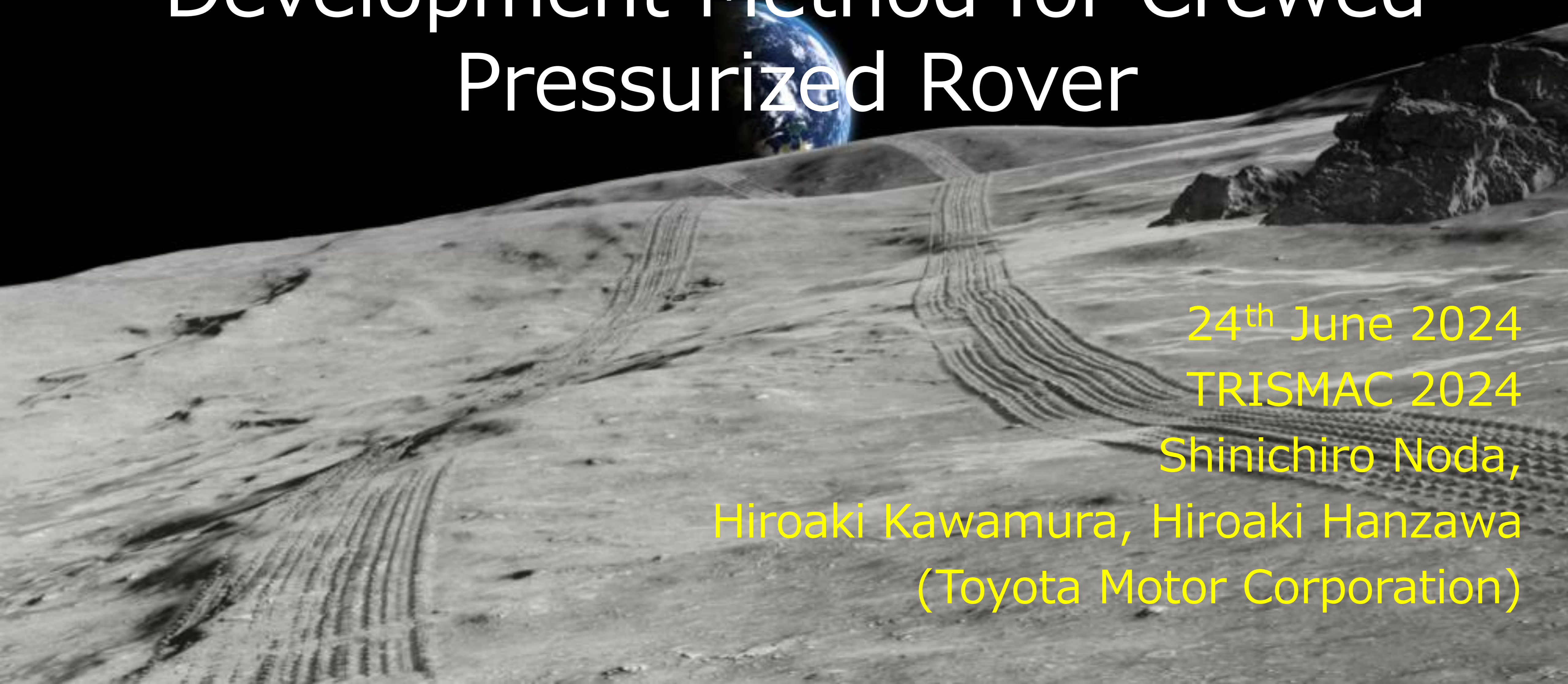

TRISMAC
Trilateral Safety and Mission Assurance Conference 2024
24–26 June 2024
ESA-ESRIN | Frascati (RM), Italy

Model Based Safety and Reliability Development Method for Crewed Pressurized Rover



24th June 2024

TRISMAC 2024

Shinichiro Noda,
Hiroaki Kawamura, Hiroaki Hanzawa
(Toyota Motor Corporation)

Our Vision and Values

We contribute to the "mass production of happiness" by inventing our new cars.

To expand the sphere of human activity by challenging manned pressurized rover

Mobility 2.0 (expansion of mobility into new areas)

Improvement of technology (engineer's dream)

Our new challenges lead to expand human capability

Technology Development to Moon

Feedback to Earth

Technology to generate electricity using only sunlight and water

- Off-road driving performance
- Autonomous driving
- Regenerative Fuel Cells
- UX

The technology developed through the manned pressurized rover development will be returned to society on Earth

Mobility 1.0 (Extension of the value of the car)
Mobility 3.0 (integration with social systems)

Contribution to a carbon-neutral society (CN)

Contribution to the development of new cities and vehicles

Background：Safety & reliability development

From the Earth

Ground Vehicle Development

LAND CRUISER
(1951～)
～**Return safely from anywhere**～

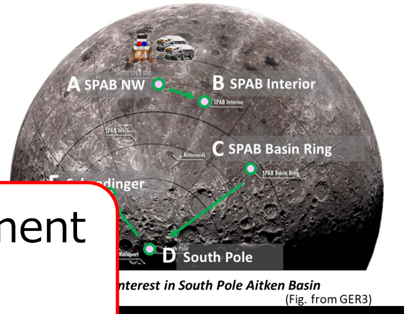
Earth environment
×
Operation

Every terrain, Everywhere

Various roads/terrains forge the vehicle development method on Earth

To the Moon

PR Development



Lunar environment
×
Operation

Uncertain road
Science Mission
(10 years)

We've never been to the Moon..

We needs to transform the development methodology

Background and Objectives

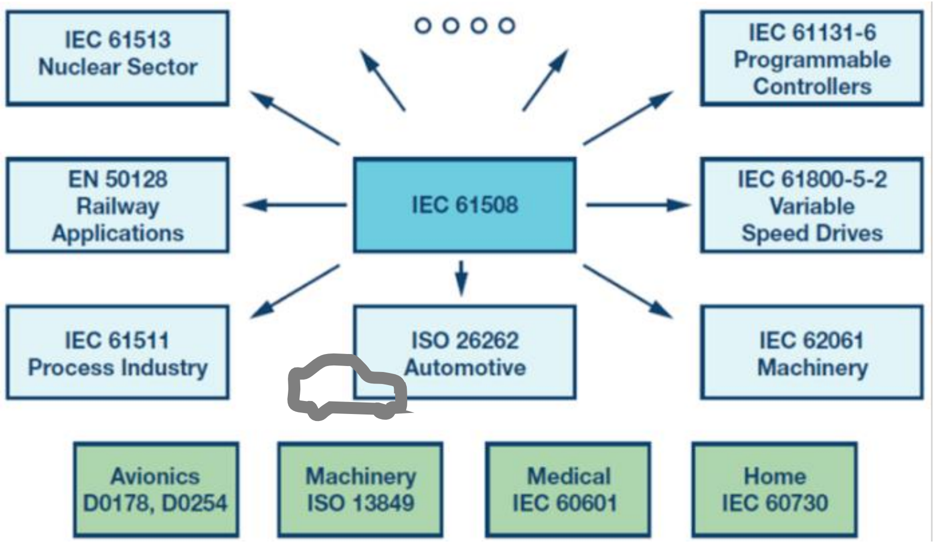
- From the ground vehicles
  - Field experience data on the earth
  - 1 Billion automotives in the worldwide.
- To the moon exploration
  - Unknown extreme environment
  - Off-road capability

