Goals within Trust-based Digital Ecosystems

Emilia Cioroaica*, Akanksha Purohit†, Barbora Buhnova‡, and Daniel Schneider*
*Fraunhofer IESE, Kaiserslautern, Germany
†Technical University of Kaiserslautern, Kaiserslautern, ‡Masaryk University, Brno, Czech Republic
*{emilia.cioroaica, daniel.schneider}@iese.fraunhofer.de
†{apurohit@rhrk.uni-kl.de} ‡{buhnova@mail.muni.cz}

***Abstract*—Within a digital ecosystem, systems and actors form coalitions for achieving common and individual goals. In a constant motion of collaborative and competitive forces and faced with the risk of malicious attacks, ecosystem participants require strong guarantees of their collaborators' trustworthiness. Evidence of trustworthy behavior derived from runtime executions can provide these trust guarantees, given that clear definition and delimitation of trust concerns exist. Without them, a base for negotiating expectations, quantifying achievements and identifying strategical attacks cannot be established and attainment of strategic benefits relies solely on vulnerable collaborations. In this paper we examine the relationship between goals and trust and we introduce a formalism for goal representation. We delimit the trust concerns with anti-goals. The anti-goals set the boundaries within which we structure the trust analysis and build up evidence for motivated attacks.**

***Index Terms*—Digital Ecosystems, Software Ecosystems, Smart Ecosystems, Automotive Smart Ecosystem, Smart Grid, Trust, Goals, Tactics, Strategy.**

I. Introduction

Engineering digital ecosystems around open adaptive systems has become the enabler of technological advancements. Systems and devices from different manufacturers and even from different application domains interact and collaborate to achieve higher level goals, which would not be possible without such comprehensive collaboration. Moreover, there is a trend towards more continuous engineering, i.e. organizations and their developers dynamically enhance existing systems with runtime software updates that are continuously monitored.

We anticipate a stronger uptake of the agent-based system paradigm. Correspondingly, in the automotive domain for example, there would be smart software agents deployed on vehicles, that could also be updated dynamically at runtime. These smart agents can at the entry point of a highway collaborate with other vehicles for forming platoons. When driving in a platoon, vehicles benefit from reduced fuel consumption due to reduced air friction. However, the complex dynamics of collaborative and competitive forces existing in an ecosystem rise multiple trust concerns for all ecosystem participants. Especially when competitive forces are hidden within declared cooperations and lead to malicious attacks. At the lowest operational level, a vehicle accommodating a software update requires strong guarantees of trust from the smart software agent. Actors with declared collaborative goals that actually act in competition can insert malicious behavior together with the software update. Being received as black boxes by the host vehicle, these updates can contain intentional malicious logic faults introduced with the scope of causing harm. In the scenario provided above, the smart software agent can suddenly accelerate or decelerate and cause multiple car crashes within the platoon. Such a behavior can be caused by *logic bombs* [1] that remain dormant in the host for a certain amount of time, and trigger when an event happens or certain conditions are met.

Trust is an essential enabler for the emerging trend of digital ecosystems. Without trust, user acceptance and thus market success would be impacted or even prevented. Further, not only user trust is required, but also trust between companies and other stakeholders (e.g. legislators and official bodies). Both aspects translate into the requirement that systems in the field need to be have a basis for computing trust between themselves for enabling cooperative relationships to form dynamically between formerly unknown participants. But the creation of trust requires mechanisms for accounting entities to their actions, responses, achievements and failures in a way that also enables negotiations, decision making and ultimate identification of undesired behaviors. In this sense, goals are concepts that enable analysis and modelling of stakeholders interests and concerns [2]. A goal is an evidence of accepted objective fulfilled by system agents [3]. In the area of safety in particular, system functions, regarded in our work as operational goals, have been formalized for enabling safety argumentation. The top most priority of trust evaluation of systems operating in the field is their safety. Also, in the safety domain, a wide range of all possible deviations and formalization of operational goals have been defined. Therefore, at the operational level, it is enough to consider definition of anti-goals from safety as the one presented in [4]. For trust reasoning at higher levels, however, we adapt the goal formalization from the safety domain by considering a two-fold approach: identification of goal artifacts used in literature and analysis of directive documents, such as the ones from the European Commission.

