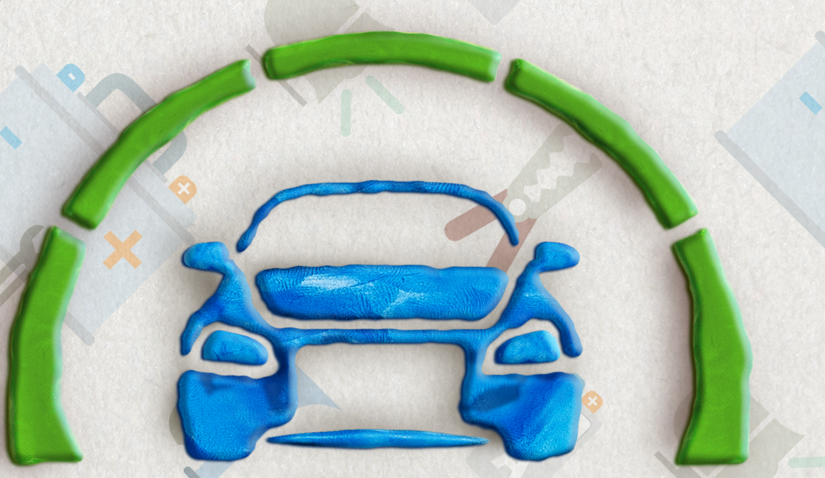
StarLine

# Skilful master

# ABC



LLC “SPA StarLine”

# Skilful master handbook

## Information and reference publication for car safety specialists

Saint-Petersburg
2017

LLC “SPA StarLine”
Authors: A. A. Borisov, M. Yu. Kurchin,
V. V. Suslov, S. G. Filimonov, M. P. Chausov

Compiler: S. A. Potryasayev, D. V. Yunak

Author of idea and editor-in-chief: T. A. Amindzhanov

Design, makeup: F. B. Akhmetov
Illustrator: M. V. Borscheva
Photographers: D. V. Vedernikov, A. V. Saukkonen

**Skilful Master Handbook**:
Information and reference publication for car safety specialists /
A. A. Borisov, M. Yu. Kurchin and others;
compiler S. A. Potryasayev, D. V. Yunak;
editor-in-chief T. A. Amindzhanov [LLC “SPA StarLine”] — 3-rd
ed., revised and enlarged — Spb: 2017 — 148 p.

ISBN 978-5-93768-044-8

The first Russian publication of this kind is aimed at enhancing the level of beginning installers of security systems and car alarms, as well as at solidifying the knowledge of skilled masters. It contains data on installation of car security equipment, starting from the elementary physics laws and ending with technologies of wire connection at installation of additional electronic components in the car, marking of electronic components and recommendations on workplace arrangement. The book is written in a simple and plain language.

If you find a mistake or a misprint, please send it to e-mail address reklama@starline.ru

ISBN 978-5-93768-044-8

# Table of Contents

# Foreword

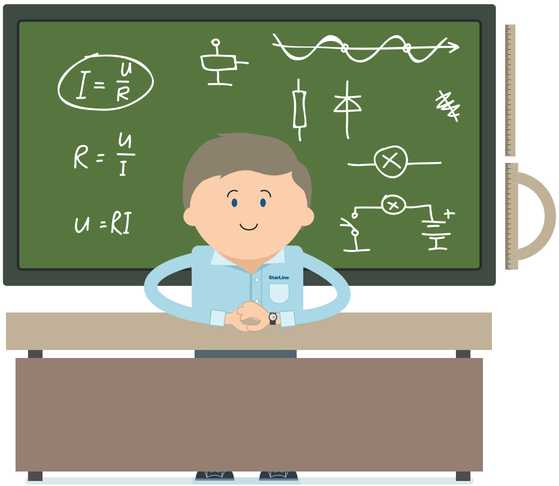
I often hear many complaints from participants of the car security market about allegedly "ham-handed" installers who spoil all great designs of developers and are guilty of everything... I disagree with this point of view. Though scampers are everywhere, the cause of failures is much more frequently in another area. Smart and conscientious installers of additional equipment are simply lack knowledge, skills, and sometimes they simply have no access to the required information. Having made a search, I discovered in surprise that, by a strange coincidence, a person who chose the profession of additional equipment installer has almost no possibilities of getting a professional education. You will not find in Russia and in the whole world a college, technical school or courses where this popular profession can be mastered.

A person wishing to study independently will also encounter a great number of difficulties, because no simple and convenient textbooks for self-education have been published earlier. It is high time to restore justice and lend a helping hand to our helpers and partners in assurance of Russian citizens' safety — installers and car electricians. We decided to share our many years' experience and to write a book for people wanting to eliminate gaps in their knowledge and increase their professional level. Read, try, learn and try to be true professionals in your own country.

*Temur Amindzhanov,*<br>
*President of*<br>
*"UltraStar" and "StarLine" Companies*

Part 1

# Fundamental laws of electricity

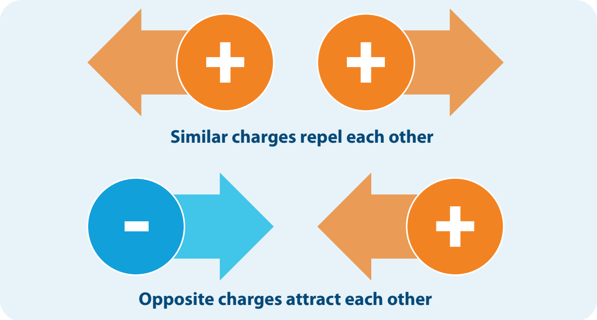


Chapter 1.1

# Direct current

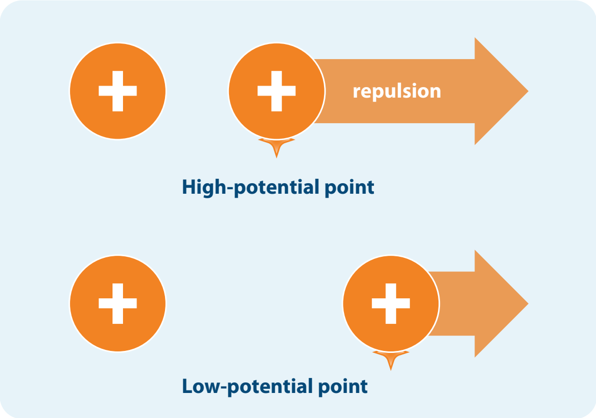
## 1.1.1. What is electricity?

The school physics course assumes that electric current is the ordered motion of charged particles. Charged particles in metals are electrons, in nonmetals — ions. What makes these particles move in an orderly manner? Electrical charges of the same signs repel each other, those of different signs attract each other. The space where forces of mutual attraction or repulsion between electrical charges act is called the electric field. Electric field forces act on any charge, placed in it, by moving it. The closer you move one electric charge carrier to another with the same sign, the greater force you will have to apply to resist the repulsion force, and greater potential energy will be accumulated by the charge.


+
+
Similar charges repel each other
-
+
Opposite charges attract each other

**Electrical charges**

Make the following experiment: bring one magnet to another fixed on its position — so that they repel each other. First you will feel slight resistance. Remember the magnet's position — this is the low-potential point. Shorten the distance between the magnets, and the repulsion force will be more noticeable. This is the high-potential point. And now abruptly let go the magnet you moved — it will spring aside though you did not push it. At that, it will rush to the low-potential point you remember.

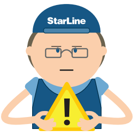


**Magnets experiment**

Though other forces act on magnets, this example demonstrates the behavior of charged particles in the electric field: they try to go from the high-potential point to the low-potential point.

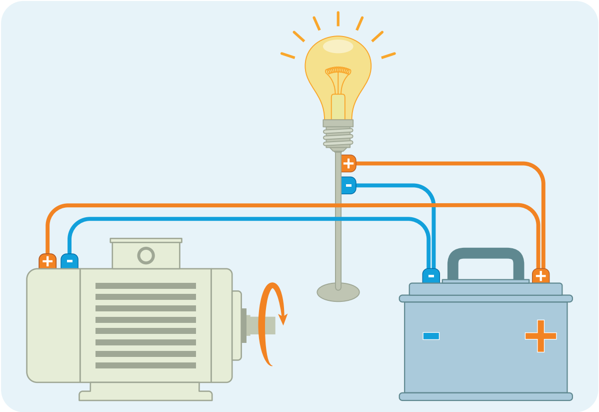
In the conventional car storage battery, chemical reactions on the minus terminal cause the formation of excessive negatively charged particles (electrons), while their shortage is observed on the positive terminal. Potentials difference occurs between the terminals; it is called **voltage**.

But still there is no electric current, since free charged particles are almost absent in the air under the normal conditions. If points with different potentials are connected by a conductor, usually a metallic wire, electrons from the negative terminal of the storage battery will start moving towards the positive one.



**This ordered motion of charged particles is what we call electric current.**

Despite the fact that electrons actually move from the negative terminal to the positive one, it is assumed that current goes from the plus to the minus. This current direction was established at random even before the discovery of electrons. The number of electrons on the negative terminal decreases with time, and increases on the positive one. This occurs until the potentials become equal. Electric current stops after their equalization. A car generator supports the excess of electrons on the negative terminal and creates a potentials difference (voltage).

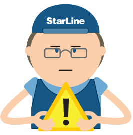


**Generator and storage battery**

Thus, existence of electric current requires the potentials difference and a connected conductor with free charged particles. The current source and conductor form together a closed electric circuit.

## 1.1.2. Characteristics of direct current

Direct current is characterized by two parameters — amperage and voltage. **Current intensity (amperage)** is, simply speaking, the number of charged particles moving orderly in a conductor. The greater their number, the greater work may be performed by electric current.



**Work performed in unit time is called power.**

The terms "high load" and "low load" are applied in practice. The load means a current consumer with a certain power. Thus, a large load has a large power. It means that the current in this conductor performs great work at each time moment. For this, a considerable number of charged particles must move orderly in the conductor, i.e. large current passes through it.

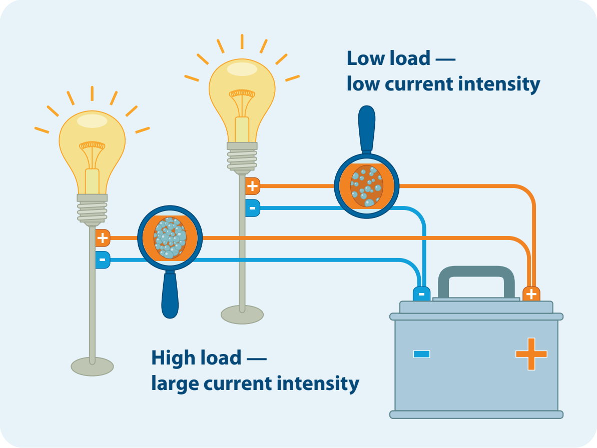
The division into high and low load is conventional and is mainly used to compare the value of one load with another, but not to designate a specific value of consumer power.

Amperage is measured in amperes or its derivatives: milliamperes (thousandths of ampere), microamperes (millionths of ampere).

**Amperage measuring units**

1 A = 1000 mA
(one ampere = one thousand milliampere)

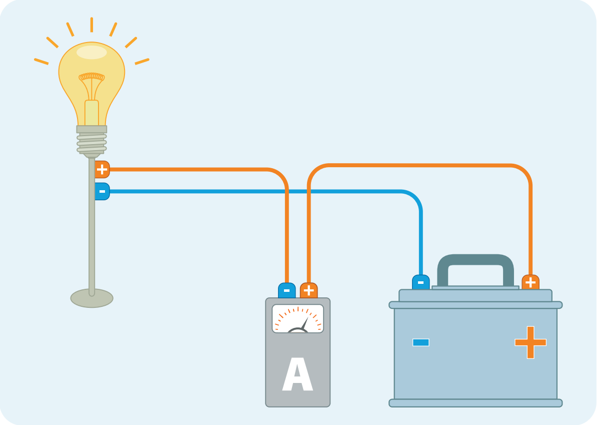
1 mA = 0,001 A = 1000 μA
(one milliampere = one thousandth ampere = one thousand microampere)



**Load and amperage**

Amperage is measured by means of a special instrument — **ammeter**, connected in the electric circuit in series with the consumer (meaning the following circuit: storage battery — conductor — ammeter — conductor — consumer — conductor — storage battery). The ammeter must be connected while observing the polarity marked on it. Besides, most of such instruments have different sockets for connection of probes depending on current intensity being measured. Bear it in mind that incorrect use of the ammeter, e.g. its connection in parallel to a current source, causes a short circuit and inevitable instrument failure!

What do we need amperage measurement for? What's the use in determining the number of charges? There is considerable use. Using only the ammeter, we can promptly assess installation correctness and avoid expenses on replacement or repair of damaged equipment. Instrument readings will show whether the circuit has leaks and failures. When selecting a fuse rating, knowledge of the consumption current value will also be helpful.



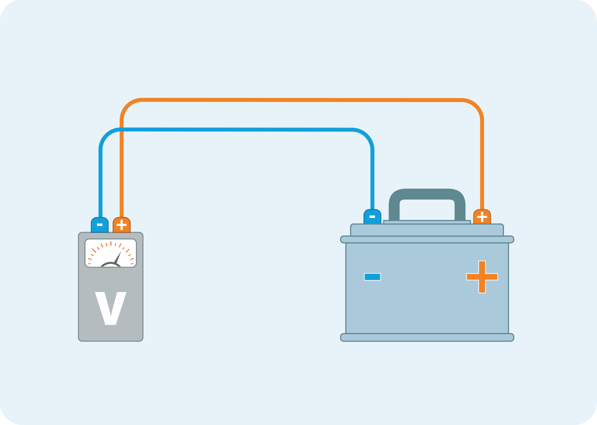
**Ammeter connection**

### Current consumption

| | |
|---|---|
| Serviceable security system in the standby mode | 20–40 mA |
| Starter at the starting moment with cold engine | up to 250 A |
| Horn at the sounding moment | 1–1,5 A |
| Conventional car kill-relay at actuation moment | 80–150 mA |
| Lock activator | 5–7 A |
| Hazard lights | 5–10 A |
| Passenger interior lighting | 2–3 A |
| Window raiser motor | 10–15 A |

If current in some circuit exceeds the design value, something is out of order. What may this lead to? For instance, installation of a very powerful horn (or two at once, to make it louder) may cause failure of the electronic key which controls the horn. Timely monitoring of amperage will protect the security system against breakdown.

**Voltage** is usually measured in volts or millivolts.



**Voltmeter connection**

**Voltage measuring units**

1 V = 1000 mV

(one volt = one thousand millivolt)

1 mV = 0.001 V = 1000 µV

(one millivolt = one thousandth volt = one thousand micro volt)

Timely use of a voltmeter will allow for avoiding many a trouble. It is an indispensable tool for installation of security systems and additional blockings. Detailed electric diagrams are often unavailable and the necessary circuits have to be found on one's own.

