Fault Tolerant Steer-By-Wire Reliability Evaluation with Mechanical Backup

G. Zuo[*1] H. Kumamoto[*1] O. Nishihara[*1] R. Hayama[*2] S. Nakano[*2]
Graduate School of Informatics, Kyoto University [*1]
(Kyoto, 606-8501 Japan, 075-753-3367, kumamoto@i.kyoto-u.ac.jp)
Research & Development Center, Koyo Seiko Co., Ltd. [*2]
(Nara, 634-8555 Japan)

A fault tolerant steer-by-wire (SBW) system requires an operation procedure to cope with partial system degradations. This paper presents a reliability quantification method that converts the operation procedure into an augmented Markov transition diagram where each state represents either a normal SBW, or a partially degraded or a completely failed SBW. The system reliability is quantified in terms of the state probabilities calculated from a numerical integration of the Markov diagram specified by component failure rates. A structural design was already proposed and an example of operation procedure was derived in our previous study for a SBW system consisting of a principal SBW, a standby SBW and a mechanical backup hopefully with a power assist feature. The proposed method is demonstrated by an application to this SBW design. It turns out that the SBW system demonstrates a considerably high reliability through the introduction of mechanical backup. The power assist, however, is rarely available during the mechanical backup mode. This lack of power assist can be reduced by increasing reliability of ECU (Electronic Control Unit).

Keywords: *steer-by-wire, reliability, fault tolerance, partial system degradation, Markov diagram*

1. Introduction

A SBW (Steer-By-Wire), in its literal sense, has no mechanical connection[1, 2, 3] found in conventional power steering systems. The road-wheels can be actuated independently of the hand-wheel according to sophisticated control laws to assist steering capability of drivers. The hand-wheel can be designed to receive suitable reaction torque to enhance the human-vehicle steering interface. The SBW thus provides an indispensable hardware device in which various driver support systems for the ITS are built.

A complete loss of steering may occur for the SBW when important components such as ECU (Electronic Control Unit) fail. A prudent operation procedure, i.e., a type of software design, is required to cope with partial system degradations, together with a fault-tolerant hardware design for prevention of the partial as well as complete system failures.

Amberkar[4] listed potential candidates of methods of analyzing reliability of SBWs. Few papers have clarified methods actually feasible to quantify reliabilities of various SBW designs. An operation procedure to cope with partial SBW degradations has to be clarified and taken into account for this reliability quantification. The purpose of this paper is to give a new quantification method actually feasible.

The authors[5] used fault trees, minimal cut sets, minimal path sets to derive an operation procedure for a SBW with a mechanical backup.

The present paper quantifies this SBW design with the mechanical backup to demonstrate the method proposed here. The operation procedure[5] is, through a suitable state augmentation, converted into a Markov transition diagram where each state represents either a normal SBW, or a partially degraded or a completely failed SBW. The system reliability is quantified in terms of the state probabilities calculated by a numerical integration of the Markov diagram specified by component failure rates.

2. SBW with mechanical backup

2.1. Fault-tolerant design

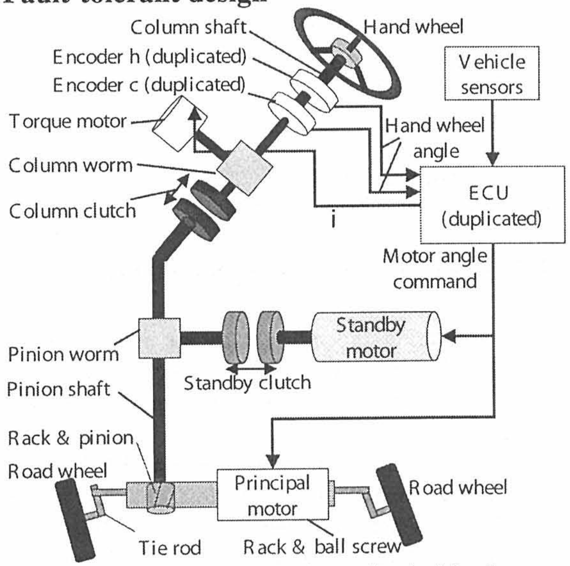


Fig. 1 Fault-tolerant SBW with mechanical backup.

