ARSaP

Case Studies on ICT System Failure caused by Software Deficiencies

The 2nd AsiaSASI WORKSHOP

Held by Aviation Safety Council, TAIWAN

主催:台湾行政院飛航安全調査委員會

June 13-14, 2013. Taipei, TAIWAN

Organization of Aviation & Railway Safety Promotion, Japan

非営利特定活動法人　航空･鉄道安全推進機構

MATSUDA Hiroshi　松　田　　宏

TOPICS

- ICT System in Aviation
  (ICT: Information & Communication Technology)
- Software in ICT System
- Quality of Software
- Types of System Failures
- Case Studies
- “Study of Failure”
- Conclusions

ICT in Aviation System

- Information and Communication Technology (ICT) is now used widely in many aviation systems as follows;
  - Airborne Systems:
    - Embedded Control Systems (i.e. Engine Control, Flight Control, etc)
    - Management Systems (i.e. Flight Management system (FMS), Communication Management, Air Data Computer (ADC), etc)
    - Communication/ Navigation/ Surveillance (CNS) Systems
  - Ground based Systems:
    - Operation Support (i.e. Flight Operation, Maintenance, etc)
    - Air Traffic Services (i.e. AIS, ATC/ATM, MET, S&R, etc)
    - Network Services (i.e. ATN, Air-Ground Comm. (Voice/Data Link), Satellite Comm., etc)