### 1.1.3. Ohm's law for a circuit section

Ohm's law is very simple — we may say it consists of "three letters" — but it answers many questions. You will use accurate calculation instead of the expensive trial and error method. Which fuse should be installed? Which wire cross-section should be taken? How many consumers can be connected in a circuit and what power may they have? The Ohm's law gives the correct answers. It determines the relation between values of voltage, current and resistance of a circuit section.

The pattern of this dependence can be written in the form of formula:

$$I = \frac{U}{R},$$

where I — current intensity (A); U — voltage (V); R — resistance (Ohm).

This formula can be converted by expressing either voltage or resistance from it:

$$U = I \times R$$

$$R = \frac{U}{I}$$

Please note that voltage in all the given formulas is expressed in volts, current — in amperes, while resistance — in ohms.

We have just recalled the voltage and current intensity, now we have to deal with the third characteristic — resistance.

**Resistance R** — is a quantity showing how difficult it is for current to pass through a conductor or consumer. Resistance is measured in ohms (Ohm).

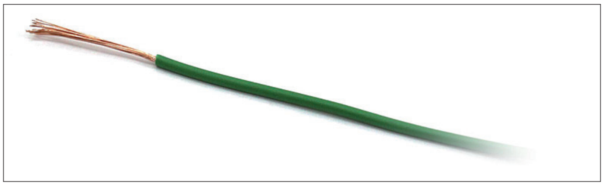
**Resistance measuring units**

1 kOhm = 1000 Ohm

(one kilo ohm = one thousand ohm)

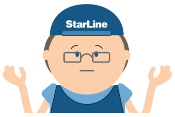
The higher the resistance value, the greater this conductor resists the current. Any conductor is characterized by its electric resistance. Mounting wire are usually made of low-resistance materials (e.g. copper).

Why should the wire resistance be the minimum?



**Copper wire**

The answer is simple. The higher the resistance, the less charged particles reach the consumer and the less work is performed by the current. Particles "lost on the way" will heat up the wire.



**Wire heating due to incorrectly calculated resistance may in some cases cause inflammation.**

**How can we reduce wire resistance?** There are three variants. Use the following:

**1)** a wire of material with lower specific resistance (e.g. resistance of silver is lower than that of copper, but wires made of pure silver are too expensive);

**Wires of different cross-section**

**2)** a shorter wire (the longer the conductor, the longer the distance that the charged particles have to go. If we shorten this distance, losses will decrease);

**3)** a wire of larger cross-section (in this case it will be easier for the charges to pass through the metal).

While the first two methods are not always applicable, the third one is the most widespread. Correct selection of wire cross-section (this parameter, but not the diameter, is usually specified for conductors) will prevent many problems, the most unpleasant of them being the inflammation of wiring. The following table is convenient to use:

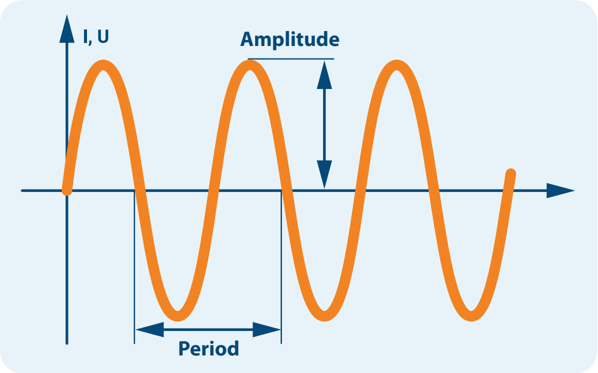
**Table for selecting cross-section of a wiring copper wire depending on consumed current value**

| Required cross-section of copper wire strands (mm$^2$) | Maximum design current (A) |
|---|---|
| 0,17 | 1,0 |
| 0,33 | 2,0 |
| 0,52 | 3,0 |
| 0,67 | 4,0 |
| 0,84 | 5,0 |
| 1,0 | 6,0 |
| 1,7 | 10,0 |
| 2,7 | 16,0 |
| 3,3 | 20,0 |
| 4,2 | 25,0 |
| 5,3 | 32,0 |
| 6,7 | 40,0 |
| 8,4 | 50,0 |
| 10,5 | 63,0 |

Chapter 1.2

# Alternating current and its characteristics

In addition to direct (time-invariant) current there is alternating current changing its value and direction with time. Electric power generators, including those on cars, generate alternating current then converted into direct one. As a rule, alternating current changes in time as per the sinusoidal law. There are additional parameters for its description — **frequency and amplitude**.



**Amperage**

Frequency is the quantity showing the number of full oscillations of current (or voltage) per second. Frequency is measured in hertz (one hertz is equal to one oscillation per second).

**Frequency measuring units**

1 kHz = 1,000 Hz

(one kilohertz = one thousand hertz)

1 MHz = 1,000 kHz = 1,000,000 Hz

(one megahertz = one thousand kilohertz = one million hertz)

It can be determined using a special instrument — frequency meter, but in practice the oscilloscope is usually used, showing both the frequency and signal waveform. Another parameter, called **period** is related to frequency. Period is the time of one full oscillation. It is measured in seconds.

**Oscillation period measuring units**

1 ms = 0.001 s

(one millisecond = one thousandth second)

1 μs = 0.001 ms = 0.000 001 s

(one microsecond = one thousandth millisecond = one millionth second)

Oscillation frequency is a quantity reciprocal of period:

$$f = \frac{1}{T}$$

or

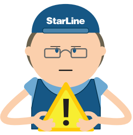
$$T = \frac{1}{f},$$

where f — frequency (Hz); T — period (s).

Amplitude is the sinusoid height, i.e. the maximum current value measured from the zero level. Amplitude is measured in the same units as the primary quantity, i.e. alternating current amplitude is measured in amperes, alternating voltage amplitude — in volts. The frequency of 50 Hz is usually used in the domestic power network. **Network voltage value is assessed** not according to amplitude, but **according to its effective value,** allowing for simple determination of alternating current power. The effective value can be calculated according to the voltage and current amplitude using the ratio:

$$U_э = 0{,}707\ U_m.$$

What is the voltage amplitude in the domestic power network? 220 volt? No! It turns out to be 311 volt, while the effective voltage value is 220 volt. The term “effective (value)” is often omitted.



**All instruments show effective values during measurement in alternating current circuits.**

Depending on frequency value, oscillations were named differently; the names are given below.

**Please note:** oscillations may be freely emitted in the air medium only starting with the frequency of 100 kHz. However, the same oscillations can be perfectly transmitted via wires, which ensure their wide use in car immobilizers. In short, a signal from the key-transponder, inserted in the ignition lock, is transmitted in the air medium to the receiver antenna installed on this lock. On the other side, when the module of factory immobilizer bypass is used, the signal from the key-transponder, hidden in the underhood space, goes via the wires to the same antenna.

**Frequency range of various oscillations**

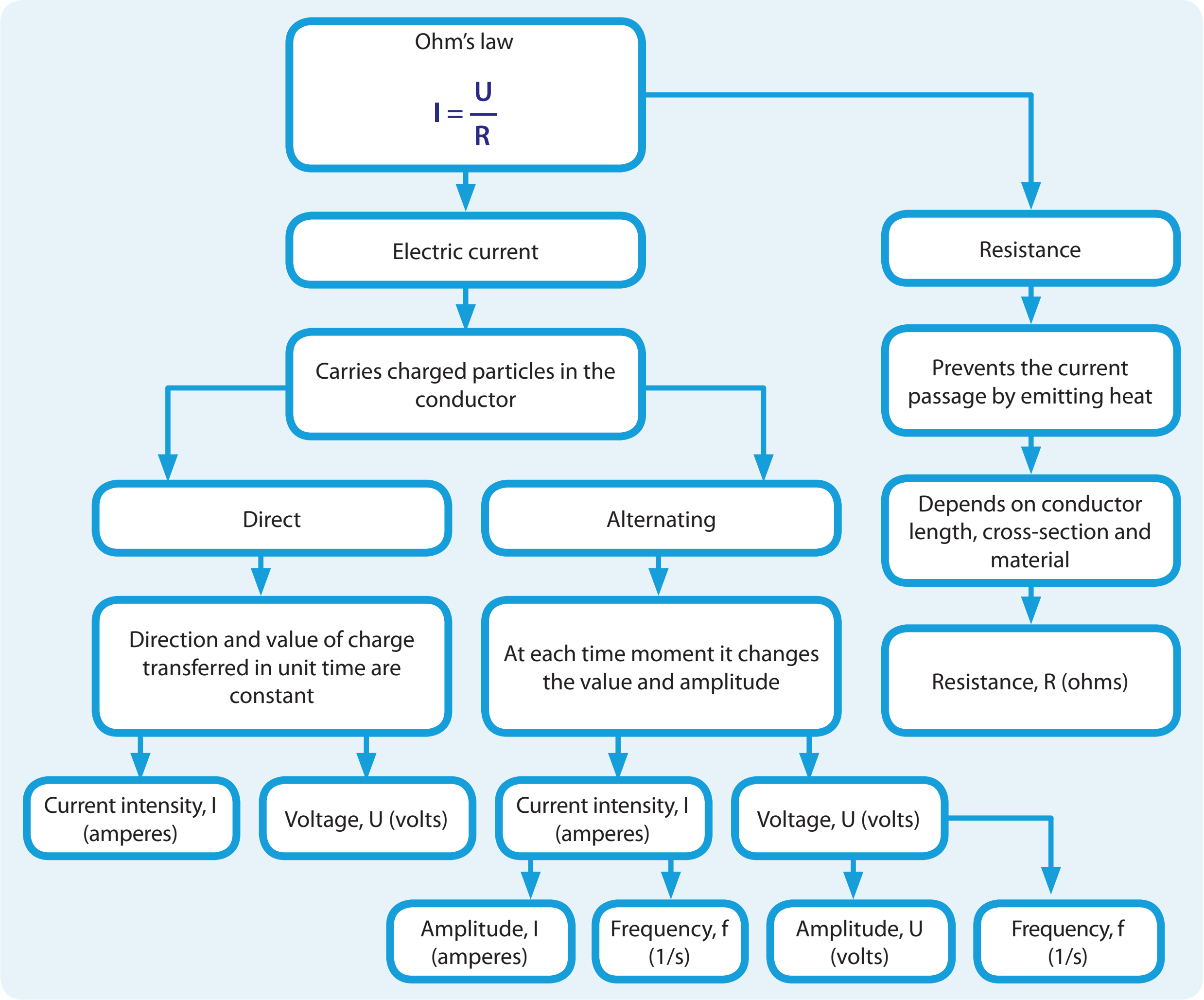
| Oscillation name | Frequency range (Hz) |
|---|---|
| Sound | 20–20000 |
| Ultrasonic | 20 000–100 000 |
| Radio waves | $100\,000–3 \times 10^{11}$ |
| Infrared rays | $1{,}5 \text{ x } 10^{11}–4 \times 10^{13}$ |
| Visible light | $4 \text{ x } 10^{14} –7{,}5 \times 10^{14}$ |
| Ultraviolet rays | $10^{15}–10^{17}$ |
| X-rays | $10^{18}–10^{19}$ |
| Gamma-rays | $10^{20}$ |

You can study the field of radio frequency application using the following table

**Applicability of radio signals**

| Radio signals | Wavelength | Frequency | Application |
|---|---|---|---|
| Long waves (LW) | 1–10 km | 30–300 kHz | Radio broadcasting<br>Transponders (90-120 kHz)<br>Park radars (30 kHz) |
| Medium waves (MW) | 100–1000 m | 300–3000 kHz | Radio broadcasting |
| Short waves (SW) | 10–100 m | 3–30 MHz | Radio broadcasting<br>Amateur radio communication (27 MHz) |

| Radio signals | Wavelength | Frequency | Application |
|---|---|---|---|
| **Ultrashort waves (USW)** | | | |
| a) meter | 1–10 m | 30–300 MHz | Radio broadcasting, television |
| b) decimeter | 1–10 dm | 300–3000 MHz | Radio broadcasting<br>Cellular communication (900 MHz and 1,800 MHz)<br>GPS-navigation<br>Car alarm remote controls 433 (92 MHz and 867.8 MHz) |
| c) centimeter | 1–10 cm | 3–30 GHz | Radar location<br>Bluetooth (2.4-2.48 GHz);<br>Volume sensors<br>Immobilizers |
| d) millimeter | 1–10 mm | 30–300 GHz | Radar location |


Ohm's law
$I = \frac{U}{R}$
Electric current
Resistance
Carries charged particles in the conductor
Prevents the current passage by emitting heat
Direct
Alternating
Depends on conductor length, cross-section and material
Direction and value of charge transferred in unit time are constant
At each time moment it changes the value and amplitude
Resistance, R (ohms)
Current intensity, I (amperes)
Voltage, U (volts)
Current intensity, I (amperes)
Voltage, U (volts)
Amplitude, I (amperes)
Frequency, f (1/s)
Amplitude, U (volts)
Frequency, f (1/s)

**Ohm's law. Memo diagram**

Part 2

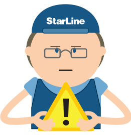
# Main elements in an electric circuit

*The theory of electricity is almost over, we just need to consider the main elements of an electric circuit that may be needed during security equipment installation.*

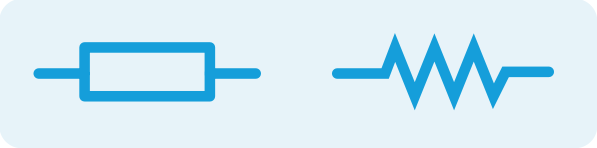
## Chapter 2.1
# Resistor

The simplest and most widespread element is the resistance (resistor). At first sight, it is a completely useless element which only consumes electric power. But some devices can be created only based on the resistor. For instance, one needs to connect a LED to a source of +12 V direct voltage. If this is done directly (the anode — to +12 V, the cathode — to the ground), then, according to the Ohm's law, current may reach high values due to the low diode resistance in the forward direction and fixed voltage.

