Intelligent Control of Autonomous Vessels: Bayesian Estimation Instead of Statistical Learning?

Amolkumar Bhoyar¹, Rajneesh Sharma², Sukratu Barve³, Rakesh Kumar Rana⁴

^{1,2} (M. Tech) Consultant, ³ (Ph. D.) Assistant Professor, ⁴ (Ph. D.) Honorary Senior Advisor

^{1,2,3}Savitribai Phule Pune University, ⁴Honorary Senior Advisor

^{1,2,3}Pune, ⁴New Delhi, INDIA

^{1,2,3,4}([amolbhoyar](mailto:amolbhoyar@gmail.com), [rajneesh.sharma.88](mailto:rajneesh.sharma.88@gmail.com), [sukratu](mailto:sukratu@gmail.com), [rkrana14](mailto:rkrana14@gmail.com)) @gmail.com

Synopsis

Marine vessels have been recently considered for redesign with a view towards autonomous operation. This brings forth a number of safety concerns as regards malware attacks on intra-vehicle communications systems as well as on sensor based communication with their environment. Designing suitable hybrid systems or cyber physical systems as the above, which are data driven, involves a challenge by way of difficulty in abstraction. The current modeling paradigm for cyber physical systems is based upon the abstract idea of a hybrid automaton which involves discrete as well as continuous mathematical models for the physical device (marine vessel/s). Incorporating statistical inference techniques to introduce an element of autonomy in this has been recently proposed in literature. An engineering situation is explored in which a pair of marine vessels is being deployed to navigate avoiding collision with the help of deterministic control as well as with a particle filtering state estimator. A security intrusion is considered to occur in the communication channels and the robustness of the system is studied with the state estimation. Such intrusions can indeed be expected to defeat the collision protection design if sufficiently intense. However, better protection is offered by such Bayesian estimation based intelligent control as compare to statistical learning base control. Our results suggest that the hybrid automaton modeling paradigm with autonomy incorporated needs to be suitably abstracted in order to better design their defence against cyber-attacks.

Keywords— Automated navigation, cyber physical systems, autonomy, simulation.

1. Introduction

The recent demonstration of an autonomous marine vessel carrying out a successful trip on a designated route has brought up several questions from stakeholders regarding concerns like safety, reliability and resilience. Such marine craft have several component systems which have computational as well as physical aspects in their function. The complexity is so enormous and the ubiquity of such devices is so high that some authors have proposed that an entire marine craft (except the human beings on it) could be considered as a complex cyberphysical system [0]. Design and analysis of such systems is fraught with difficulties and pose considerable challenges [0]. In view of this, the National Institute of Standards in Technology has advanced a unifying Conceptual Framework for Cyber-Physical Systems [0] so that the challenges could be framed in a holistic manner. Within such a framework Aspect Oriented Design, for example is one philosophy that has been suggested to address such complexity (Advice, join points, join cuts etc.) Designing such cyberphysical systems having a further design dimension of autonomy is bound to increase these challenges.

Safety is an important stakeholder concern out of these challenges. Safety assessments indicate that the software component of the ship should be most emphasized [0] as regards vulnerability. Adversarial attacks are likely to affect the software component the most and thus put at most risk the control system of the entire craft or fleet of craft. Further, in heavy marine craft this challenge is aggravated by an issue with actuation as only three actuator variables, rudder angle, propeller pitch and propeller speed are available [0]. The inertia in heavy vessels makes ship controllability an extremely

difficult challenge especially under rough weather conditions. The rudder and propeller control systems, i.e. only available control units for vessel actuation, may fail to control vessels under rough sea going conditions. When ships are navigating under moderate or high speeds (i.e. over 3-4 knots), the capabilities of thrusters are negligible. Therefore, control solutions developed for autonomous surface vehicles (ASVs) and autonomous underwater vehicles (AUVs) are not acceptable for large vessels as they turn out to be under-actuated for autonomous real time operation. Hence, the controllability of under actuated autonomous vessels under various navigation conditions would be an area of critical concern in the future. Coupled with the challenges in the design of marine vessels as autonomous cyberphysical systems, safety under adversarial attack is put at considerable risk.

