## Motivation

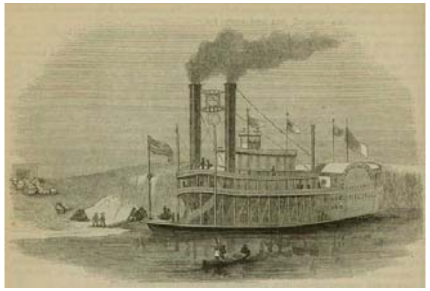
## Introduction

- □ Steam engine and software
- □ Ariane 5
- □ Safety verification and reliability analyses
- □ Testing and verification

## Introduction

... When George Ealer saw the chimneys plunging aloft in front of him, he knew what the matter was; so he muffled his face in the lapels of his coat, and pressed both hands there tightly to keep this protection in its place so that no steam could get to his nose or mouth. He had ample time to attend to these details while he was going up and returning. He presently landed on top of the unexploded boilers, forty feet below the former pilot-house, accompanied by his wheel and a rain of other stuff, and enveloped in a cloud of scalding steam. All of the many who breathed that steam, died; none escaped. ...

Mark Twain: Life on the Mississippi



## Introduction of the Steam Engine in the Industrial Revolution

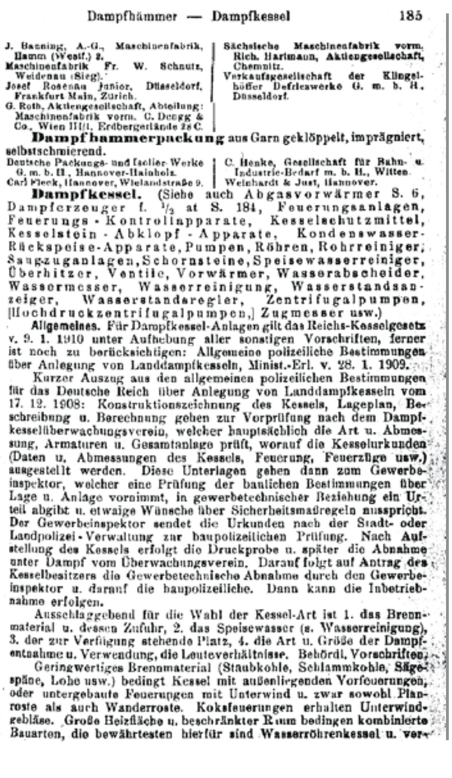
- □ Well-known personalities (J. Watt among others) are warning of the dangers of high pressure machines.
- □ Use of the more efficient high pressure machines is prefered to the safer low pressure steam engine.
- □ From 1816 to 1848 in the United States 233 explosions of steamboats were recorded with 2562 people killed, 2097 people injured and a property damage of more than 3 million US$.
- □ Causes:
  - ▪ Use of the new technology accelerates more than the required skills can be developed.
  - ▪ The theoretic principles are not completely known.
  - ▪ Construction standards and safety standards do not exist.
  - ▪ Hardly any standard components do exist.
  - ▪ Designers do not need a special training.
  - ▪ No control authority controlling the safety of the system and no control regulation do exist.

## Solution of the Problems

- □ Establishment of the engineering science engine construction with areas such as physics, material science etc.
- □ Construction of machines by special trained, skilled persons (engineers)
- □ Creation of construction and safety standards, together with the creation of standard components
- □ Establishing of test standards in the form of laws; (in Germany: "Reichs-Kesselgesetz" from 9. 1. 1910) and the formation of a testing/control organisation (steam engine inspection authority)

copmare: Joly: Technisches Auskunftsbuch für das Jahr 1919, 25. Auflage

## Solution of the Problems



Dampfhämmer — Dampfkessel 185

J. Banning, A.-G., Maschinenfabrik, Hamm (Westf.) 2.
Maschinenfabrik Fr. W. Schnutz, Weidenau (Sieg).
Josef Rosenau junior, Düsseldorf, Frankfurt Main, Zürich.
G. Roth, Aktiengesellschaft, Abteilung: Maschinenfabrik vorm. C. Deegg & Co., Wien III/1, Erdbergerlände 28 C.
Sächsische Maschinenfabrik vorm. Rich. Hartmann, Aktiengesellschaft, Chemnitz.
Verkaufsgesellschaft der Klingelhöffer Defrieswerke G. m. b. H., Düsseldorf.

**Dampfhammerpackung** aus Garn geklöppelt, imprägniert, selbstschmierend.

Deutsche Packungs- und Isolier-Werke G. m. b. H., Hannover-Hainholz.
Carl Fleck, Hannover, Wielandstraße 9.
C. Henke, Gesellschaft für Bahn- u. Industrie-Bedarf m. b. H., Witten.
Weichardt & Just, Hannover.