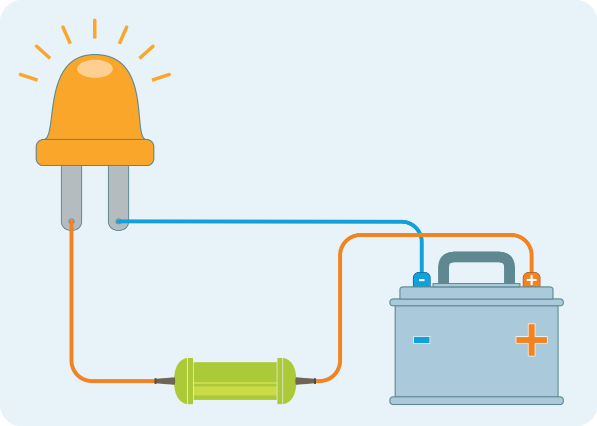
**The light-emitting diode (LED)** is usually **rated for a low current**, that's why it will burn out at once. To avoid this, we add a resistance of the calculated rating to the "source — LED" circuit. A part of "excess" energy will be dissipated on this resistance, and the current of the required value will pass through the LED.



**The resistor is characterized by two main parameters — resistance value and dissipated power.**



**Resistor designation in circuit diagram**



**Dissipation of excess energy by the resistance**

Fixed resistors in circuit diagram are usually shown as rectangles or zigzags (in foreign diagrams).

As mentioned earlier, the resistor resistance value is measured in ohms and shows to which extent it hinders the passage of electric current. This parameter is compulsorily marked on the resistor package. For unification, all manufacturers agreed to make resistors of strictly determined ratings, called rows. For instance, the rating row E12, comprising the following 12 numbers:

**Resistor ratings**

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1,0 | 1,2 | 1,5 | 1,8 | 2,2 | 2,7 | 3,3 | 3,9 | 4,7 | 5,6 | 6,8 | 8,2 |

It means that the resistance value of resistors, corresponding to this row, is equal to, say, 2.7 Ohm or 2.7 kOhm, but the resistance with the rating of 3 Ohm cannot be in this row. Therefore, if calculation of a ballast resistance yields a number which is not a multiple of any of the values in the row, the nearest value from the standard row shall be chosen.

**Resistor appearance**

Resistor, in particular low-power ones, have the length of several millimeters and a diameter of about millimeter. A rating with decimal point cannot be read on such a part. Therefore, when the rating is specified, the decimal point is substituted by the letter corresponding to the measuring units (K — kiloohms, M — megaohms, E or R for units of Ohms). Any rating is shown by three symbols maximum. For instance, 4K7 means a resistor with the resistance of 4.7 kOhm, 1R0 — 1 Ohm, M12 — 120 kOhm (0.12 MOhm), R100 — 0.1 Ohm etc. However, even in this form the marking of ratings on small resistors is difficult and marking by color stripes is used (see fig. on page 21).

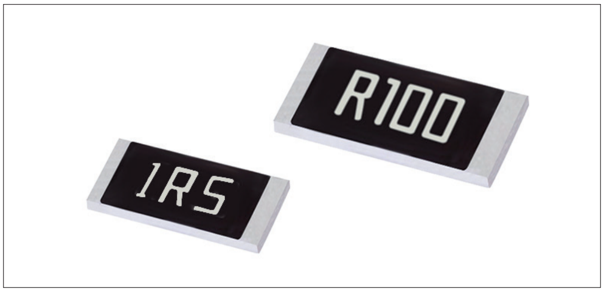
The resistors shown above have wire leads inserted into holes on printed circuit boards. This type of wiring is called point-to-point. Modern security systems use the so-called chip-resistors for surface mounting using the SMD-technology (surface mounted device). This technology is the most popular method for engineering and assembly of electronic units on printed circuit boards at present. SMD-resistors are tiny radio components. It is rather difficult to see and solder them.

The coding described above or coding only by digits is possible for SMD-resistors. The most frequent coding is with 3 digits:

ABC means ABx10C Ohm (for instance, 102 — it is 10x102 Ohm = 1 kOhm).

Accordingly, 152 — 1.5 kOhm, 100 = 10 Ohm, 821 — 820 Ohm. Resistors less than 10 Ohm are always coded with a letter, e.g. 1R5 or 1E = 1.5 Ohm.

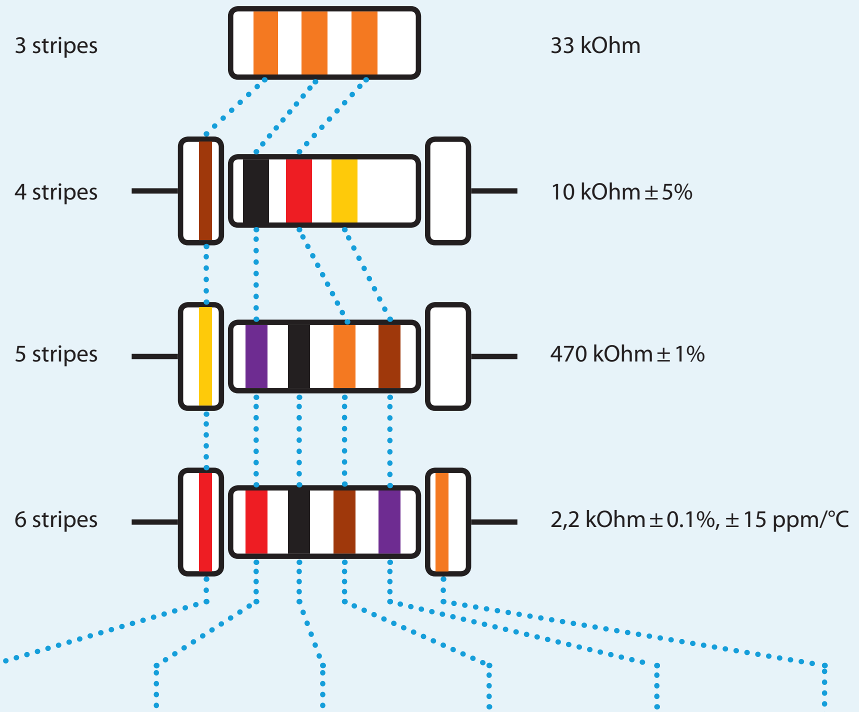
Zero-resistance resistors (jumpers on the board) are coded with one digit — 0.



**SMD-resistors of different ratings**

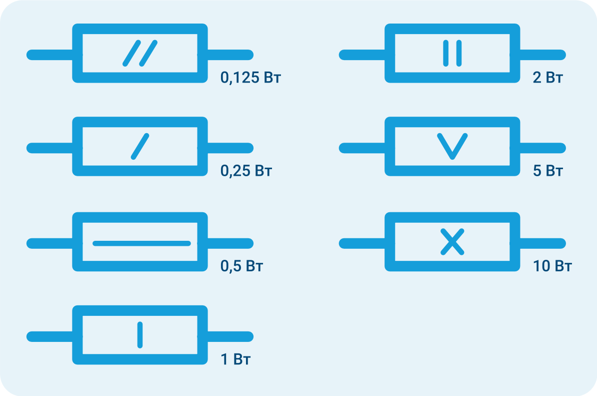
The second important resistor parameter is **rated power**. Passing current heats up the resistor. The largest power that a resistor may dissipate in the given conditions — is the rated power. This parameter is the higher, the more heat the resistor can dissipate without burning out. Power is measured in watts. It is marked on circuit diagram directly on the conventional representation. Power on a real resistor is marked only on large packages. If this parameter is lacking, power is determined according to the resistor size. The resistor may burn out if its power is incorrectly selected. This will occur if you use a resistor with power lesser than it must dissipate.

However, you may use a resistor with knowingly larger power than necessary for the specific case. Thereat, it will be more expensive and larger, which is not always convenient. Consequently, resistors

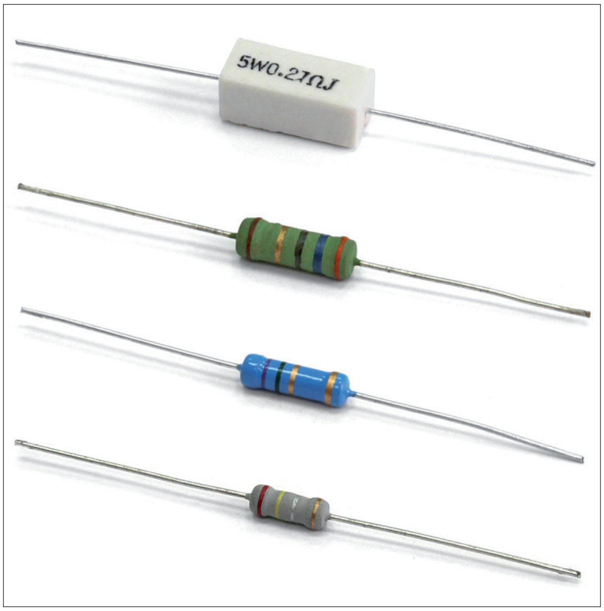


| | | | | | | |
|---|---|---|---|---|---|---|
| Silver | | | | 0,001 | 10 | |
| Gold | | | | 0,1 | 5 | |
| Black | | 0 | 0 | 1 | | |
| Brown | 1 | 1 | 1 | 10 | 1 | 100 |
| Red | 2 | 2 | 2 | $10^2$ | 2 | 50 |
| Orange | 3 | 3 | 3 | $10^3$ | | 15 |
| Yellow | 4 | 4 | 4 | $10^4$ | | 25 |
| Green | 5 | 5 | 5 | $10^5$ | 0,5 | |
| Blue | 6 | 6 | 6 | $10^6$ | 0,25 | 10 |
| Violet | 7 | 7 | 7 | $10^7$ | 0,1 | 5 |
| Grey | 8 | 8 | 8 | $10^8$ | 0,05 | |
| White | 9 | 9 | 9 | $10^9$ | | 1 |
| Color | 1-st digit | 2-nd digit | 3-rd digit | Multiplier | Allowance, % | Temperature coefficient of resistance, , ppm/°C |

**Explanation of resistor marking**



**Designation of resistor dissipation power in the diagram**



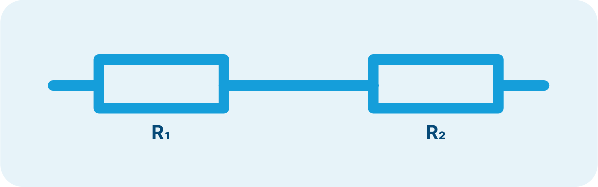
**Resistors of different power**

should be correctly selected according to this parameter. Resistors with a power of 0.125-0.25 W are sufficient for most low-current circuits. Resistors of larger power must be selected for power circuits (e.g. switch-on of the actuator in case of “smart” blocking). Sometimes the resistor of the necessary rating or power is not at hand. What to do in such a situation? You can create a resistor on your own! Of course, we mean the connection of several prefabricated resistors in a certain way to obtain the required characteristics.

**Burned-out resistor**

Incorrectly selected resistor power causes its burn-out!

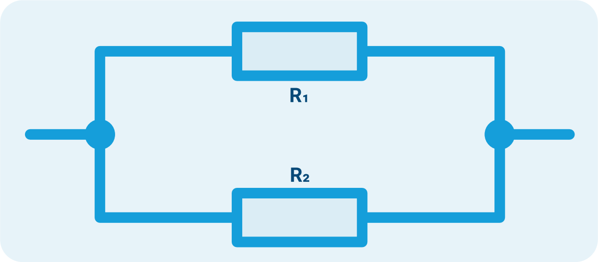
Resistors can be connected in series or in parallel.



**Series connection of resistors**

$$R_{tot} = R1 + R2.$$

Total resistance of a resistor string increases in case of series connection and decreases in case of parallel connection.



**Parallel connection of resistors**

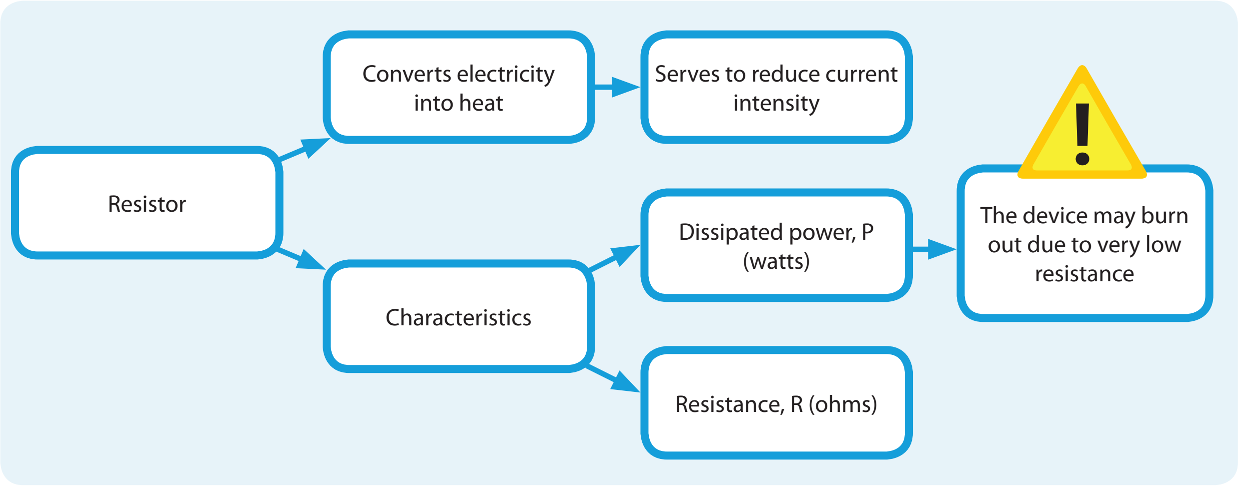
$$R_{tot} = \frac{R1 \times R2}{R1 + R2}.$$

Parallel connection allows for using separate low-power resistors to create one more powerful resistor.

Thus, parallel connection of two resistors with the rating of 50 Ohm and the power of 0.25 W, total resistance will be equal to 25 Ohm, while total power — 0.5 W.

**It must be noted**, that this method should be avoided in everyday practice.

**Using a resistor with suitable characteristics is always better and more reliable.**


Resistor
Converts electricity into heat
Serves to reduce current intensity
Characteristics
Dissipated power, P (watts)
Resistance, R (ohms)
The device may burn out due to very low resistance

**Resistor. Memo diagram**

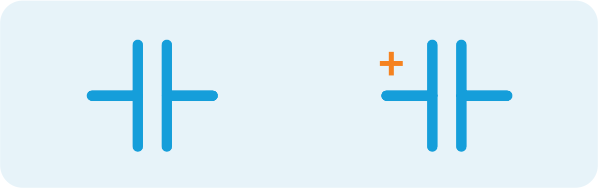
Chapter 2.2

# Capacitor

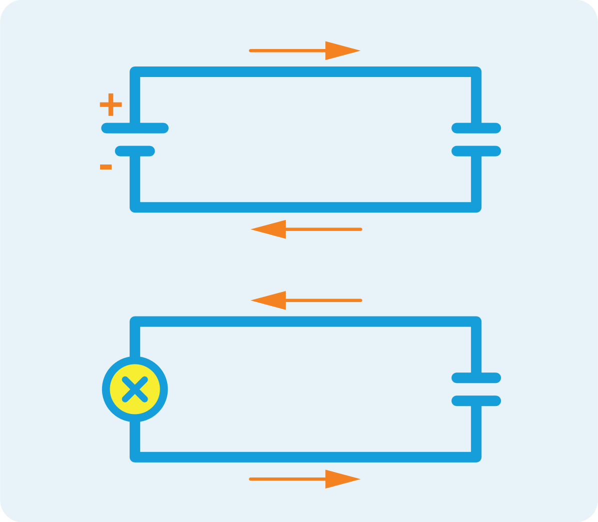
The word "capacitor" means "accumulator". What does it accumulate? The capacitor accumulates electric charge and stores it for some time (up to several tens of hours). In this respect the capacitor can be compared to a storage battery — first it collects the charge and then gives it away as needed.