Cockpit

Air Traffic Control

Engine Control

Flight Management System

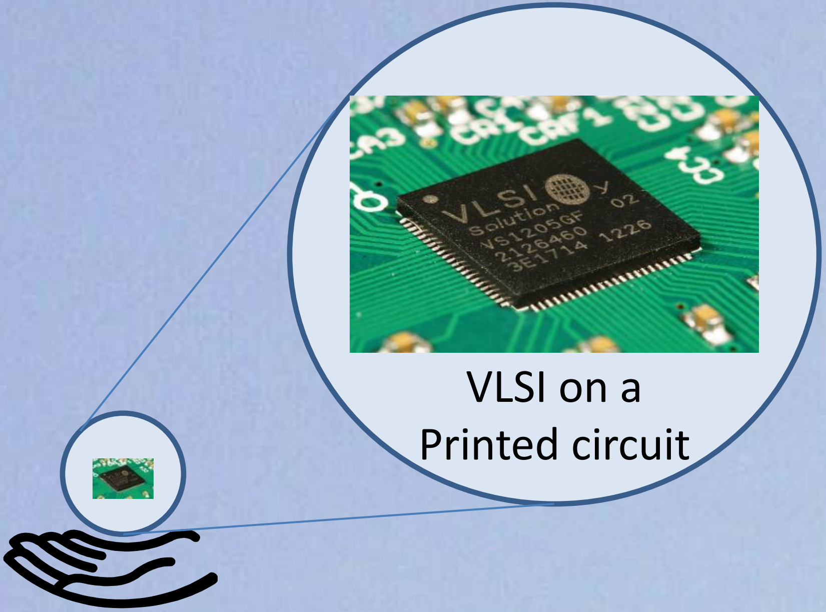
Air Traffic Management

SATCOM

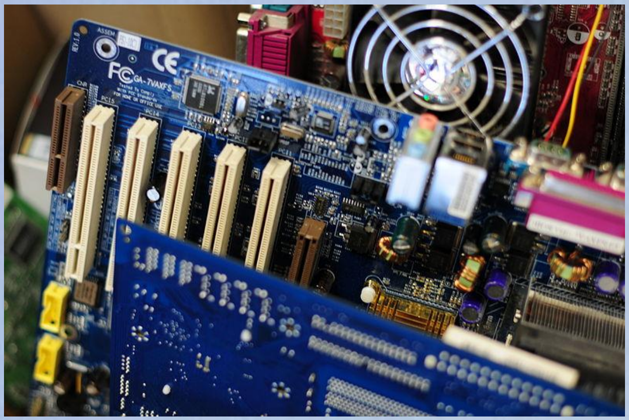
Software in ICT System

- ICT system consist of the following three parts;
  - Hardware: processor, memory and input/output devices
    - “Stored Program” (von Neumann) type digital computer
    - Using small & cheep Very Large Scale Integration (VLSI) tips
    - Number of transistors on a VLSI doubles in every 18 month (Moore’s Law)
  - Software: program code , data & documents
  - Network: high speed digital communication
- Number of program codes is “astronomical”
    - Automobile: 7 Million (excludes Nav. system)
    - Mobile Phone: 10 Million
    - Banking System: 100 Million

