Human-machine systems resilience – Safety application

Lya Gu, Simon Enjalbert, Frédéric Vanderhaegen

Human-Machine Systems Resilience – Safety Application

Liya GU[1,2,3], Simon ENJALBERT[1,2,3], Frédéric VANDERHAEGEN[1,2,3]

[1]*Univ Lille Nord de France, F-59000 Lille, France*
[2]*UVHC, LAMIH, F-59313 Valenciennes, France*
[3]*CNRS, UMR 8530, F-59313 Valenciennes, France*
(guliya0000@hotmail.com, simon.enjalbert@univ-valenciennes.fr, frederic.vanderhaegen@univ-valenciennes.fr)

Abstract: In this paper, we aim to analysis the resilience of Human-Machine Systems (HMS). We apply a definition of resilience in resilience engineering to describe the ability of HMS to recover from disturbances. The resilience of HMS is assessed by using the system safety as an indicator. The interpretation of the evolution of a safety indicator leads to the HMS resilience characterization. A perspective can be to propose the actions of humans to improve the resilience of studied HMS.

Keywords: Human-Machine system, Resilience.

1. INTRODUCTION

The so-called Human-Machine Systems (HMS) is a system in which the functions of the worker and the machine are interrelated and necessary for the operation of the system. Although there are many works about how to design, modelling and analysis HMS, they aim to explore the human-machine interface (Dearden and Harrison, 1997), to analyze the tasks and functions allocation, to design the barriers and to assess the risks (Zio, Mercurio, Podofillini and Dang, 2006), etc. Few works have been done to assess the ability of systems to recover the performance from a disturbance. This ability is an important target to evaluate the stability of systems, thus our research work focus on the assessment of this ability of HMS. And we borrow the conception of resilience in resilience engineering (Hollnagel and Woods, 2006) to name this ability. In this article, we limit that the resilience of systems depends on the reaction of operators.

The article is organized as follows. In the second section, we give the brief overview of resilience in existing works. A formulation to assess the potential resilience of HMS is given in the third section. In the forth section, the computation results are presented. Finally, we give the conclusion and perspectives.

2. STATE OF THE ART ON RESILIENCE

Nowadays, the concept of resilience is applied not only in the field of ecology but also in other scientific communities as important indicators of assessment. For HMS, the following definition given in the resilience engineering can be adopted 'Resilience is the intrinsic ability of an organization (system) to keep or recover a stable state allowing it to continue operations after a major mishap or in presence of a continuous stress (Hollnagel and Woods, 2006)'. The selected concept of resilience is tightly related to the theory of safety management. The safety assessments usually focus on what can go wrong, and how such developments can be prevented, whereas, resilience engineering focuses on how system can succeed under varying and unpredictable conditions. For the reason of tight relations between resilience and safety of systems, the safety of system can be an indicator of resilience.

Several different measurements of resilience have been proposed in literature. The measurement of Martin evaluates the resilience by maximum intensity of an absorbable force by the system without perturbing its functioning or its regulation mechanisms (Martin, 2005). In Luo and Yang, (2002), the measurement of the instantaneous is linked with the speed of recovery of the disturbance. Both of them do not consider the time of recovery which is an important requirement according to the definition of resilience. The resilience can also be calculated by the opposite of the tangent of the result of ratio between resistance and the recovery time of an attack or a disturbance (Perez-España H. and Arreguín-Sanchez, 2001). However the arctangent function is not a continuous function. All these measurements are related to a minimum acceptable threshold of performance of systems about defined resilience indicators (which is defined by the designers or users of systems). When a disturbance occurs, the system should try to insure its performance to be better than the threshold. If its performance has already been worse than the threshold, the system should try to make it return to the threshold as early as possible or to make it not too bad or too far to the threshold one.

3. HMS RESILIENCE

3.1 System safety

In this paper, the safety of the system is determined by the sum of influence of factors considered and given by the following expression (1):

$$Safety(t) = \sum_{i=1}^{n} (\varpi_i a_i(t) \sum_{k=1}^{m_i} \gamma_i^{\,k}) \qquad (1)$$

Where *n* is number of factors. Each factor corresponds to one safety criteria, such as the velocity, the distance of brake, awareness of drivers, etc. for the transport systems. For each factor $i \geq 1$, a factor value a_i is considered. For instance, the velocity of transport systems can be a factor value. Different factor values have different effects to the safety of systems. Therefore, the levels of factor value are defined for each factor *i*. mi indicates number of levels defined for factor *i*. Each level corresponds to an interval of value for a factor. For instance, for the factor of velocity, it is possible to be over speed, normal speed or slow speed. ϖ_i is weight of factor i defined to balance the importance of factors values in the equation. γ_i^k is influence of factor *i* if a_i is including in the level *k*, γ_i^k is defined as a uniform distributed random variable between 0 and *Rik* where *Rik* is the most probably important influence for factor *i* of level k, otherwise γ_i^k is equal to 0.

The defined function allows representing the evolution of the safety for the considered HMS. Then the characterisation of systems resilience can be shown by the evolution of the defined function in the past period of time and the value of disturbance.