**Capacitors of different types and models**

The capacitor is shown in circuit diagram as two parallel lines perpendicular to the conductor.

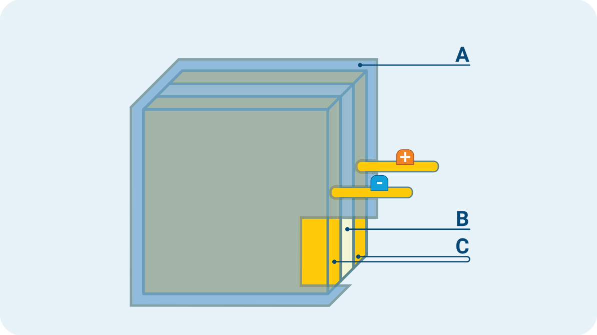


**Conventional designation of nonpolar and polar capacitors**



**Capacitor charging and discharging**

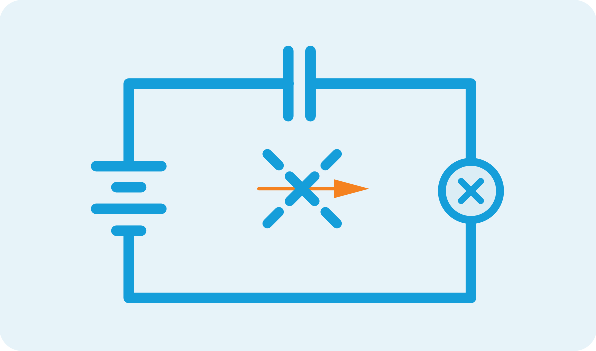
Energy is accumulated in a storage battery due to complex chemical reactions, while nothing of the kind occurs in the capacitor. Literally, the best capacitor is current-conducting sheets in vacuum. Since the ideal vacuum is difficult to achieve, the simplest capacitor is a device consisting of two metal sheets and an air layer between them. If the sheets are connected to a power source, the capacitor will accumulate charge. Then, if an electric lamp is connected instead of the source, it will be illuminated for some time due to the electricity stored in the capacitor. At present, solid-state dielectrics (nonconducting substances) are used instead of air in capacitors.



**Capacitor design. A – package, B – dielectric, C – current-conducting plates**

Let us note one of the capacitor's important properties — it does not pass electric current. Alternating current may pass through the capacitor conventionally. Why is it so? Let's try and figure it out. If a discharged capacitor is connected to a DC electric circuit, it will start discharging at once. Current will flow in the circuit, charge carriers will accumulate on the capacitor sheets. Thereat, particles on the plates become close-packed, the number of particles additionally falling on the plates is decreasing. The same occurs to the current in the circuit. The current will stop as soon as "all places" on the plates are "occupied".

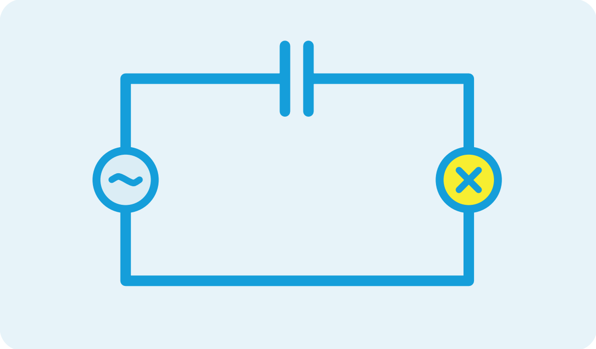
This process can be compared to the filling of an empty bus at the terminus— the doors open and a crowd of passengers rushes in. But soon all the seats and free places are occupied and no one will push one's way in, though there are still many people on the stop. The same is with our circuit — despite its connection to the source, there will be no current in it after capacitor charging.



**Capacitor and direct current**

Alternating current, reversing its direction, is flowing in the circuit under consideration. In the course of capacitor charging, the current direction changes at a certain moment and discharging begins, and then the capacitor receives charge again, but at this time of the opposite polarity. Such oscillations occur until the alternating current source operates in the circuit. Thus, the motion of electrons, i.e. current flow, is constantly observed in the circuit with alternating current and capacitor.

This capacitor property allows using it, for instance, for separation of the current direct component from the alternating one.



**Capacitor and alternating current**

The capacitor's main characteristic is capacitance. As any other vessel (e.g. a fuel can), it is synonymous to capacity, i.e. the larger the capacitor capacitance, the more energy it will store. Capacitance is measured in farads, but one farad is a very large capacitance, therefore derived values are used more often.

### Capacitance units

1 µF = 0.000,001 F

(one microfarad, µF = one millionth farad)

1 nF = 0.001 µF

(one nanofarad, nF = one thousandth microfarad, µF)

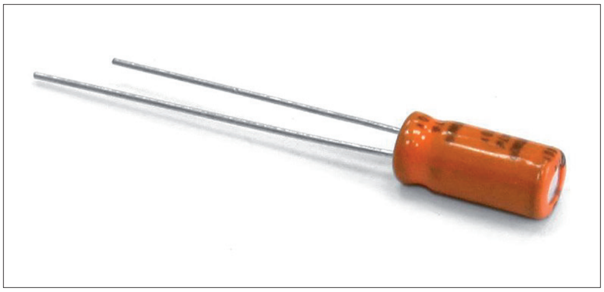
1 pF = 0.000,001 µF

(one picofarad, pF = one millionth microfarad, µF)

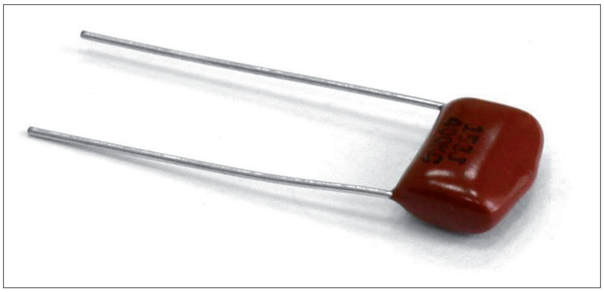
Car audio equipment uses special capacitors with capacitance of units (up to 15) of farads, which compensate supply voltage sags at a high sound level.

### Capacitors can be polar and nonpolar

The former require observance of connection polarity: the lead marked plus must be connected to the plus, but not to the minus. What will occur in the other case? The capacitor will fail. Thereat, this fact will be "announced" by a loud clamp and splashing of the content in every direction. That's why pay attention to marking on the capacitor housing and printed circuit board (connection polarity is marked on all boards in installation places of polar capacitors).



**Polar capacitor**



**Nonpolar capacitor**

The nonpolar capacitor does not have this shortcoming, it can be connected in the circuit without observing polarity.

But polar capacitors cannot be completely abandoned, because all high-capacitance capacitors are polar.

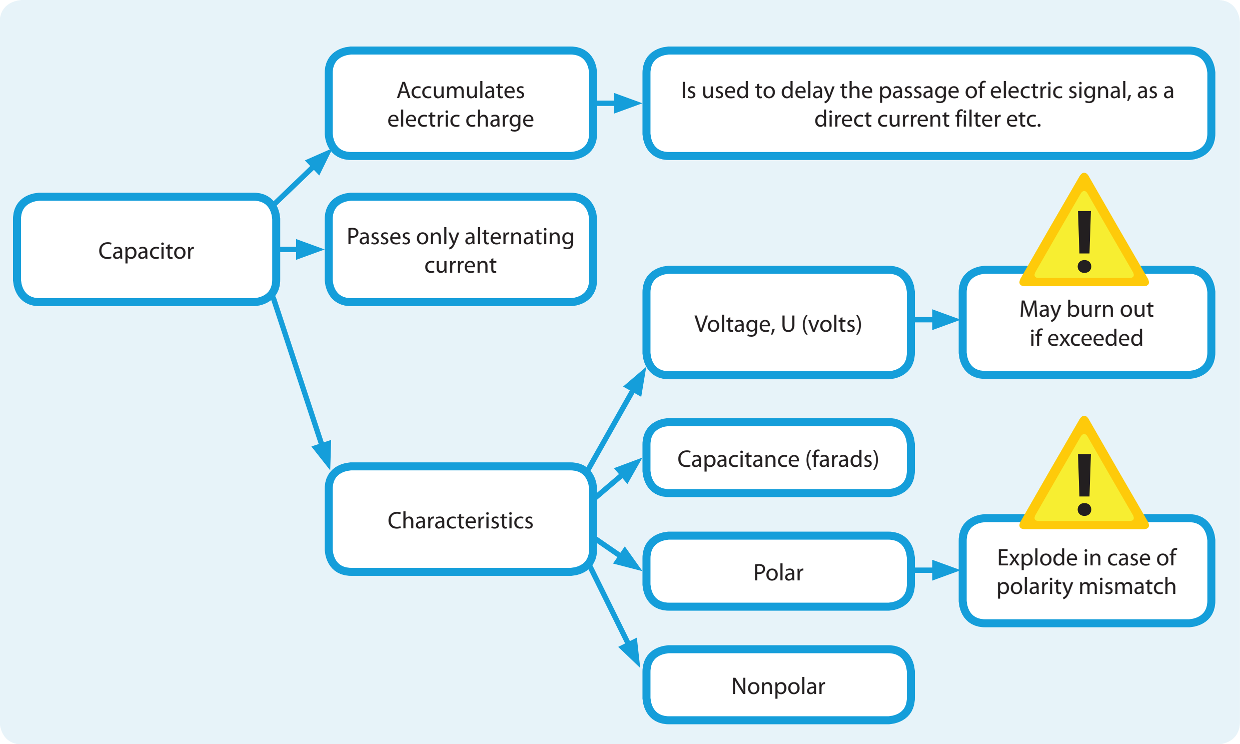
The second important capacitor parameter is the operating voltage. Since a thin dielectric layer is located between the capacitor plates (sheets), exceeding of the specified voltage may cause electric breakdown (short circuit) inside the capacitor and its failure.

**Incorrectly selected capacitor operating voltage causes its failure or even an explosion!**

Capacitor rated voltage should be selected with some margin, i.e. for a 12 V circuit one should take a capacitor, for instance, marked 16 V. For the same purpose one may take a capacitor of 25 V, but it is usually more expensive and larger.

Polar capacitors have voltage and connection polarity marked directly on the housing, nonpolar ones — usually only capacitance. Capacitors are used in electronics as a component of electric filters, resonant circuits and separating elements in amplifier stages. Together with the resistance they are used as a time-setting circuit in generators and timers. In installation of car security systems, for instance, the capacitor ensures a delay of relay actuation or release. It can be also used in connection of the engine start monitoring circuits for separation of the current direct component from the alternating one.

**Exploded capacitor**


Capacitor

Accumulates electric charge

Is used to delay the passage of electric signal, as a direct current filter etc.

Passes only alternating current

Characteristics

Voltage, U (volts)

May burn out if exceeded

Capacitance (farads)

Polar

Explode in case of polarity mismatch

Nonpolar

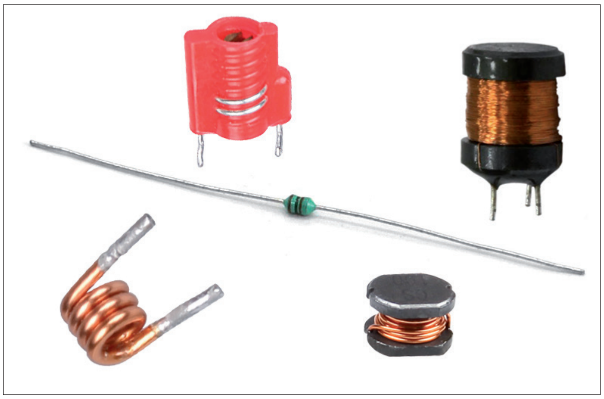
**Capacitor. Memo diagram**

Chapter 2.3

# Inductance

The radio component called inductance is a simple wire twisted in the form of a spiral or coil. That's why it is often called an inductance coil or simply a coil. Coils are usually multilayer (i.e. the wire is laid in several layers), they are wound on a special core enhancing the inductive properties.

The coil in a direct-current circuit is a standard conductor having only resistance. However, alternating current will pass through it in a completely different way. The coil, figuratively speaking, prevents any current change: both increase and decrease. Operation of the inductance can be understood on a simple example of inertia. Let us try to move a non-started car — this will require some effort because its weight is large. But it will be much more difficult to stop the accelerated car.



**Inductance coil appearance**

The inductance coil has two parameters which should be pointed out — inductance, measured in henry, and permissible current.

### Inductance units

1 mH = 0,001 H

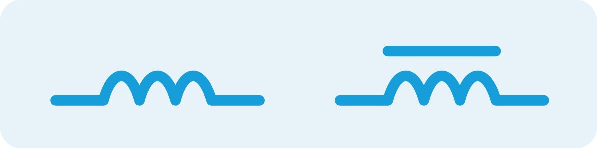
(one millihenry = one thousandth henry)

1 μH = 0.000,001 H

(one microhenry = one millionth henry)

The inductance value determines the extent to which the coil will resist the current change: the larger this parameter, the more difficult it is for alternating current to "overcome" the coil and then to "stop". This parameter is influenced by many

**Inductance coil with tuning**

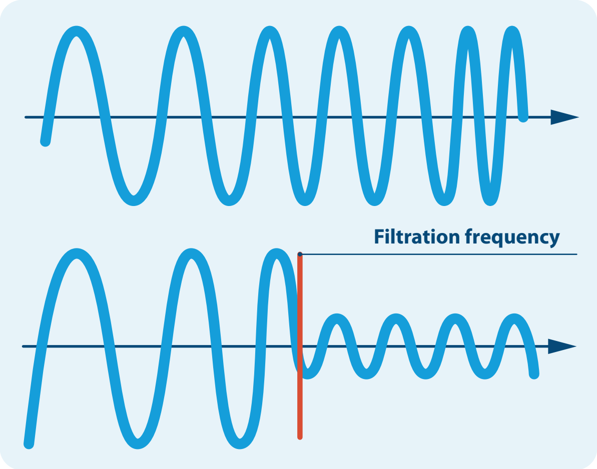


**Conventional designation of air-cored inductance coil and cored inductance coil**

factors: the number of coil turns, its diameter, sizes, conductor material. In some coils the core can move along the axis, thus allowing for inductance adjustment.