Hardware



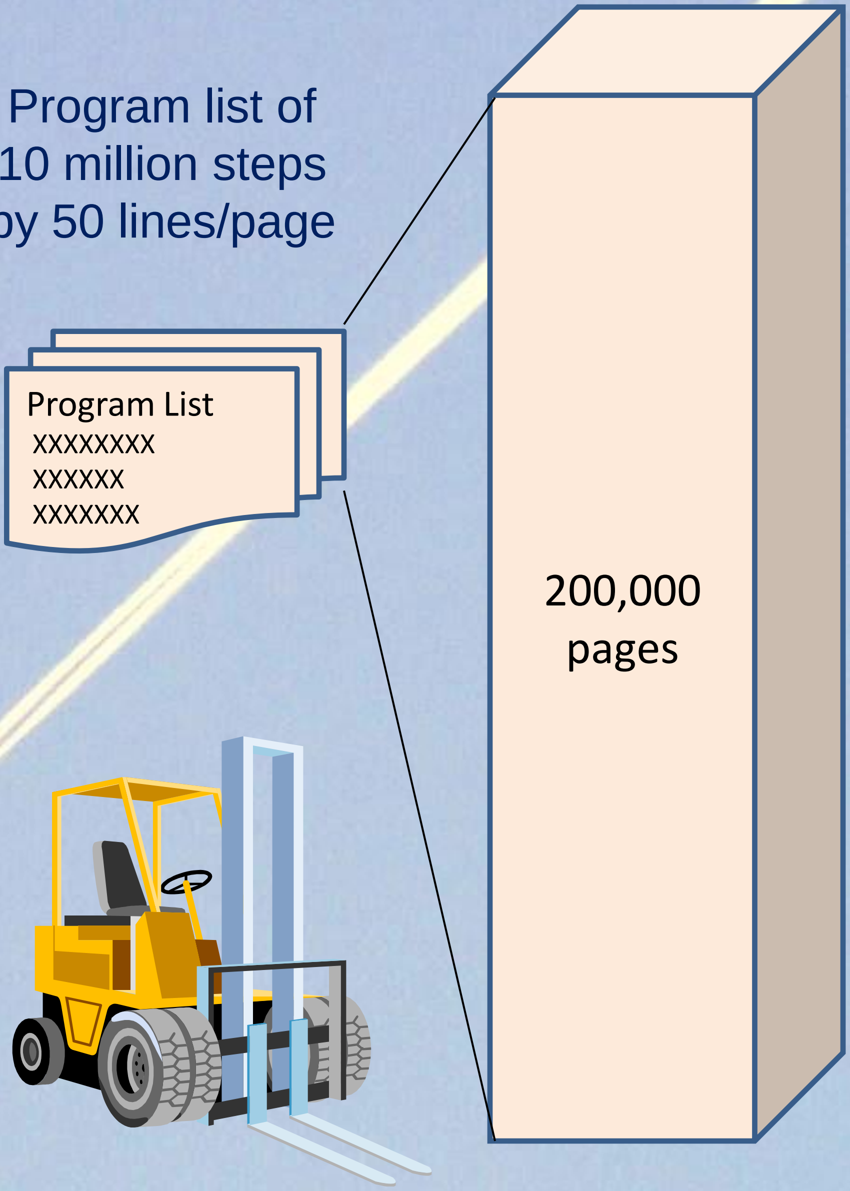
VLSI on a Printed circuit



Connectors for printed circuits

Software

Program list of 10 million steps by 50 lines/page



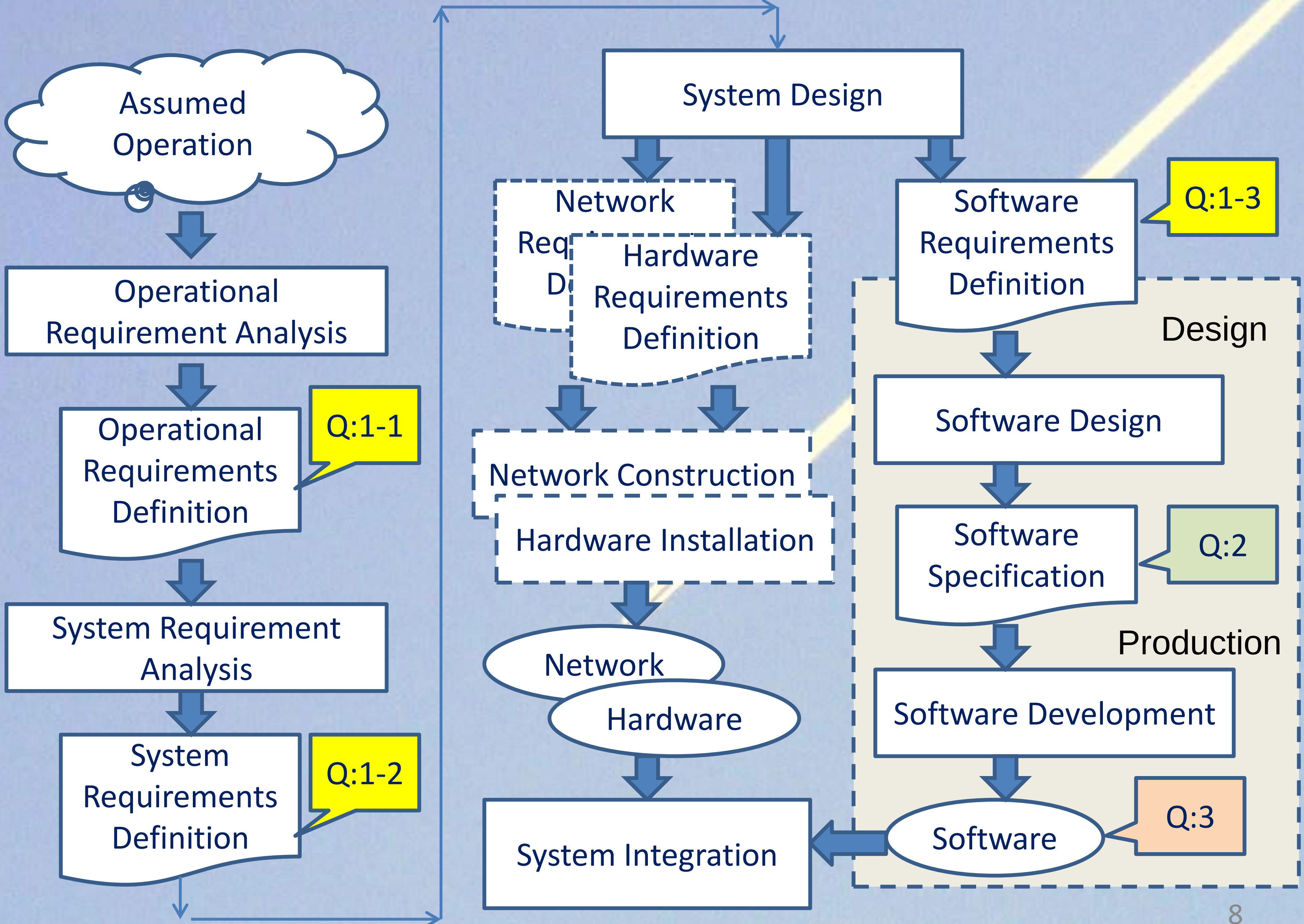
Quality of Software

- Quality of software has <u>three aspects</u>;
  1. <u>Requirement</u> Quality
  2. <u>Design</u> Quality
  3. <u>Production</u> Quality
- Software is a different a production
  - ➢ Consists of algorithm and data (no shape, no weight, …)
  - ➢ It’s soft and MTBF/MTTR are not proper measure of reliability
- Software is <u>too complex </u>to test all conditions

  No. of combination of
  “m“ out of “n”

$$ {}_{n}\mathrm{C}_{m} = \frac{n \times (n-1) \times \cdots \times (n-m+1)}{m \times (m-1) \times \cdots \times 1} $$

- Defined, designed and developed by <u>erroneous</u> “<u>humankind</u>”, that means to be not “<u>perfect</u>”



Assumed Operation

Operational Requirement Analysis

Operational Requirements Definition

Q:1-1

System Requirement Analysis

System Requirements Definition

Q:1-2

System Design

Network Req D

Hardware Requirements Definition

Software Requirements Definition

Q:1-3

Design

Software Design

Software Specification

Q:2

Production

Software Development

Software

Q:3

Network Construction

Hardware Installation

Network

Hardware

System Integration

