White Paper “Harmonization of Classification Levels”

Protection objective: confidentiality

Version:	1.0
Date:	April 19, 2018
Classification:	public

VDA | Verband der Automobilindustrie

Content

Introduction/motivation

Information security is a crucially important issue for companies. Due to increasing connectivity and information exchange within the value chain it will continue to grow.

The Information Security working group of the German Association of the Automotive Industry (VDA[1]) has described the fundamental requirements for information security in the VDA ISA[2] (Information Security Assessment) catalog that is used for security assessments within the automotive supply chain. As the working group we would like to provide advice on the implementation of the requirements.

One key element in achieving a needs-oriented level of information security is the classification and labeling of information. Information classification designates the categorization of information in various levels according to its value for a company.

The VDA ISA catalog defines organizational and technical requirements for the different classification levels, which are intended to achieve effective information security with a reasonable and expedient effort.

Most companies have already implemented classification levels, for example by establishing a system for the classification and protection of information by introducing appropriate regulations.

A comparison within the automotive industry reveals differences between the companies regarding both the number and the designation of the classification levels. Especially in the case of information exchange, such differences can lead to confusion that in turn results in uncertainties.

The Information Security working group therefore considers the creation of a standard scheme for classifying information both as useful and supportive for the business, as well as the recommendation of implementation strategies.

This White Paper describes the working group's proposal for determining such a scheme focusing on the protection objective of confidentiality; this means that

[1] https://www.vda.de/en

[2] https://www.vda.de/en/services/Publications /information-security-assessment.html

information is not made accessible to unauthorized persons, organizations or processes. Additionally, the protection objectives such as availability, integrity and reliability are not the focus of this White Paper.

Classification of information

Both the information security standard ISO/IEC 27001 and the VDA ISA catalog state classification of information as an essential requirement for effective information security.

“Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.”

“An appropriate set of procedures for information labeling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organization.”

[ISO/IEC 27001:2013]

“To what extent is information classified according to its protection needs and are there regulations in place regarding labeling […]?”

“A consistent scheme for the classification of documents/information is in place and implemented.”

“Classification of information is done according to defined criteria, e.g. value, legal requirements, confidentiality, integrity and availability.”

[VDA-ISA 4.0]

During classification of information (in terms to confidentiality), the possible effects (potential damage) for companies are assessed in case of unintentional disclosure of information to an unauthorized group of recipients.

Inappropriate classification of information and the resulting handling can lead to risks like the loss of information if the chosen classification level was too low or unprofitable additional effort if the chosen classification level was too high.

The VDA ISA catalog defines the following general protection classes for companies, depending on the potential damage:

Protection class	Description
Normal	The potential for damage is low, of a short-term nature and limited to a single company.
High	The potential for damage is considerable, or of a medium-term nature, or not limited to a single company.
Very high	The potential for damage threatens the company's existence, or is of long-term nature, or is not limited to a single company.

Table 1: Protection classes as in the VDA ISA

For the protection objective of confidentiality, in practice these protection classes are allocated to the company's own scheme for classifying information.

Until now the automotive industry did not possess a unified classification scheme with the consequence that when information is exchanged between companies, it is assigned to the company-individual classification levels differently, and, subsequently, also labeled and interpreted differently. This situation can lead to an unintended different handling of information requiring protection.

As of November 16, 2017, VDA's Information Security working group agreed on a four-level scheme for classifying information.

Based on that decision the following recommended levels for classifying information and their allocation to the protection classes have been defined and specified in the VDA ISA:

Protection class in VDA ISA	**Classification level (German name)**	**Classification level (English name)**
-	Öffentlich	Public
Normal	Intern	Internal
High	Vertraulich	Confidential
Very high	Streng vertraulich	Strictly confidential

Table 2: Standard scheme for classifying information

The classification level “public” is not allocated to any protection class in the VDA ISA. However, it is included in the White Paper because many companies use this classification level. Most of them have specific persons or offices authorized for classifying and processing “public” information (e.g. corporate communication or marketing departments).

The respective requirements for the secure handling of information (e.g. encryption) are - derived from the three other classification levels / protection classes listed in Table 2 - defined and described in the VDA ISA catalog.

Labeling of information

Proper labeling is a prerequisite for the secure handling of information. Information should therefore be labeled in accordance with its confidentiality classification.

In addition to the document owner, both the recipient and the processor of the information have to be familiar with the classification levels and therefore be aware of and apply the associated requirements for handling the information.

Correct labeling is particularly in the case of transferring confidential or strictly confidential information between companies (e.g. to partner companies and suppliers) absolutely essential. The form[3] of the information and its classification level have to be taken into account while labeling information.

Alongside a standardized classification scheme and the corresponding labeling in the document, the Information Security working group regards a standardized labeling system, e.g. color-coding when the digital information is opened (e.g. e-mail, presentation file) as an important feature for sensitization. This is especially important for IT applications.

Hereby the recipient would have a clear visual indication of the classification level of the digital information. Furthermore, a colored signal (e.g. a colored bar) would bring about a unified understanding of the classification levels which would be the same in all countries and languages (see Table 3).

[3] E.g. digital, physical or oral

Protection class in VDA ISA	Classification level	Colored signal (for IT applications)
-	Public	-
Normal	Internal	Green
High	Confidential	Yellow
Very high	Strictly confidential	Red

Table 3: Allocation of colored signals to the classification levels

Conclusion and recommendation

This White Paper provides orientation for harmonized and standardized classification levels in relation to confidentiality. In addition, and in conjunction with the requirements of the VDA ISA, it helps to prevent misunderstandings and risks during the exchange of information and thus fosters appropriate information handling.

The VDA recommends its members to use this White Paper for orientation and for the implementation of the scheme described for the classification of information in companies.

List of authors

Name	Company	E-mail address
Jens Frölich	AUDI AG	jens.froelich@audi.de
Thomas Donner	BMW AG	thomas.donner@bmwgroup.com
Oliver Schmitt	Robert Bosch GmbH	oliver.schmitt@de.bosch.com
Jürgen Rilling	Daimler AG	juergen.rilling@daimler.com
Thomas Harich	MAHLE GmbH	thomas.harich@mahle.com
Matthias Teuscher	Rheinmetall AG	matthias.teuscher@de.rheinmetall.com
Burkhard Kesting	ZF Friedrichshafen AG	burkhard.kesting@zf.com

Document version history

Version	Date	Status, remarks
1.0	April 19, 2018	Final