Objectives

- Safety & Reliability Development;

  combination with <u>ground vehicle</u> and spacecraft

Functional Safety ISO 26262



ISO26262 Process

Effect Analysis of functional failure

System FMEA is conducted to assess the importance of function.
ASIL was determined based, **Severity (S), Exposure (E), and Controllability (C)**
※ASIL : Automotive Safety Integrity Level

＜Effect analysis＞

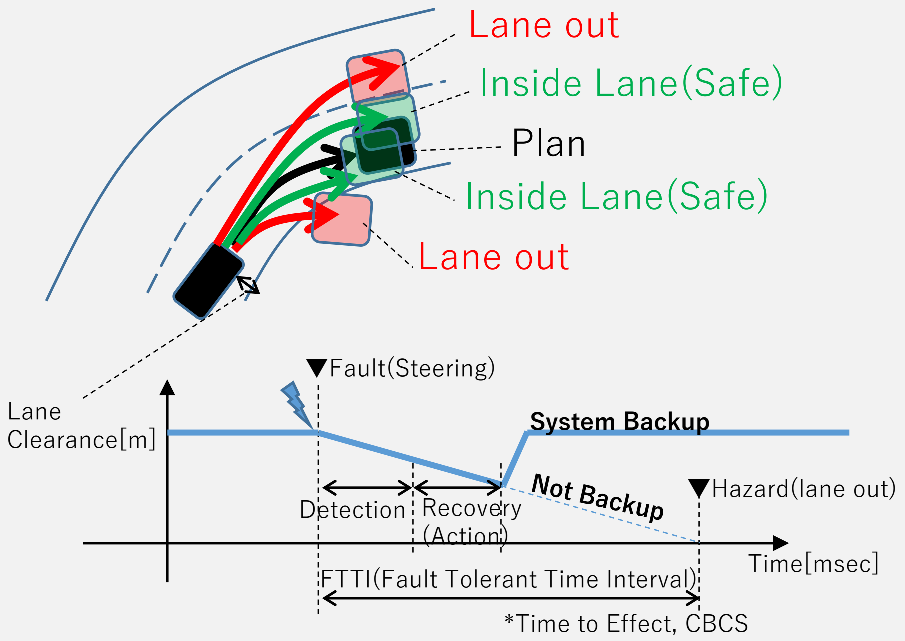
Function	scene	Guide word	Effect	S	E	C	ASIL
Str.	Local road	Over					
		Low					
		Loss					
		Vibrate					
		Opposite					
	Highway	Over	Lane out (to center)				
		Low	Lane out (from center)				
		Loss	Lane out (from center)	S3 (Serious Injure)	E4 (Frequently, depend on driver)	C3 (Hard to control by driver)	D
		Vibrate					
		Opposite					

＜ASIL Matrix＞

S	E	C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	ASIL A
	E4	QM	ASIL A	ASIL B
S2	E1	QM	QM	QM
	E2	QM	QM	ASIL A
	E3	QM	ASIL A	ASIL B
	E4	ASIL A	ASIL B	ASIL C
S3	E1	QM	QM	ASIL A
	E2	QM	ASIL A	ASIL B
	E3	ASIL A	ASIL B	ASIL C
	E4	ASIL B	ASIL C	ASIL D

Define Safety Goal

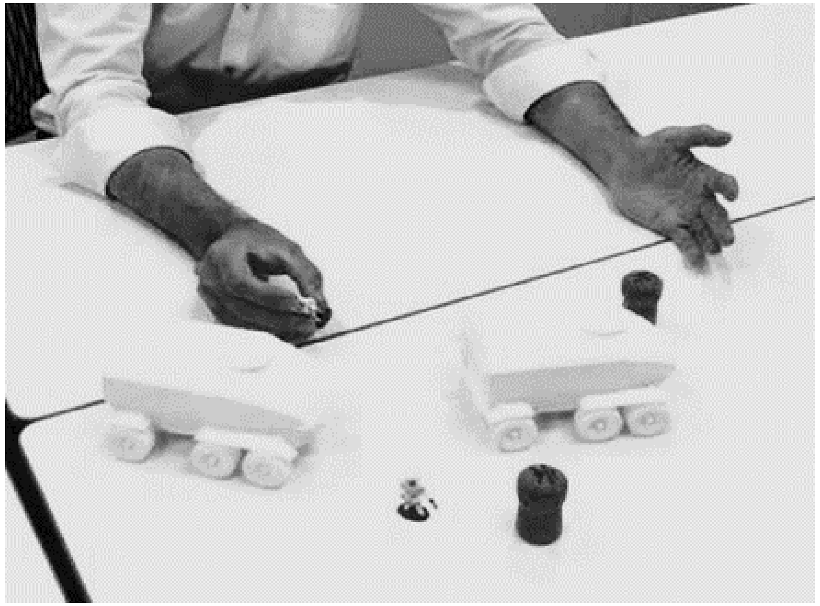
Recovery steering action,
as soon as possible **before vehicle lane out**.