In this work, coordinated motion under adversarial attack is considered with two such under actuated surface craft in mind designed primarily for following with collision avoidance. Specifically, the coordination is considered to be implemented with the help of deterministic as well as with intelligent control. The intelligent control is implemented via a particle filtering state estimator. The manner in which statistical learning can be implemented is described in the hybrid automaton model for the purpose of intelligent control. A security intrusion is considered to occur in the communication channels. It is then described how learning based control has been recently shown to be highly vulnerable to adversarial intrusions while state estimation control according to our results suggest robustness of the intelligent control system based upon it. The difference between the two methods of intelligent control is well captured by the abstract concept of the hybrid automaton and is important for understanding vulnerabilities of the design.

The results suggest that the hybrid automaton modeling paradigm with autonomy incorporated needs to be suitably abstracted in order to better design their defence against cyber-attacks. It is suggested that the Bayesian control paradigm is better suited for intelligent control than the learning paradigm. Finally, it is pointed out that a man on-loop control with partial autonomy could be better implemented with Bayesian control.

2. Control Systems, Intelligent Control and Mathematical Modeling

A general control system is represented in the following diagram which can be used as a paradigm for representing various aspects of the complex cyberphysical system that one seeks to view the marine craft (or the fleet of marine craft) as Figure 1.

The focus in this work is restricted to only one aspect of the performance of vessel namely physical navigation as far as safety is concerned when autonomy has been incorporated into the cyberphysical system.

Figure 1: A general block diagram of a control system.

A general framework for autonomous ship navigation has been illustrated in Figure 2 above 0. Comparing with the general control system in Figure 1, it is found that the aspect of autonomy enters the cyberphysical system in the navigation and guidance blocks. Often, aspects of image processing associated with the sensor signal involve machine learning and thus are termed as autonomy in the control system. This is a part of information processing but rather associated with navigation more than guidance.

Figure 2: A general framework for autonomous ship navigation 0.

Similarly, Bayesian estimation control is associated with navigation more than guidance. But statistical learning methods mostly get associated with guidance and control in many designs. Thus, one needs to thus address different manners in which intelligent control can be implemented in control systems. In general, intelligent control can be classified into the following sub-domains based upon their mathematical (or statistical) nature 0:

- Statistical learning control

- Bayesian Estimation control
- Fuzzy control
- Learning-Fuzzy control
- Expert Systems control

This work is restricted to only the first two and so it is assumed that autonomy can be built into the model in two manners, statistical learning and by statistical estimation which is usually classified as being under statistical decision theory. In Bayesian estimation, we assume some amount of knowledge about the distributions of the observation X which in the case would be the sensor signals for the measurand and the quantity of interest Y which in our case would be the variables for actuation. Such knowledge can come from a careful analysis of the physical characteristics of the problem at hand, or it can be gleaned from previous experience. The measurand signals change with time and are mathematically represented as a stochastic process. The internal state of the system, also a stochastic process is changed depending upon the measurand signal and using statistical filtering. The measurand depends upon the state according to an algebraic model.

Contrary to this ease of scientific fidelity for mathematical modeling, there are situations where it is practically difficult to model the science of the problem at the same time, one may not have enough experience to develop complete and accurate probability models. In such cases, it is natural to adopt a statistical learning approach [10]. Statistical learning methods are based on developing decision rules or estimators based only on a collection of training examples, rather than predetermined probability models. Statistical learning methods are often said to be distribution free, since they do not assume particular probability models. In practice statistical learning models are implemented as follows. Signals from sensors (generally optical or visual images) are fed to trained regression/classification based statistical learning models and a set of action sequence to be provided to the actuators is obtained from the model. These are then passed on to the actuators provided the confidence measure, which is also returned, is within acceptable levels. However, the deployment of such a model cannot be carried out without suitable training imparted to it. In case of marine vessels such an application has been recently discussed in [10]. Before autonomy is brought into the design it is important to address formal models of a cyberphysical system as it currently defined.

2.1 Cyberphysical Systems and Hybrid Automata

The notion of cyber-physical system (CPS) was keyed by James Truchard from National Instruments in 2006. He demonstrated the concept of a CPS by use of a LEGO R MINDSTORMS R

NXT robot and stressed on the “deeply integrated, real-time interaction between computer and physical components.” [10] The diversity of such systems posed challenges especially regarding interfacing the physical and cyber components which brought up the need for abstraction. A unifying framework was found to be required for modeling cyberphysical, which allows easy interfacing and consistency [10]. Formal Models used to represent Cyber Physical Systems are reviewed in [10]. The behavior and control of a cyberphysical system can be abstractly represented in terms of a concept called hybrid automaton. This concept is briefly described below based on [10]. Further details are available in literature [10] for elaborate study.