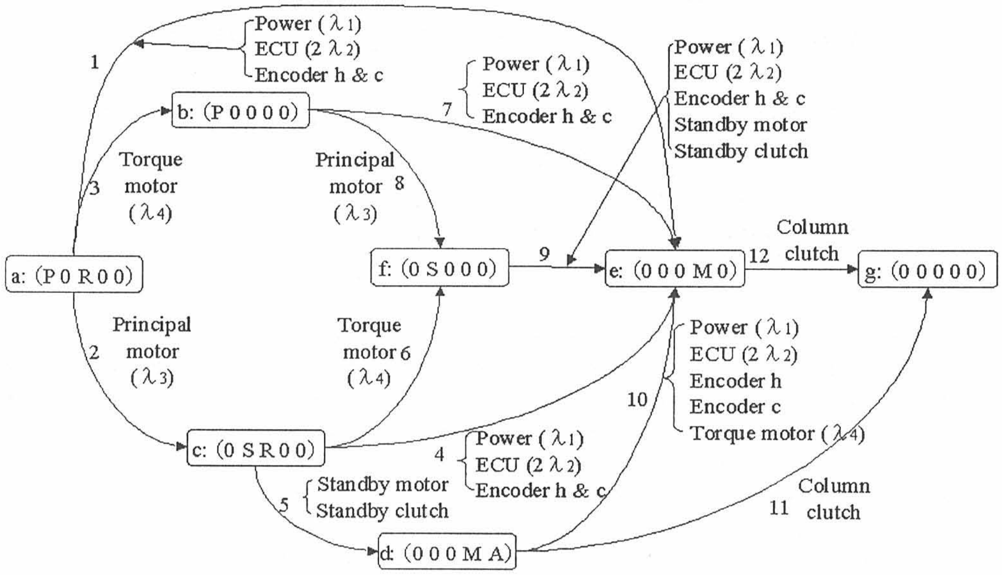


Fig. 2 State transition diagram for a SBW with mechanical backup.

A principal motor functions as a steering actuator as shown in Fig. 1.

A standby motor is a backup actuator. The reaction-torque is acted on the hand-wheel by a torque motor. The three motors are commanded by duplicated ECUs. When both principal and standby motors fail, the road-wheels and hand-wheel are mechanically connected via a column clutch, thus reducing to a conventional "manual" steering. The torque motor, in turn, is used to generate an assist-torque during this manual steering mode.

The hand-wheel torque is detected by a pair of upside and downside encoders to measure a twist angle in between, and the hand-wheel angle is measured by either one of the encoders in the pair. The upside encoder itself is duplicated as well as the downside one to facilitate failure detection.

The angle command to the principal or standby motor is determined by integrating data from the encoders sensing the hand-wheel torque and angle, and data from vehicle sensors measuring vehicle speed, lateral acceleration, and yaw-rate.

In the simplest case the angle command can be made proportional to the hand-wheel angle.

2.2. Procedure coping with partial failures

The operation procedure[5] can be represented by a state transition diagram shown in Fig. 2. Each of the 7 states "a" to "g" consists of five elements enclosed by parentheses.

1) The 1st element is a principal SBW (PSBW) index. Symbol P (Principal) denotes a normal PSBW where the road-wheels are actuated by the principal motor, while 0 denotes a failed PSBW.
2) The 2nd is a standby SBW (SSBW) index. Symbol S (Standby) denotes a normal SSBW with the road-wheels actuated by the standby motor, while 0 denotes a failed SSBW.
3) The 3rd is a reaction-torque index. Symbol R (Reaction) is the existence of the reaction-torque to the hand-wheel, while 0 the non-existence.
4) The 4th is a manual steering index. Symbol M (Manual) denotes the manual steering through the mechanical coupling, while 0 the manual steering failure.
5) The 5th is an assist-torque index. Symbol A (Assist) denotes availability of the assist-torque as a power steering, while 0 the unavailability.