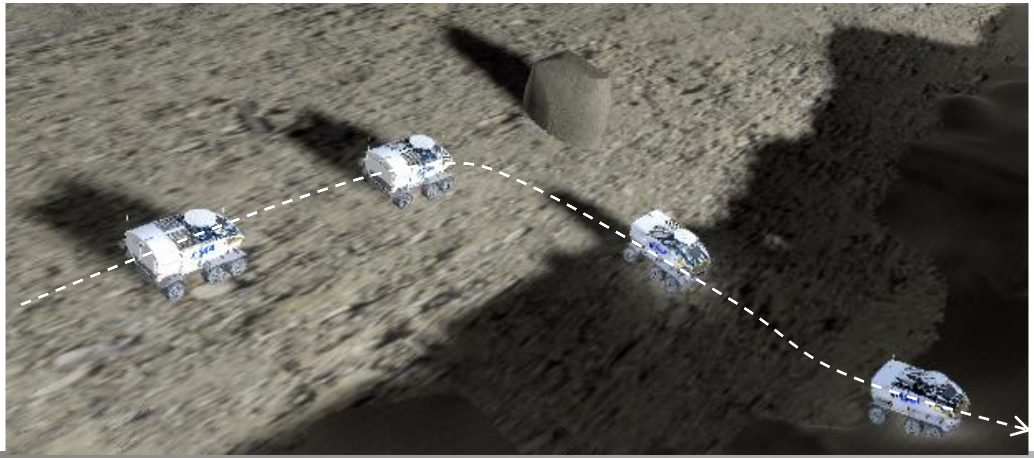


Detection and recovery action shall be completed before hazardous event.

Automobiles are promoting safety development in accordance with **ISO 26262**, oriented from **general safety development. Good tailoring with spacecraft development is necessary**.

Systems engineering : scenario analysis





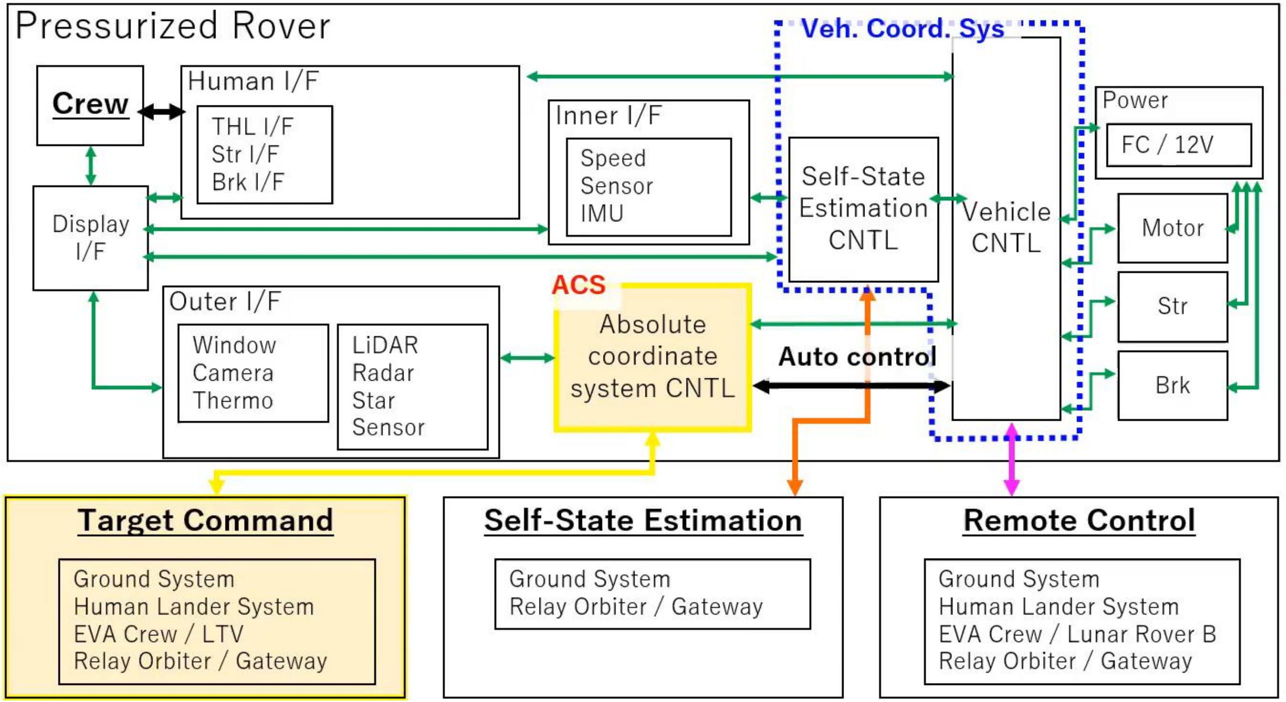
HAZOP guideline words

Main scenario ↓

Extraction of nominal or off-nominal event

		Arbitrary action	hunting	Not work	reverse	noise	over	under	extra	part	early	late	others
	ユースケースがうまく動いたときのシナリオ	勝手に作動	ハンチング	無（不作動）	逆（反対）	他 例：想定外の動作	大（過大）	小（過小）	類（余計な何かが起きる）	一部	早い	遅い	その他（ガイドワード以外）
1	外部システム（与圧、[illegible]ステーション、地上 etc）との通信状態を確認[illegible]	勝手に通信ＯＦＦとなる	通信がON/OFFを繰り返す	外部システムとの通信が確認できない	受信できるが送信できない 送信できるが受信できない	違う外部システム（他の宇宙機）の通信と混		通信状態を確立するが、通信速度が過小					宇宙電波のノイズが重畳する
2	曝露ローバを電[illegible]Ready 状態にする	勝手に電源ダウン		電源Onにできない Ready状態にならない		Ready処理がフリーズする			Ready状態になるが、走行し始めない/指令を受け付けない	正常のはずがReady処理の一部がどうしても異常判定を繰り		Ready処理時間が想定よりもかかる	電源起動部が隕石衝突で破損
3	曝露ローバの状[illegible]る（走行距離、電力量、冷却水温、[illegible]度、ライト点灯等）		値が一定にならない	プロセス途中でエラーが発生して停止			実際より大きな値が測定される。伝達される。	実際より小さな値が測定される。伝達される。					暴露ローバの外観から、破損が確認される
4	曝露ローバを暖[illegible]	勝手に温度が上昇する	温度がふらつく	温度が上昇しない	温度が下がる	別の熱ループ温度が上がる	目標温度を越える	目標温度に達しない	配管にボイドが発生し、熱輸送ができない	配管内が凍り、熱輸送ができない	目標温度に達するのに、想定より早い	目標温度に達するのに、想定より時間がかかる	配管が熱応力で破損する ラジエータがMMODで破損す
5	曝露ローバを試[illegible]（走る･曲がる･止まるの確認）	勝手に走る・曲がる・止まる	動きがふらつく	指示に対し不作動	操作に対し、逆に動く		操作に対し過大に動く	操作に対し過小に動く					
6	曝露ローバの自[illegible]把握する	自己位置ロストする	正しい位置と間違った位置がチャタリングする	前回位置から動かない	自己位置を間[illegible]える	高度計[illegible]しない	[illegible]位置からも大き[illegible]		[illegible]しまう（滑走、[illegible]			自己位置推定に時間がかかる	
7	暴露ローバーの[illegible]外部システム（与圧、ステーション、地[illegible]伝える	通信できない	通信接続が不安定 断続状況になる	自己位置を外部システムに伝えない		相[illegible]先[illegible]する		通信速度が過小				データ収集・伝達に 時間が掛かる	
8	曝露ローバが前[illegible]確認する	勝手にカメラがズームする	カメラが揺れてブレる	・カメラが不動 ・情報伝達手段が不作動	[illegible]た向きにカメラが向かない	映し出される映像が乱れる	[illegible]大で通信ひっ迫する		[illegible]像が飛び飛びに表示される			映し出される映像にタイムラグがある	
9	曝露ローバが与[illegible]追従できる走行経路を決定する	与圧ローバの能力パラメータの一部が勝手に書き換わっている		与圧ローバも追従できる走行経路がない									
10	アクセルONで発進・加速する	加速と同時に自動操縦が遠隔操縦に切り替わって暴走	加速がハンチングする	指示に対して発進しない	指示に対する動きが逆になる(発進と停止が逆)		指示に対して加速度が過大						

