# High integrity systems

Prof. dr hab. inż. Janusz Górski (WETI PG)

## Introduction:

In general, the concept of integrity refers to consistency of actions, values, methods, measures, principles, expectations, and outcomes. Integrity of a system can be understood in internal and external terms. A system lacks internal integrity if, for instance, includes inconsistencies between specifications and implementations of its components. A system lacks external consistency if, for instance, its internal state inadequately represents the target environment of this system.

High integrity system is such system where expectations related to its internal and external integrity are very high. Consequently, it requires that the most advanced assurance methods and techniques are being applied during the whole lifecycle of the system.

The objectives of the course:

To develop understanding of the role and scope of high integrity systems and to present selected methods and techniques of designing and analyzing such systems.

## The scope of the course:

1. The concept of risk; Risks and technology;
2. High integrity systems – definitions, examples
3. Hazards and accidents; Examples;
4. Managing risks and safety barriers concept; The ALARP principle;
5. Risk assessment methods and risk management strategies;
6. Risks related to software; the nature of software faults;
7. Fault tolerance and redundancy;
8. Reliability: theory and practice;
9. Common Cause Failures and diversity;
10. Human errors, modeling and analysis;
11. The concept of safety culture;
12. The concept of safety case and the related tools;
13. Risk management process - an overview;
14. Risk analysis methods: Hazard Analysis, HAZOP, ETA
15. Risk analysis methods: FTA, FMEA, FMECA, CCA

## Bibliography:

1. E. Hollnagel, D. D Woods, N. Leveson, Resilience Engineering, Concepts and Precepts, TJ International, 2008
2. N Leveson, SAFEWARE: System Safety and Computers, published by Addison Wesley, 1994
3. P Neumann, Computer Related Risks, published by ACM Press, New York, 1995

**Projekt „Rozwój interdyscyplinarnych studiów doktoranckich na Politechnice Gdańskiej w zakresie nowoczesnych technologii" jest współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego.**

4. Tom Anderson and Peter Lee, Fault Tolerance: Principles and Practice, published by Springer-Verlag, New York, 1990

5. SAFECOMP Conference portal (www.safecomp.org)

| TERMINY WYKŁADÓW | | | |
|---|---|---|---|
| Data | Dzień tygodnia | Godzina | Sala |
| 2013-05-24 | piątek | 9.15-13.00 | 234 NE |
| 2013-06-06 | czwartek | 9.15-12.00 | 209 NE |
| 2013-06-07 | piątek | 9.15-13.00 | 234 NE |
| 2013-06-14 | piątek | 9.15-13.00 | 234 NE |