Types of System Failure

- Qualitative analysis on typical cases of ICT system failures using open information
- Cases include other industries as useful references
- Cases are sorted by the following types;

Type-1: Simple “bug” of Software

Type-2: Lack of Consideration in Design (Software Only)

Type-3: Lack of Consideration in Design (Hardware related)

Type-4: Insufficient Definition of System Requirements

Type-5: Improper Assumptions on Operational Conditions

Type-6: Others (Miss Operation, Failure of Infrastructure, etc)

Type-1: Simple “bug” of Software

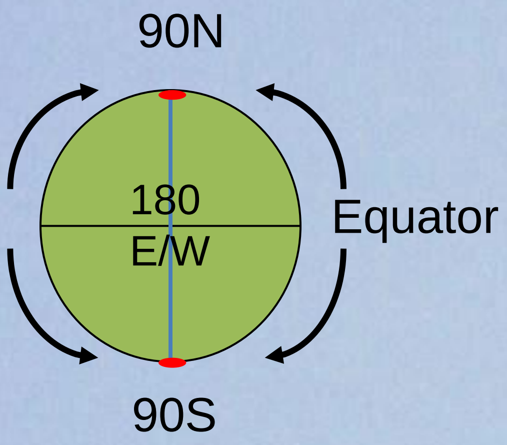
- En-route ATC Radar Data Processing (RDP) system failed at 1911 JST on 8th April 2004.
  - 130 domestic flights delayed over 30 min.
  - Probable cause was software bug in processing illegal data in FPL.

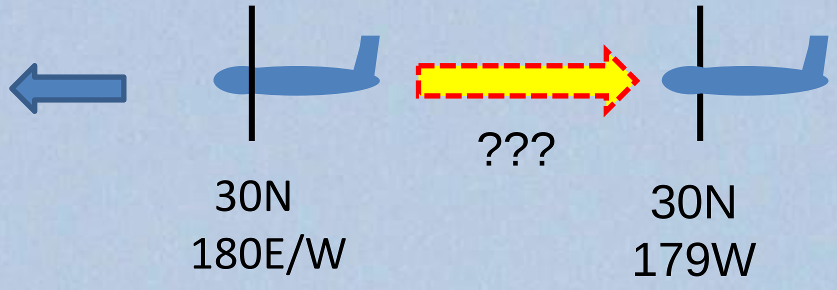
Software
軟件(軟體)

Bug
（虫）

Type-1: Simple “bug” of Software (2)

- FMS indicated a wrong position as 180S180W when crossing latitude of 180E/W in west bound flight.
  - ➢ The wrong value was “default” (initial value) in program codes.
- FMS indicated the wrong position as 30N179W when crossing latitude of 180E/W in west bound flight.
  - ➢ The result of internal calculation was 30.00N179.99W
  - ➢ 0.99 degrees was neglected in wrong conversion calculation.