The permissible coil current is chiefly determined by the diameter of the wire it is made of.

For alternating current, inductance coil impedance also depends on its frequency. The higher the frequency, the less time remains for overcoming of the inductive obstacle by the current. It means the less current will be passed by the coil. This property is often used in the socalled filters — elements separating the alternating current of one frequency from alternating current of another frequency or frequency range.



**Frequency separation by an inductive filter**

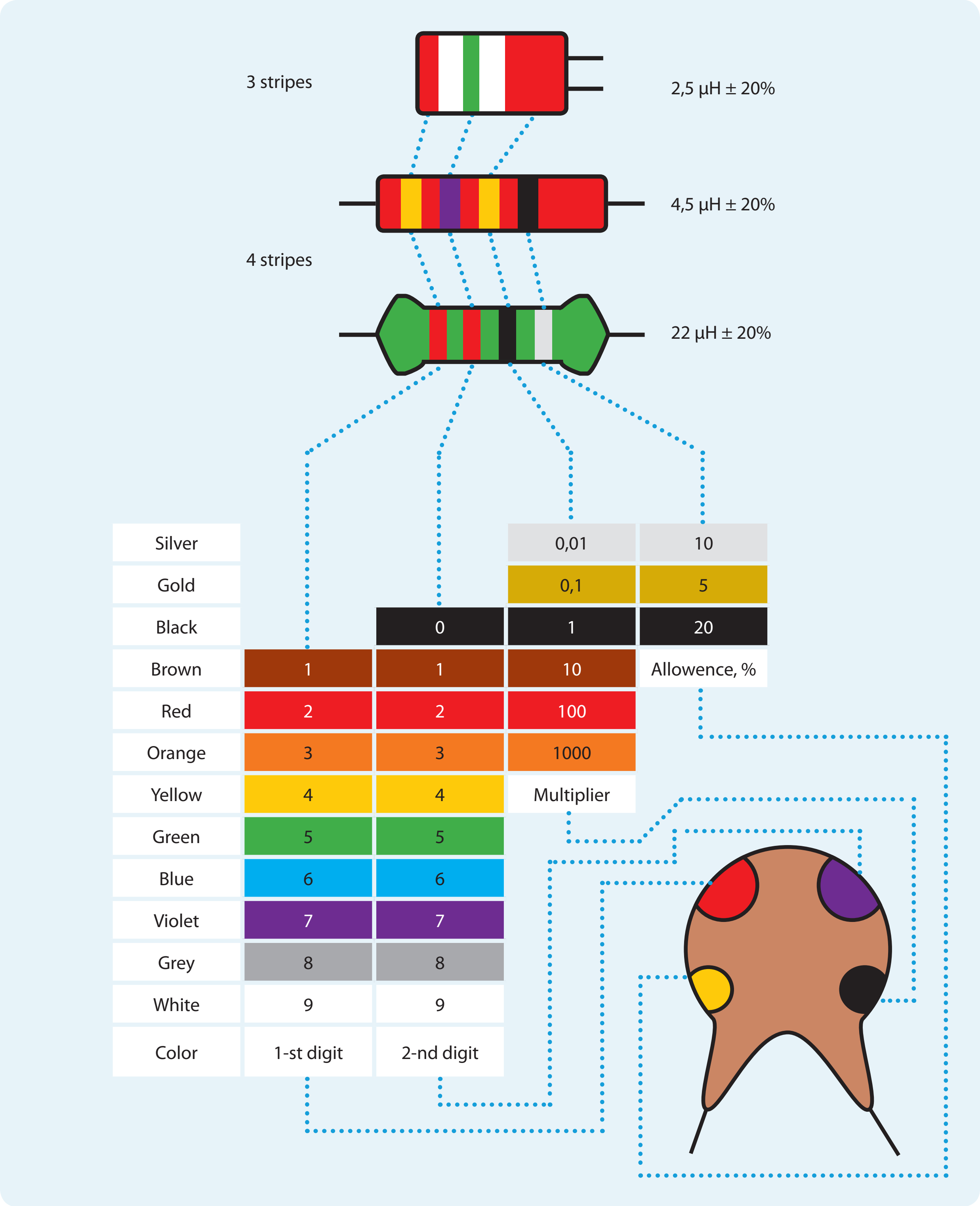
The inductance coil behaves similarly not only at alternating current but also at switch-on or switch-off of direct current, when current gradually increases from zero to the maximum value (or decreases from the maximum value to zero) — in this it is similar to alternating current. Therefore powerful inductance coils (sometimes called chokes) are often installed at power inputs of some devices for smoothing of possible current ripple and equipment protection.

Inductance coils are very widely used in car electrical equipment, e.g. in ignition coils, acoustic loudspeakers, electric motors and other devices. Inductance value is usually marked on the coil housing as alphanumeric marking, colored stripes or dots. The first two digits show the value in microhenry (μH), the last one — the number of zeroes. The letter after the digits shows the allowance (the extent to which real inductance may differ from the digit in the marking). For instance, code 101J means 100 μH with ±5 % allowance. If the last letter is absent — 20 % allowance. Exceptions: for inductance less than 10 μH the decimal point is letter R, while for inductance less than 1 μH — letter N.

Allowance can be also designated with other letters:

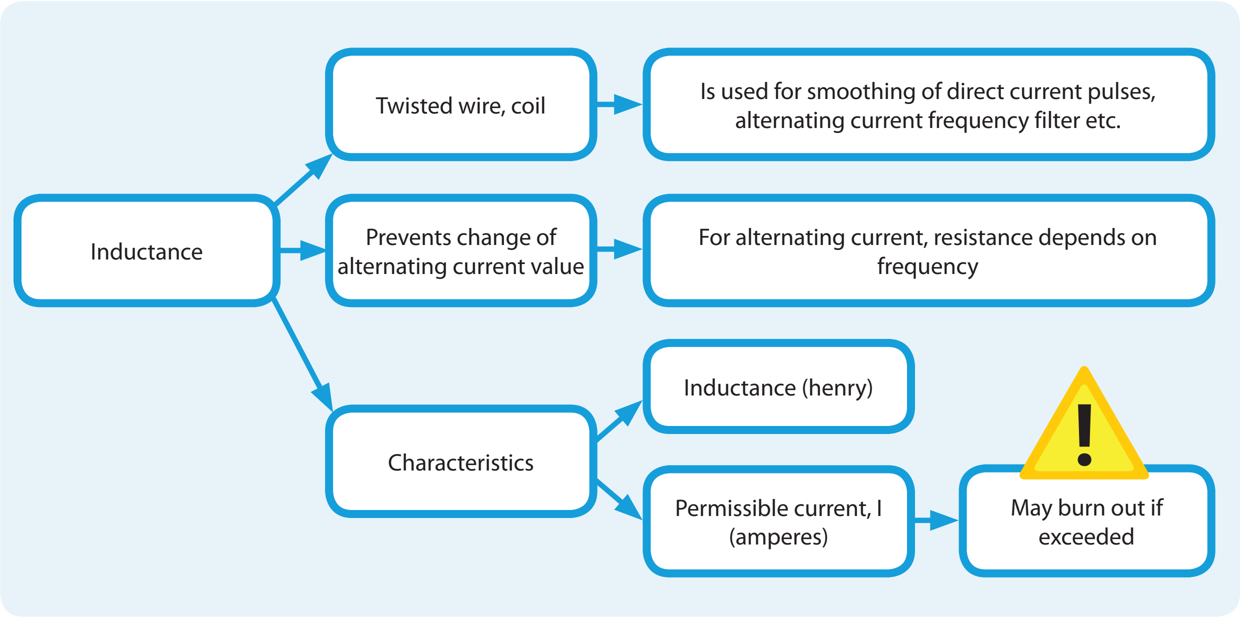
**D = ±0,3 nH;**
**J = ±5 %;**
**K = ±10 %;**
**M = ±20 %.**

Sometimes inductance coils are marked directly in microhenry. The color marking of coils is similar to the marking of "striped" resistors.



| Color | 1-st digit | 2-nd digit | Multiplier | Allowence, % |
|---|---|---|---|---|
| Silver | | | 0,01 | 10 |
| Gold | | | 0,1 | 5 |
| Black | | 0 | 1 | 20 |
| Brown | 1 | 1 | 10 | |
| Red | 2 | 2 | 100 | |
| Orange | 3 | 3 | 1000 | |
| Yellow | 4 | 4 | | |
| Green | 5 | 5 | | |
| Blue | 6 | 6 | | |
| Violet | 7 | 7 | | |
| Grey | 8 | 8 | | |
| White | 9 | 9 | | |

**Inductance coil marking**


Inductance
Twisted wire, coil
Is used for smoothing of direct current pulses, alternating current frequency filter etc.
Prevents change of alternating current value
For alternating current, resistance depends on frequency
Characteristics
Inductance (henry)
Permissible current, I (amperes)
May burn out if exceeded

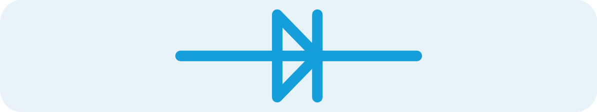
**Inductance. Memo diagram**

Chapter 2.4
# Diode

The diode is a semiconductor device whose main property is unidirectional conductivity.

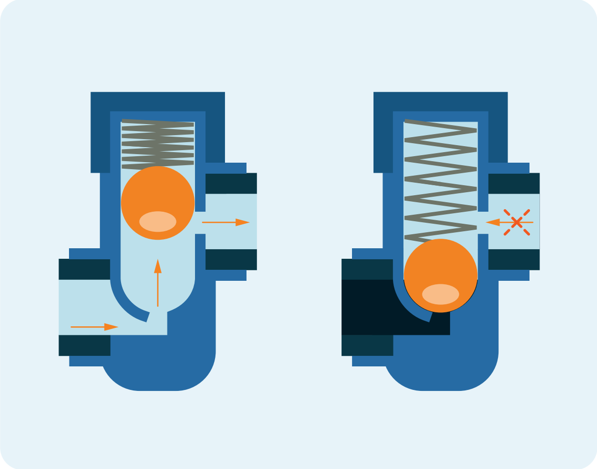
What is a semiconductor? This is not a conductor as a metallic wire, not a dielectric as insulation, but something in between. Semiconductors are made of silicon contained in sand. Silicon in the usual state is a dielectric, but special treatment imparts to it specific properties, allowing for passage of electric current under certain conditions. The diode uses a combination of two types of semiconductors with different characteristics. This combination discloses a new useful property — the diode passes current in one direction and does not pass it in the other one. Thanks to this behavior, diodes are widely used in installation of security equipment — for isolation of door limit switches, "cutoff" of pulses of certain polarity, shunting of relay windings in order to reduce induction surges at actuation.

The diode can be compared with a valve passing water in one direction and preventing its return flow.



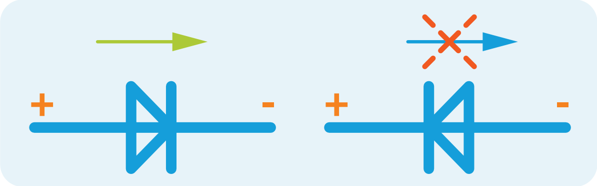
Conventional designation of rectifier diode

Current passes through the diode in the direction of the arrow in the conventional designation.

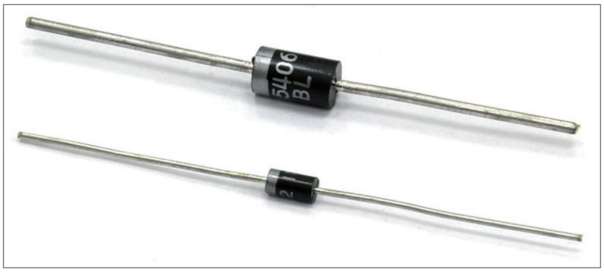


Diode analogue — water valve

The diode has two leads — anode and cathode. If anode potential exceeds the cathode potential,



The diode passes current in one direction only



**Types of rectifier diodes**

the diode is open (current is flowing), if vice verse — it is closed (current is not flowing). To determine the location of the anode and the cathode, the casing of rectifier diodes has marking in the form of conventional designation or a stripe at the cathode.

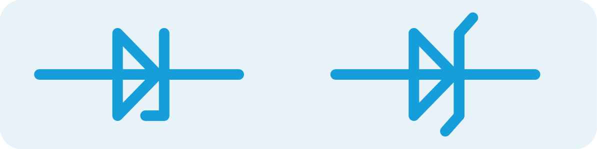
The main parameter of a rectifier diode is the permissible current which the diode may pass in the reverse direction without overheating. The following characteristics are also important: the permissible reverse voltage, forward voltage drop on the diode (since the diode is not ideal, it has low resistance), forward pulse current, reverse leakage current. These parameters are usually stated in reference books.

In addition to conventional rectifier diodes, other semiconductor devices are also used in security equipment installation; their design is similar to the conventional rectifier diode. These are the so-called Zener diodes and light-emitting diodes.

## 2.4.1. Zener diode

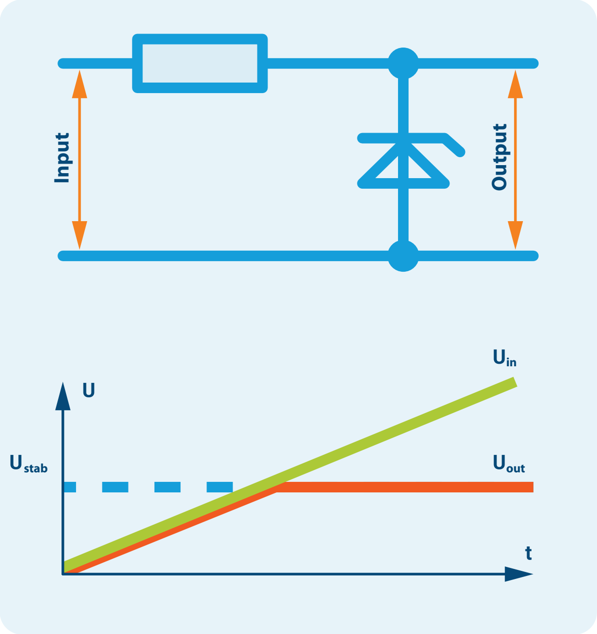
The Zener Diode has functions similar to the diode. Similarly to the diode, it passes current in one direction and stops it in the other. But electric breakdown occurs at a certain moment in case of the reverse current direction, and Zener diode resistance drops abruptly. Electric breakdown in this case is reversible (if there is no thermal breakdown due to too high current intensity).