A hybrid automaton H is a six-tuple (Q, X, D, D_0, f, R) where Q is a finite set of variables taking discrete values called discrete variable set, X is a finite set of variables taking continuous values called continuous variable set, $D \subset Q \times X$ is the domain, members of which are called states, $D_0 \subset Q \times X$ is the set of initial conditions or initial states, $f: Q \times X \rightarrow P(Q \times X)$ is the reset relation. $P(A)$ denotes the power set of set A .

The set Q represents the set of modes of operation in which the cyberphysical system is designed to operate. X is the set of continuous variables which represent the dynamical state of the cyberphysical system. In our case, they would be the variables representing the positions and velocities of the marine craft composing the fleet.

Either of the two approaches of intelligent control could be incorporated in a hybrid automaton as autonomy which, as found earlier, enters in the information processing block in the diagram. This processing can be divided into guidance navigation and control (GNC) for our application. Bringing in autonomy would change the design of the navigation and guidance process out of GNC [10]. It would now be either statistically learned (image recognition from sensor signals, neural network learned guidance) or works on a stochastic process via Bayesian estimation (trajectory estimation and control) The inputs from navigation measurements are used differently in each of the two cases. In the first case they are features and in the second they are inputs to a filter. The Bayesian approach to controller design often requires an important effort in deriving the so called system model and measurement model, which are the mathematical relationships linking the state variables to the sensor measurements available in the controlled system. In this respect, it is very closely linked to the system-theoretic approach to control design. In terms of the hybrid automaton, this would amount to changing the automaton state probabilistically with alphabet (transition conditions) instead of deterministically doing so (spontaneous transitions

versus forced transitions as termed in the paper) from the pre-jump state 0.

This probabilistic action by statistical learning occurs in four manners in commonly encountered situations.

- Control parameter identification: Learning control translates to a parameter identification 0 if the structure of the control law is given but the parameters are unknown.
- Control design as regression problem of the first kind: Learning control approximates a general nonlinear mapping from sensor signals to actuation commands, if the sensor signals and the optimal actuation command are known for every state. One example is the computation of sensor feedback from a known full state feedback.
- Control design as regression problem of the second kind: Learning Control may also identify arbitrary nonlinear control laws which minimize the cost function of the plant. In this case, neither a model, nor the control law structure, nor the optimizing actuation command needs to be known. The optimization is only based on the control performance (cost function) as measured in the device.
- Reinforcement learning control: The control law may be continually updated over measured performance changes (rewards) using reinforcement learning 0.

Such probabilistic transition action does not depend only on the pre-jump state. The past states of the automaton would also have to be considered when one identifies the features in the learning model, especially in points 3 and 4 above. Though there are transition probabilities involved, these probabilities are learned as parameters using rewards and penalties. The role of the loss function which is optimized and design of reward/penalty is critical as they depend upon training data. This training needs to be abstractly captured to address the way the transition probability parameters are obtained. Training corresponds to the abstract set of entire state trajectories being mapped to the set of loss functions used for arriving at the probabilistic transition action. Thus the design of the loss function would critically affect the choice of probabilities of state transition 0. Unfortunately that poses a serious drawback.

It was realized in 2013 0 that learning based models are subject to poor performance on adversarial attacks 0. These attacks including black box attacks even of the type “single pixel” or “a few pixel” and can be targeted or untargeted 00. Such an attack on a learned guidance system would affect the regressed variable, namely the course action or control. Minor changes to the measurement input

causes severe failure in appropriateness of the course of action to be taken 0. Typically noise supplied to the measurement input misclassifies the response needed to be chosen from the learned behavior leading to catastrophic failure. The fact that a loss function has been employed for getting optimized plays a very important role in generating such vulnerability in design 0.

The reason for such vulnerability appears to be in the fundamentally different manner in which the algorithms simulate the human faculty of sensing and identification. They tend to work based on weak and local statistical irregularities which is very different from the causal relationships between parts of the information set that humans are sensitive to 0.

It is therefore suggested that the Bayesian estimation control based conception of abstract hybrid automaton rather than the statistical learning based control. The performance of one such example, a particle filter vehicle following model for marine craft has been demonstrated.

3. Bayesian Estimation Control: A Simulated Example and Advantages

Control laws for craft have a proposed method of classification (though it was introduced in the context of air vehicles) 0. Motivated by application to surface marine vessels, an engineering problem is considered involving two such marine craft coordinating their motion in a two dimensional spatial domain. Results are presented on how robust such a particle filter based control would be to an attack on the sensor inputs to the following craft as regards position of the leading craft.

