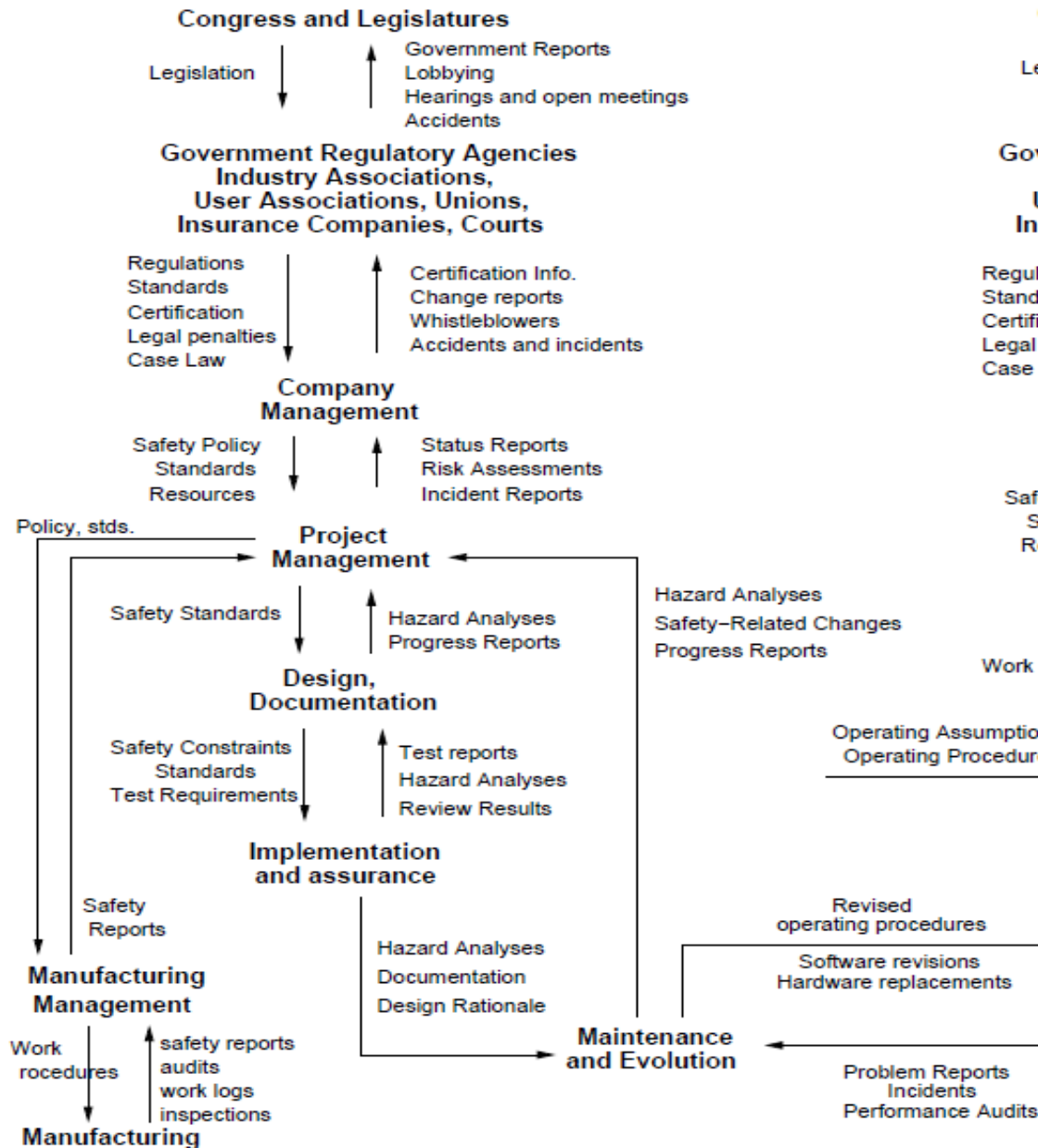


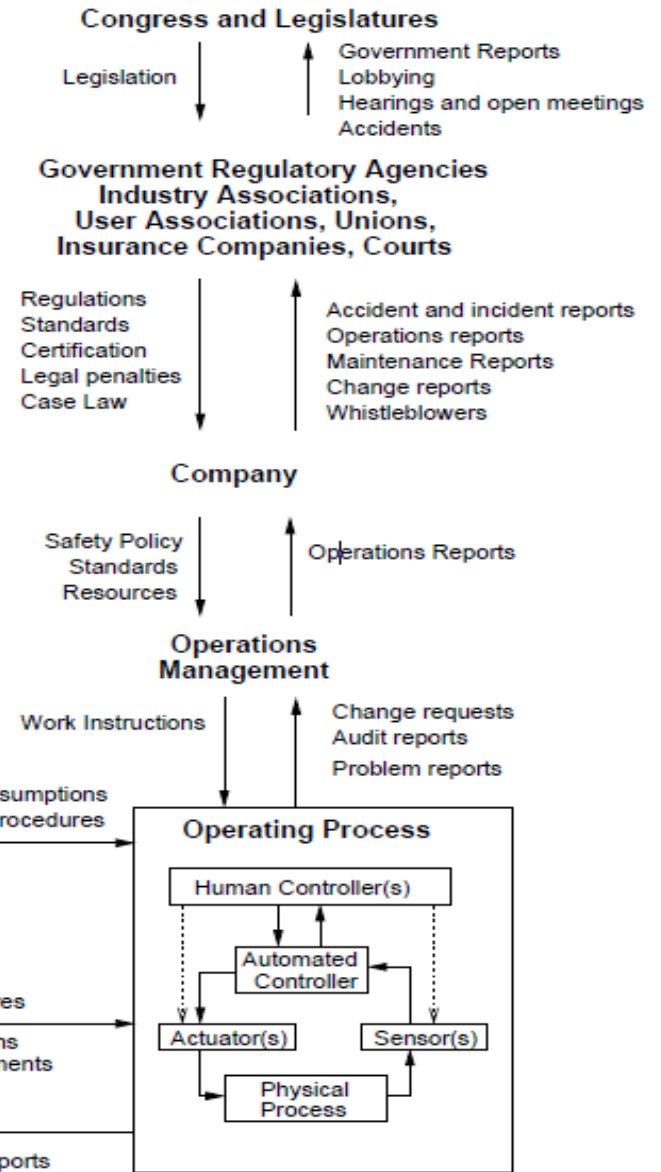
APPLYING STAMP TO IMPROVE THE EVALUATION OF SMS

Robert J. de Boer, Raymon van der Maarel
Aviation Academy, Amsterdam University of Applied Science
2nd European STAMP Workshop
Stuttgart, September 22nd 2014

SYSTEM DEVELOPMENT



SYSTEM OPERATIONS



[Levenson 2004]