This circumstance, by force of Ohm's law, allows for maintaining the voltage at the circuit section downstream of the Zener diode virtually at the same specified level regardless of input voltage value.

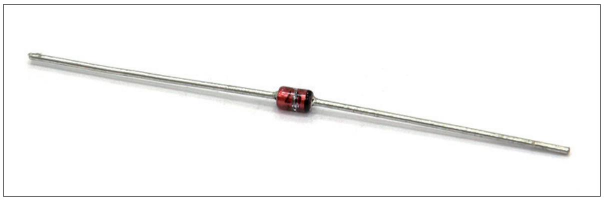


**Conventional designation of Zener diode on Russian and foreign circuit diagrams**

The main parameter of the Zener diode is the stabilized voltage (Ustab) — output voltage which the Zener diode tries to maintain. Another essential parameter is power determined by the consumption current of a specific circuit. Zener diodes are similar in appearance to rectifier diodes and differ only by marking.



**Using a Zener diode for output voltage stabilization**

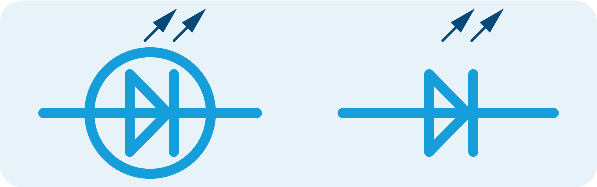


**Miniature Zener diode in a glass housing**

### 2.4.2. Light-emitting diode

The light-emitting diode is a diode converting current into light. As the conventional diode, it has unidirectional conductivity.

LEDs differ by rated forward current (it is usually 10-20 mA), by color, by housing type. Connection polarity is also important for the LED. In round diodes with two leads one lead is usually shorter and has an electrode inside the LED of a larger size (usually it is the cathode).



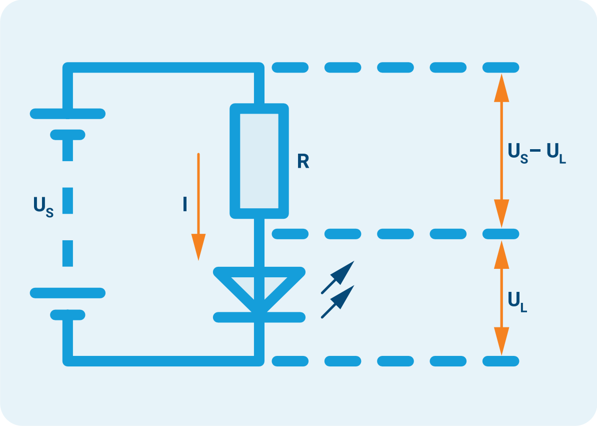
**Conventional designation of LED in circuit diagrams**

**Types of LEDs**

The standard characteristics of the LED are the maximum current and voltage drop. Let us designate these characteristics as **$I_L$** and **$U_L$** respectively.

According to Ohm's law:

$$R = \frac{U_S - U_L}{I}.$$



**LED connection diagram**

Thereat, some reliability margin of the LED should be available. The standard reliability factor is 0.75 — ratio of the actual (design) current, passing through the LED, to the maximum one (stated in the characteristics). The final formula is obtained with account of this correction:

$$R = \frac{U_S - U_L}{0{,}75 \times I}.$$

It should be also taken into consideration that resistor power (**P**) is sufficient for it not to burn out, i.e. not less than:

$$P = \frac{(U_S - U_L)^2}{R},$$

where measuring units are P — W, $U_S$ и $U_L$ — V, R — Ohm.

Having obtained the precise resistance and power values, one must select resistor ratings from the standard row — with upward rounding.

### What should you do if you have a LED but do not have its precise characteristics?

The majority of most popular LEDs have similar characteristics: voltage drop for yellow and red LEDs is 2-2.5 V; for blue, green, white ones — 3-3.8 V. The standard current of a low-power LED is 10-20 mA. By providing higher LED current than the rated value, we will burn it for sure, that's why the calculation should be made for the extreme case: vehicle power system voltage (Us) 14 V (typical value with the operating engine), voltage drop on the LED 2.5 V, consumption current 10 mA.

The required resistance will be

$$R = \frac{14{,}0\text{-}2{,}5}{0{,}75\text{x}0{,}01} \approx 1{,}5\ \text{kOhm},$$

while power will be

$$P = \frac{(14{,}0\text{-}2{,}5)^2}{1500} \approx 88\ \text{mW}$$

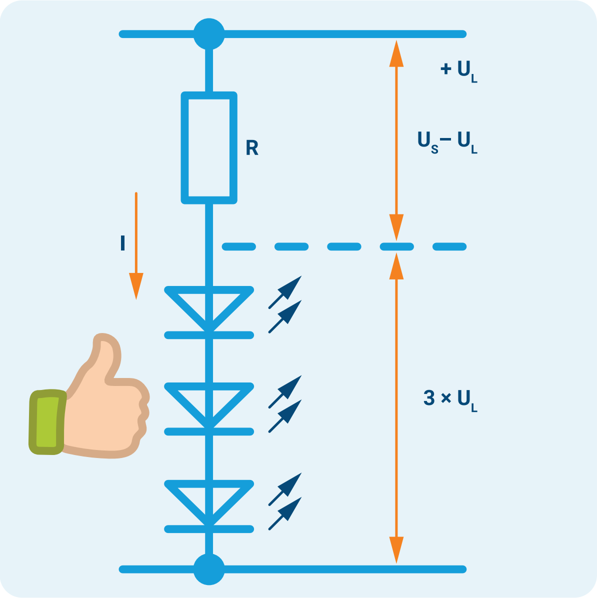
### What to do if you want to connect several LEDs?

Connecting several LEDs in parallel using one resistor is an **incorrect solution**. LEDs usually have a certain parameter spread, different voltage drop, that's why one of the diodes may glow brighter and take more current, which multiply accelerates the natural degradation of the LED crystal and eventually causes its failure. When you need to connect several LEDs, use a current-limiting resistor for each, or connect them in series.

In this case, formulas for calculating the current-limiting resistor are:

$$R = \frac{U_S - (U_{L1}+U_{L2}+U_{L3}+\ldots+U_{Ln})}{0{,}75 \times I},$$

where measuring units are R — Ohm, US, ULn — V, I — A;
n — number of LEDs.

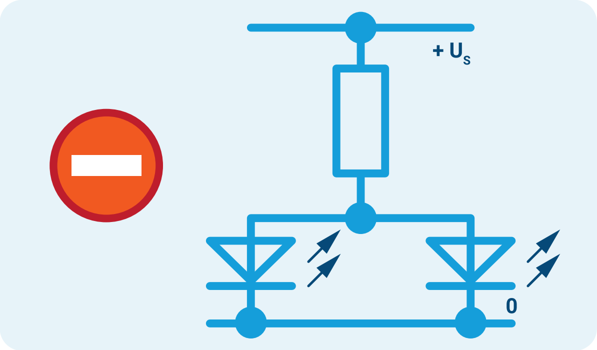


**Correct connection diagram of LEDs**

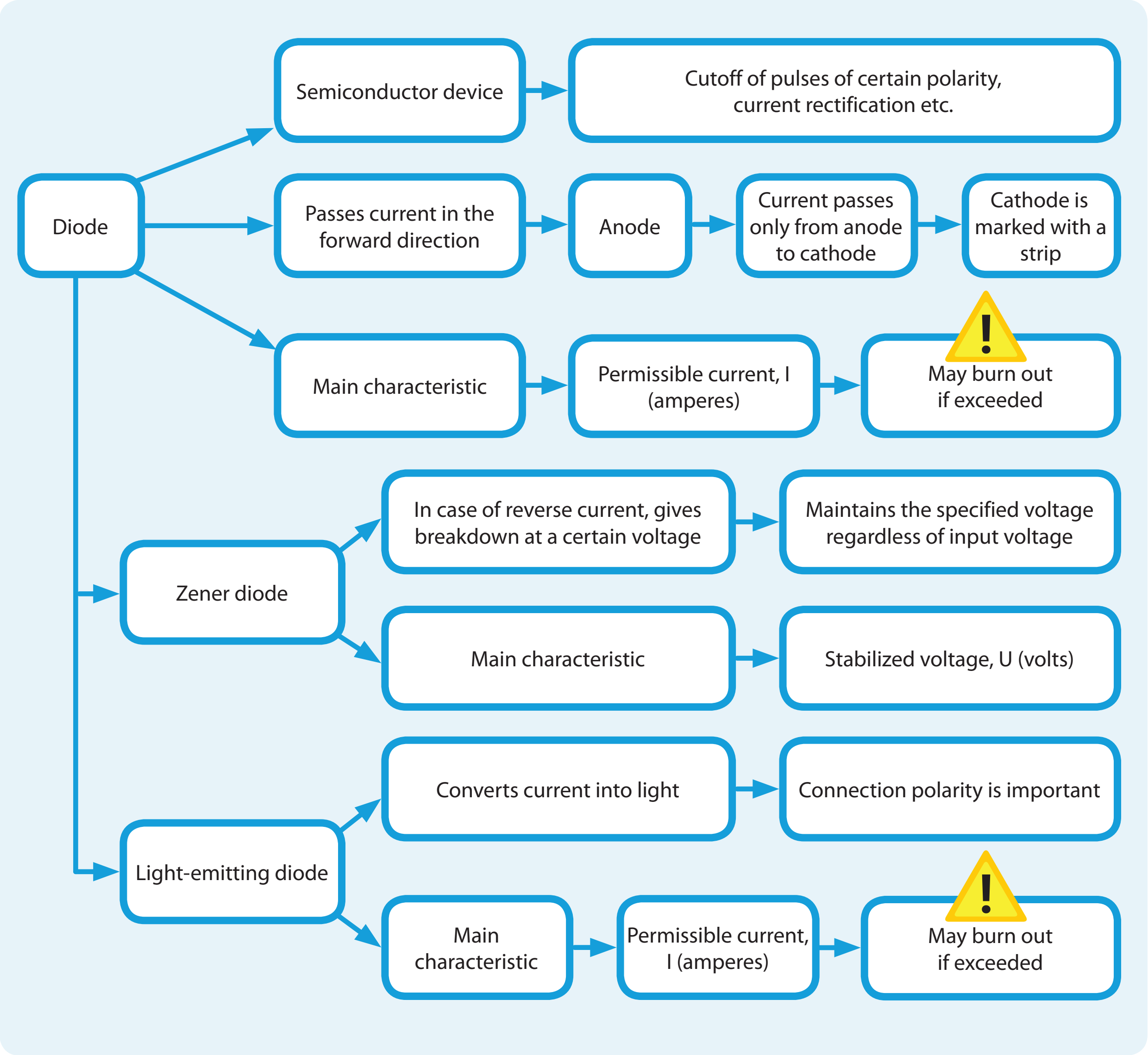
Resistor power shall be sufficient for it not to burn out, i.e. not less than:

$$P = \frac{2 \times (U_S - (U_{L1}+U_{L2}+U_{L3}+\ldots+U_{Ln}))}{R},$$

where measuring units are R — Ohm, US, ULn — V, P — W;
n — number of LEDs.



**Incorrect parallel connection diagram of LEDs**


Diode

Semiconductor device → Cutoff of pulses of certain polarity, current rectification etc.

Passes current in the forward direction → Anode → Current passes only from anode to cathode → Cathode is marked with a strip

Main characteristic → Permissible current, I (amperes) → May burn out if exceeded

Zener diode

In case of reverse current, gives breakdown at a certain voltage → Maintains the specified voltage regardless of input voltage

Main characteristic → Stabilized voltage, U (volts)

Light-emitting diode

Converts current into light → Connection polarity is important

Main characteristic → Permissible current, I (amperes) → May burn out if exceeded

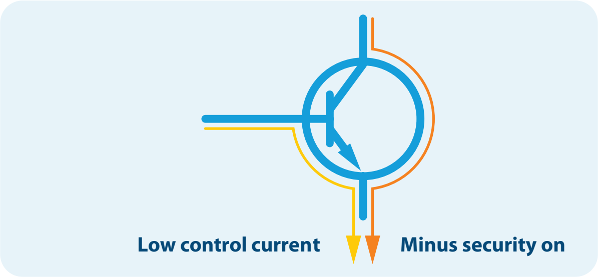
**Diode. Memo diagram**

Chapter 2.5

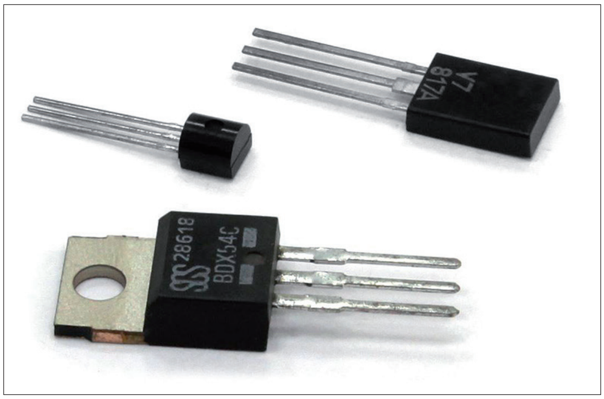
# Bipolar transistor

Transistor is a semiconductor device that allows for controlling high load currents by means of low control currents, thanks to which it can be used for signal amplification.

The transistor, as opposed to the diode, has three leads. Such leads in bipolar transistors are called the base, the emitter and the collector. The bipolar transistor consists of a semiconductor crystal (with alternating layers of conductivity of different types), a casing and metallic leads soldered in the electric circuit. Bipolar transistors are of two types — **n-p-n** and **p-n-p**.

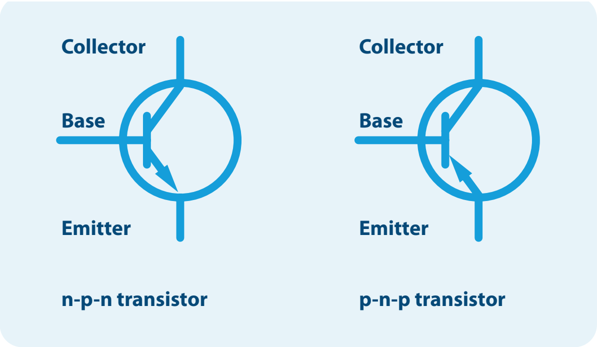


**The transistor controls large current by means of low one**



**Types of bipolar transistor package**

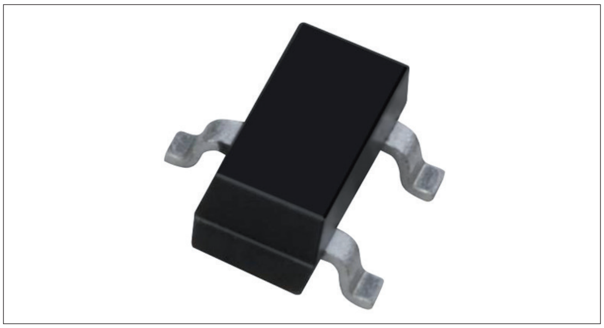
n-p-n transistors pass current from the collector to the emitter, p-n-p — vice versa. The main charge carriers in n-p-n transistors are electrons, while in p-n-p transistors — the so-called “holes” which are mobile (in terms of power transfer speed), accordingly, n-p-n transistors are switched over faster in the general case.