3.2 Evaluation of resilience

The evolution of system safety during a period of time is presented by a curve in Figure 1. In normal case, the safety level of systems is described as the baseline situation which means that the system is in safety. When a disturbance occurs, the safety of systems is influenced and the level of safety is declined. When the system (the operators or machines) is aware of the change of the situation or when they anticipate the change, they execute actions to keep or to recover the stable state of the safety. In order to measure the resilience, a minimum acceptable threshold of safety is defined in research works. The threshold indicates a lower safety level than that of baseline situation.

In this article, we propose that the resilience of system is related to the level of safety of systems in the past time when the level is under the defined acceptable threshold and to the value of perturbation. Thus the area presented in Figure 1 indicates the resilience of HMS.

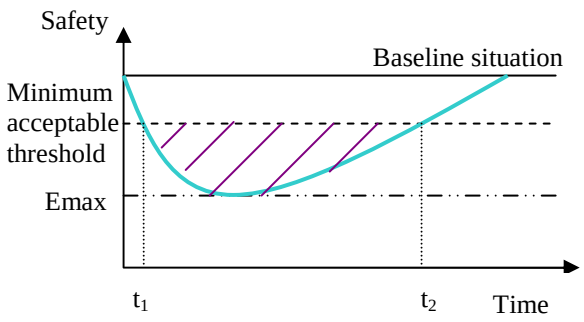

Fig. 1 Proposed measurement of resilience.

In Fig.1, the bigger the shadowy area is, the less the system is resilient, which means that in order to improve the resilience of systems, we should minimize the recovery time t_2-t_1 and the amplitude of the change E_{max} which is caused by disturbances.

4. APPLICATION TO HUMAN-MACHINE SYSTEMS

The COR&GEST (French acronym for Railway Driving and Traffic Management) platform, developed by the LAMIH in Valenciennes, is used to simulate railway driving systems. We use this platform to experiment our proposition of evaluation of resilience. Two factors influencing the safety of systems are considered in our work. They are the velocity of train *Ve* and the recovery time *Rt*. the train is in safety by thinking of the factor of velocity, when the velocity of train equal to the predefined limited *Vp*, In the other word, the bigger the velocity is, the more dangerous the system is. In this article, we do not consider the case that velocity of train is smaller than the predefined one because few accidents are caused by this reason in reality. While the recovery time describe a period of time to make the velocity of train accord with the predefined limited. For instance, there is a transformation area in front of the train and the limited velocity to corner is smaller than that for the straight rail. The driver brakes the train. The period of time to complete the action of brake is called the recovery time. In order to keep the safety of systems, the recovery time should not exceed a theoretic limit called available time *At* which is usually defined by designers. *Ve* and *Rt* vary according to the situations.

According to our proposed method in expression (1) for safety evaluation, the studied system safety can be determined by the following equation (2) for the two considered factors:

$$Safety(t) = \varpi_v (Ve(t) - Vp(t)) \sum_{k=1}^{2} \gamma_V^{\,k} + \varpi_r Rt(t) \sum_{k=1}^{2} \gamma_T^{\,k} \qquad (2)$$

Where γ_V and γ_T are influences of factors velocity and recovery time, respectively. The influences are variable according to the value of factors. Two levels *k* are defined for each factor, which means that a limited value is defined for each factor. The part below the limit is called level 1 and the other part is level 2. The limited value of velocity is defined by *Vp*+10 which is defined by platform as an emergency limit. According to the KVB (speed control by beacons) standard, when the velocity of trains is bigger than *Vp*, an alarm sounds and the control panel indicate to the driver to adjust the trains speed without delay. When the velocity passed the emergency limit, the KVB automatically engages emergency brakes on the train. For the factor of recovery time, the limited value is defined as 80% of available time *At*, which is proposed by the designer of platform. The drivers gain time to dilatorily execute following operations if they finish previous operations in the 80% of available time *At*. If *Ve* (*Rt*) is including in the level 1, the influence $\gamma_V^{\,1}$ ($\gamma_T^{\,1}$) is defined as a uniform distributed random variable between 0 and 1,

otherwise $\gamma_V{}^2$ ($\gamma_T{}^2$) is uniform distributed random variable between 0 and 3. A more important influence value means that the system is in a more dangerous condition. ϖ_v (ϖ_r) is the weight of velocity (recovery time), respectively. They are proposed to balance the importance of two factors in the presentation of safety of systems. In our work, ϖ_v (ϖ_r) are respectively given in following expressions (3) and (4):

$$\varpi_v = \frac{1}{\overline{Ve - Vp}} \qquad (3)$$

$$\varpi_r = \frac{1}{At} \qquad (4)$$

Where $\overline{Ve - Vp}$ is the mean of the difference between the real velocity *Ve* and the predefined one *Vp*.