Digital ecosystems until now have been engineered with considerations of separated trust concerns that have been focused on distinct areas such as robustness or user trust. But the hybrid and complex nature of ecosystems dynamics characterized by interactions among diverse actors such as users, businesses, official bodies, systems, system components and developers requires a unified consideration of trust concerns. Ecosystems need an instrument for health self-

regulation that can, for example support a trustworthy reaction of a developer to user demands through provision of on-the-fly software updates. Only through a self-regulating mechanism that enables continuous scrutiny of its health, an ecosystem can grow well. The health of an ecosystem is an indicator of how well the business performs [5].

In this paper, we examine the relationship between goals and trust and we introduce a formalism for goal representation. The formalism captures key aspects of goals, enables their expression in a natural language and tracing between multiple levels of computation. We consider goal evaluation to be the mechanism for self-regulating ecosystems, the one that can bring transparency in the trust building process and enable re-considerations of tactics and strategies. For this, we extend the previous platform for runtime prediction and trust computation [6] by considering the goals of ecosystem entities. In this way, evidence gained from runtime computations supports the tactical decisions of ecosystem entities and their strategic analysis, which in turn supports reconfiguration. Provided as an extension of a previous reference architecture for trust-based digital ecosystems we have introduced in [7], the current work continues with the demonstration of concepts expressiveness and reusability, by continuing with examples from the automotive and energy domains.

In the following, Section II presents an overview of digital ecosystems together with our vision of building trust. Section III presents the related work and concepts we use in defining the artifacts for goal definition from the trust perspective we introduce in Section IV. In Section V we present conclusions and future work.

II. Background

The systems around us have always been engineered for trust. Traditional design time activities have always been directed towards ensuring that at runtime the systems operate as expected. In recent years, however, systems have been designed to be open and adaptive, with the emergent fourth industrial revolution bringing system designs at completely new levels with challenging aspects for trust. For achieving acceptance, nowadays not only the systems are designed for being able to freely cooperate and collaborate with each other in unknown context, but the whole society is designed around emergent digital solutions [8]. The technological innovation in our daily lives is supported by a continuous and hybrid engineering process that extends outside system boundaries. Organizations, developers and even user behaviors are continuously engineered for supporting the development of a trusted digital society. This leads to the considerations of new structural and behavioral meta entities that are known as *digital ecosystems* [9], [10].

Generally, ecosystems emerge and evolve around the motivation and incentives of participating actors. The participation of an actor in an ecosystem is realized through the introduction or usage of a product that offers a service to other ecosystem participants. However, because actors may not have only collaborative goals, but competitive and malicious goals as well, a comprehensive trust analysis of ecosystem participants is needed. For this, we have introduced in [7] the concept of *trust-based digital ecosystems* that inspects digital ecosystems from a trust perspective. The reference architecture that we have proposed enables instantiation of digital twins for this type of ecosystems.

In this paper, we continue the work on defining architecture elements for trust-based digital ecosystems that exemplify the relationship between goals and trust. For this, we structure trust concerns at three levels: *strategic*, *tactical* and *operational*. From existing literature we extract goal artifacts that fit in the trust structure and we provide tracing between them. Tasks and decisions that drive the actions of entities participating in trustworthy collaborations have been classified in the literature at three hierarchical levels [11]. In our vision, this classification supports self-regulating mechanisms of digital ecosystems by enabling their re-organization, reconfiguration and decision making at all necessary major steps. For example, at the operational level, fail-over behavior can be triggered in case of detected failures. At the tactical level, cooperations can be adapted for ensuring achievement of strategic goals.

III. Related Work

Trust is the most noticeable factor in determining the effectiveness of a relationship [12]. Trust describes the positive expectation about behaviour of others in vulnerable situations. Scholars mainly differentiate between belief-based trust [13], [14] and computation-based trust [15], [16] regarding a quantified reputation. Studies have found that the development of trust and its continuation is a crucial factor, especially when coalitions are formed. Trust decreases the level of defensiveness and increases stability among the group or individuals participating in the trusted relationship. In this sense, the authors of [17] developed a framework in which trust is considered an internal state of trustor (trusting actor) who expects desirable behaviour from a trustee (trusted actor). The authors identified motivation, behaviour, and gratification to be intrinsic properties of a trustee. Motivation is the main driver for goal analysis. Long ago, motivation has also been considered to be a central factor in driving actions [18]. In our work we follow the same determinant for evaluating trust. Namely, in a top-down approach, the motivation defined at higher strategic levels is refined for different domains, quantified in tactical benefits within domains and mapped to responses of system operations. The responses are the ultimate evidence of implemented actions. Bottom up, close analysis of interrelation between operational goals propagates to upper tactical anti-goals to ultimately define strategic anti-goals and a ultimate malicious motivation. Similarly, in our work, for building trust, we trace down the motivation from the strategic level until the operational level. For the reasoning of motivational attacks, we trace evidence from the operational level until the strategic level, by following the correlations of *anti-goals*. In the process of argumenting planned attacks, tracing of operational anti-goals provide evidence of what is being done maliciously on the system (the *What?* of the

attack). Multiple malicious actions further on can describe attack tactics (the *How?*) and support evidence of motivational attacks at the level of strategic anti-goals (the *"Why?"* of the attack). By enabling analyses of responses we propagate evidence from runtime execution to tactical guarantees and satisfaction of initial strategic goals and anti-goals.

