic. This final question again, clearly asking if the user trusts the system enough to open the harbour to traffic, provides an opportunity to record the player's trust in autonomous systems and allow a comparison with the biases recorded at the start of the event. The structure of this baseline confrontation also provides the event controllers the potential to investigate ability to normalise the

Fig. 5. A NAF scenario overview. Each symbol and number shown in the map signifies a briefing focus area.

level of trust the teams have in autonomous systems; if the players show a higher than average level of trust in the systems, the results shown here could show the autonomous systems performing poorly, potentially lowering their trust before the subsequent confrontations. Conversely, if a team has been shown to be sceptical of autonomous system performance and low levels of trust are shown, the results of very successful autonomous system operation could be communicated prior to subsequent runs of the scenario.

Following the completion of the baseline confrontation, the first of two IoS technology-assisted confrontations is played. The technology assisted confrontations first require the players to review and discuss a wide range of potential future technologies that may assist them in the execution of the scenario and the analysis of the autonomous system outputs. A key consideration in the design of the DTEX framework is in supporting and recording the discussion within each blue team in an attempt to identify the anticipated benefits and drawbacks of each of the IoS technologies. Due to the fact that in this first event, the teams will be presented with over 60 separate IoS technologies, the DTEX framework has been designed to support their analysis in two stages. The first stage involves a quick sort of the technologies focusses on the initial reaction following the review of a small set of supporting information including the technology name, method of operation and key benefits. The IoS card technologies that the teams consider suitable for further investigation are added to a technology shortlist. This shortlist then forms the basis for the following activity in the confrontation where the teams are asked to discuss and combine technologies, resulting in a final three technologies that will be applied to a re-run of the scenario. Each run provides an augmented data set on which the teams can decide whether to open the harbour for traffic. This decision point, where the players are presented with an updated set of autonomous system outputs and asked to make a decision, again provides an opportunity to collect

information on their level of system trust with a further subjective survey. The change in trust implied by the survey results provides a data set that may allow the effectiveness of the technologies used to be assessed, a key output from this activity.

A second technology based confrontation allows the player's learning to be applied, repeating all of the technology shortlisting and review actions form the previous spiral to be executed, providing an opportunity for each team's experiences and learning to be discussed during the selection of an updated technology combination. The DTEX event ends with a recap of the key activities and a request to support any further, offline exchanges of information in the coming days. An overview of the complete, model-based gameplay stream designed for the event is provided in Fig. 6.

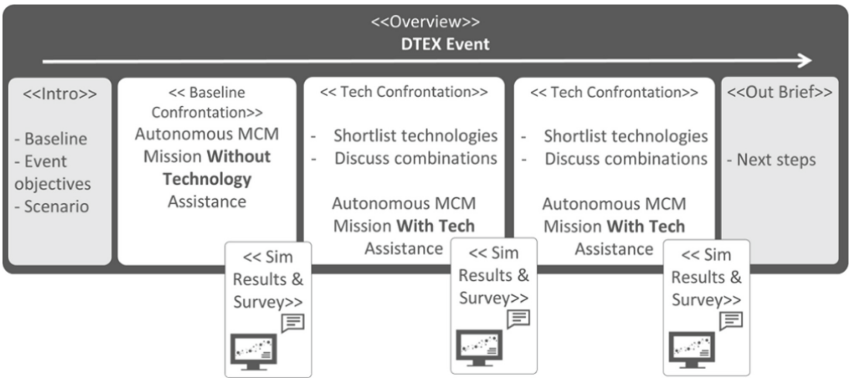

Fig. 6. Overview of the designed DTEX gameplay stream

3.2 Technology Stream

To support the identified DTEX event gameplay stream, a range of modelling based technologies have been employed that allow it to be executed effectively and efficiently in an online, distributed environment. The complete event is designed to be executed on a range of commercially available video-conferencing (VTC) platforms, the key requirements of which are ease of access to allow all participants to join and video recording, allowing subsequent analysis of the team's discussion and software interaction.