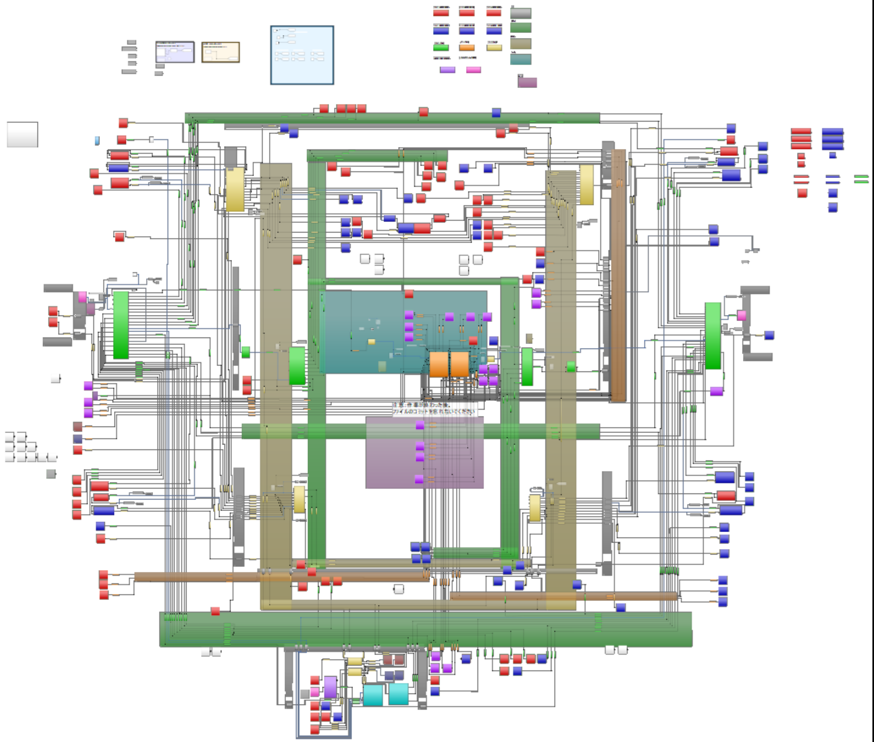
Visual validation of systems functions' behavior



Safety & Reliability model (FMEA)

System safety/reliability modeling

Connecting each subsystems by
“Power”, “communication”, “Thermal”, “Force”



Safety (1FT)

INPUT : failure flag of each components
OUTPUT : failure tolerance flag

Comp.	Failure mode
Battery	Over
	Low
	Loss
W/H	Open
	Short
	Unstable
RLY	Open
	Short
	Unstable
FUSE	Open
DCDC	Over
	Low
	Loss

	INPUT(test case)						OUTPUT				Flag 1: OK 0: NG	Failure rate
	MAIN(leg 1)					SUB (leg 2)	Drive force	Steering	thermal	GNC		
	120V BAT + Generator			RLY-A	RLY-B	・・・						
	Loss	Double	Half	OPEN	OPEN	・・・						
Base FR [ppm]	①	②	③	④	⑤	⑨						
TEST-CASE-**	*					*	×	○	×	×	0	①×⑨
TEST-CASE-**				*		*	○	○	○	○	1	④×⑨
TEST-CASE-**						*	×	×	○	×	0	⑧×⑨

Reliability

INPUT : failure rate of each components
OUTPUT : estimation of failure rate

Failure rate from FMEA :

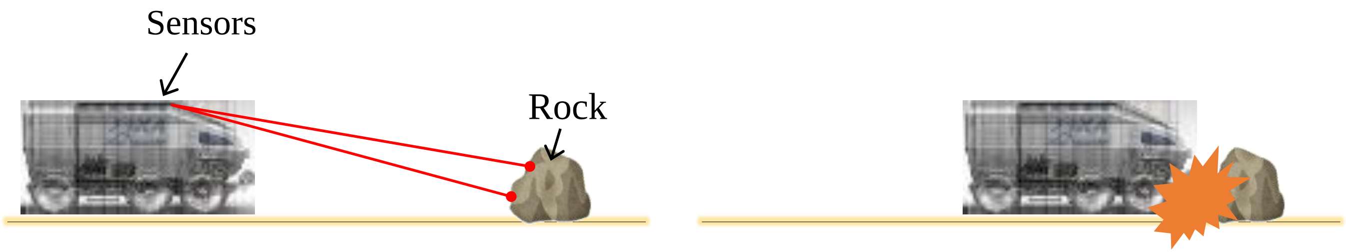
$$F = \sum f_1 \times p_d \times \left(\frac{t_{repair}}{t_{all}}\right) \times f_2 + f_1(1-d) \times \left(\frac{t_{all}}{t_{all}}\right) \times f_2$$