Multiple operations directed towards achieving strategic goals and anti-goals are performed within tactical context. According to [17], contextual properties are the ones that influence interactions within social grouping. In our work, the tactical benefits result into operational context. The operational context is part of the triggering condition for system functions.

Similar to the framework we present in this paper, the framework presented in [2] links trust to goals. It uses the agents and goal-oriented concepts to model and analyse multiple interests and how they might be addressed or compromised in alternative environments and systems. As we will describe in Subsection IV-C, focusing on the analysis of software behavior our platform follows a similar approach.

Later, the authors of [19] presented an extension of the previous framework using explicit trust characteristics and goal models to visualize and elicit trust expectations in relationships. They've concluded that when goal models can be analyzed, trust transparency increases. This can be achieved, for example, through visualization on how goal contributions and dependencies incline an actor's behaviour towards trust. We complement this work by considering anti-goals that support the deductive evidence of attack strategies.

The authors of [3] opt for precise semantics that describe wanted and unwanted system behaviors. In the same way, we center the interpretation of behavior on goal analysis that provide evidence for collaborative success factors, but we give the analysis of unwanted effects a separate path. We opt for this approach in order to enable a specialized process for deriving evidence and enable analysis of causes for attacks and failures. For analysis of goal satisfaction, the authors of [20] specify *objective functions* that are refined according to a goal model. In our work, the objective functions are operational goals.

Bosch in [10] was the first one to consider actors – businesses, suppliers and consumers – as acting entities in an ecosystem. "Undirected developers" are those who push innovation but at the same time are capable of introducing accidental or intended malicious behavior into the ecosystem. Further on, in [21] Bosch states the need to evaluate the value provided by the ecosystem partners. Companies may play different roles in different ecosystems. The strategy a company uses in engaging with other stakeholders may differ depending on the company's role in that ecosystem. In our work, ecosystem components represent the value that requires trust analysis.

Anti-goals have been firstly introduced in [22] as malicious obstacles that obstruct safety or security goals of systems. In our work, we start from anti-goals at the operational level, defined according to existing safety guidelines, and we extend the anti-goal definition at the higher levels of cooperative trust analysis. Through analysis of anti-goals, evidence for motivation of attacks can be deduced. Our anti-goal refinements correspond to the popular fault trees used for modeling and documentation of hazards in safety-critical systems [23] and to threat trees used for modeling and documenting potential attacks in security-critical systems [24], [25].

IV. Goals definition

As discussed previously, goals are concepts that account entities to their actions. They give a base for judging achievements and failures, as they enable negotiations and decision making. When represented in a machine-readable format, they support the automatic reasoning of trust, through runtime computation of reputation. For enabling goal representation, we continue with formalizing their definitions in three layers "strategic-tactical-operational". The strategic goals are given by high authorities, such as governments and associations of organizations.

From the tactical to the operational level, we follow a top-down approach, in a 4C step-wise-refinement of goals: From Cooperation, to Collaboration (tactical), Coordination and ultimate Communication (operational). We based our top-down argumentation and decomposition of goals on the work of Jones [26]. In this sense:

- **Cooperation** is the work on a task that shares the profits or benefits of doing so. It sets out a win-win benefit between two entities.
- **Collaboration** is the willingness of an actor to work jointly with another one on a given task. This can portray a mayor benefit for the entity requesting collaboration and a minor benefit for the collaborating entity.
- **Coordination** is the process of causing parts to function together in a proper order. There is no notion of benefit included here. At this level, systems, components, processes and tasks at most implement coordination mechanisms.
- **Communication** is the exchange of information and forms the basis for all the other upper C's concerns.

Starting from existing goal formalization practices used in the safety domain, such as the Goal Structure Notation(GSN) [27] [28], we continue with a two-fold approach for formalizing goals for trust. We use the goal artifacts identified in Section III and mapping of goal artifacts identified in the literature and safety formalism to information present in directive documents that present strategic developments of industries in Europe. We've then deepen the analysis of the European strategic goals by surveying directions into two major domains to which the directive document is pinpointing: the automotive and energy domains.