Type-2: Lack of Consideration in Design (Software Only)

- Operation of all melting pods of an aluminum factory in New Zealand stopped on December 31st 1996.
  - Process of the 366th day of a leap year was not considered.
  - The loss was about 1 million NZD.

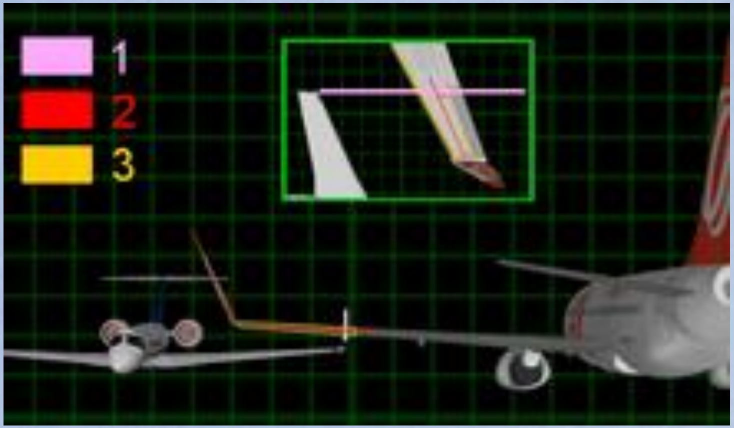
- ATC Flight Data Processing (FDP) system failed at 0700 JST on March 1st 2003.
  - 215 flights were canceled, 1,500 flights were significantly delayed and more than 300 thousand passengers waited at the airports.
  - The cause was a conflict of two processes in the system, statistics and communication with the Defense Agency.
  - Possibility of the conflict was not considered.

Type-3: Lack of Consideration in Design (Hardware related)

- Derivative trading system in Tokyo Stock Exchange failed on August 7th 2012.
  - The first cause was malfunction of a network switch.
  - Software was improper for automatic exchange to backup switch.
- Performance of KDDI exchange system for mobile phones reduced significantly on January 25th 2012.
  - The first cause was a detection of memory shortage, but enough backup memory was still remained in exact.
  - No software function was prepared for memory redundancy.

Type-4: Insufficient Definition of System Requirements (1)

- B737-800 of Gol Transport Aeros and Embraer Legacy 600 of Excel Air collided on September 29th 2006.
  - Two flights were in the same route in Brazil and at the same FL.
  - Embraer landed at the nearest airport, but B737-800 was broken in the air, fallen to the ground and killed 154 crews and passengers.
  - One of the probable causes is assumed to be confusing FLs on ATC system display, requested FL in FPL or approved FL by ATC.