**Dampfkessel.** (Siehe auch Abgasvorwärmer S. 6, Dampferzeuger f. ½ at S. 184, Feuerungsanlagen, Feuerungs-Kontrollapparate, Kesselschutzmittel, Kesselstein-Abklopf-Apparate, Kondenswasser-Rückspeise-Apparate, Pumpen, Röhren, Rohrreiniger, Saugzuganlagen, Schornsteine, Speisewasserreiniger, Überhitzer, Ventile, Vorwärmer, Wasserabscheider, Wassermesser, Wasserreinigung, Wasserstandsanzeiger, Wasserstandsregler, Zentrifugalpumpen, [Hochdruckzentrifugalpumpen,] Zugmesser usw.)

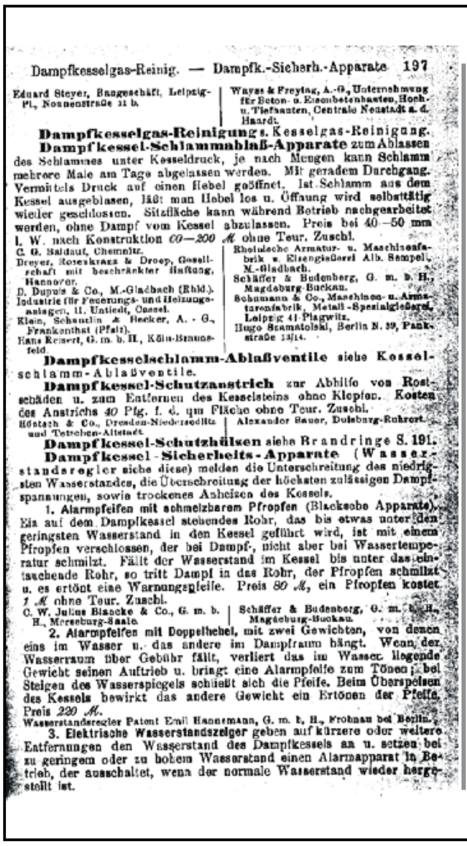
**Allgemeines.** Für Dampfkessel-Anlagen gilt das Reichs-Kesselgesetz v. 9. 1. 1910 unter Aufhebung aller sonstigen Vorschriften, ferner ist noch zu berücksichtigen: Allgemeine polizeiliche Bestimmungen über Anlegung von Landdampfkesseln, Minist.-Erl. v. 28. 1. 1909.

Kurzer Auszug aus den allgemeinen polizeilichen Bestimmungen für das Deutsche Reich über Anlegung von Landdampfkesseln vom 17. 12. 1908: Konstruktionszeichnung des Kessels, Lageplan, Beschreibung u. Berechnung gehen zur Vorprüfung nach dem Dampfkesselüberwachungsverein, welcher hauptsächlich die Art u. Abmessung, Armaturen u. Gesamtanlage prüft, worauf die Kesselurkunden (Daten u. Abmessungen des Kessels, Feuerung, Feuerzüge usw.) ausgestellt werden. Diese Unterlagen gehen dann zum Gewerbeinspektor, welcher eine Prüfung der baulichen Bestimmungen über Lage u. Anlage vornimmt, in gewerbetechnischer Beziehung ein Urteil abgibt u. etwaige Wünsche über Sicherheitsmaßregeln ausspricht. Der Gewerbeinspektor sendet die Urkunden nach der Stadt- oder Landpolizei-Verwaltung zur baupolizeilichen Prüfung. Nach Aufstellung des Kessels erfolgt die Druckprobe u. später die Abnahme unter Dampf vom Überwachungsverein. Darauf folgt auf Antrag des Kesselbesitzers die Gewerbetechnische Abnahme durch den Gewerbeinspektor u. darauf die baupolizeiliche. Dann kann die Inbetriebnahme erfolgen.

Ausschlaggebend für die Wahl der Kessel-Art ist 1. das Brennmaterial u. dessen Zufuhr, 2. das Speisewasser (s. Wasserreinigung), 3. der zur Verfügung stehende Platz, 4. die Art u. Größe der Dampfentnahme u. Verwendung, die Leuteverhältnisse. Behördl. Vorschriften.