A. Formalization of Goals

For defining strategic goals, we have looked at the highest strategic directives in Europe and we have surveyed the European Green Deal [29]. In this regard, the European Commission is an actor of a digital ecosystem that states strategic goals for organizations that take part in the ecosystem. For example, the European Commission states that for achieving

the target for 2030 of reducing greenhouse gas emissions by at least 50% compared to 1990 levels, and no net emissions by 2050, it is essential for all sectors of economy to work towards a sustainable future. Policies needs to be reevaluated for clean energy supply across the economy, industry, production and consumption, to name a few. One of the main strategic goals of the European Commission is to transform the European economy while creating a sustainable future. For exemplification, in the current paper we provide a minimum sufficient number of examples. For more examples we direct the reader towards [30].

For the strategic goal, we have identified five different artifacts, namely:

- The **Ecosystem Entity** is the non-cyber-physical part of the ecosystem, to which a strategic goal is applied. It is the one that supports the consequences and/or the benefits.
- The **Response** is the desired property that the ecosystem entity is planned to hold over time.
- The **Stimulus** is the condition that triggers the initiation of the strategic goal.
- The **Motivation** is the incentive for creating the response of the strategic goal. It is a trigger for adapting ecosystem entity own behaviour towards goal achievement.
- The **Quantified strategic benefit** is a quantitative achievement of a goal.

In this way, a strategic goal can be expressed using natural language in the following way:

"***Ecosystem entity*** shall ***response*** when ***stimulus*** in the context of ***motivation*** with the benefit(s) ***quantified strategic benefit***."

Following the above structure, the following strategic goal have been defined based on the text in the document [29].

All sectors of EU economy shall ***adopt European Green Deal*** when ***tackling climate and environmental challenges*** for ***creating a sustainable economy*** with the benefit(s) ***of achieving no net emissions of greenhouse gases by 2050***.

For enabling the analysis of its fulfilment, we've further on decomposed strategic goals into *domain strategic goals*. One of these sectors of EU economy is the automotive domain which generates turnover of over 7% of EU GDP. One such group in the automotive domain is, ACEA (European Automobile Manufacturers Association (ACEA) [31], a group of 16 major European automobile manufacturers, advocates of automobile industry. The association acts as a portal to provide expert knowledge on vehicle related regulation in the field of modern transportation. ACEA transforms strategic goals of governments into strategic goals of automotive companies. For example, ACEA provides action plans that supports the achievement of targets defined in European Green Deal with respect to mobility.

The tracing between strategic goals and domain strategic goals is achieved through decomposition of the *response* of the *strategic goal* into a) more concrete statements that become the *motivation* for individual *domain specific strategic goals* and b) concrete *responses* of the entities that act in specific domains.

The template for defining domain strategic goals is:

"***Ecosystem entity*** shall ***response*** for ***motivation*** with the benefit(s) ***quantified strategic benefit***."

Based on the literature presented by ACEA, we have identified the following domain strategic goals.

(Automotive) Domain Strategic Goal 1: *Truck manufacturers and logistics operators* shall *enable connected driving* for *reducing fuel energy consumption and create a safer, cleaner and more efficient road transportation* with the benefit(s) of *reducing carbon emissions by up to 10%*.

(Automotive) Domain Strategic Goal 2: *The policy makers in automotive domain* shall *allow introduction of High Capacity Transport (HCT) systems* for *reducing CO2 emissions*, with the benefits of *reaching a reduction of 15% to 40% at the individual vehicle level*.

In the energy domain, we've defined the following domain strategic goals:

(Smart Grid) Domain Strategic Goal 1: *European member states* shall *update national energy and climate plans by 2023* for *contributing to EU-wide targets* with the benefit(s) of *reaching the 2030 climate ambition*.

(Smart Grid) Domain Strategic Goal 2: *The Trans-European Networks – Energy (TEN-E) Regulation* shall *foster the deployment of innovative technology and infrastructure* for *upgrading existing smart infrastructure* with the benefit(s) of *transitioning to clean energy at affordable price*.

If at the strategic level, authorities define goals for the benefit of organizations, citizens and other ecosystem participants, at the tactical level, goals are defined for enabling system cooperations in the field. These are open declarations of an ecosystem participant, that other ecosystem participants can relate to.