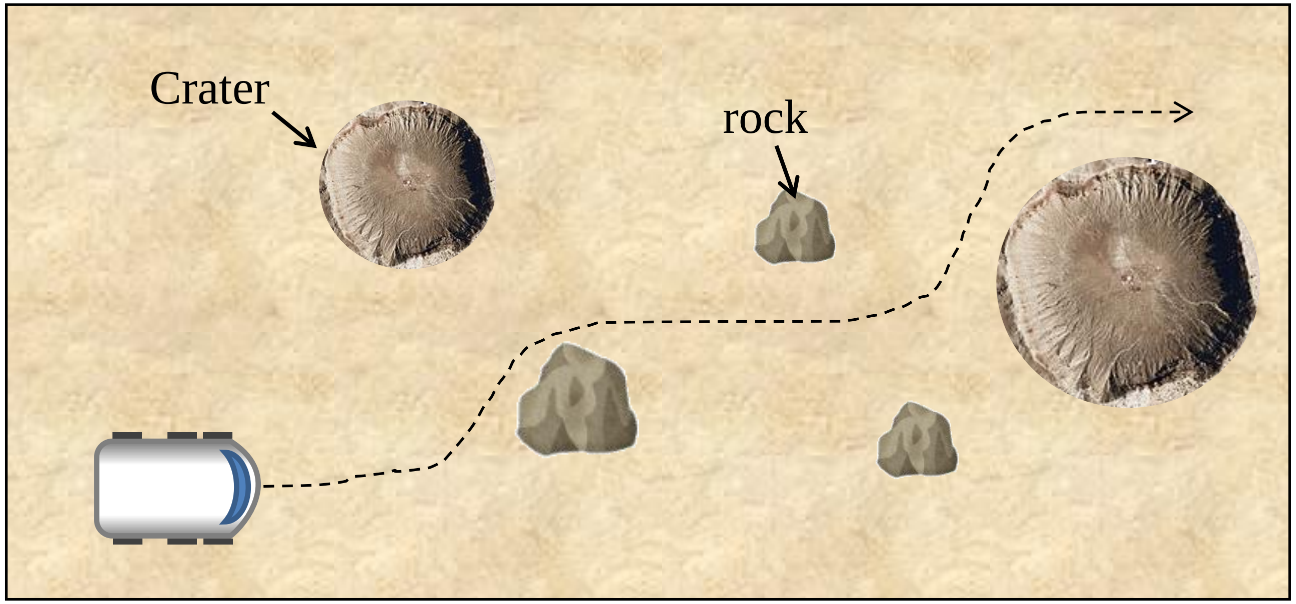
p_d:probability of failure detection,
f_1:primary failure rate, f_2: secondary failure rate

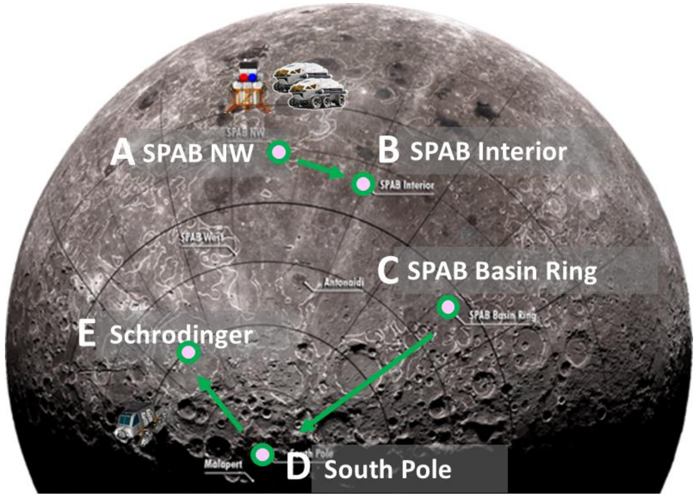
Estimate of failure rate for every fail combination

Autonomous driving on the Lunar terrain

After detecting rocks and craters, PR driving avoid them







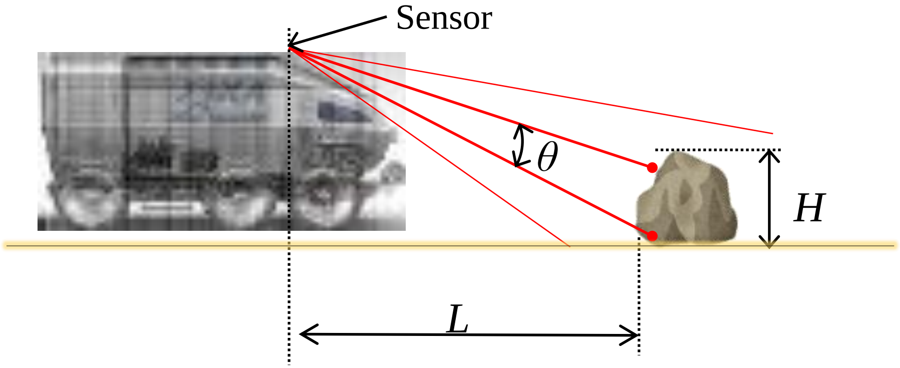
Regions of Interest in South Pole Aitken Basin
(Fig. from GER3)

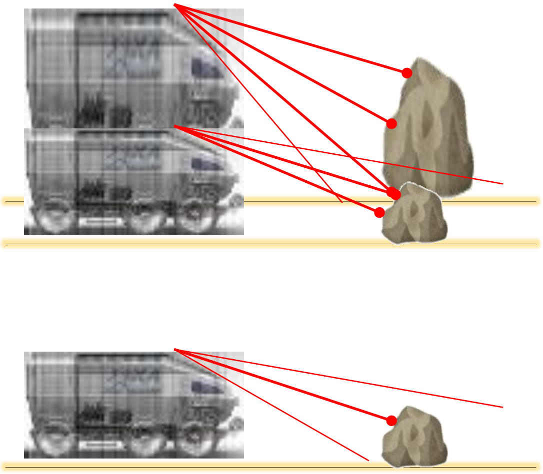
Uncertain driving route
Uncertain surface profile

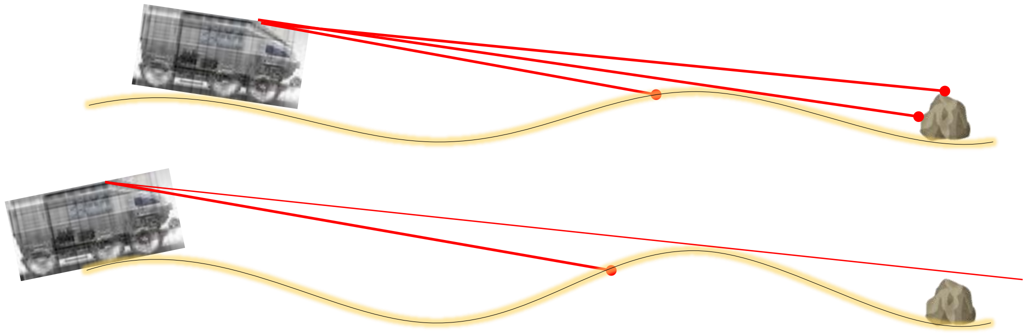
Risk of misdetection of obstacles -> high load into the vehicle