CONTENTS

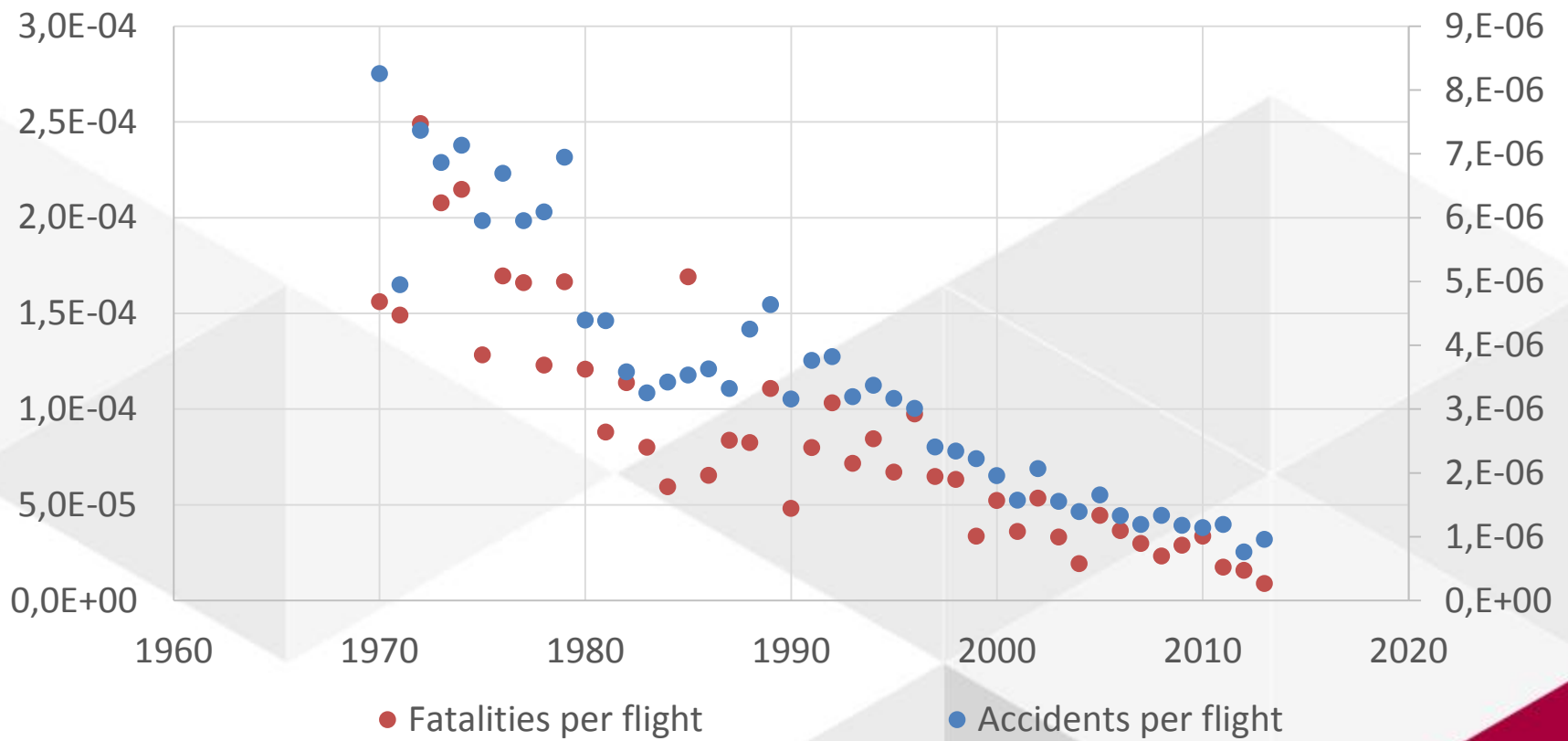
- Background
- Purpose
- Approach
- Results
- Conclusions

BACKGROUND

www.international.hva.nl



AVIATION SAFETY HAS REACHED AN ALL-TIME LOW IN 2013



CHANGING OVERSIGHT: FROM COMPLIANCY-BASED TO A RISK-BASED



PURPOSE

www.international.hva.nl



PURPOSE

- To identify the value of applying STAMP to the European aviation regulatory system
 - Identify risks that have not previously been identified for the change from a compliancy-based to a performance-based oversight
 - Assess value of methodology
- The scope of the current study is limited to aviation maintenance
 - maintenance companies are relatively small
 - vulnerable for complex and inefficient regulatory systems
 - Besides, the decreasing number of in-flight safety issues forces the industry to pay more attention to on-ground hazards

APPROACH

www.international.hva.nl



APPROACH

- The current study has applied a modified five-step STPA methodology:
 - Identify hazards and safety requirements
 - Define functional control structure
 - Identify control actions
 - Allocate safety requirements to components
 - Determine control loop effectiveness.
- Results compared to previously identified EASA risks

RESULTS

www.international.hva.nl



INITIAL FORMULATION OF HAZARDS

- Competent staff shall carry out and sign off maintenance.
- Maintenance shall be carried out according to the latest legislation and job cards.
- Safety shall be ensured by defining organisation-wide processes that provide for effective risk-based decision making.
- The industry shall continuously improve safety by learning from occurrences or incidents at any level.



REDEFINED HAZARDS WITH EASA

- Regulations are not prescribed resulting in unsafe operations of maintenance organisations
- Maintenance organisations do not comply with prescribed regulations resulting in unsafe operations of maintenance organisations;
- Risks, other than the risks mitigated by prescribing regulations, are not identified and thus not mitigated resulting in unsafe operations of maintenance organisations
- Feedback on the functioning of the regulatory system is not provided resulting in a not completely effective regulatory system in terms of preventing the three aforementioned hazards from happening