For enabling tracing, the *response* of *domain strategic goals* is refined into *tactical activities* and the *motivation* into *common benefits*. For exemplifying the definition of tactical goals in the automotive domain, we have selected the (Automotive) Domain Strategic Goal 1 and we have surveyed literature papers that describe tactics for cooperations, like the ones presented in [32] and [33].

Overall, we have identified four artifacts, around which we center the definition of tactical goals. These artifacts are:

- **Ecosystem Entity** is a cyber-psychical entity that can judge benefits and disadvantages of possible cooperations and collaborations.
- **Response** is a tactical activity that provides concrete action plans for satisfying part of the response of entities at the domain strategic level.

- **Stimulus** at the tactical level is the context in which operational goals are activated.
- **Common Benefit** can be queried by entities that want to join an ecosystem.

Tactical goals can be expressed in natural language using the following template:

"***Ecosystem entity*** shall ***response*** when ***stimulus*** with ***common benefit***."

Examples of tactical goals from the automotive domain:

(Automotive) Tactical Goal 1: *The Platoon Service Provider (PSP)* shall *create a platoon plan* when *receiving platoon requests from vehicles* with the benefit of *enabling platoon formation*.

(Automotive) Tactical Goal 2: *The Platoon Service Provider (PSP)* shall *create platoon routes* when *receiving routing information from transport companies* with the benefit of *enabling platoon formation*.

For definition of tactical goals in the energy domain, we have surveyed the Smart Grids Task Force Expert Group 4 -– Infrastructure Development [34] that specifies the KPI (Key Performance Indicators) of cooperation within the energy sector.

(Smart Grid Tactical Goal 1): *Distributed Energy Resources* shall *form coalitions* when *they can only provide fluctuant energy* for *satisfying the energy demands of users*.

(Smart Grid Tactical Goal 2): *Distributed Energy Resources* shall *transmit and distribute energy* when *they overproduce* for *reducing congestion risks in transmission networks*.

The ultimate trust evaluation relies on runtime computations that create evidence of correct operation in the field. For achieving tactical goals, at the operational level, systems and system components respond to stimulus and operate in certain contexts. The *stimulus* of tactical goals become the *context* of operational goals. System functions that implement operational goals are activated in established context. The context of operational goals is a combination of internal and external states of the system. For example, if the achievement of the tactical goal to join a platoon requires acceleration, then the function responsible for acceleration is activated in context of joining the platoon.

We have defined the following template for natural language expression of operational goals.

- **Ecosystem Entity** is a system component, hardware resource or software component that implements a system function.
- **Response** is the output provided by the system function.
- **Stimulus** is the input provided to the system function.
- **Context** is the environmental part that starts the execution of a system function.

With the following template, goals can be defined at operational level:

"***Ecosystem Entity*** shall ***response*** when ***stimulus*** in context of ***context***".

For the definition of operational goals in the automotive domain, we have surveyed multiple papers that analyze the operation of CACC (Collaborative Adaptive Cruise Control). CACC is an intelligent part of a vehicle that enables inter-vehicular collaborations based on exchange of context and operational information [35], [36].

(Automotive) Operational Goal 1: *The platoon members* shall *maintain string stability* when *they adapt their speed* in context of *driving in a platoon*.

(Automotive) Operational Goal 2: *The CACC of platoon leader* shall *transmit target acceleration* when *speed increases are triggered* in context of *overtaking situations*.

In the smart grid domain, through the deployment of software smart agents, connectors boxes within DER can autonomously form coalitions for satisfying the tactical goals such as provision of flexible amounts of energy. For this, at the operational level, the following goals need to be fulfilled:

(Smart Grid) Operational Goal 1: *The connector box, part of a DER* shall *transmit state information* when *it receives a triggered request*.

(Smart Grid) Operational Goal 2: *A Virtual Power Plant* shall *start a broadcast for bids* when *it receives information about deficit of energy production.*

B. Formalization of Anti-Goals

For formalizing the definition of *strategic anti-goals*, we have negated artifacts from the *strategic goals*. We have started from negating either *the response* or the *benefit* and we have asked the following questions:

- **Who?**: Who is responsible for the negated benefit and/or response?
- **Why?**: Why the responsible wants to achieve the anti-goal?
- **How?**: How the anti-goal is achieved?
- **What?**: What is achieved by the strategic anti-goal?
- **How much?**: How much does the anti-goal affect the goal?

The answer to the first question *"Who?"* gives the **subject** for the second question "Why?". The answer to the question *"Why?"* gives the **cause** of the strategic anti-goal. The answer to the question *"How?"* gives the **path** for the strategic anti-goal. *"What?"* indicates the **risk** of the strategic goal. *"How much?"* gives the **estimated/quantitative effects** of the strategic anti-goal.