Model based methodologies, applied at a technical level, allowed the design of an interactive and intuitive NAF-based dashboard. This web-based dashboard provides a range of user specific views, via the login options in Fig. 7, that guide the user through the complete DTEX event. Figure 8 provides one example of the ability to communicate key event structures, where an interactive and linked NAF view of the game flow is presented.

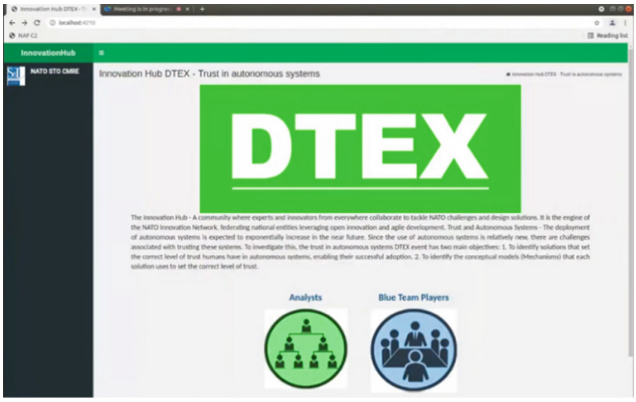

Fig. 7. A screenshot of the NAF-based dashboard allowing customised login

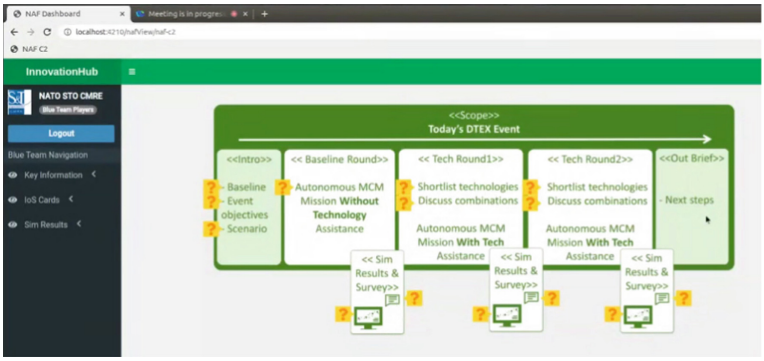

Fig. 8. A screenshot providing players with an interactive and navigable overview of the DTEX event

The availability of this prototypical dashboard allows all of the subsequent technology stream developments to be linked and utilized by the players. Ordered by game flow, the first role of the technology is to support the elicitation of information from the teams in a series of subjective surveys. These surveys utilized online questionnaire provider platforms [18] to create intuitive and interactive surveys that could be linked to the relevant sections of the NAF gameplay flow in the dashboard. The results of each survey can be saved and stored for analysis after the event.

A range of M&S technologies have been applied to support the articulation of the event scenario. With an example provided in Fig. 9 where the operation and limitations of an autonomous underwater vehicle is being investigated, multi-media visualizations have been created to provide intuitive information concerning all of the key scenario technologies and events.

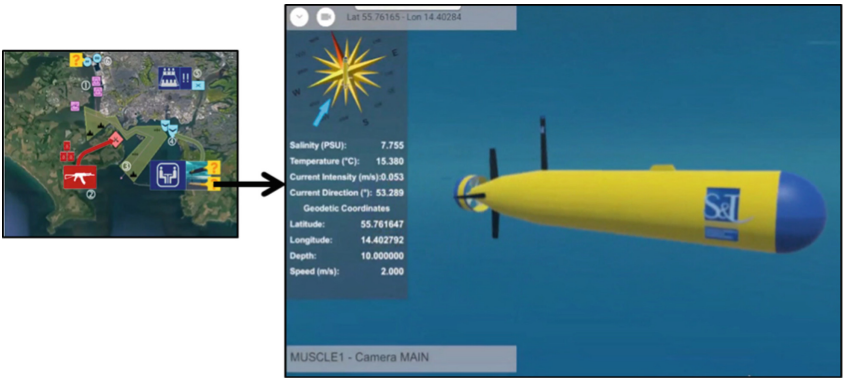

Fig. 9. Linked information allowing users to investigate specific scenario aspects