SYSTEM SAFETY REQUIREMENTS FOLLOW FROM THE HAZARDS

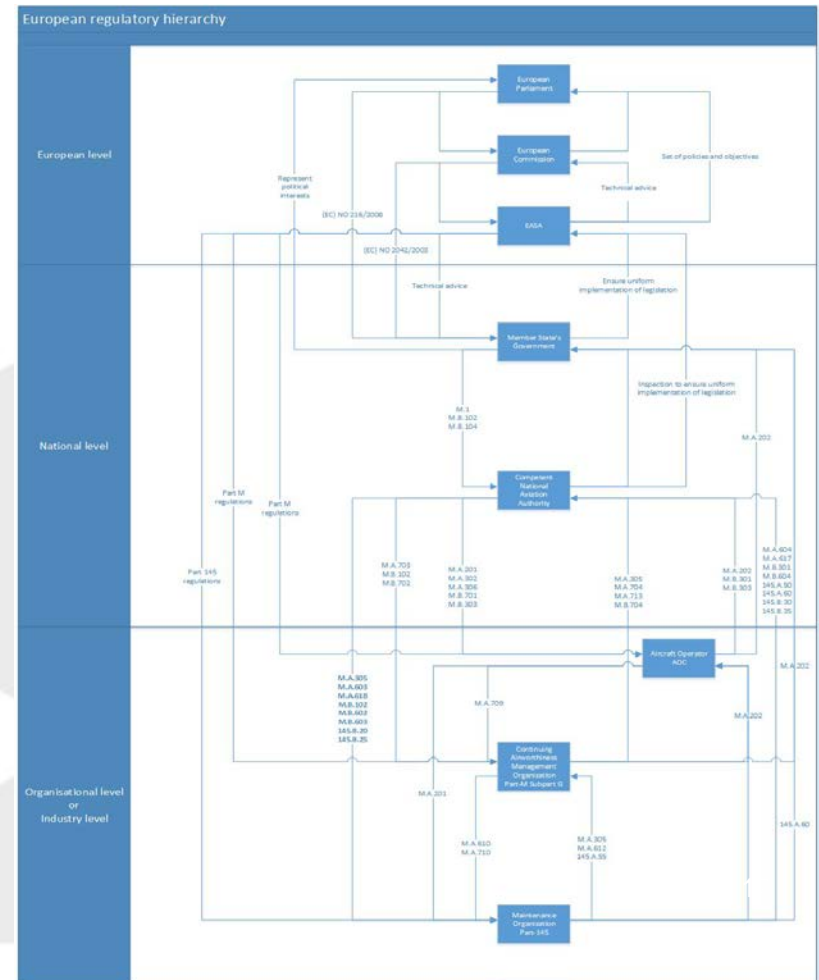
1. (Risk) control in the form of regulations shall be in place at any level.
2. A system which properly oversees and enforces regulations shall be in place.
3. Industry and organisations shall identify and mitigate risks.
4. Feedback on the functioning of the system shall be provided.

FUNCTIONAL CONTROL STRUCTURE

simple



Detailed (illegible)