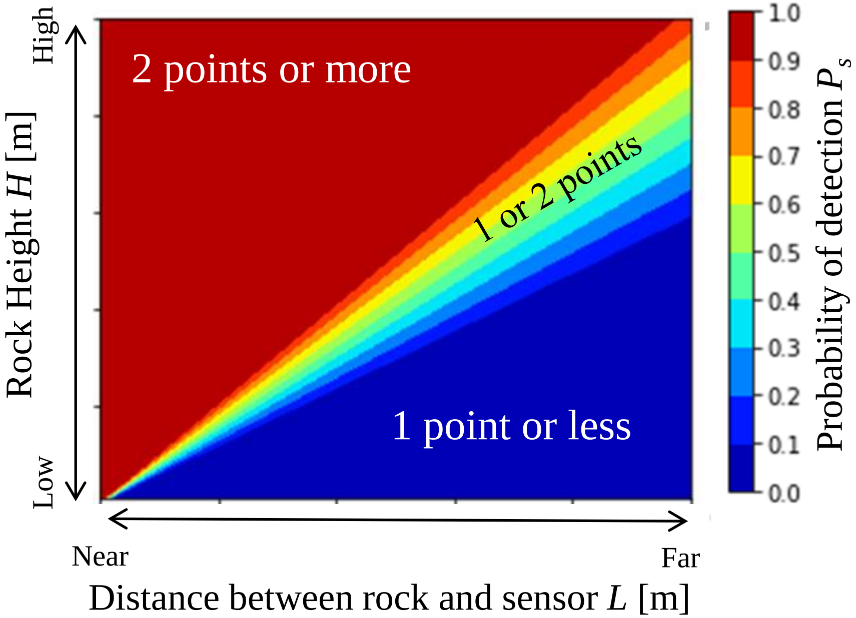
The probability of rock detection

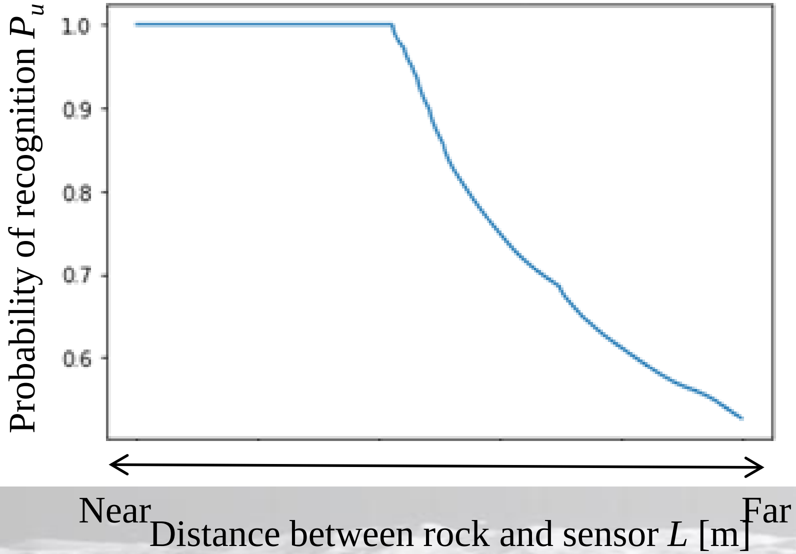
The rock height estimation accuracy;
- depends on the sensing resolution.
- needs reactions from at least two points.