The multi-media explanations of key scenario events prepare the players for the execution of the baseline confrontation. This confrontation, along with the subsequent iterations, utilizes a complete federation of simulators to execute the scenario without the need for human intervention. Within this scenario, key autonomous system aspects such as asset motion, sensor performance and on-board processing capabilities, run as if the mission were being completed in the scenario area. The federation logs results of the scenario so that they can be displayed after confrontation, as required by the gameplay stream. In the second and third confrontation, the simulation and its related results also consider the IoS technologies selected by the teams. The presence of these technologies affect the performance of the system, altering the quality and quantity of the results presented to the teams at the end of the confrontation. This varying set of simulation generated data, with examples shown in Fig. 10 and Fig. 11, provide a key input that will alter the team's response to the final question, asking if they would reopen the harbor, and allow an estimate of the ability for the technology to shape trust to be made.

In addition to providing a framework around the M&S federation that runs the scenario and generates technology dependent results, the NAF–based dashboard also provides a number of tools that support the shortlisting and analysis of the IoS technologies provided to each team. To support shortlisting, a user interface has been developed that provides players with an overview of key IoS information and three options; to discard, shortlist or potentially consider its inclusion in the confrontation. An example of this functionality is contained in Fig. 12. Once complete, a second stage in the shortlisting process allows the players to review and modify their shortlisted cards, with the option to discard further technologies if desired or required. Once a suitable shortlist has been established, the NAF-based dashboard stimulates group discussion by providing the players with the capability to graphically drag, drop and sort the cards into a series of editable categories. A screenshot of this functionality, shown directly after the completion of card shortlisting, is provided in Fig. 13.