**Types of bipolar transistors**

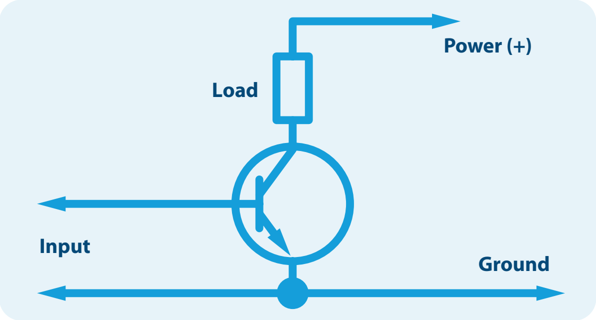
StarLine security systems use modern compact transistors intended for surface mounting (SMD-mounting).

The transistor displays its amplification properties in the main circuits of three kinds: common-emitter (CE), common-base (CB) and common-collector (CC).



**SMD-transistor**

In case of transistor connection according to the CE circuit, the input signal comes between the base and emitter, while the load is connected between the collector and power source. This circuit is the most widespread since it yields the largest power amplification (in thousand times).

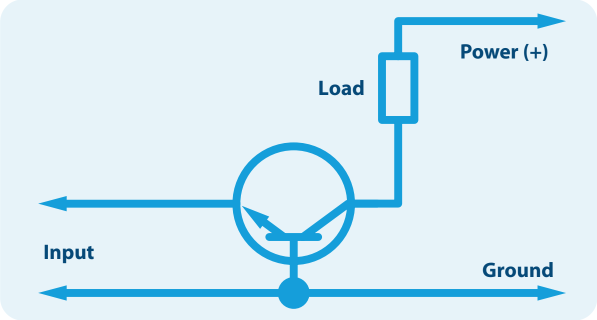


**Connection diagram for a bipolar common-emitter transistor**

The advantages of the common-emitter circuit are the large current amplification factor and input resistance larger than in a common-base circuit. Besides, power supply requires two unidirectional sources, i.e. one power source may suffice in practice.

The only serious disadvantage are worse temperature and frequency properties as compared to the common-base circuit.

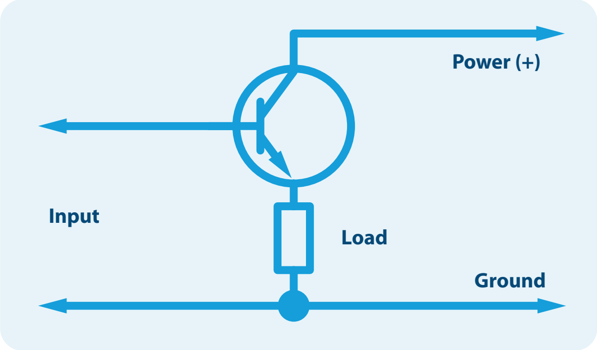
The input signal in the CB circuit is supplied to the emitter and base, while the load is connected between the collector and power source. The transistor input circuit is an open emitter junction, that's why input resistance is low (tens of ohms).



**Connection diagram layout for a bipolar common-base transistor**

Disadvantages of the circuit diagram: it does not amplify current and two different voltage sources are required for its power supply. But the common-base circuit has good temperature and frequency properties.

The input signal in the CC circuit comes to the "collector — base" junction, passes through the load, while the load itself is connected to the emitter and



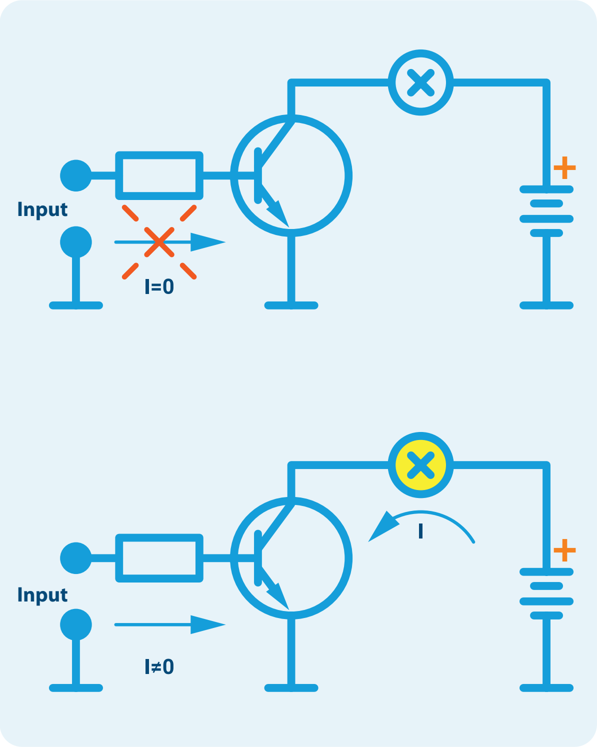
**Connection diagram for a bipolar common-collector transistor**

power source. Output voltage in this circuit is equal to the input one, that's why it was called an "emitter follower". When a common collector is connected, signal voltage is not amplified but only repeated. At that, emitter load can be very low, amplifier output resistance measures hundreds and even tens of ohms. At the same time, input resistance is very high — hundreds of kiloohms and even megaohms.

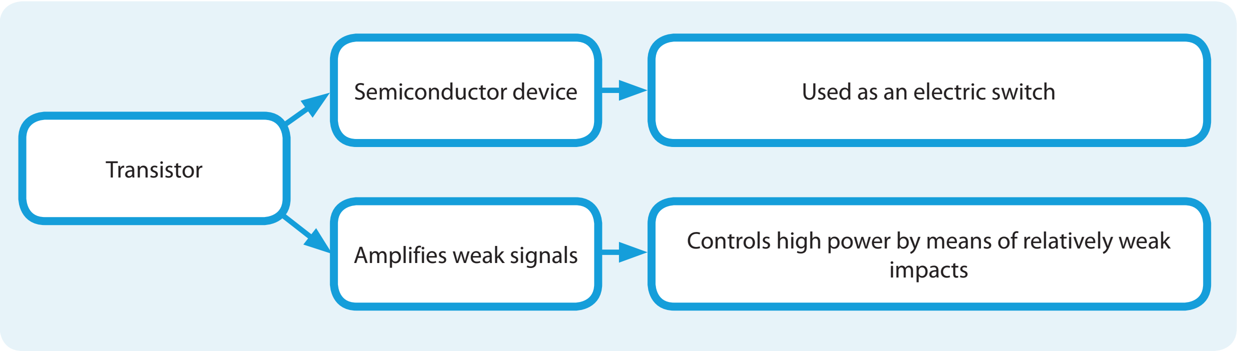
When mounting car security equipment, the bipolar **transistor is most often used as a switch**, which is either closed (does not conduct current or open (passes current).

Transistor unlocking or locking in the switch mode occurs at current supply to its base. For instance, the security system states: "the additional channel is built according to the "open collector" circuit". It means that the security system unit contains a bipolar transistor of n-p-n type, included according to the OE circuit. When this channel actuates, ground will appear on the output (via the transistor's conducting structure), while in the initial state the output is not connected with anything.

As a rule, outputs made according to the "open collector" circuit allow for a small load current (up to 300 mA). It means that a powerful load cannot be connected directly to this output — the security system switch will fail. An additional relay must be used for connection to such an output.



**Transistor operation as a switch**

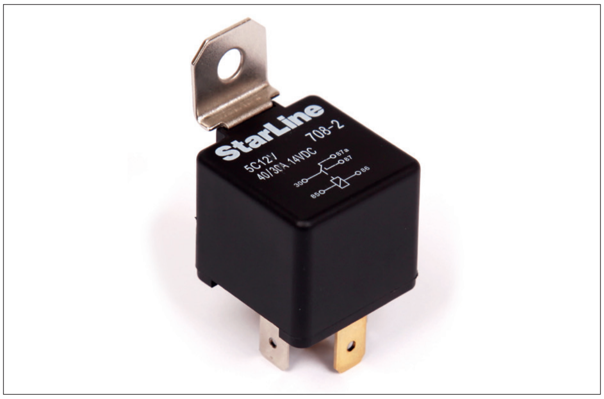

Semiconductor device
Used as an electric switch
Transistor
Amplifies weak signals
Controls high power by means of relatively weak impacts

**Transistor. Memo diagram**

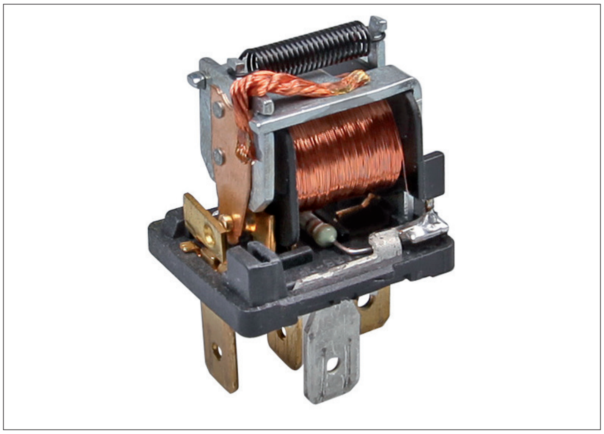
Chapter 2.6

# Relay

The relay is often used in security system installation.

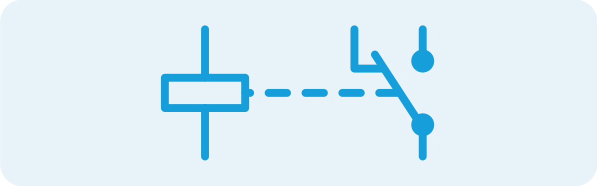


**Standard five-contact relay**



**Relay design**

**The relay consists of two main parts — a winding with core (electromagnet) and a group of contacts.** Both these parts are joined in one package. When voltage occurs on the winding, one of the relay contacts is attracted to the electromagnet and is closed with the other one. Simultaneously, opening with the third contact may occur.

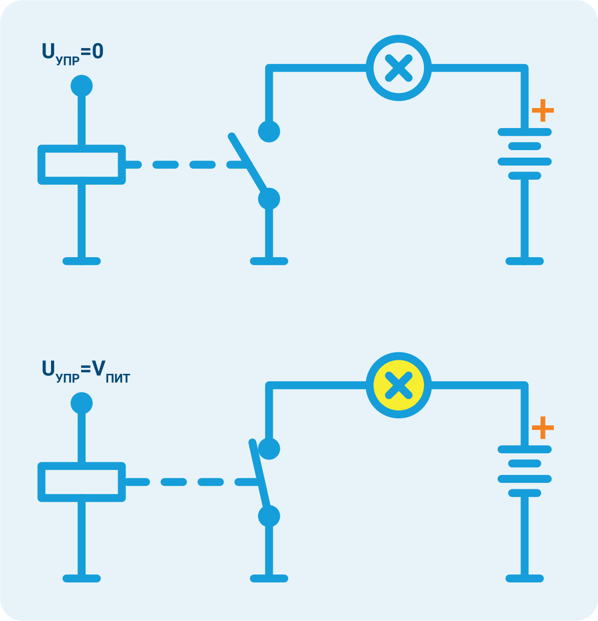


**Relay conventional designation**

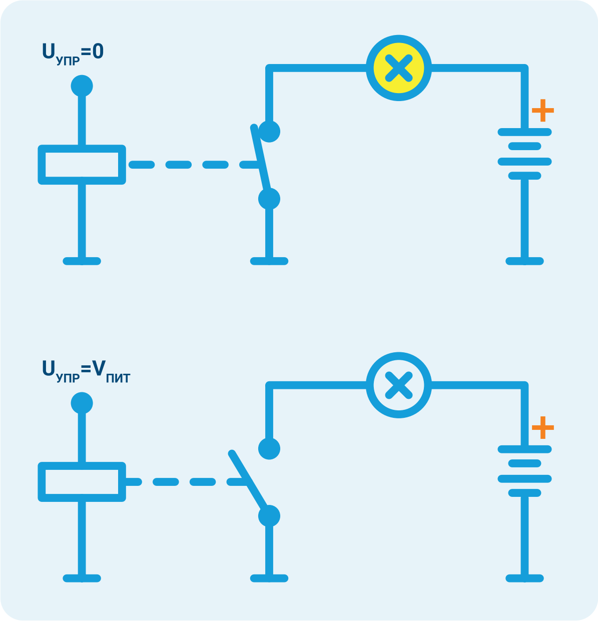
The relay on circuit diagram is usually designated in the form of these two parts. The dashed line shows a mechanical link between the winding and contacts. Relays can be subdivided into several groups according to type and number of contacts.

## 2.6.1. Normally-open relay

The output contacts are open in the initial condition, current does not pass through them. When the relay actuates, the contacts close and

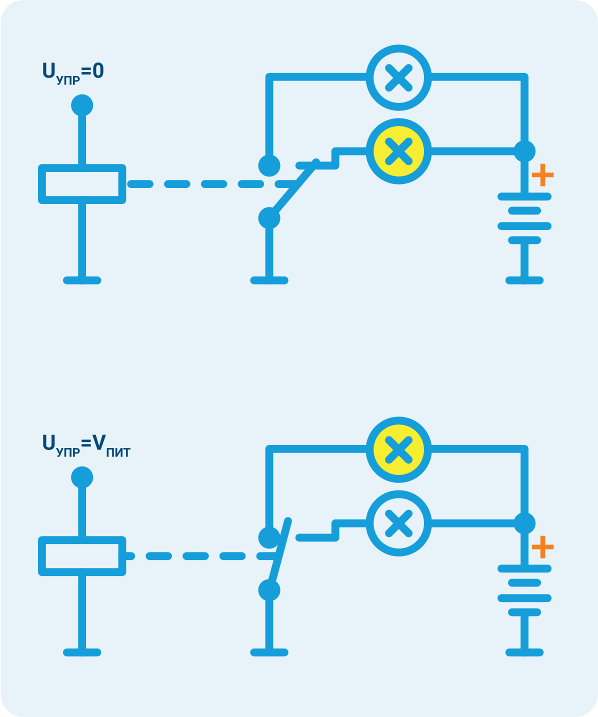


**Normally-open contact**



**Normally-closed contact**

electric current starts flowing in the circuit. This contact type is called NO (normally open).