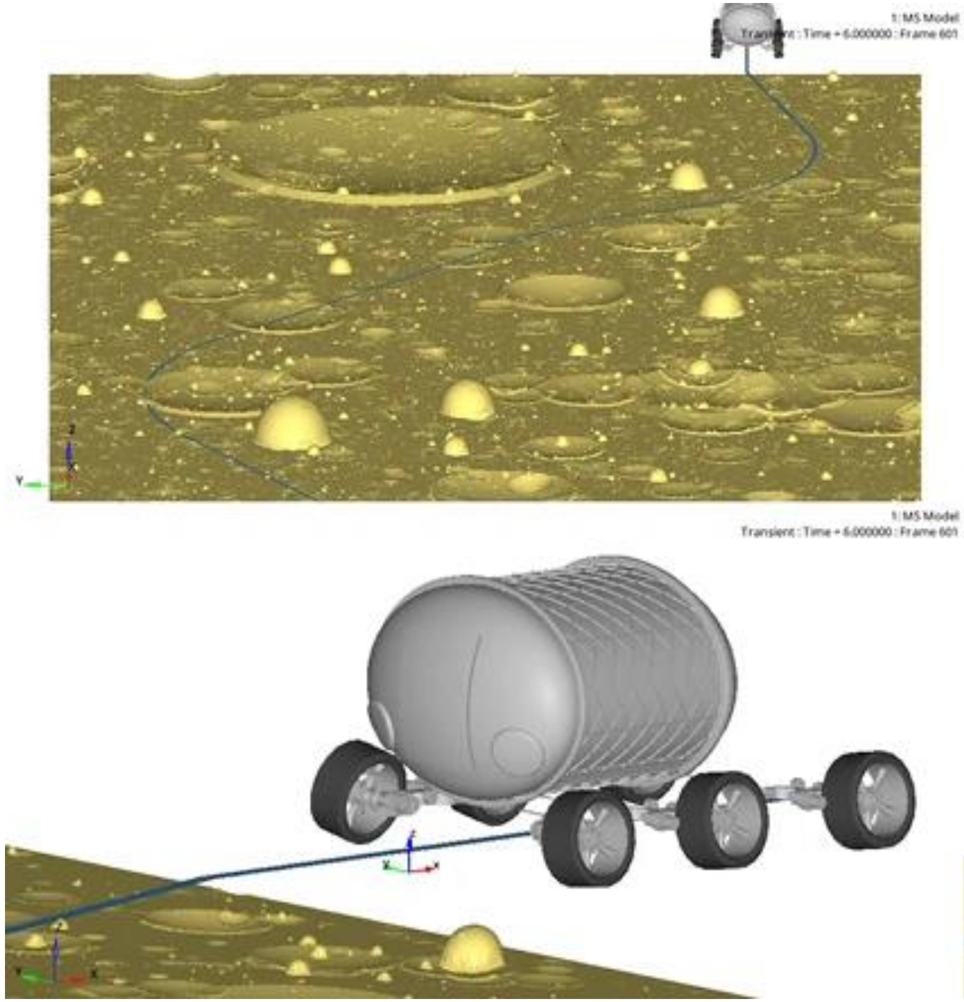




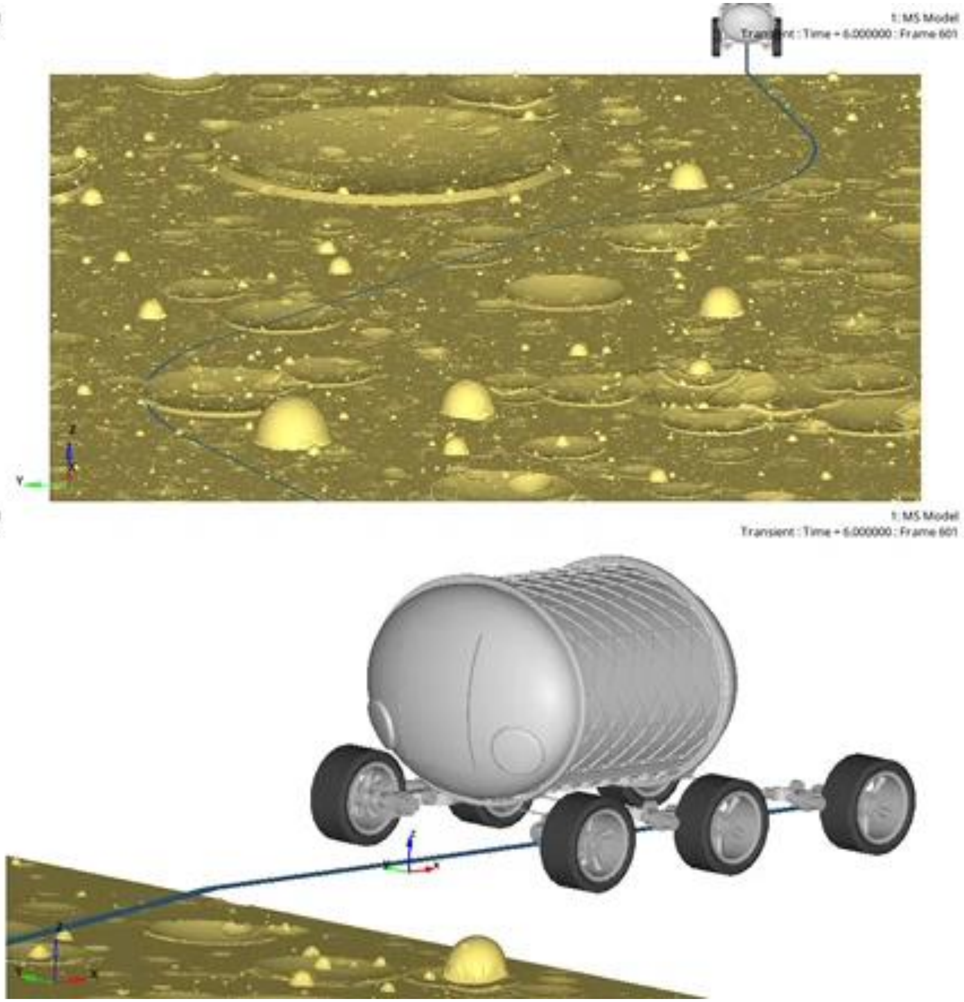


Detection probability is estimated using sensing resolution and lunar surface profiles.

Example of driving on the Virtual Moon surface



1 G simulation

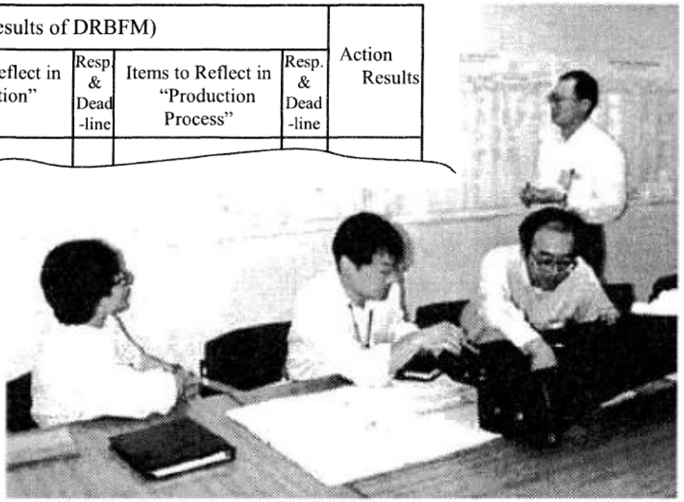


1 /6 G simulation

DRBFM (Design Review Based on Failure Mode)

Component Name／Changes	Function	Concerns Regarding Change (Failure Mode)		When and How Concern Points appear		Effect to Customer (System)	Importance
		Potential Failure Mode due to Change	Any Other Concerns? (DRBFM)	Root Cause / Dominant Cause	Any Other Consideration for Cause? (DRBFM)		

Current Design Steps to avoid Concerns (inc. Design Rule, Design Standard & Check Items)	Recommended Actions (Results of DRBFM)						Action Results
	Items to Reflect in "Design"	Resp. & Dead-line	Items to Reflect in "Evaluation"	Resp. & Dead-line	Items to Reflect in "Production Process"	Resp. & Dead-line	



SAE Paper 2003-01-2877

There are always gaps between the design documents and products/usage. **Design Review** is the best approach to remove them.