SAFETY REQUIREMENTS VERSUS CONTROL STRUCTURE & IDENTIFICATION OF FLAWS

Allocated safety constraints		Safety constraints per top-level element per system		
All control in the form of functions shall be placed in any one		Maintenance is carried out in such a way that the aircraft does not function as intended and crashes or causes a serious safety hazard unless necessary and effective measures shall be in place		
Category	Requirement	Requirement	Requirement	Requirement
Function	ASA Invariants and generic options and answers on technical questions to the European Commission.	ASA Invariants and generic findings related to standardisation within Member States to the European Commission.	ASA presents the outcomes of the review of the industry to safety to the European Commission.	ASA presents the outcomes of the review of the industry to safety to the European Commission.
Process Model	European Commission poses questions and answers on questions in order to fine legislation.	European Commission identifies gaps between desired transmission and presentation of findings related to standardisation within Member States and current transmission and presentation of findings related to standardisation within Member States.	European Commission uses these outcomes to discuss whether certain safety performance fits the expectations of the European Commission.	European Commission uses these outcomes to discuss whether certain functioning of the system fits the expectations of the European Commission.
Control Algorithm	European Commission generally requires control action as a function of gaps from EASA and related to standardisation within Member States.	European Commission generally requires control action as a function of gaps from EASA and related to standardisation within Member States.	European Commission generally requires action to the legislation.	European Commission generally requires the provided solutions in response to the legislation.
Actuator	European Commission commands EASA to transmit and present options and answers on technical questions to the European Commission.	European Commission commands EASA to transmit and present findings related to standardisation within Member States.	European Commission commands EASA to identify high level risks within the aviation industry and come up with possible risk mitigation solutions and present them to the European Commission.	European Commission commands EASA to address shortcomings in the functioning of the regulatory system and provide solutions or adaptations to the regulations.
Function	Member State signs a document in which it voluntarily agrees with providing legally binding powers to the European Commission.	Findings related to standardisation within a member state are issued to the European Commission by EASA.	N/A	N/A
Process Model	European Commission verifies whether conditions and agreements are kept according to the Member State.	European Commission identifies gaps between desired standardisation and current Member State within a specific Member State.	N/A	N/A
Control Algorithm	European Commission generally requires control action as a function of findings from the Member State and its National Aviation Authority to cooperate in the European system.	European Commission generally requires control action as a function from gaps in control of finding a specific Member State.	N/A	N/A
Actuator	European Commission informs gaps to Member State.	European Commission issues findings or recommendations.	N/A	N/A
Function	National Aviation Authority transmits documents related to providing the competence of the National Aviation Authority to EASA.	Member state provides initial and information related to how to use a preference within Member State.	Member state send their State Safety Program to EASA, in which high level risks applying to the State are provided together with a mitigation solution, to be reviewed and Member State reports documents on safety findings coming from the industry to EASA.	Member State provides EASA with a file on Command Response Document in order to give feedback on the proposed actions and amendments, and participate and give inputs in ESO meetings.
Process Model	EASA identifies gaps between desired competence and current competence of National Aviation Authority.	EASA identifies gaps between desired competence of EASA and the current implementation of the Member State.	EASA reviews the submitted State Safety Program and studies existing resources reports and findings and identifies gaps between desired situation regarding to their specific finding and the current implementation of the finding.	EASA processes questions and comments of file on Command Response Document and EASA processes input from ESO meetings.