We evaluate the safety according to expression (2) for a railway driving system. In order to determine the safety threshold, we define an exceeding train velocity under "10km/h" of the predefined value *Vp* as acceptable and γ_V is a uniformly distributed number between 0 and 1. Otherwise γ_V is a uniformly distributed number between 0 and 3. The acceptable recovery time is under the 80% of the available time. If bigger than 80%, γ_T is a uniformly distributed number between 0 and 3. Otherwise it is between 0 and 1.

The evolution of the studied system safety is presented in Fig.2. The threshold, represented by the green line, equals to 3.33 safety units. Situations with a smaller safety value are safer than the ones with bigger values. The most safety situation presented in the figure occurs at the 17th unit of time with 0.02 safety units, while the most dangerous situation occurs at the 19th unit of time with 13.18 safety units. The reason for the 19th unit of time to be so dangerous is the driver did not recognize the situation modification and did not decelerate the train. That is why the difference between the real velocity and the predefined one is important. The safety value could be increased, and the system more and more dangerous, when the difference between the real velocity and the predefined one is increasing and/or when the ratio of recovery time and the available time is increasing. However, the situation with a small safety value, such as the situation at the 17th unit of time, indicates the driver recognized a situation modification quickly enough to adjust the velocity of the train in time.

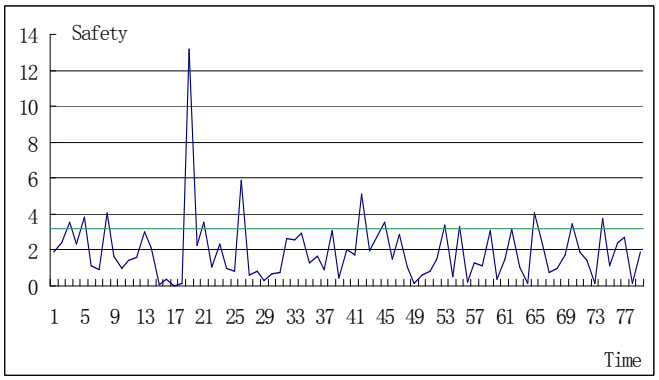

Fig. 2 Evolution of system safety.

According to the definition of resilience presented in the above section, the system is considered to be resilient if the driver can adjust the velocity to the predefined one to ensure the system safety when a situation modification occurs. The resilience of system can be evaluated by the area determined by the continuous curvature and the green line. The bigger the area under green line is, the more resilient the system is. Situations corresponding to the area above the threshold indicate more dangerous cases which can lead to accidents.

5. CONCLUSIONS

In this paper, we propose to evaluate the Human-Machine Systems (HMS) and assess the potential resilience of systems. The State of Art of resilience is given and we employ an adopted definition for HMS. The system safety is defined as an indicator of resilience. We proposed a measure to evaluate the resilience based on this indicator in order to evaluate safety performance of studied HMS. The resilience of railway driving simulation system is presented.

In further works, we may utilise BCD model to propose actions for human operator in order to improve the resilience of HMS.

6. ACKNOWLEDGMENTS

The present research work has been supported

By International Campus on Safety and Intermodality in Transportation,

The Nord-Pas-de-Calais Region,

The European Community,

The Regional Delegation for Research and Technology,

The Ministry of Higher Education and Research,

The National Center for Scientific Research,

and The Scientific Group on Surveillance, Safety and Security of the Big Systems.

The authors gratefully acknowledge the support of these institutions.

REFERENCES

Chaali-Djelassi A. (2007). *Modélisation et prédiction des franchissements de barrière basées sur l'utilité espérée et le renforcement de l'apprentissage application à la conduite automobile. Phd.* Thesis de Université de Valenciennes et du Hainaut-Cambrésis.

Dearden A.M., Harrison M.D. (1997). Impact and the design of the Human-Machine Interface. *IEEE Aerospace and Electronic Systems Magazine*, volume 12(2), pp 19-25.

Hollnagel E. and Woods D.D. (2006). *Resilience Engineering: concepts and precepts*, chapter Epilogue: Resilience Engineering Precepts. Ashgate publishing, Ltd.,

Luo M.Y. and Yang C.S. (2002). Enabling fault resilience for web services. *Computer communications*, volume 25(3), pp 198-209.

Martin. S. (2005) *La résilience dans les modèles de systèmes écologiaues et sociaux.* Phd thesis, Ecole Normale Supérieure de Cachan.

Paton D. and Daly M. (2007). Measuring community resilience. *3rd societal planning for natural hazards research forum*. New Zealand.

Perez-España H. and Arreguín-Sanchez F. (2001). Aninverse relationship between stability and maturity in models of aquatic ecosystems. *Ecological modelling*, volume 145 (2-3), pp 189–196.

Vanderhaegen F.(2004). The benefit-cost-deficit (BCD) model for human error analysis and control. *IFAC/IFORS/IEA symposium on analysis, design, and evaluation of human machine systems*. USA. 7-9 Sep.

Zio E., Mercurio D., Podofillini L. and Dang V.N. (2006). Human-Machine System dynamic model for accident scenario analysis. *Proceedings of European Safety and Reliability Conference*. Estoril, Portugal.