Logical review process over reviewer's impression

FMEA + Design Review
⇒ **DRBFM**

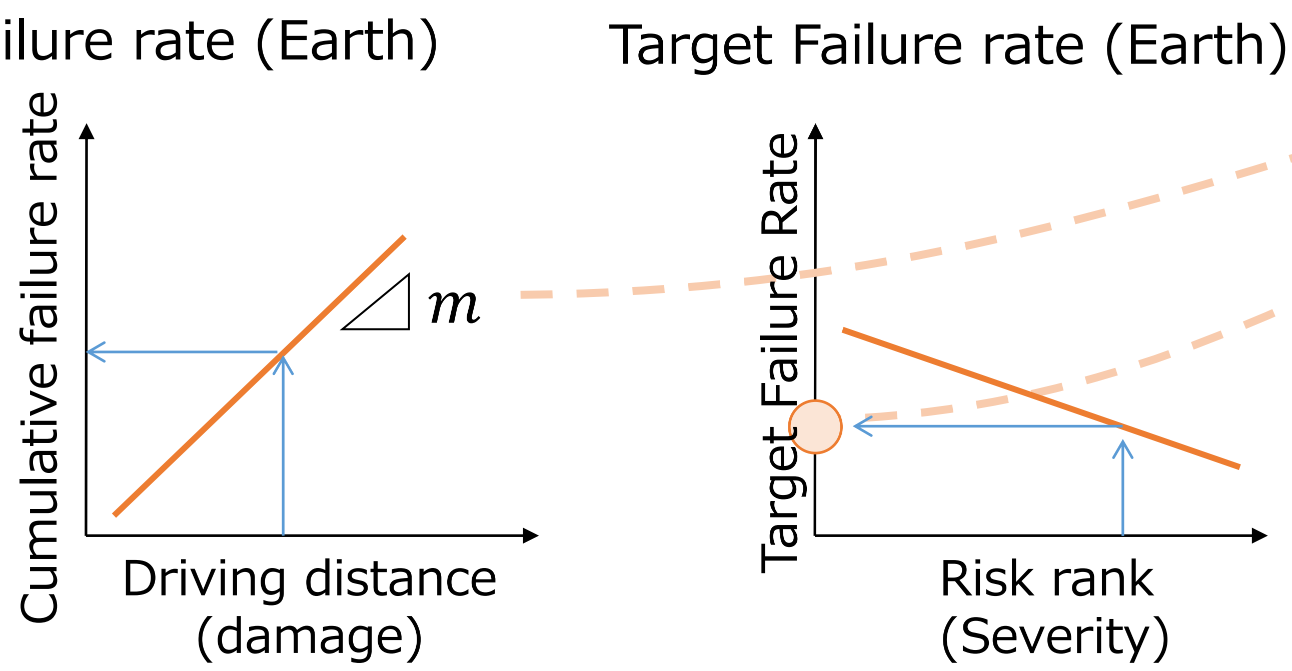
Toyota's prevention method for reliability concerns; GD^3

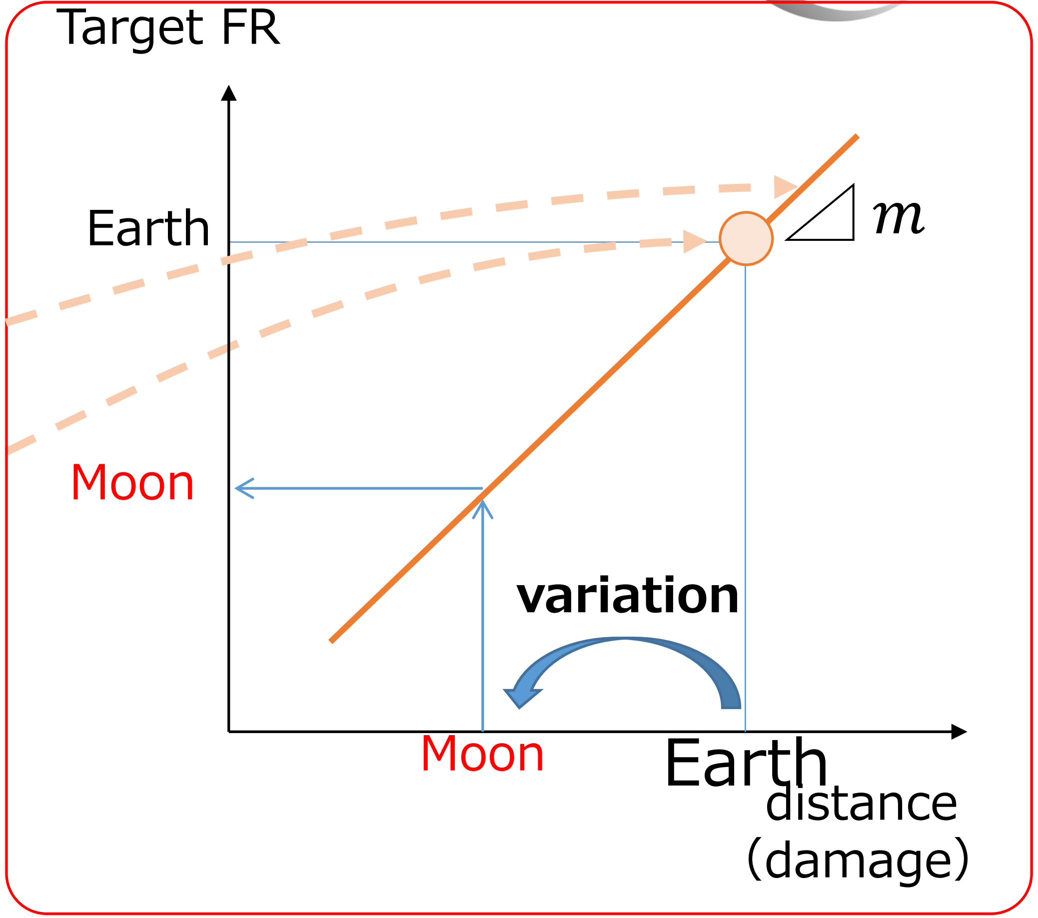
- Good Design
- Good Discussion
- Good Dissection

We consider unexpected concerns too with DRBFM

Failure rate estimation based on ground vehicle experience

Considering the changes to the
(using Weibull distribution)





failure modes, targets (Earth) x variation (environment)
-> target (Moon)

Conclusions

Safety & reliability development;

- Considering extreme environment on moon surface.
- Using the automotive development experience as carmaker.

Future work

- Clarifying a lot of unknowns, uncertainness.

Our Vision and Values

We contribute to the “mass production of happiness” by inventing our new cars.

To expand the sphere of human activity by challenging manned pressurized rover

Mobility 2.0 (expansion of mobility into new areas)

Improvement of technology (engineer's dream)

Our new challenges lead to expand human capability

Technology Development to Moon

Feedback to Earth

Technology to generate electricity using only sunlight and water

- Off-road driving performance
- Autonomous driving
- Regenerative Fuel Cells
- UX

The technology developed through the development of manned pressurized rover will be returned to society on Earth

Mobility 1.0 (Extension of the value of the car)
Mobility 3.0 (integration with social systems)

Contribution to a carbon-neutral society (CN)

Contribution to the development of new cities and vehicles


MOON
ROAD
CREATION
TOYOTA