Control Algorithm	EASA generally requires control action as a function of gaps between desired competence and current competence. EASA can issue position paper on safety barriers, that is not allowed to enforce. The European Commission issues the Member State if its National Aviation Authority does not meet the desired competence. Member state will send file (L1 and/or AAD) to Member State.	EASA generally requires control action as a function of gaps between desired competence and current competence. EASA can issue position paper on safety barriers, that is not allowed to enforce. The European Commission issues the Member State if its National Aviation Authority does not meet the desired competence. Member state will send file (L1 and/or AAD) to Member State.	EASA generally requires control action as a function of submitted State Safety Program and generally requires control action as a function of gaps between desired situation regarding to their specific finding and the current implementation of the finding. Member state to make their State Safety Program in response to EASA and EASA processes and relevant safety findings.	EASA allows questions from the Member State or submit proposed actions or amendments and EASA will input from ESO meetings to adjust proposed actions or amendments.
Actuator	N/A	N/A	N/A	EASA provides the Member State with Command Response Documents to let the Member State comment on the proposed actions and amendments and table states the EASA's participation in the ESO.
Function	N/A	N/A	N/A	EASA provides EASA with a file on Command Response Document in order to give feedback on the proposed actions and amendments, and participate and give inputs in ESO meetings.
Process Model	N/A	N/A	N/A	EASA processes questions and comments of file on Command Response Document and EASA processes input from ESO meetings.
Control Algorithm	N/A	N/A	N/A	EASA allows questions from the EASA or submit proposed actions or amendments and EASA will input from ESO meetings to adjust proposed actions or amendments.
Actuator	N/A	N/A	N/A	EASA provides the Member State with Command Response Documents to let the EASA comment on the proposed actions and amendments and table states the EASA's participation in the ESO.
Function	N/A	N/A	N/A	EASA provides EASA with a file on Command Response Document in order to give feedback on the proposed actions and amendments, and participate and give inputs in ESO meetings.
Process Model	N/A	N/A	N/A	EASA processes questions and comments of file on Command Response Document and EASA processes input from ESO meetings.
Control Algorithm	N/A	N/A	N/A	EASA allows questions from the EASA or submit proposed actions or amendments and EASA will input from ESO meetings to adjust proposed actions or amendments.
Actuator	N/A	N/A	N/A	EASA provides the Member State with Command Response Documents to let the EASA comment on the proposed actions and amendments and table states the EASA's participation in the ESO.
Function	Continuing Airworthiness Management Organisation (CAMO) provides a certificate of airworthiness and a certificate of compliance to the National Aviation Authority (CAA) as described in 145.A.43.	Continuing Airworthiness Management Organisation (CAMO) provides a certificate of airworthiness and a certificate of compliance to the National Aviation Authority (CAA) as described in 145.A.43.	Continuing Airworthiness Management Organisation (CAMO) provides a certificate of airworthiness and a certificate of compliance to the National Aviation Authority (CAA) as described in 145.A.43.	Continuing Airworthiness Management Organisation (CAMO) provides a certificate of airworthiness and a certificate of compliance to the National Aviation Authority (CAA) as described in 145.A.43.
Process Model	National Aviation Authority identifies gaps between general content of maintenance programme as described in 145.A.30 and current content of maintenance programme.	National Aviation Authority identifies gaps between general content of maintenance programme as described in 145.A.30 and current content of maintenance programme.	National Aviation Authority identifies gaps between general content of maintenance programme as described in 145.A.30 and current content of maintenance programme.	National Aviation Authority identifies gaps between general content of maintenance programme as described in 145.A.30 and current content of maintenance programme.
Control Algorithm	National Aviation Authority can generate required control action as a function of gaps.	National Aviation Authority can generate required control action as a function of findings. Depending on the level and the nature of the finding, the National Aviation Authority can generate a corrective action and a time limit for the subsequent approval.	National Aviation Authority can generate required control action as a function of findings. Depending on the level and the nature of the finding, the National Aviation Authority can generate a corrective action and a time limit for the subsequent approval.	National Aviation Authority can generate required control action as a function of their opinion about the Safety Management System.
Actuator	National Aviation Authority provides CAMO (PMA-M) approval, see (PMA-M) and standards to the Continuing Airworthiness Management Organisation.	National Aviation Authority provides CAMO (PMA-M) approval, see (PMA-M) and standards to the Continuing Airworthiness Management Organisation.	National Aviation Authority provides CAMO (PMA-M) approval, see (PMA-M) and standards to the Continuing Airworthiness Management Organisation.	National Aviation Authority provides CAMO (PMA-M) approval, see (PMA-M) and standards to the Continuing Airworthiness Management Organisation.