3.1 Motion Model and Hybrid Automaton

There are roughly three approaches to multi-agent coordination reported in the literature, namely leader following, behavioural, and virtual structures 0. The algorithm has been implemented using the virtual structure approach as behavioural approach (covering collision avoidance in a natural manner) and leader following approach would both have been required. The marine craft are designed to manoeuvre according to the following model. The leading craft follows a path which is independently decided. It can be predetermined or decided on the fly. The following craft however attempts to maintain a distance beyond a square region centered on the leading craft. If the following craft enters into this region a strong braking thrust is applied by the craft impeding its further movement in the same direction. If the following craft is beyond the region, a thrust is applied accelerating the following craft towards the leading craft. This thrust magnitude is kept proportional to the separation between the craft in this mode of

operation. This rule of dynamical motion of the craft is referred to as the motion model.

The above design can be represented as a hybrid

Figure 3: Hybrid Automaton

automaton described below.

The continuous variables of the hybrid automaton are x_1, y_1, v_{x1}, v_{y1} representing the position coordinates and velocity components of the following craft, and x_2, y_2, v_{x2}, v_{y2} representing the position coordinates and velocity components of the leading craft. The system of a pair of craft which we refer to as the fleet thus has a dynamical state which is specified by eight variables. These change in time as dependent variables of an ordinary differential equation in each of the mode of operation of the hybrid automaton as shown above. The differential equation itself contains the information about the dynamical motion rule used and thus is obtained from the motion model detailed above. Two modes of operation ("in square mode" and "out of square mode") form the set Q of discrete variables of the automaton.

3.2 Incorporating Autonomy in Hybrid Automaton

As such the entire hybrid automaton is deterministic (in the sense that no probabilistic dynamics has been designed into it) The introduction of the stochastic element in the dynamics is characteristic of intelligent control that we seek to address. In the broader context of the engineering application which we have considered, the safety of such a design of marine craft with intelligent control therefore depends critically on how the stochastic element has been incorporated in the hybrid automaton. Introduction of intelligent control in stochastic dynamics could either be carried out as statistical learning or as Bayesian estimation. In the former, transition probabilities would be attached to the mode transitions of the automaton which would be

learned from training data. The ODEs have ordinary dependent variables (which are not random variables) In the latter, which is chosen to implement further, one introduces instead random variables as dependent variables in the ODE keeping the transitions deterministic (non-stochastic) For a rigorous definition of a stochastic hybrid automaton (and it incorporates both of the above approaches) one can refer to [10]. In further work Bayesian estimation is considered as the form of intelligent control that one seeks to implement on the following craft. One replaces the x_1 and y_1 of the following craft in the dynamics by their estimates obtained using particle filtering. These estimates now appear in the ODEs and they being random variables contain the stochastic part of the dynamics involved in the intelligent control of the automaton. Particle filters based tracking has been studied but with respect to another filter and for a single craft [11]. One sets up via x_1 and y_1 estimates, a way of navigating or tracking under possibly spurious signals for the measurand. In such a Bayesian estimation method of incorporating intelligent control, we have a limited number of variables in the control system which would ultimately be exposed to adversarial intrusion. In this case, it would be the measurand random variable. The variance observed is taken to indicate the intensity of the adversarial attack.

4. Results and Discussion of Simulation of the Stochastic Hybrid Automaton

It is shown below that the dynamics for various attack intensities, indicated by the variance of the measurand. The parameter of the particle filter (number of particles) is specifically studied as defence against such attacks.

In the figure below are shown trajectories of the two craft. A rectangular domain size of 100 km by 1000 km is considered. The leading craft has a predetermined trajectory. The following craft is expected to follow the shown trajectory if the whole system had been secure and there was no particle filter estimator used.

Now an intrusion is considered in the measurand signal processing. The signal to the following craft as regards its own position is now compromised. The craft system detects a random signal with variance (which can be monitored) The craft now employs a particle filtering estimator to ascertain its position and use the results in the dynamical model for guidance instead of the actual position which it cannot sense. Initial cases have been run with lesser number of particles in the filter which show that the attack is successful in disrupting the path of the following craft. However, one finds that the attack can be defeated with a sufficiently large number of particles.

This observation holds for a range of signal variances as shown in the other figures below.