Geringwertiges Brennmaterial (Staubkohle, Schlammkohle, Sägespäne, Lohe usw.) bedingt Kessel mit außenliegenden Vorfeuerungen, oder untergebaute Feuerungen mit Unterwind u. zwar sowohl Planroste als auch Wanderroste. Koksfeuerungen erhalten Unterwindgebläse. Große Heizfläche u. beschränkter Raum bedingen kombinierte Bauarten, die bewährtesten hierfür sind Wasserröhrenkessel u. ver-

## Solution of Problems



Dampfkesselgas-Reinig. — Dampfk.-Sicherh.-Apparate 197

Eduard Steyer, Baugeschäft, Leipzig-Pl., Nonnenstraße 31 b.
Wayss & Freytag, A.-G., Unternehmung für Beton- u. Eisenbetonbauten, Hoch- u. Tiefbauten, Centrale Neustadt a. d. Haardt.

**Dampfkesselgas-Reinigung** s. Kesselgas-Reinigung.

**Dampfkessel-Schlammablaß-Apparate** zum Ablassen des Schlammes unter Kesseldruck, je nach Mengen kann Schlamm mehrere Male am Tage abgelassen werden. Mit geradem Durchgang. Vermittels Druck auf einen Hebel geöffnet. Ist Schlamm aus dem Kessel ausgeblasen, läßt man Hebel los u. Öffnung wird selbsttätig wieder geschlossen. Sitzfläche kann während Betrieb nachgearbeitet werden, ohne Dampf vom Kessel abzulassen. Preis bei 40—50 mm l. W. nach Konstruktion *60—200 ℳ* ohne Teur. Zuschl.

C. G. Haldauf, Chemnitz.
Dreyer, Rosenkranz & Droop, Gesellschaft mit beschränkter Haftung, Hannover.
D. Dupuis & Co., M.-Gladbach (Rhld.).
Industrie für Feuerungs- und Heizungsanlagen, H. Untiedt, Cassel.
Klein, Schanzlin & Becker, A.-G., Frankenthal (Pfalz).
Hans Reisert, G. m. b. H., Köln-Braunsfeld.
Rheinische Armatur- u. Maschinenfabrik u. Eisengießerei Alb. Sempell, M.-Gladbach.
Schäffer & Budenberg, G. m. b. H., Magdeburg-Buckau.
Schumann & Co., Maschinen- u. Armaturenfabrik, Metall-Spezialgießerei, Leipzig 41-Plagwitz.
Hugo Scamatolski, Berlin N. 39, Pankstraße 13/14.

**Dampfkesselschlamm-Ablaßventile** siehe Kesselschlamm-Ablaßventile.

**Dampfkessel-Schutzanstrich** zur Abhilfe von Rostschäden u. zum Entfernen des Kesselsteins ohne Klopfen. Kosten des Anstrichs *40* Pfg. f. d. qm Fläche ohne Teur. Zuschl.

Höntsch & Co., Dresden-Niedersedlitz und Tetschen-Altstadt.
Alexander Bauer, Duisburg-Ruhrort.

**Dampfkessel-Schutzhülsen** siehe Brandringe S. 191.

**Dampfkessel-Sicherheits-Apparate** (Wasserstandsregler siehe diese) melden die Unterschreitung des niedrigsten Wasserstandes, die Überschreitung der höchsten zulässigen Dampfspannungen, sowie trockenes Anheizen des Kessels.

1. **Alarmpfeifen mit schmelzbarem Pfropfen** (Blacksche Apparate). Ein auf dem Dampfkessel stehendes Rohr, das bis etwas unter den geringsten Wasserstand in den Kessel geführt wird, ist mit einem Pfropfen verschlossen, der bei Dampf-, nicht aber bei Wassertemperatur schmilzt. Fällt der Wasserstand im Kessel bis unter das eintauchende Rohr, so tritt Dampf in das Rohr, der Pfropfen schmilzt u. es ertönt eine Warnungspfeife. Preis *80 ℳ*, ein Pfropfen kostet *1 ℳ* ohne Teur. Zuschl.

C. W. Julius Blancke & Co., G. m. b. H., Merseburg-Saale.
Schäffer & Budenberg, G. m. b. H., Magdeburg-Buckau.

2. **Alarmpfeifen mit Doppelhebel,** mit zwei Gewichten, von denen eins im Wasser u. das andere im Dampfraum hängt. Wenn der Wasserraum über Gebühr fällt, verliert das im Wasser liegende Gewicht seinen Auftrieb u. bringt eine Alarmpfeife zum Tönen; bei Steigen des Wasserspiegels schließt sich die Pfeife. Beim Überspeisen des Kessels bewirkt das andere Gewicht ein Ertönen der Pfeife. Preis *220 ℳ*.

Wasserstandsregler Patent Emil Hannemann, G. m. b. H., Frohnau bei Berlin.

