Log ical Methods in Computer Science Vol . 8 (4 : 17) 2012 , pp . 1 44 www . l m cs - online . org Sub mitted Published Jan . 7 , 2011 Nov . 23 , 2012 A COMPLE TE AX I OM AT IZ ATION OF QU ANT IFIED D IF FER ENT IAL D YN AM IC LOG IC FOR DISTR IB UT ED HY BR ID SYSTEM S AND RE PL AT Z ER Carnegie Mellon University , Computer Science Department , Pittsburgh , PA , USA e - mail address : a pl at zer @ cs . cm u . edu Abstract . We address a fundamental mismatch between the combinations of dynamics that occur in cyber - physical systems and the limited kinds of dynamics supported in analysis . Modern applications combine communication , computation , and control . They may even form dynamic distributed networks , where neither structure nor dimension stay the same while the system follows hybrid dynamics , i . e ., mixed discrete and continuous dynamics . We provide the logical foundations for closing this analytic gap . We develop a formal model for distributed hybrid systems . It combines quant i ed di erential equations with quant i ed assignments and dynamic dimension ality - changes . We introduce a dynamic logic for verifying distributed hybrid systems and present a proof calculus for this logic . This is the r st formal ver i cation approach for distributed hybrid systems . We prove that our calculus is a sound and complete ax iom at ization of the behavior of distributed hybrid systems relative to quant i ed di erential equations . In our calculus we have proven collision freedom in distributed car control even when an unb ounded number of new cars may appear dynamically on the road . 1 . Introduction Many safety - critical computers are embedded in cyber - physical systems like cars [H ES V 91 , S RS + 06] and aircraft [D MC 05]. How do we know that their designs will work as intended ? Most initial designs do not . And some deployed systems still do not . Ens uring the correct functioning of cyber - physical systems is a central challenge in computer science , mathematics , and engineering , because it is the key to designing smart and reliable control . Scientists and engineers need analytic tools to understand and predict the behavior of their systems . As systems become ever more complex , it becomes prohib itive ly expensive or impossible to 1998 AC M Subject Classification : F . 3 . 1 , F . 4 . 1 , D . 2 . 4 , C . 1 . m , C . 2 . 4 , D . 4 . 7 . Key words and phrases : Di erential dynamic logic , Dist ributed hybrid systems , Ax iom at ization , The orem proving , Quant i ed di erential equations , Proof theory . An extended abstract has appeared at C SL 10 [Pl a 10 c]. This material is based upon work supported by the National Science Foundation under NS F CARE ER Award CNS - 10 54 246 , NS F EXP ED ITION CNS - 09 26 181 , and under Grant Nos . CNS - 10 35 800 and CNS 09 3 1985 , by the NASA grant N NG - 05 GF 84 H , and by the ON R award N 0001 4 - 10 - 1 - 01 88 . DOI : 10 . 2 168 / LM CS - 8 (4 : 17) 2012   test all possible interactions and rule out unsafe behavior by simulation . Form al verification techniques are used routinely to overcome this for finite systems . But for cyber - physical systems , there is not even a foundation for verification that would cover all required behavior . There is a fundamental mismatch between the actual dynamics of cyber - physical system applications and the limits imposed by current modeling and analysis . Cyber - physical systems in automotive , aviation , railway , and power grids combine communication , computation , and control . Comb ining computation and control leads to hybrid systems [ACH H 92 , Bra 95 , Hen 96 , B BM 98 , Pl a 10 b], whose behavior involves both discrete and continuous dynamics originating , e . g ., from discrete control decisions and differential equations of motion . Comb ining communication and computation leads to distributed systems [Lyn 96 , AL 01 , Ad BO 10], whose dynamics are discrete transitions of system parts that communicate with each other . They may form dynamic distributed systems , where the structure of the system is not fixed but evolves over time and agents may appear or disappear during the system evolution . Comb inations of all three aspects (communication , comput a ( ) ( ) tion , and control) are used in sophisticated applications , e . g ., co (2) (2) (3) (3) (4) (4) (1) (1) operative distributed car control [H ES V 91] and decentralized aircraft control [PS FB 07]. Neither the structure nor dimension of the system stay the same , because new Figure 1 : Dist ributed car control . cars can appear on the street or leave it ; see Fig . 