Because they guide the provision of different answers, the questions are mutually exclusive. By covering all concerns present in the official European documents, the artifacts collectively create a complete set of optimum information for definition of anti-goals. Bellow we provide one example of a strategic anti-goal:

- **Subject**: Public and private investors.

- **Cause**: Public and private investors unwilling to switch to sustainable practices.
- **Path**: Only one-time investment made towards sustainable businesses and switching back to highly profited legacy businesses.
- **Risk (opposes motivation)**: Frustrate the efforts of the EU (efforts of EU will be in-consequential)./ Lock-in into unsustainable practices.
- **Effects (opposes quantifiable benefits)**: No more than 60% reduction of carbon emission.
- **Adjustment mechanism**: More ambitious EU strategy on adaptation to climate change.
- **Expected Impact**: Access to data and instruments that to integrate climate change into risk management practices in the private and public sector.
- **Constraints of the adjustment**: Continuation of significant stress on the environment, in spite of mitigation efforts.

At the operational level, the anti-goals are defined according to the SHARD principle [4]. In [30], we provide examples of anti-goals which are typical system failures.

C. Platform for runtime evaluation of goals

The goal extension we provide in Fig. 1 provides a structure for trust computation and derivation of possible attack strategies. It extends the platform for the runtime prediction and trust computation we have introduced in [6]. Predictive simulation involves the execution of algorithm behavior at much higher speeds than the wall clock time. The reputation of a software smart agent is build by monitoring its functional and non-functional properties, such as reaction times. These together provide evidence of the operational goals of software smart agents. A malicious behavior can, for example, be observed if a software smart agent provides late replies in specific technical situations. A late reaction on decreasing acceleration can cause crashes within a platoon.

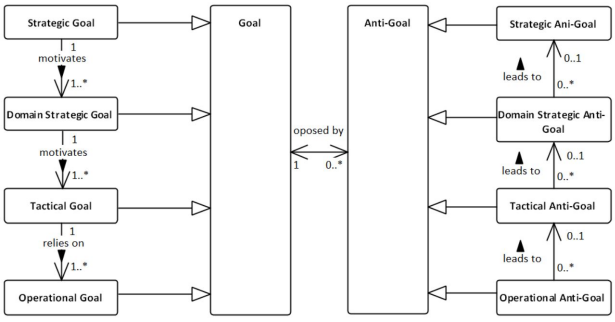

Fig. 1. Goals classification for dynamic trust evaluation

With the extension provided in this paper, after discovering malicious behavior of software smart agents within a runtime predictive simulation, a bottom up reasoning of tactics and strategies for attacks can be deduced and argumented by evidence that is computed at runtime. Whereas, for the constructive building of trust, a top-down approach enables reconfiguration from the tactical level, where possible cooperations can be negotiated until the operational level. At the operational level, fail-over behavior can be activated when faults in the field are discovered. Fail-over behaviors can bring a system into a safe state in face of hazardous events [37].

The early change of tactics and strategies is beneficial for an ecosystem participant for two reasons. Firstly, it enables the participant to stay out of collaborations that do not support its ultimate strategic goals. Secondly, when its enhanced functionality depends on runtime activation or provision of updates, evaluating goals of elements existing in its composition, an ecosystem entity gets the chance to reconfigure internally early enough for displaying an ultimate trustworthy behavior to its collaborators.

TABLE I
OVERVIEW OF GOALS

Element	***Description***
Strategic Goal	*A Strategic Goal* is a solution statement for an existing issue in the world that can be issued by governments and authorities around the world. For example, reduce CO2 emissions
Domain Strategic Goal	A *Domain Strategic Goal* is a translation of strategic goals responses into a domain. For example, Reduce fuel consumption in the automotive domain.
Tactical Goal	A *Tactical Goal* is the decomposition of response of a domain strategic goal into cooperations and collaboration benefits of two or more ecosystem entities. For example, formation of vehicle platoons.
Operational Goal	An *Operational Goal* is a concrete implementation of a system function. For example, decrease acceleration within a platoon.
Goal	A *Goal* is the basic concept that translates into actions.
Strategic Anti-Goal	A *Strategic Anti-Goal* is the ultimate strategy for attacks identified at the lower computation levels. For example, increase the CO2 emissions, increase costs.
Domain Strategic Anti-Goal	A *Domain Strategic Anti-Goal* is a strategic anti-goal that manifest into a specific domain. For example, increase acceleration within a platoon, or increase rotation of a robot arm in a factory.
Tactical Anti-Goal	A *Tactical Anti-Goal* is the result of multiple operational anti-goals that shows a tactic attack. For example, the plan of an attack through shipment of multiple software smart agents. Only at specific events of interconnected SW agents, a malicious behavior can be expressed.
Anti Goal	An *Anti-Goal* is an intended malicious fault that opposes a concrete operational goal. An operational anti-goal could be the sudden acceleration of a vehicle.