Analysis of the mid air collision

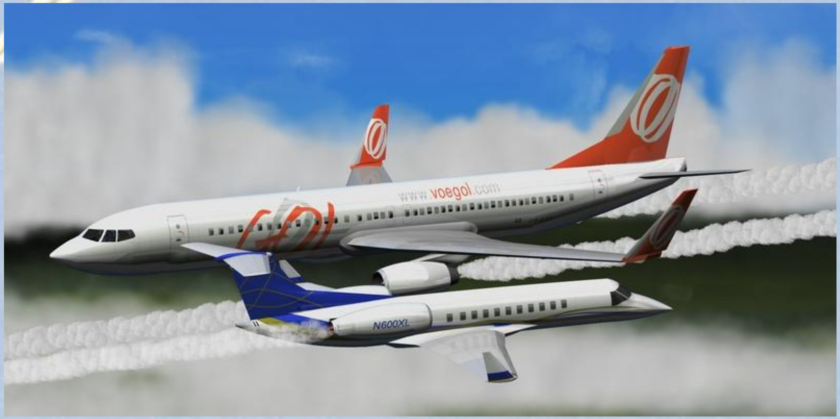
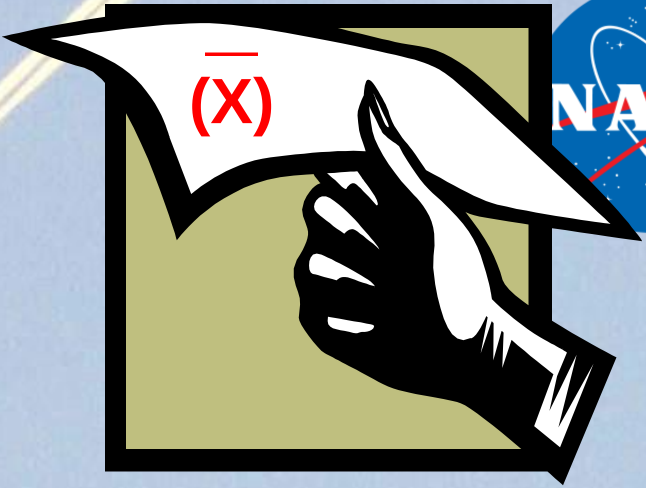


Image of the mid air collision

Type-4: Insufficient Definition of System Requirements (2)

- Mariner 1 rocket was out of course and exploded by command 293 seconds after launch in July 22nd 1962.
  - ➢ Rocket scientist passed his requirements to a programmer by hand written formula to use smoothed radar data by “x “with a “bar”
  - ➢ The programmer didn’t understand the meaning of the “bar” on the top of “x” and wrote wrong FORTRAN program without smoothing.

Launch of Mariner 1



Hand written formula for course control calculation

Type-5: Improper Assumptions in Operational Conditions (1)

- Accounting system of Mizuho Bank failed and all the ATM services stopped during March 19th – 21st 2011.
  - A large number of transfers to donate to the Great Earthquake and Tsunami victims concentrated into one specific bank account.
  - Number of transfers was unnecessarily limited too small, and recovery process in the night could not complete before morning.
  - Online process in daytime could not start in the next morning because of time order constrains. Unprocessed transfers continued to stack.

ATM service

Huge donation

Time constraints

Type-5: Improper Assumptions in Operational Conditions (2)

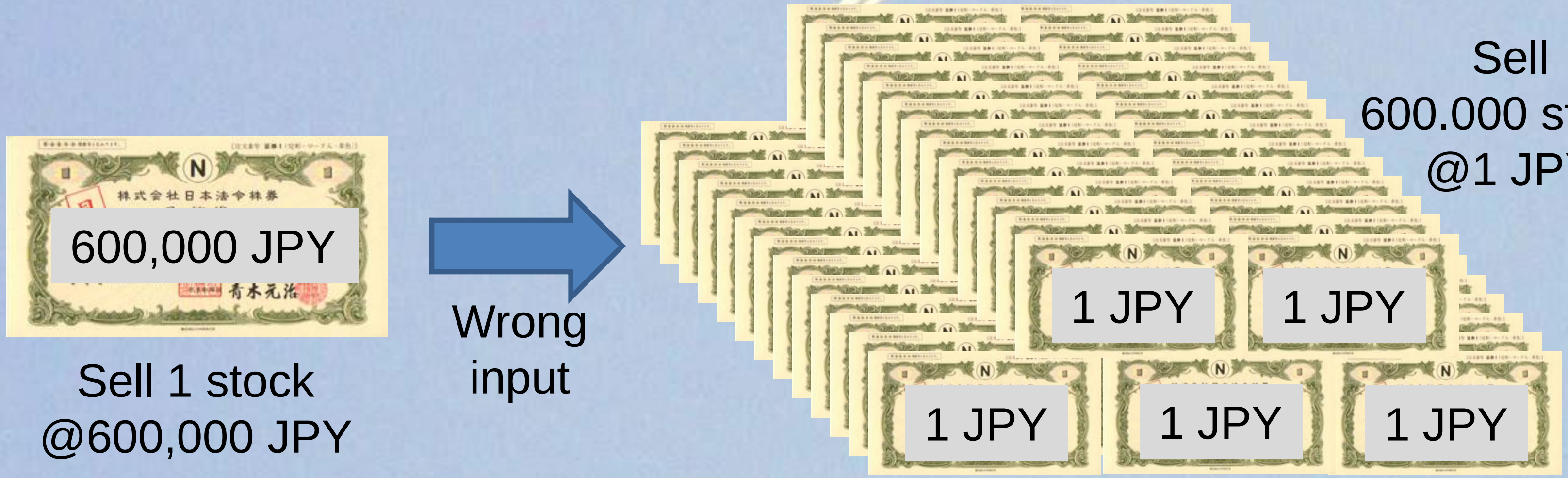
- Trading system of Tokyo Stock Exchange was over flown in January 18th 2006.
  - Capacity of the system was too small and had no expandability
  - Sudden increase of number of trades according to 1/100 divide of face value of the Live Door stock, very popular at that time.