3. **Elektrische Wasserstandszeiger** geben auf kürzere oder weitere Entfernungen den Wasserstand des Dampfkessels an u. setzen bei zu geringem oder zu hohem Wasserstand einen Alarmapparat in Betrieb, der ausschaltet, wenn der normale Wasserstand wieder hergestellt ist.

## Steam Engine and Software?

- □ Computer and software are – as once the steam engine in the industrial revolution – the new technologies on the threshold of the information society.
- □ Use of software accelerates more than the knowledge of their safe construction grows.
- □ Today in some areas the survival of people depends on the correct function of software.
- □ In the area of construction methods for software – the area of software engineering respectively software technology – methods and technologies are known, but only insufficiently established in practice (contructive and analytic QA-methods).
- □ Research deals with the realisation of standard components and the reusability of components (reuse, class libraries).

## Steam Engine and Software?

- □ Standards for the construction and quality assurance of software partially exist already (e.g., ISO 9001).
- □ A new science – computer science – is already established.
- □ No regulation exists yet concerning the qualification of software developers.

## Ariane 5

***June 4., 1996, Kourou / Fr. Guyana:***
Maiden flight of the Ariane 5

```
...
declare
  vertical_veloc_sensor: float;
  horizontal_veloc_sensor: float;
  vertical_veloc_bias: integer;
  horizontal_veloc_bias: integer;
  ...
begin
  declare
    pragma suppress(numeric_error, horizontal_veloc_bias);
  begin
    sensor_get(vertical_veloc_sensor);
    sensor_get(horizontal_veloc_sensor);
    vertical_veloc_bias := integer(vertical_veloc_sensor);
    horizontal_veloc_bias := integer(horizontal_veloc_sensor);
    ...
  exception
    when numeric_error => calculate_vertical_veloc();
    when others => use_irs1();
  end;
end irs2;
```

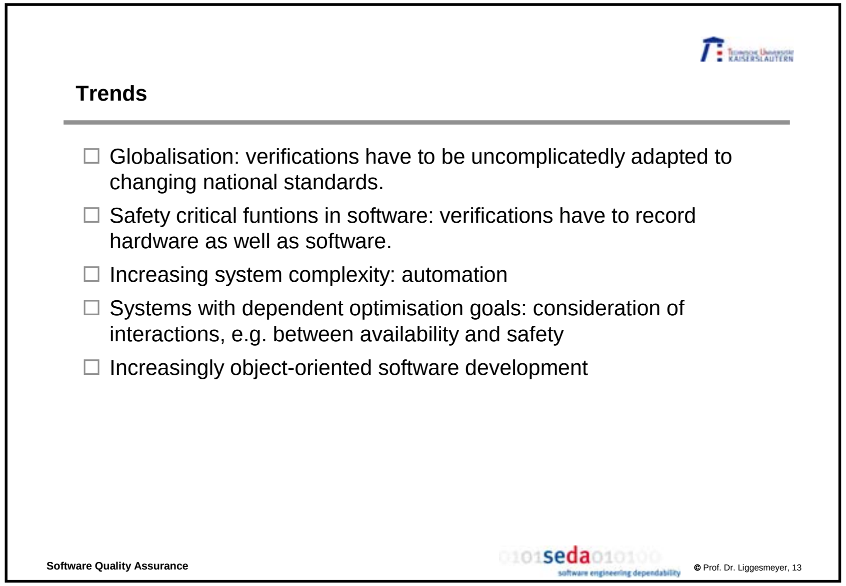
## Ariane 5

- □ Cause
  - 37 sec. after engine start (30 sec. after liftoff) Ariane 5 had a horizontal velocity of 32768.0 (internal units). The integer conversion of the 64-bit floating point variable caused a data overflow. The second flight controller experienced the same problem 72 msec before and thus was not operational at that time. Diagnosis data were propagated to the main flight computer. These data were interpreted as valid flight data. Incorrect steering commands were sent. These caused a mechanical overload and finally Ariane 501 exploded.
- □ Effect
  - Total financial loss of 850 Million Euro