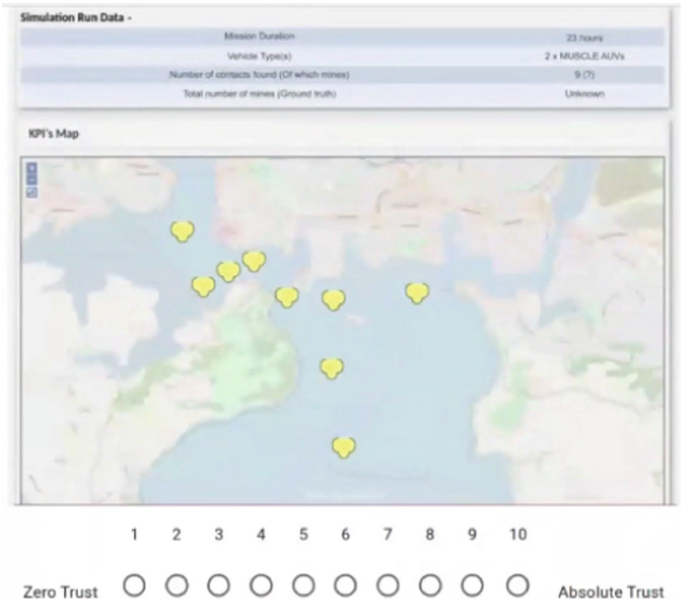

Fig. 10. Basic simulation outputs before the application of IoS technologies

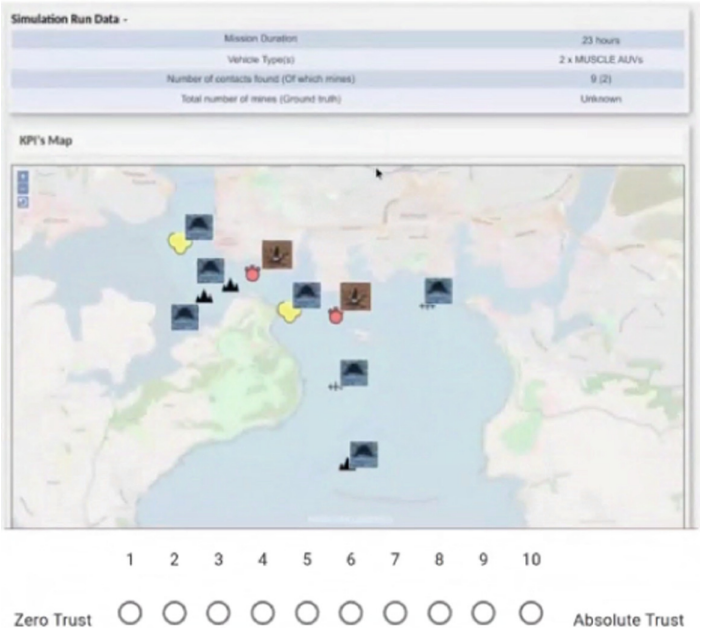

Fig. 11. Simulation outputs augmented with additional information following the application of IoS technologies

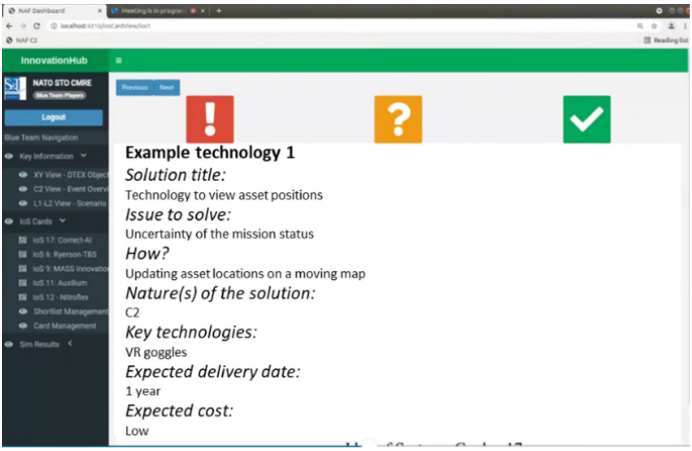

Fig. 12. A screenshot of the teams rapidly selecting or discounting cards using the '!', '?' and '✓' buttons

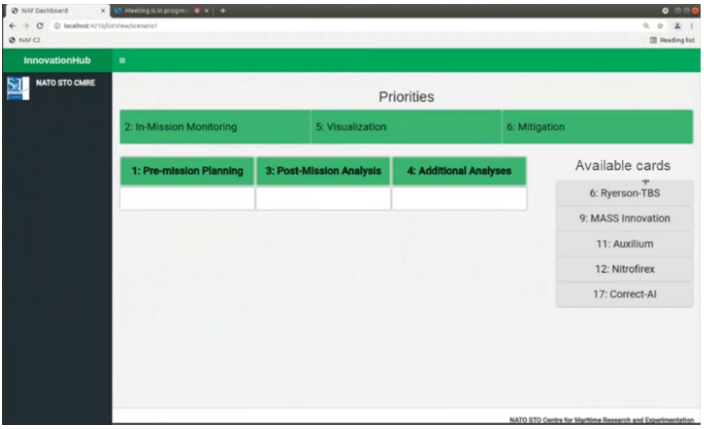

Fig. 13. A screenshot of functionality that allows team members to graphically sort, group and organise selected cards

By combining all of these tools and capabilities into one, seamless framework that can be utilized by all geographically distributed team members provides a technical solution to all of the interactions envisioned in the gameplay steam design.

3.3 Human Stream

Despite the technical nature of the trust in autonomous systems topic and the large number of IoS technologies to be assessed, the presence of the NAF-dashboard and model based approaches utilised in its design increase the ability to include players from communities outside maritime autonomous systems, providing access to other skills and experiences. This allows the test of the platform, and the acquisition of valuable

data on the technologies that are likely to affect trust in autonomous systems, to be executed without further detailed consideration of the human stream. Each DTEX event should contain blue team players that are external to the design activities described in this document and should be facilitated by team members that can assist with time-management and ensure the correct use of the prototype tools. In addition, observers in both M&S and gameplay development activities may be present during the DTEX event to drive further improvements to the approach.