Some combinations of the five elements are infeasible. The total number of feasible states turns out to be 7. There are 12 feasible transitions.

State "a" thus denotes principal SBW with reaction torque, "b" principal SBW without reaction torque, "c" standby SBW with reaction torque, "f" standby SBW without reaction torque, "d" manual steering with assist-torque, "e" manual steering without assist-torque, and "g" denotes a complete loss of steering.

The state transitions are denoted by arrows labeled by component failures: "Power" denotes power failure, "ECU" denotes failure of either one of the two ECUs, "Encoder h" failure of either one of the two upside encoders, "Encoder c" failure of either one of the two downside encoders, "Encoder h&c" both failures of upside and downside encoders, "Torque motor" failure of torque motor, "Principal motor" failure of principal motor, "Standby motor" or "Standby clutch" failure of standby motor or standby clutch, and "Column clutch" denotes a column clutch failure. Symbols "c" and "h" used for encoders denote "column-side (downside)" and

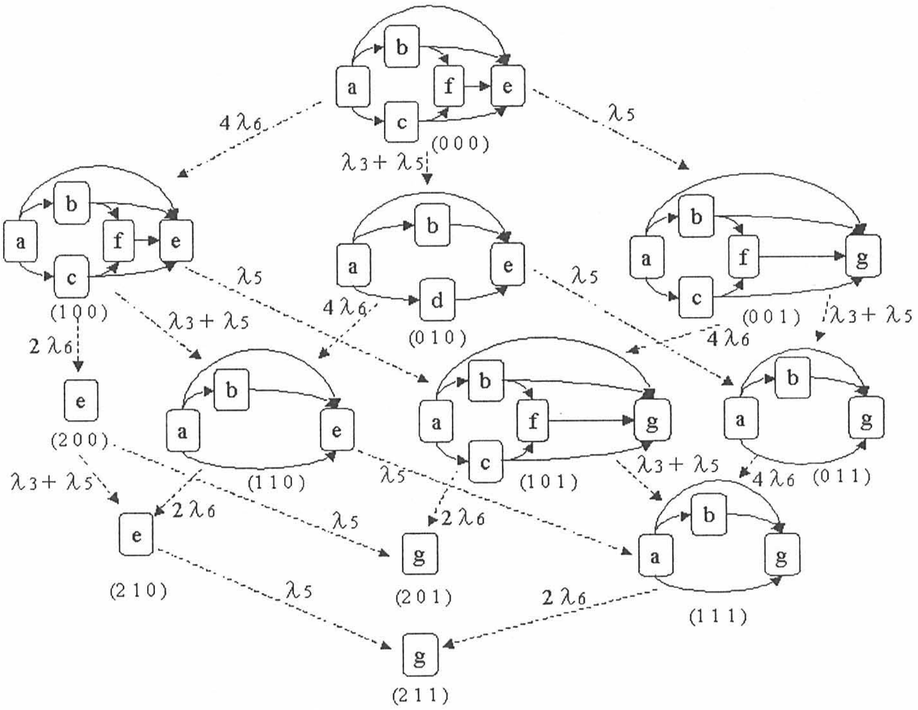


Fig. 3 Layer structure of Markov state transition for a SBW with mechanical backup.

"hand-side (upside)", respectively

The duplicated ECU detects its failure by output comparison; the ECU failure is thus defined as a failure of either one of the two ECUs; the same is true for the duplicated upside encoders or the downside encoders.

Symbol λ beside a component name along a transition arrow denotes a failure rate of the component. Failure rates of encoder h, encoder c, standby motor, standby clutch, and column clutch are not shown because these rates eventually disappear from Fig. 2 and reappear in an augmented diagram of Fig. 3.

The following component failure rates are taken from famous MIL-HDBK-217F [8, 9, 10] where FIT denotes "failures in time" of 10^9 hours:

1) A power source: $\lambda_1 = 1.5$ FIT.
2) A ECU: $\lambda_2 = 15$ FIT.
3) A principal or a standby motor: $\lambda_3 = 20.5$ FIT.
4) A torque motor $\lambda_4 = 0.5$ FIT.
5) A standby or a column clutch: $\lambda_5 = 2.5$ FIT.
6) An encoder: $\lambda_6 = 20$ FIT.