1 stock

100 stocks

Type-6: Others (Miss-operation, Failure of Infrastructure, etc)

- Wrong “sell order” input caused overflow of the Tokyo Stock Exchange (TSE) system on December 8th 2006.
  - Mizuho Security ordered to sell 600,000 stocks at 1 JPY, instead of 1 stock at 600,000 JPY. Confirmation message was ignored.
  - TSE system was over flown by a focused “buy orders” for the bargain. Mizuho could not cancel the wrong order until system was recovered.
  - Mizuho claimed for 41.4 billion JPY compensation. The case is still under justice, but TSE has already paid 13.2 billion JPY tentatively.



600,000 JPY

Sell 1 stock @600,000 JPY

Wrong input

Sell 600.000 stocks @1 JPY

1 JPY

1 JPY

1 JPY

1 JPY

1 JPY

Type-6: Others (Miss-operation, Failure of Infrastructure, etc) (2)

- Electric power supply to all ATC system at Haneda Int'l Airport stopped on August 2nd 2005.
  - Electric power was supplied from battery by wrong setting during scheduled maintenance and the battery was fully discharged finally.
- New Super computer of the Meteorological Satellite Center stopped for 12 hours on February 5th 2013.
  - Cooling water control system sent wrong order to stop all the pumps.

Control Tower of Haneda Int'l Airport
New (left) & Old (right: used at the time)

Max. 847 TFLOPS

New Super Computer at
the Meteorological Satellite Center

“Study of Failure (失敗学)”

- “Study of Failure” is a new, holistic engineering field
  - ➢ Proposed in early 2000s by Dr. HATAMURA Yohtaro (畑村洋太郎), a professor of Creative Mechanical Engineering
- The study started by his fact finding that many students make similar mistakes in experiments
- The Study of Failure;
  - – shows that many failures are predictable and preventable, because of similar causes with similar mechanism
  - – consists of the following 3 parts;
    - ➢ Cause Analysis (CA)
    - ➢ Failure Prevention (FP)
    - ➢ Knowledge Distribution (KD)

温故知新

Keep the old, know the new.

Conclusions

- Most of causes seem to be common, repeated often in the past, simple, primitive and easy to fix
- The failures were predictable and preventable, if similar cases in the past were known
  - “Out of assumption” might be an excuse for ignorance & idleness
- Learn the past more (including other industries)
  - Old cases are useful to prevent similar failures in new system
  - Cases in other industries might be often good references in aviation
- Communicate each other; users & engineers
  - Specialist knows everything in his field, but nothing about others
  - Good imagination helps avoidance of possible future problems.

Thank you!

Any question?