4 Event Execution Results and Discussion

The distributed, model-based DTEX framework discussed in this paper was tested in a NATO DTEX prototype trial event in June 2021. The event, advertised with the flyer shown in Fig. 14, allowed the complete set of tools linked within the NAF-based dashboard to be utilized to guide a single blue-team consisting of two players through the process. While limitations were present in the form of reduced IoS technology coverage, lower simulation fidelity and few blue team players, observers could comment on all event stages. Further, the blue team players were provided with the opportunity to comment on the success of the event.

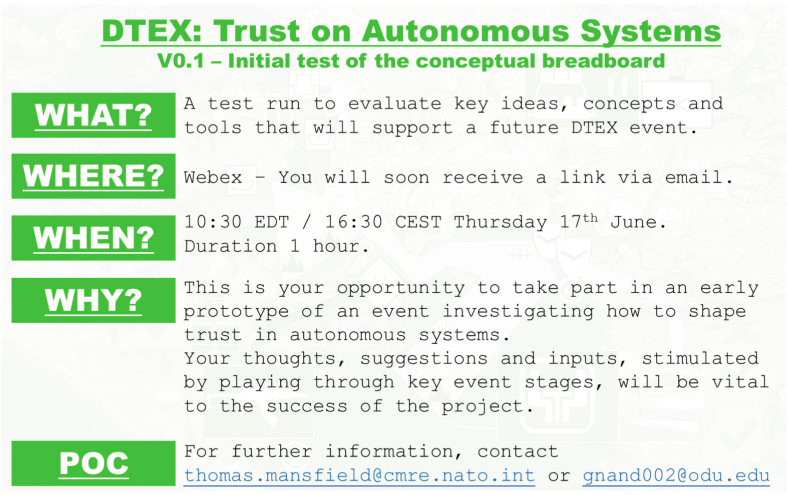

Fig. 14. Invitation to the first test of the DTEX framework prototype

Feedback from the observers and players identified that the structure of the event was clear and all participants could contribute where required. One particular success in this area stemmed from the fact that the players in the blue team had vastly differing levels of experience of autonomous systems prior to the event, with one player expert on their use and another a relative newcomer to the subject. The use of the NAF-based dashboard and all of the linked capabilities provided a common reference point that allowed both players to contribute their opinions in search for the optimal selection of technologies.

This task is likely to have been very difficult in the absence of such a clear and intuitive toolset providing a common reference point for both players' opinions. Conversely, one potential shortcoming of the designed architecture was observed in the collecting of information in the subjective surveys. One survey was provided per team and consensus was required to reply with a single, integer on a scale of trust. Due in part to the differing backgrounds of the blue team players, achieving consensus was not always possible. While the discussion this prompted was useful in the assessment of the technologies, there may be a future opportunity to allow the players to respond separately or to input their perceived level of trust onto a non-numeric scale.

5 Conclusion and Future Activities

The work reported in this paper marks a first step in exploring the ability of emerging and potentially disruptive technologies to shape human trust in autonomous systems in the context of maritime military deployments. The final objectives of the work are to identify the emerging technologies that most effectively set the correct level of human trust in autonomous systems, allowing the conceptual models (mechanisms) that each solution uses to set the correct level of trust to be identified and understood.

In pursuit of these objectives, this paper presents the development of a future distributed and simulation based DTEX framework that uses model-based methodologies to communicate complex information in an intuitive and accessible manner. This framework has been designed and tested in an NATO project exploring correctly setting trust in autonomous systems, supporting an analysis into the opportunities for a future M&S-based synthetic environment to monitor operator inputs and provide outputs in a series of interactive, end-user driven events. In this specific event, M&S methodologies and techniques were applied to answer the questions; how and when can trust be measured?

Further work is now planned to continue the development of this prototype framework, increasing simulation fidelity and improving the capability to support the communication of the scenario and the collection of simulation results with the full set of IoS technologies. It is anticipated that multiple, reusable, easily configurable synthetic environments will be developed, creating a library from which to draw upon for future DTEX depending on the problem space addressed by specific exercises. This will enable rapid creation of events. To improve the ability of the framework to measure trust, further work is planned to move away from the current reliance of subjective surveys and further increase the ability of the framework to obtain actionable data by monitoring and analyzing player's software interactions throughout the wargame.