2.3. Quantitative reliability assessment

2.3.1. Layer structure of state transition diagram

A quantitative reliability assessment starts at the state transition diagram of Fig. 2. Unfortunately, this diagram lacks Markov property.

A transition to "d" (manual with assist-torque) from state "c" (standby SBW with reaction-torque) occurs by the sum of failure rates of standby motor and standby clutch, given that these two components were normal when state "c" was visited. However, this transition occurs instantly when standby motor was already failed before the visit to state "c". The transition rate from state "c" to "d" changes according to standby motor and clutch states at the visit to parent state "c", which indicates that the Markov property of the transition diagram is lost.

Similarly, column clutch and encoder h&c are shown to be factors influencing transition rates.

The original diagram is reconfigured into a layer structure to yield a Markov state transition diagram. Each of the 7 states in Fig. 2 is called a main state, while the state shown by triple in Eq. 1 a sub state.

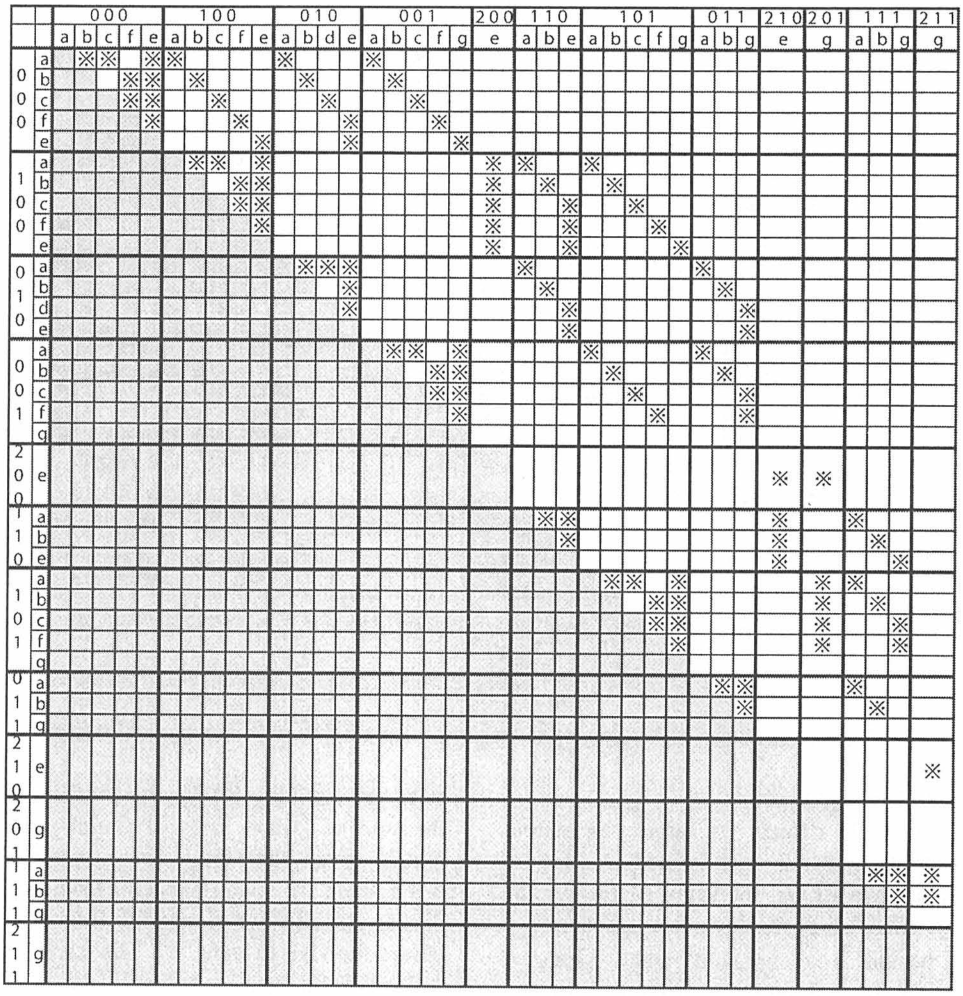
$$\text{(encoder h\&c, standby motor \& standby clutch, column clutch)} \tag{1}$$

The "encoder h&c" have three component states: full in-service denoted by 0, half in-service by 1, and both out-of-service by 2.