V. CONCLUSION AND FUTURE WORK

Starting from safety formalism for goal representation, in this paper we have provided definitions and model classification for trust analysis. The work constitutes a starting point for defining mechanisms that enable an ecosystem to self-regulate its health. By setting the base that enables goals analysis at major levels of trust formation, ecosystems can

gain self-efficacy in the sense that they can self-organize and execute different course of actions for achieving their upper most strategic goals.

In our work, the process of trust building follows two path: one of argumentation and one of computation. For the argumentation of trust, we will further on build on the goals formalization and their expression in natural language. This will support trust argumentation within a general trust assurance case. For computing evidence that supports a dynamic trust argumentation, we will extend on reputation computation for software behavior.

ACKNOWLEDGMENT

This work is co-funded from the European Union's Horizon 2020 research and innovation programme under grant agreement No 952702 (BIECO) and by ERDF "CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence" (No. CZ.02.1.01/0.0/0.0/16_019/0000822).

REFERENCES

[1] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE transactions on dependable and secure computing*, vol. 1, no. 1, pp. 11–33, 2004.

[2] E. S. Yu, "Towards modelling and reasoning support for early-phase requirements engineering," in *Proceedings of ISRE'97: 3rd IEEE International Symposium on Requirements Engineering*. IEEE, 1997, pp. 226–235.

[3] A. Cailliau and A. van Lamsweerde, "Assessing requirements-related risks through probabilistic goals and obstacles," *Requirements Engineering*, vol. 18, no. 2, pp. 129–146, 2013.

[4] P. Fenelon, J. A. McDermid, M. Nicolson, and D. J. Pumfrey, "Towards integrated safety analysis and design," *ACM SIGAPP Applied Computing Review*, vol. 2, no. 1, pp. 21–32, 1994.

[5] S. da Silva Amorim, F. S. S. Neto, J. D. McGregor, E. S. de Almeida, and C. von Flach G Chavez, "How has the health of software ecosystems been evaluated?: A systematic review," in *Proceedings of the 31st Brazilian Symposium on Software Engineering*. ACM, 2017, pp. 14–23.

[6] E. Cioroaica, T. Kuhn, and B. Buhnova, "(Do not) trust in ecosystems," in *Proceedings of the 41st International Conference on Software Engineering: New Ideas and Emerging Results*. IEEE Press, 2019, pp. 9–12.

[7] E. Cioroaica, S. Chren, B. Buhnova, T. Kuhn, and D. Dimitrov, "Reference architecture for trust-based digital ecosystems," in *2020 IEEE International Conference on Software Architecture Companion (ICSA-C)*. IEEE, 2020, pp. 266–273.

[8] A. Schönberger and C. Elsner, "Modeling partner networks for systematic architecture derivation in software ecosystems," in *Marktplätze im Umbruch*. Springer, 2015, pp. 655–665.

[9] H. B. Christensen, K. M. Hansen, M. Kyng, and K. Manikas, "Analysis and design of software ecosystem architectures–towards the 4s telemedicine ecosystem," *Information and Software Technology*, vol. 56, no. 11, pp. 1476–1492, 2014.

[10] J. Bosch, "From software product lines to software ecosystems," in *Proceedings of the 13th international software product line conference*. Carnegie Mellon University, 2009, pp. 111–119.

[11] E. Hollnagel, A. Nåbo, and I. V. Lau, "A systemic model for driver-in-control," 2003.

[12] D. E. Zand, "Trust and managerial problem solving," *Administrative science quarterly*, pp. 229–239, 1972.

[13] I. Serov and M. Leitner, "An experimental approach to reputation in e-participation," in *2016 International Conference on Software Security and Assurance (ICSSA)*. IEEE, 2016, pp. 37–42.

[14] N. Dessi, B. Pes, and M. G. Fugini, "A distributed trust and reputation framework for scientific grids," in *International Conference on Research Challenges in Information Science*. IEEE, 2009, pp. 265–274.