1 . These systems are (d ynamic) distributed hybrid systems , i . e ., systems that combine the dynamics of distributed systems with the discrete and continuous dynamics of hybrid systems . More generally , distributed hybrid systems are multi - agent hybrid systems that interact through remote communication or physical interaction . They cannot be considered just as a distributed system (because , e . g ., the continuous evolution of positions and vel oc ities matters cru cially for collision freedom in car control) nor just as a hybrid system (because the evolving system structure and appearance of new agents can make an otherwise collision - free system unsafe). It is generally impossible to split the analysis of distributed hybrid systems sound ly into an analysis of a distributed system (without continuous movement) and an analysis of a hybrid system (without structural changes or appearance), because all kinds of dynamics interact . Just like hybrid systems are diff cult to analyze from a purely discrete or a purely continuous perspective [Hen 96 , Pl a 12]. Dist ributed hybrid systems have been considered to varying degrees in modeling languages [D GV 96 , Rou 04 , K SP L 06 , MS 06]. In order to build these systems , however , scientists and engineers also need analytic tools to understand and predict their behavior . But formal verification and proof techniques do not yet support the required combination of dynam ical effects which is not surprising given the numerous sources of und ec id ability for distributed hybrid systems verification . In this article , we provide the logical foundations to close this fundamental analytic gap . We develop quant ified hybrid programs (Q H Ps) as a formal model for distributed hybrid systems , which combine dynam ical effects from multiple sources : discrete transitions , continuous evolution , dimension changes , and structural dynamics . In order to account for changes in the dimension and for co - ev olution of an unb ounded and evolving number of participants , we general ize the notion of states from assignments for primitive system variables like x to full first - order structures . In a Q HP , function term x (i) may denote the position of car i of type C , the term f (i) could be the car registered by communication as the car following car i , and the term d (i , f (i)) could denote the minimum safety distance negotiated between car i and its follower f (i). The values of all these terms may evolve for all i as time progresses according to interacting laws of discrete and continuous dynamics , because all cars evolve simultaneously . They are also affected by changing the system dimension as new cars appear , disappear , or by recon fig uring the system structure dynamically , e . g ., by remote communication or physical interaction . The defining characteristic of Q H Ps is that they allow quant ified hybrid dynamics in which variables like i that occur in function arguments of the system dynamics are quant ified over , such that the system co - ev olves , e . g ., for all cars i of type C . This quant ification is necessary to characterize the distributed hybrid systems dynamics with an unb ounded and possibly evolving number of participants . Quant ification is also necessary to represent structural dynamics when the number of participants is not fixed . There is a crucial difference between a primitive system variable x and a first - order function term x (i), where i is quant ified over . Hybrid dynamics of primitive system variables can model a concrete number of , say , four cars (put ting scal ability issues aside), but neither a param etric number of n cars nor systems with a variable number of cars (a number n that may change over time). With first - order function symbols x (i) and hybrid dynamics quant ifying over all cars i , a single Q HP can represent any number of cars at once . Q H Ps can even represent (dis) app earance of cars by changing the domain that quant ifiers range over dynamically at runtime . Q H Ps are thus a formal model for general (d ynamic) distributed hybrid systems . Ver ification of distributed hybrid systems is challenging . We show that they have three independent sources of und ec id ability : discrete dynamics , continuous dynamics , and structural / dimensional dynamics . As an analysis tool for distributed hybrid systems , we introduce a specification and verification logic for Q H Ps that we call quant ified differential dynamic logic (Q dL). Q dL provides dynamic logic [P ra 76 , HK T 00] mod al operators [±] and h ± i that refer to the states reach able by Q HP ± and can be placed in front of any formula . Formula [±] expresses that all states reach able by system ± satisfy formula , while h ± i expresses that there is at least one reach able state satisfying . These mod alities can express necessary or possible properties of the transition behavior of Q HP ± . With its ability to specify and verify properties of (d ynamic) distributed hybrid systems and quant ified dynamics , Q dL is a major extension of prior work for static hybrid systems [Pl a 08