The "standby motor & standby clutch" has two states: both in-service denoted by 0, and one or two out-of-service by 1. The "column clutch" has two states: 0 means in-service, 1 in-failure.

The component states are enumerated below.

$$\left(\begin{bmatrix}0\\1\\2\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix}\right) \tag{2}$$



		000					100					010				001					200	110			101					011			210	201	111			211
		a	b	c	f	e	a	b	c	f	e	a	b	d	e	a	b	c	f	g	e	a	b	e	a	b	c	f	g	a	b	g	e	g	a	b	g	g
000	a		※	※		※	※					※				※																						
	b				※	※		※					※				※																					
	c				※	※			※					※				※																				
	f					※				※					※				※																			
	e										※				※					※																		
100	a							※	※		※										※	※			※													
	b									※	※										※		※			※												
	c									※	※										※			※			※											
	f										※										※			※				※										
	e																				※			※					※									
010	a												※	※	※							※								※								
	b														※								※								※							
	d														※									※								※						
	e																							※								※						
001	a																※	※		※					※					※								
	b																		※	※						※					※							
	c																		※	※							※					※						
	f																			※								※				※						
	g																																					
200	e																															※	※				
110	a																					※	※									※		※			
	b																						※									※			※		
	e																															※				※	
101	a																								※	※		※					※	※			
	b																										※	※					※		※		
	c																										※	※					※			※	
	f																											※					※			※	
	g																																					
011	a																													※	※			※			
	b																														※				※		
	g																																					
210	e																																				※
201	g																																					
111	a																																		※	※	※
	b																																			※	※
	g																																					
211	g																																					

Fig. 4 Augmented state transition matrix for a SBW with mechanical backup.

For example, (2,1,0) means that both of upside and downside encoders are failed, the standby motor and/or the standby clutch is failed, and that the column clutch is normal. It is clear that the number of sub states is 3 x 2 x 2 = 12. The number of main states is 7. Thus, the maximum number of augmented states is 12 x 7 = 84.

A number of combinations of main and sub states turn out to be infeasible because some sub states cause state transitions of main states in the original diagram of Fig. 2; these transitions immediately occur when the sub states are caused by relevant component failures. For example, augmented state a(2,1,0) is infeasible, and is replaced by state e(2,1,0).

Fig. 3 becomes the augmented state transition diagram with the Markov property where each main state is conditioned by a relevant sub state shown in parentheses below the main state.

Consider transitions between the sub states denoted by dotted arrows in Fig. 3. Three paths from a(0,0,0) to e(2,1,0) are observed along the dotted arrows. These transitions yield a layer structure classified by the sum of three elements of the sub state. The maximum number of the sum is 4 = 2 + 1 + 1, and the 12 sub states can be arranged by 5 layers.

It is observed in Fig. 3 that:

1) Main state transitions initiated by a sub state transition can be identified easily. For example, augmented state c(0,0,0) on the first layer transits to d(0,1,0) on the second layer when sub state moves from (0,0,0) to (0,1,0).
2) The transitions among main states without a sub state transition can be identified easily from Fig. 2.
3) An augmented state implying a complete loss of steering denoted by "g" is treated as an absorption state from viewpoint of main states as well as sub states. No further transition occurs once this absorption state is reached. For example, transition from g(0, 0, 1) to g(0, 1, 1) need not be considered.
4) The total number of feasible, augmented states is 37, which is smaller than the original 84.