Function	Maintenance Organisation provides maintenance programme manual to the National Aviation Authority as described in 145.A.30 and notifies proposed changes as described in 145.B.20.	Maintenance Organisation provides maintenance programme manual to the National Aviation Authority as described in 145.A.30 and notifies proposed changes as described in 145.B.20.	Maintenance Organisation provides maintenance programme manual to the National Aviation Authority as described in 145.A.30 and notifies proposed changes as described in 145.B.20.	Maintenance Organisation provides maintenance programme manual to the National Aviation Authority as described in 145.A.30 and notifies proposed changes as described in 145.B.20.
Process Model	National Aviation Authority identifies gaps between desired content of maintenance programme manual and current content.	National Aviation Authority identifies gaps between desired content of maintenance programme manual and current content.	National Aviation Authority identifies gaps between desired content of maintenance programme manual and current content.	National Aviation Authority identifies gaps between desired content of maintenance programme manual and current content.
Control Algorithm	National Aviation Authority can generate required control action as a function of gaps in terms of finding, non-compliance or finding or approval. The approval shall contain valid subject to: 1) the organisation complying in compliance with Annex I (Part M), in accordance with the provisions related to the handling of findings as specified under point 145.B.30 and 2) the competent authority finding granted access to the organisation to determine continued compliance with this Part; and 3) the certificate not being suspended or annulled.	National Aviation Authority can generate required control action as a function of findings. Depending on the level and the nature of the finding, the National Aviation Authority can generate a corrective action and a time limit for the subsequent approval.	National Aviation Authority can generate required control action as a function of findings. Depending on the level and the nature of the finding, the National Aviation Authority can generate a corrective action and a time limit for the subsequent approval.	National Aviation Authority can generate required control action as a function of their opinion about the Safety Management System.
Actuator	National Aviation Authority provides CAMO (PMA-M) approval, see (PMA-M) and standards to the Maintenance Organisation.	National Aviation Authority provides CAMO (PMA-M) approval, see (PMA-M) and standards to the Maintenance Organisation.	National Aviation Authority provides CAMO (PMA-M) approval, see (PMA-M) and standards to the Maintenance Organisation.	National Aviation Authority provides CAMO (PMA-M) approval, see (PMA-M) and standards to the Maintenance Organisation.
Function	Maintenance Organisation provides a copy of the certificate of release to service and provides the maintenance records as described in 145.A.30.	Maintenance Organisation provides accurate reports and maintenance data to the Continuing Airworthiness Management Organisation.	Maintenance Organisation provides accurate reports and maintenance data to the Continuing Airworthiness Management Organisation.	Maintenance Organisation provides accurate reports and maintenance data to the Continuing Airworthiness Management Organisation.
Process Model	Continuing Airworthiness Management Organisation takes for participation that fulfill the contract or the safety or technical conformity of release to service and maintenance records.	Continuing Airworthiness Management Organisation takes for participation that fulfill the contract or the safety or technical conformity of release to service and maintenance records.	Continuing Airworthiness Management Organisation takes for participation that fulfill the contract or the safety or technical conformity of release to service and maintenance records.	Continuing Airworthiness Management Organisation takes for participation that fulfill the contract or the safety or technical conformity of release to service and maintenance records.
Control Algorithm	Continuing Airworthiness Management Organisation can generate required control action as a function of gaps.	Continuing Airworthiness Management Organisation can generate required control action as a function of gaps.	Continuing Airworthiness Management Organisation can generate required control action as a function of gaps.	Continuing Airworthiness Management Organisation can generate required control action as a function of gaps.
Actuator	Continuing Airworthiness Management Organisation provides the Maintenance Organisation with maintenance data if necessary and provides maintenance work orders to the Maintenance Organisation as described in 145.A.30.	Continuing Airworthiness Management Organisation provides the Maintenance Organisation with maintenance data if necessary and provides maintenance work orders to the Maintenance Organisation as described in 145.A.30.	Continuing Airworthiness Management Organisation provides the Maintenance Organisation with maintenance data if necessary and provides maintenance work orders to the Maintenance Organisation as described in 145.A.30.	Continuing Airworthiness Management Organisation provides the Maintenance Organisation with maintenance data if necessary and provides maintenance work orders to the Maintenance Organisation as described in 145.A.30.
Controlled Process				