Figure 4: Communication without any Attack

Figure 5: Number of Particles= 10 & Measurand Variance= 2 (length unit)²

Figure 6: Number of Particles= 20 & Measurand Variance= 2 (length unit)²

Figure 7: Number of Particles= 30 & Measurand Variance= 2 (length unit)²

Figure 8: Number of Particles= 50 & Measurand Variance= 2 (length unit)²

Figure 9: Number of Particles= 50 & Measurand Variance= 5 (length unit)²

Figure 10: Number of Particles= 50 & Measurand Variance= 10 (length unit)²

Figure 11: Number of Particles= 50 & Measurand Variance= 50 (length unit)²

Figure 12: Number of Particles= 80 & Measurand Variance= 50 (length unit)²

Figure 13: Number of Particles= 80 & Measurand Variance= 100 (length unit)²

Thus, one could offer solutions to warding off the attack. One possible method could involve dynamically adjusting the number of particles with the monitored variance. Another possibility is to design the system with a number of particles which can defeat an attack up to a certain intensity beyond which a flag for manual override can be raised. Such features are possible in a Bayesian filtering approach unlike the learning approach wherein it is impossible to even detect certain attacks at the level of the measurand signal.

5. Conclusion

Autonomous marine vessels, especially under actuated ones are highly susceptible to adversarial attacks. Yet, it is desirable that intelligent control be further developed to make such attacks very costly. Design of intelligently controlled marine craft needs to be abstractly conceived using suitable mathematical models of cyberphysical systems. The difference between using Bayesian estimation based intelligent control and control using statistical learning is clarified using an abstract mathematical model for cyberphysical systems called (stochastic) hybrid automaton. The distinction comes across clearly in terms of invariant set conditions and transition probability rates.

Bayesian estimation based intelligent control of marine craft holds promising advantages over statistical learning based control. With fewer

degrees of freedom exposed to adversarial intrusion, it is possible to design estimators for significantly checking any stochastic disruption effected by malware. It is shown that even basic filter parameters like particle number could be effectively used to design effective safeguards in engineering problems like marine vehicle following and collision avoidance. In contrast, statistical learning based methods of intelligent control have been recently found to have vulnerabilities which are difficult to address. The origin of this difficulty lies in the manner in which intelligent control has been incorporated in the hybrid automaton (making it a stochastic hybrid automaton) When learning is incorporated, the transitions between the automaton modes become stochastic. The transition probability rates need to be learned via training. Such training involves a loss function getting optimized leading to severe vulnerability to attacks. No such training mode is required for Bayesian control.

Further, it is possible to operate the Bayesian controlled craft with scope for manual over-ride flags in case of adversarial attacks as they can be more easily detected. Such flags are difficult to design in case of learning models facing adversarial attacks like one pixel ones recently described in literature. Nonetheless, this would amount to decreasing the level of autonomy to AL-4 in the hierarchy referred to in 0. The advantage of the Bayesian filtering approach seems to be that the stochastic element in the automaton occurs in the differential equation parts in the modes of operation. That does not involve any training with operational state data and avoids any concern of design of loss functions to be optimized. Recently, an approach has been suggested to tune the Bayesian filter parameters based upon learning 0. In the authors' view, this would still suffer from the same vulnerability for learning based automata, though it would be difficult to construct adversarial examples as effect of the loss function used would be get tied up with the dynamical motion model represented by the differential equations.

References

- [Alu] Alur R. Formal verification of hybrid systems in EMSOFT (eds Chakraborty, S., Jerraya, A., Baruah, S. K. & Fischmeister, S.) (ACM, 2011), 273–278. Alur, R. Principles of Cyber-Physical Systems (MIT Press, 2015). Alur, R., Henzinger, T., Lafferriere, G. & Pappas, G. J. Discrete Abstractions of Hybrid Systems. Proc. IEEE 88, 971–984 (2000). Alur, R. et al. The Algorithmic Analysis of Hybrid Systems. Theor. Comput. Sci. 138, 3–34 (1995). Branicky, M. S. General Hybrid Dynamical Systems: Modeling, Analysis, and Control in Hybrid Systems (eds Alur,