2.3.2. Quantitative reliability assessment

Denote by $P_i(t)$ the probability that the SBW system

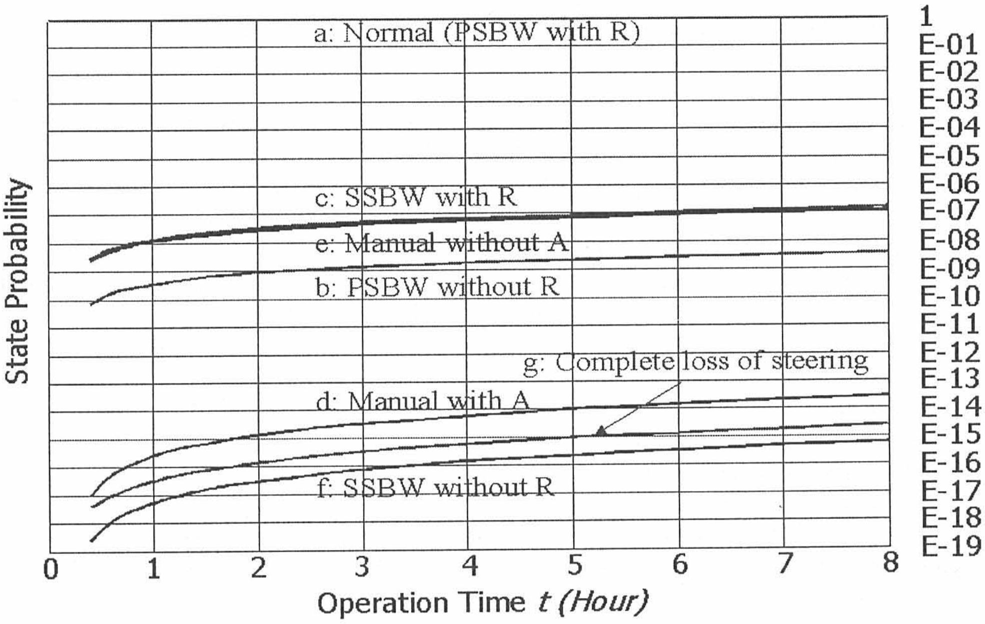


Fig. 5 Time-dependent probabilities of states for a SBW with mechanical backup.

is in state i at time t. Parameter γ_{ji} is a transition rate from state j to i, and γ_{ij} from i to j. The total number of states is $n = 37$. A Markov differential equation is used for a quantitative reliability analysis:

$$\dot{P}_i(t) = \sum_{j=1, j\neq i}^{n} \gamma_{ji} P_j(t) - P_i(t) \sum_{j=1, j\neq i}^{n} \gamma_{ij} \qquad (3)$$

The probability of each state at time t can be calculated from Eq. 3. Transition rates are determined from the component failure rates as shown in Figs. 2 and 3.

Transitions between 37 augmented states are explicitly specified by the matrix shown in Fig. 4. Symbol "*" indicates a transition from a row state to a column state. The diagonal blocks show the transitions between main states without a sub state transition. Non-diagonal blocks denote transitions between main states, given a sub state transition. The matrix becomes an upper triangular form because transition occurs downward or rightward, as shown in Fig. 3.

Consider a continuous operation up to 8 hours for a non-repairable SBW system. State probabilities are plotted in Fig. 5. Assume that the SBW system is renewed at the start of each driving. This means that the driving cannot be initiated until system degradations during the last driving have been repaired. Two time spans are considered for the continuous driving: 2 hours and 8 hours thereafter.

The probability of "state c: standby SBW with reaction-torque" is the order of one failure per 10^8 vehicles after 2 hours of continuous driving. A similar probability to "c" is obtained for "state e: manual steering without assist-torque". Even if the continuous driving increases to 8 hours, the probabilities of these system degradation states remain the order of once per 10^7 vehicles.

On the other hand, the probability of "state g: complete loss of steering" is the order of once per 10^{16} vehicles for 2 hours of continuous driving. For 8 hours driving, it still remains a small value, i.e., once per 10^{15} vehicles. The actual probability of complete loss of steering is further decreased because the SBW system can be repaired when system degradation states are detected.