Safety Requirements

Sensor
Process model
Control Algorithm
Actuator

CONTROL FLAWS ACTION 1: COMPLY WITH THE REGULATIONS



- EASA has no appropriate powers to perform enforcement actions

CONTROL FLAWS ACTION 2: CHECK COMPLIANCE OF ORGANISATIONS



- Poor financial situation of Member States may result in underperforming oversight

CONTROL FLAWS ACTION 2: CHECK COMPLIANCE OF ORGANISATIONS



- Ongoing discussion about the acceptable level of risk

CONTROL FLAWS ACTION 3: PERFORM RISK-ANALYSIS



- There is no proper risk-management capability assessment tool

CONCLUSION



CONCLUSION

- STPA highlighted four weaknesses in the European aviation regulatory system
 - EASA has no appropriate powers to perform enforcement actions
 - Authorities could give organisations too early and too much freedom in managing their own risks
 - There is no proper risk-management capability assessment tool
 - Ongoing discussion about the acceptable level of risk and an acceptable level of safety
- Issues are not completely new
 - STAMP identified these in a systematic manner
 - Executed by a novice researcher
- Methodology appropriate
 - Identify hazards and safety requirements
 - Define functional control structure
 - Identify control actions
 - Allocate safety requirements to components
 - Determine control loop effectiveness

FURTHER WORK

- Develop a risk-management capability assessment tool
 - Hopefully using STAMP
 - Dutch grant submission in December 2014
 - Tentative participants include Dutch OVV, EASA, CAA-NL, KLM, Dutch ATC, many smaller companies
 - Participants meeting October 23rd, Amsterdam
- Develop an agent-based model of safety supervision
 - In partnership with TU Delft and Free University Amsterdam



CONTACT

Aviation Academy

- Professor of Aviation Engineering: Robert J. de Boer, rj.de.boer@hva.nl
- Website: <http://www.hva.nl/aviation>