- R., Henzinger, T. A. & Sontag, E. D.) 1066 (Springer, 1995), 186–2009.
- [Bac] Back Thomas, Schwefel Hans-Paul. Spring 1993. An overview of evolutionary algorithms for evolutionary computation. 1(1):1-23.
- [Ber] Berad R. W., J. Lawton, F. Y. Hadaegh. 2001. A coordination architecture for spacecraft formation control. Institute of Electrical and Electronics Engineers (IEEE) Transactions on control systems technology. 9 :(Issue: 6).
- [Buj] Bujorianu, Luminita Manuela. 2012. Stochastic reachability analysis of hybrid systems. Springer. Platzer, A. 2011. Stochastic differential dynamic logic for stochastic hybrid programs.
- [Chr] Christian Szegedy, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian J. Goodfellow, Rob Fergus. 2013. Intriguing properties of neural networks. CoRR abs/1312.6199.
- [Dez] Dezfoulan S. Hamid, Dan Wu, Ahmad Imran Shafiq. 2012-2013. A generalized neural network approach to mobile robot navigation and obstacle avoidance proceedings. International Conference (IAS) 12. Jeju Island, Korea. 26-29.
- [Dim] Dimitris C Dracopoulos. 1997. Evolutionary learning algorithms for neural adaptive control. Springer.
- [Dra] Dracopoulos Dimitris C. August 1997. Evolutionary learning algorithms for neural adaptive control. Springer.
- [Erb] Erbes T., Shukla S. K., Kachroo P. 2005. Stochastic learning feedback hybrid automata for dynamic power management in embedded systems. Institute of Electrical and Electronics Engineers (IEEE). Mid-Summer Workshop on Soft Computing in Industrial Applications 208-213.
- [Fra] Framework for Cyber-Physical Systems. 2017. Volume 1, National institute of standards and technology special publication. 1500-201.
- [Fre] Fred S. Roberts. Vulnerabilities of cyber-physical systems: from football to oil rigs command, control, and interoperability center for advanced data analysis (CCICADA). Rutgers University.
- [Ger] Gerasimos G. Rigatos. May 2013. Sensor fusion-based dynamic positioning of ships using extended Kalman and Particle Filtering. Robotica. 31 (Issue 3).
- [Hai] Haiqing Shen, Hirotada Hashimoto, Akihiko Matsuda, Yuuki Taniguchi, Daisuke Terada, Chen Guoe. 2019. Automatic collision avoidance of multiple ships based on deep Q-learning. Applied Ocean Research. 86:268-288.
- [Hes] Hespanha J. 2004. Stochastic hybrid systems: applications to communication networks. Hybrid Systems: Computation and Control: A coordination architecture for spacecraft formation control in computer Science. Berlin: Springer, 387-401.
- [Ime] Imen Graja, Slim Kallel, Ahmed Haj Kacem, Nawal Guermouche, Saoussen Cheikhrouhou. 2018. A comprehensive survey on modeling of cyber-physical systems.
- [JLy] J. Lygeros, K. H. Johansson, S. Sastry, M. Egerstedt. 1999. On the existence of executions of hybrid automata. Institute of Electrical and Electronics Engineers (IEEE): Decision and Control. Phoenix: AZ.
- [KHJ] K. H. Johansson, M. Egerstedt, J. Lygeros, S. Sastry. 1999. On the regularization of zeno hybrid automata. Systems & control letters. 38:141-150.
- [Kha] Khaitan Siddhartha Kumar, McCalley James D. 2015. Design techniques and application of cyber physical systems.
- [LuS] Lu Sun, Mingtan Tan, Zhe Zhou. 2018. A survey of practice adversarial example attacks. Cyber-security.
- [Mar] Martin Brossard, Axel Barrau, Silvere Bonnabel. 2019. AI-IMU Dead-reckoning.
- [NiC] Ni Ceo. 2006. Keynote address National science foundation workshop. Business Wire.
- [Pan] Panos J. Antsaklis, Kevin M, Passino Kluwer. 1993. An Introduction intelligent and autonomous control. Norwell (MA): Kluwer academic publishers.
- [Per] Perera Lokukaluge P. 2018. Autonomous ship navigation under deep learning and the challenges in colregs.
- [San] Sanfelice Ricardo G. 2015. Analysis and design of cyber-physical systems: A hybrid control systems approach.
- [Tec] Technology outlook 2025. DNV-GL.
- [Vap] Vapnik V. N., 1998. Statistical learning theory. New York. Wiley.
- [Wie] Wieland Brendel, Matthias Bethge. 2019. Approximation CNNs with bag of local features models works surprisingly. ICLR.
- [Wro] Wrobel Krzysztof, Montewka Jakub, Kujala Pentti. October 2018. Towards the development of a systems theoretic model for safety assessment of autonomous merchant vessel. Antonioli GE. Proceedings of the 3rd reliability engineering and system safety. 178, 209-224.