## Information concerning the Situation in the Development of software intensive systems

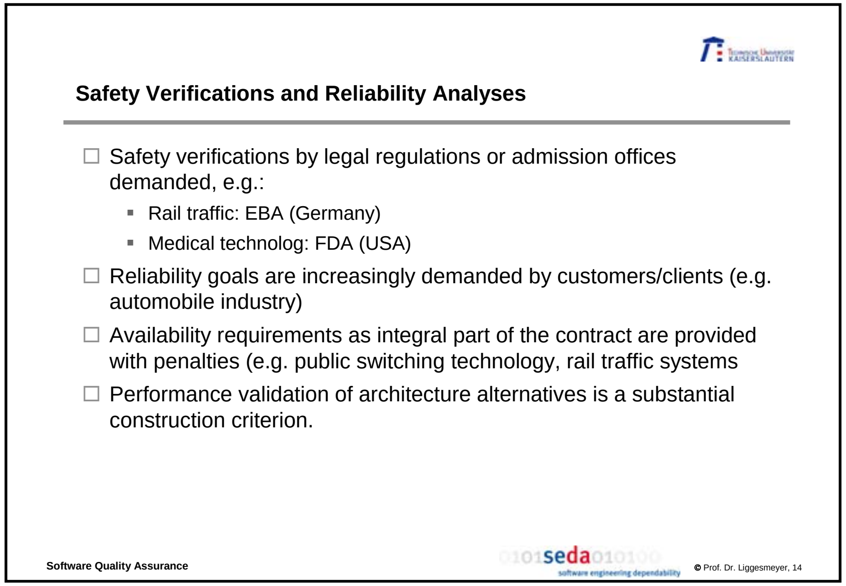
There is an expanded and more lengthy process of product approval because FDA has significantly increased the scope and complexity of the review process. These actions have led to much more uncertainty surrounding the regulatory process and have significantly increased the financial investment and time required to develop and commercialize new medical products. The net result of these policies has been significant delays in the approval of new products. It now takes a company more than two years, on average, to obtain f.e. pre market approval. Often, the process takes much longer. Review times have also climbed steadily.

(from: A. H. Magazine, “The Impact of Regulation”, in: Medical Device Technology, March 1997, pp. 38 ff, ISSN 10 48 - 66 90)



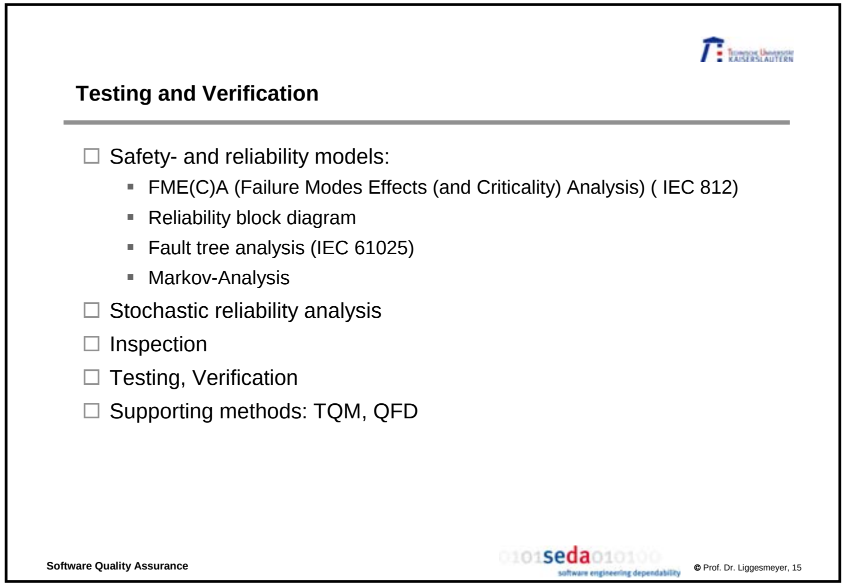
## Trends

- □ Globalisation: verifications have to be uncomplicatedly adapted to changing national standards.
- □ Safety critical funtions in software: verifications have to record hardware as well as software.
- □ Increasing system complexity: automation
- □ Systems with dependent optimisation goals: consideration of interactions, e.g. between availability and safety
- □ Increasingly object-oriented software development



## Safety Verifications and Reliability Analyses

- □ Safety verifications by legal regulations or admission offices demanded, e.g.:
  - Rail traffic: EBA (Germany)
  - Medical technolog: FDA (USA)
- □ Reliability goals are increasingly demanded by customers/clients (e.g. automobile industry)
- □ Availability requirements as integral part of the contract are provided with penalties (e.g. public switching technology, rail traffic systems
- □ Performance validation of architecture alternatives is a substantial construction criterion.



## Testing and Verification

- □ Safety- and reliability models:
  - FME(C)A (Failure Modes Effects (and Criticality) Analysis) ( IEC 812)
  - Reliability block diagram
  - Fault tree analysis (IEC 61025)
  - Markov-Analysis
- □ Stochastic reliability analysis
- □ Inspection
- □ Testing, Verification
- □ Supporting methods: TQM, QFD