[15] B. Zong, F. Xu, J. Jiao, and J. Lv, "A broker-assisting trust and reputation system based on artificial neural network," in *IEEE International Conference on Systems, Man and Cybernetics*. IEEE, 2009, pp. 4710–4715.

[16] G. Yin, D. Shi, H. Wang, and M. Guo, "Repcom: Towards reputation composition over peer-to-peer communities," in *2009 International Conference on Computational Science and Engineering*, vol. 2. IEEE, 2009, pp. 765–771.

[17] J. Riegelsberger, M. A. Sasse, and J. D. McCarthy, "The mechanics of trust: A framework for research and design," *International Journal of Human-Computer Studies*, vol. 62, no. 3, pp. 381–422, 2005.

[18] B. Weiner, "Attributional theories of human motivation," *Human motivation: metaphors, theories, and research. Newbury Park, CA: Sage*, 1992.

[19] S. Faily and I. Fléchais, "Eliciting and visualising trust expectations using persona trust characteristics and goal models," in *Proceedings of the 6th International Workshop on Social Software Engineering*, 2014, pp. 17–24.

[20] E. Letier and A. Van Lamsweerde, "Reasoning about partial goal satisfaction for requirements and design engineering," in *Proceedings of the 12th ACM SIGSOFT twelfth international symposium on Foundations of software engineering*, 2004, pp. 53–62.

[21] J. Bosch and H. H. Olsson, "Ecosystem traps and where to find them," *Journal of Software: Evolution and Process*, vol. 30, no. 11, p. e1961, 2018.

[22] A. Van Lamsweerde, "Elaborating security requirements by construction of intentional anti-models," in *Proceedings. 26th International Conference on Software Engineering*. IEEE, 2004, pp. 148–157.

[23] N. G. Leveson, *Safeware: system safety and computers*. Addison-Wesley, 1995.

[24] A. P. Moore, R. J. Ellison, and R. C. Linger, "Attack modeling for information security and survivability," Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst, Tech. Rep., 2001.

[25] G. Helmer, J. Wong, M. Slagell, V. Honavar, L. Miller, and R. Lutz, "A software fault tree approach to requirements analysis of an intrusion detection system," *Requirements Engineering*, vol. 7, no. 4, pp. 207–220, 2002.

[26] S. Jones, *A discussion of issues and systems relevant to computer supported cooperative work*. Department of Computing Science and Math., Univ., 1990.

[27] T. Kelly, "A systematic approach to safety case management," *SAE transactions*, pp. 257–266, 2004.

[28] I. Habli, W. Wu, K. Attwood, and T. Kelly, "Extending argumentation to goal-oriented requirements engineering," in *International Conference on Conceptual Modeling*. Springer, 2007, pp. 306–316.

[29] E. Commission *et al.*, "The european green deal," *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Brussels*, p. 24, 2019.

[30] A. O. Emilia Cioroaica. (2020) Strategic and tactical goals. [Online]. Available: https://drive.google.com/drive/folders/1y9yMeHSxL3YbZXUOz0vVCrdoUgJCpLPx?usp=sharing

[31] E. A. M. Association. (2020) European automobile manufacturers' association. [Online]. Available: https://www.acea.be/about-acea/who-we-are

[32] S. van de Hoef, "Coordination of heavy-duty vehicle platooning," Ph.D. dissertation, KTH Royal Institute of Technology, 2018.

[33] R. Janssen, H. Zwijnenberg, I. Blankers, and J. de Kruijff, "Truck platooning," *Driving the*, 2015.

[34] V. Giordano, S. Vitiello, and J. Vasiljevska, "Definition of an assessment framework for projects of common interest in the field of smart grids," *JRC Science and policy reports*, 2014.

[35] L. Cui, J. Hu, B. B. Park, and P. Bujanovic, "Development of a simulation platform for safety impact analysis considering vehicle dynamics, sensor errors, and communication latencies: Assessing cooperative adaptive cruise control under cyber attack," *Transportation Research Part C: Emerging Technologies*, vol. 97, pp. 1–22, 2018.

[36] C. Lei, E. M. van Eenennaam, W. K. Wolterink, J. Ploeg, G. Karagiannis, and G. Heijenk, "Evaluation of cacc string stability using sumo, simulink, and omnet++," *EURASIP Journal on Wireless Communications and Networking*, vol. 2012, no. 1, p. 116, 2012.

[37] R. Adler, P. Feth, and D. Schneider, "Safety engineering for autonomous vehicles," in *Dependable Systems and Networks Workshop, 2016 46th Annual IEEE/IFIP International Conference on*. IEEE, 2016, pp. 200–205.