Note that the assist-torque is less available during the manual steering; this is clear from a comparison of probabilities of states "e" and "d". The designer's intent to provide a power steering feature during the manual mode is not achieved. Calculations showed that this was due to the ECU high failure rate. Improvement of the ECU reliability can reduce the probability of state e.

3. Conclusion

A reliability quantification method for a SBW is presented and an assessment is performed for a demonstration.

1) A fault tolerant SBW design with a mechanical backup is considered.
2) Operation procedures to cope with partial system

degradations are described and eventually converted into a Markov transition diagram.

3) A quantitative reliability assessment taking the operation procedure into account is performed based on the Markov diagram. It turns out that the SBW design demonstrates a considerably high reliability through the introduction of mechanical backup.
4) The power assist, however, is rarely expected during the mechanical backup mode.
5) This lack of power assist can be reduced by increasing the ECU reliability.

Future subjects include:

1) The mechanical backup mode without the power assist might be hazardous due to the excessive manipulation power required to stabilize the vehicle after the transition to the mode. More sophisticated backup designs without the mechanical coupling are to be assessed from a point of view of safety as well as reliability.
2) The component failure rates have wide ranges of uncertainties and more in-depth quantification is required by varying the failure rates in order to reflect present status of our knowledge about the component reliabilities.

4. References

[1] S. Nakano, T. Takamatsu, O. Nishihara, H. Kumamoto. Research on SBW vehicle control (1) - Reaction-torque and front steering wheel control. Transaction of Society of Automotive Engineers of Japan (in Japanese) 2000; 31(2): 53-58.

[2] S. Nakano, S. Nishizaki, S. Nishihara, H. Kumamoto. Research on SBW vehicle control (2) - Improvement in *D** control vehicle response. Transaction of Society of Automotive Engineers of Japan (in Japanese) 2002; 33(3): 121-126.

[3] S. Kleine and J. L. Van Niekerk. Modeling and control of a steer-by-wire vehicle. Vehicle System Dynamics Supplement 1998; 28: 114-121.

[4] S. Amberkar, B. J. Czerny, etc. A comprehensive analysis technique for safety-critical automotive systems. SAE Technical Paper: (2001-01-0674).

[5] G. Zuo, H. Kumamoto, O. Nishihara and S. Nakano. Reliability and safety analysis of fault-tolerant steer-by-wire system. Journal of the Japan Society for Precision Engineering (in Japanese) 2003; 69(8): 1141-1146.

[6] H. Kumamoto and E. J. Henley. Probabilistic risk assessment and management for engineers and scientists. New York: IEEE Press 1996.

[7] O. Nishihara, G. Zuo and H. Kumamoto. Curvature output driver model for a steer-by-wire vehicle. CD-ROM Proc. of the 8th World Congress on Intelligent Transport Systems 2001.

[8] MIL-HDBK-217 F. Reliability prediction of electronic equipment. US-DOD 1995.

[9] Practical application of MIL-HDBK-217 F. Kansai Electronic Industry Development Center (in Japanese) 1999.

[10] New reliability prediction technique. Kansai Electronic Industry Development Center (in Japanese) 2000.

G. Zuo is currently a Candidate of Ph.D. in the Graduate School of Informatics, Kyoto University. His research interests include fault tolerance and ubiquitous networking.

H. Kumamoto is a Professor at Graduate School of Informatics, Kyoto University. His research interest is in the areas of ITS, human systems, reliability/safety analyses, fault tolerance systems, etc.

O. Nishihara is an Associate Professor at Graduate School of Informatics, Kyoto University. His research interest includes dynamics of human machine systems, ITS, and haptic interfaces, etc.

S. Nakano completed his Ph.D. in Informatics at Kyoto University. He is a General Manager of Koyo Seiko Co., LTD. Research & Development center. His research interest is in human machine haptic interfaces.

R.Hayama received the B.S. degree in Electronics from Ritsumeikan University. He is an Assistant Manager of Koyo Seiko Co., LTD. Research & Development center. His research interest is in human machine haptic interfaces.

Received: 4 May 2004
Revised: 18 August 2004
Accepted: 3 September 2004
Editor: Yoshihiro Suda