All three streams of the model-based framework identified in this paper are intended to remain as a persistent capability, allowing M&S methodologies to support the analysis of a wide range of emerging technologies in a across a broad spectrum of domains, disciplines and activities.

Acknowledgements. The work reported in this paper has been funded by NATO Allied Command Transformation (ACT) Innovation Hub.

References

1. de Rosa, F., Mansfield, T., Jousselme, A.-L., Tremori, A.: Modelling key performance indicators for improved performance assessment in persistent maritime surveillance projects. In: Ahram, T.Z., Karwowski, W., Kalra, J. (eds.) AHFE 2021. LNNS, vol. 271, pp. 295–303. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-80624-8_37
2. Harper, A., Navonil, M., Yearworth, M.: Facets of trust in simulation studies. Eur. J. Oper. Res. **189**, 197–213 (2021)
3. Abbass, H.A., Scholz, J., Reid, D.J. (eds.): Foundations of Trusted Autonomy. SSDC, vol. 117. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-64816-3
4. Lee, J.D., See, K.A.: Trust in automation: designing for appropriate reliance. Hum. Factors J. Hum. Factors Ergon. Soc. **461**(1), 50–80 (2004)
5. Bindewald, J.M., Rusnock, C.F., Miller, M.E.: Measuring human trust behavior in human-machine teams. In: Cassenti, D.N. (ed.) AHFE 2017. AISC, vol. 591, pp. 47–58. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-60591-3_5
6. Evans, A.M., Revelle, W.: Survey and behavioral measurements of interpersonal trust. J. Res. Pers. **46**(2), 1585–1593 (2008)
7. Robinette, P., Wagner, A.R., Howard, A.M.: Investigating human-robot trust in emergency scenarios: methodological lessons learned. In: Mittu, R., Sofge, D., Wagner, A., Lawless, W.F. (eds.) Robust Intelligence and Trust in Autonomous Systems, pp. 143–166. Springer, Boston (2016). https://doi.org/10.1007/978-1-4899-7668-0_8
8. Rusnock, C.F., Miller, M.E., Bindewald, J.M.: Framework for trust in human-automation teams. In: Industrial and Systems Engineering Conference, Pittsburg, USA (2017)
9. Johnson, N., Patron, P., Lane, D.: The importance of trust between operator and AUV: crossing the human/computer language barrier. In: OCEANS 2007, Aberdeen, UK (2007)
10. Wu, X., Stuck, R.E., Rekleitis, I., Beer, J.M.: Towards a framework for human factors in underwater robotics. Proc. Hum. Factors Ergon. Soc. Ann. Meet. **59**(1), 1115–1119 (2016)
11. OECD: Measuring trust. In: OECD Guidelines on Measuring Trust, Paris, France, pp. 115–154. OECD (2017)
12. Hu, W.-L., Akash, K., Jain, N., Reid, T.: Real-time sensing of trust in human-machine interactions. Cyber-Phys. Hum.-Syst. **49**(32), 48–53 (2016)
13. Khawaji, A., Chen, F., Zhou, J., Marcus, N.: Using galvanic skin response (GSR) to measure trust and cognitive load in the text-chat environment. In: 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems, Seoul (2015)
14. Andre, H., Sihombing, P.P., Sfenrianto S., Wang, G.: Measuring consumer trust in online booking application. In: ICITISEE (2019)
15. Feigh, K.M., Dorneich, M.C., Hayes, C.C.: Toward a characterization of adaptive systems: a framework for researchers and system designers. Hum. Factors J. Hum. Factors Ergon. Soc **56**(4), 1008–1024 (2012)
16. NATO Allied Command Transformation: Disruptive Technology Assessment Game Handbook. NATO ACT, Norfolk, USA
17. North Atlantic Treaty Organization (NATO): NATO Architecture Framework. Architecture Capability Team Consultation. Command and Control Board, Brussels, Belgium (2018)
18. Google: Google - Create effortless forms. Google. https://www.google.com/forms/about/. Accessed 21 July 2021