**Change-over contact**

## 2.6.2. Normally-closed relay

Until the relay actuates, the output contacts are closed. Current passes freely through them, as through a conventional conductor. When the relay actuates, the contacts open, the circuit is broken, and the current stops flowing. The contact of this type is called NC (normally closed).

## 2.6.3. Relay with change-over contacts

One of the two circuits is closed in the initial state, upon relay actuation the first circuit is opened, while the second one is closed. This device has one common contact for two circuits, i.e. the circuits are not independent - CO (change-over).

For simultaneous control of several independent circuits there are relays not with one pair of contacts but two and more, e.g. DT (double-throw).

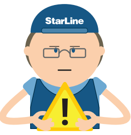
**Multicontact relay**

**Main parameters of the relay** that must be known for correct selection during security equipment installation:

1) permissible current which the relay may pass through its output contacts;
2) output contact type (normally-open, normally-closed, change-over), number of such contacts;
3) relay consumption current, actuation voltage;
4) dimensions (which is particularly important for hidden blocking).

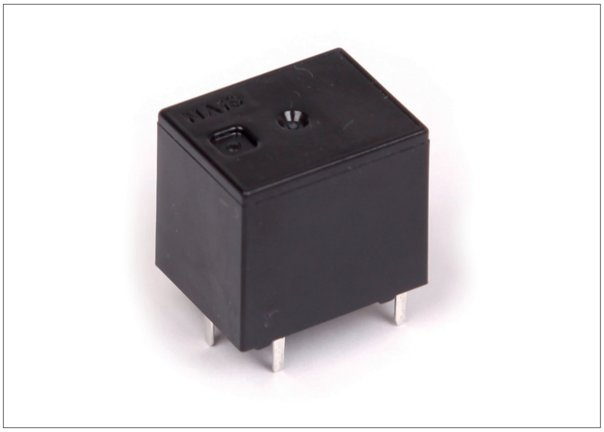
Let us deal with these parameters in greater detail.

**The permissible current** supplied to the contacts is determined both relay sizes and materials it is composed of. For instance, contacts in expensive relays are placed in a sealed capsule filled with inert gas. This allows for prevention of contact oxidation and increase of device reliability.



**You should select a relay of correct power, otherwise there is high risk of its failure at the most crucial moment and damage of car equipment.**

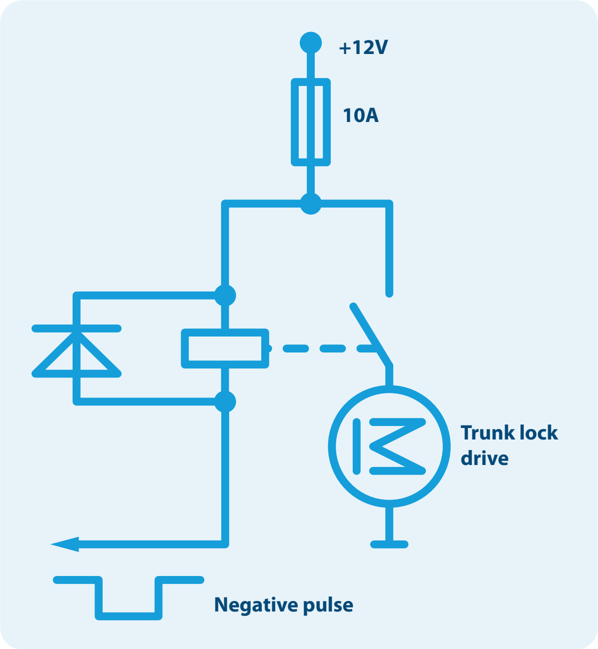
For instance, exceeding of the permissible switching currents may cause a short circuit, while exceeding of control currents may cause inflammation.



**Low-current relay**

**The output contact type** is determined based on which circuit and when exactly needs to be blocked. For instance, the trunk needs to be opened on command from the auxiliary output of the security system. The power of the auxiliary channel is not sufficient for its direct connection to the trunk activator. Therefore it is necessary to use a relay with a pair of normally open contacts, so that it closes the activator power circuit only upon appearance of a control pulse on the security system's auxiliary output. It will work as follows: the control signal is absent in the initial state, the relay is de-energized, the activator circuit is open. When a pulse appears, the relay closes the output contacts, current flows through the activator, and the lock opens.

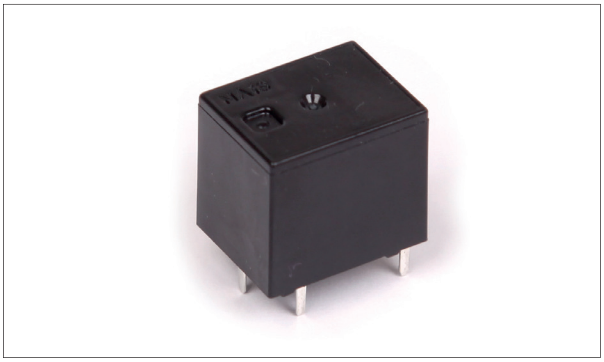
Consumption current is also important, because if the relay is incorrectly selected according to this parameter, the storage battery will be discharged within a short time. For instance, additional engine blocking during security system installation was provided by means of a conventional car four-contact relay. When arm is activated, it is switched on and opens some significant circuit (e.g. the gasoline pump wire). However, current will flow through the relay winding in case of such switch-on.



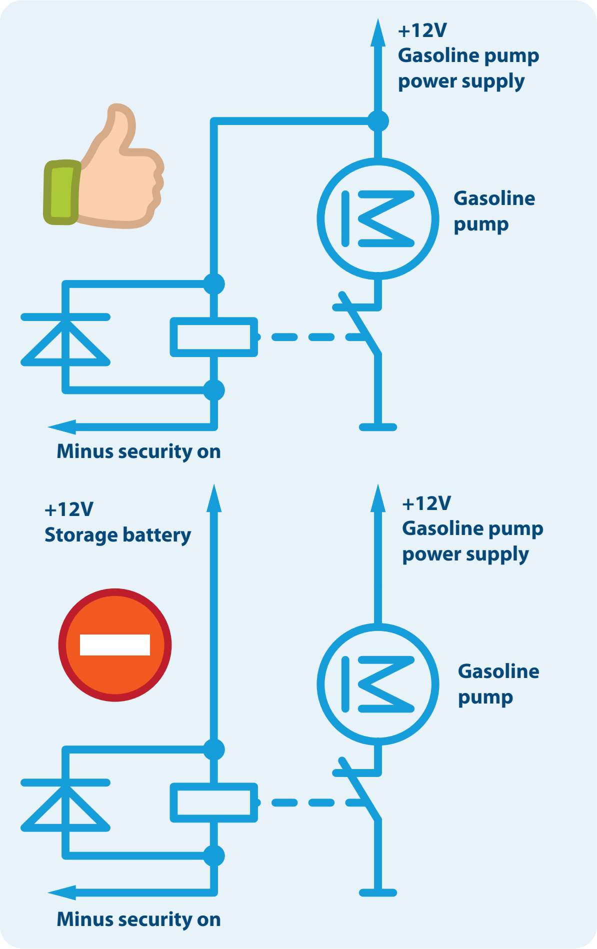
**Using an additional relay for trunk unlocking**

Despite the fact that it is low (approximately 0.05-0.1 A), two-three similar blockings may exhaust the whole energy of the storage battery within less than three weeks of downtime. In this case, another blocking circuit should be used: the relay will break the protected circuit only upon ignition switch-on.

Relays are subdivided into non-polarized and polarized ones. The former usually have considerable dimensions, consume larger current and may switch a high load.



**Non-polarized car relay**



**Blocking connection diagram**

For instance, a standard car non-polarized relay consumes current up to 0.1 A and switches current up to 40 A.

The polarized relay has two stable conditions. It consumes current only at the moment of switchover and switches current up to 10 A. Now polarized relays are rarely used, in most cases they can be replaced by microcircuits.

Upon actuation, self-induction current surges occur in the relay winding; they can be rather significant. To prevent them from causing

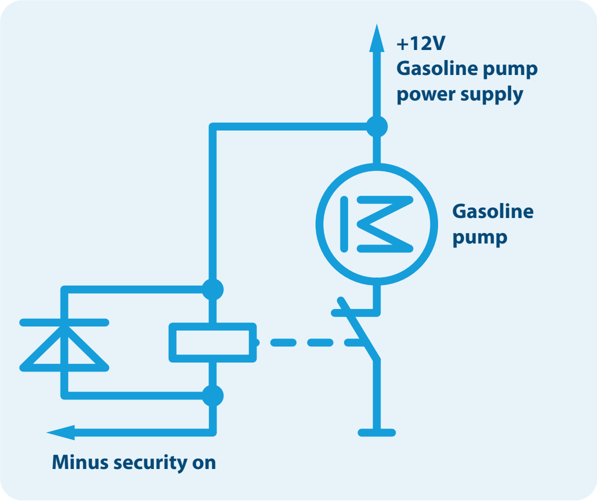
**it is strongly recommended to shunt the winding of any diode using a diode,**

security system malfunctions, i.e. to solder the rectifier diode between two contacts of the relay winding so that the diode anode is connected with the ground, while the cathode — with the contact where the plus occurs.

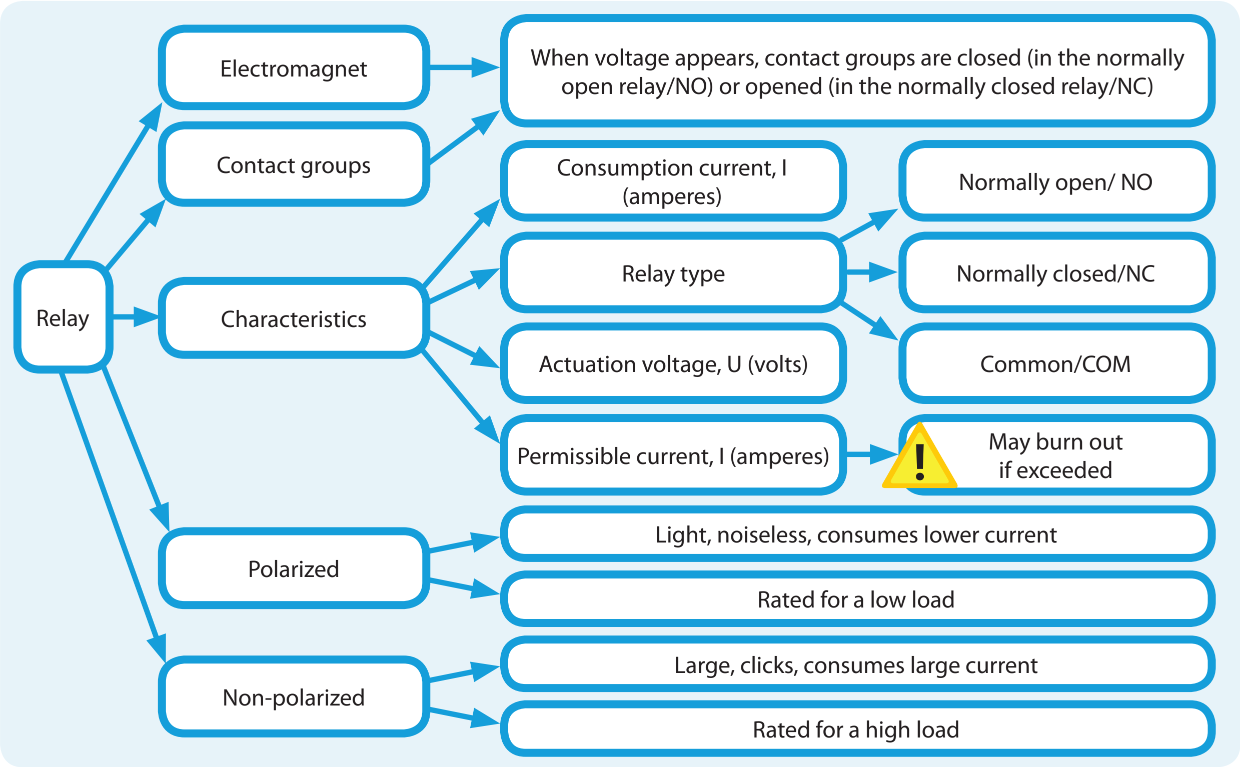
In this case the diode will not affect the control signal, because the diode resistance is very high at reverse voltage. When an induction surge occurs, all current will pass through the diode and will be suppressed by it.

## 2.6.4. Power switch

Given all the advantages of electromagnetic relays (cheapness, reliability, simplicity), they have their disadvantages. Exceeding of the maximum permissible switching current may cause sticking or burning of relay contacts, burnout of printed circuit board tracks. Moreover, switching current is directly related to relay sizes. That is, the higher the current, the larger the relay. And this directly influences the dimensions of the security system block. Clicks at relay actuation do not make security system installation more hidden.



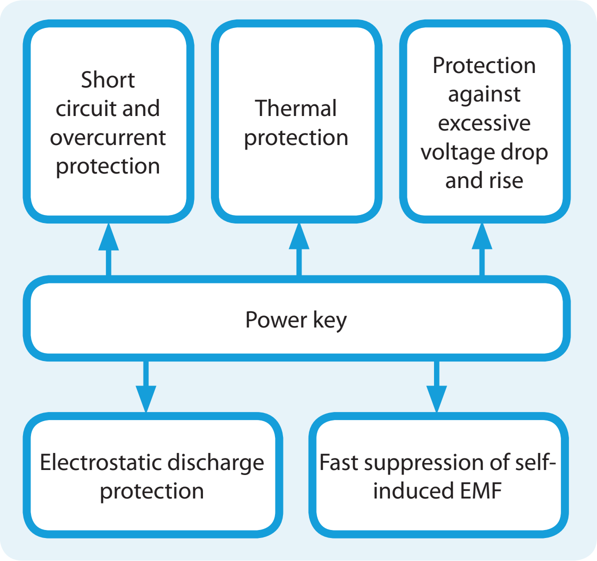
**Protective diode connection**


Relay
Electromagnet
Contact groups
Characteristics
Polarized
Non-polarized
When voltage appears, contact groups are closed (in the normally open relay/NO) or opened (in the normally closed relay/NC)
Consumption current, I (amperes)
Relay type
Actuation voltage, U (volts)
Permissible current, I (amperes)
Normally open/ NO
Normally closed/NC
Common/COM
May burn out if exceeded
Light, noiseless, consumes lower current
Rated for a low load
Large, clicks, consumes large current
Rated for a high load

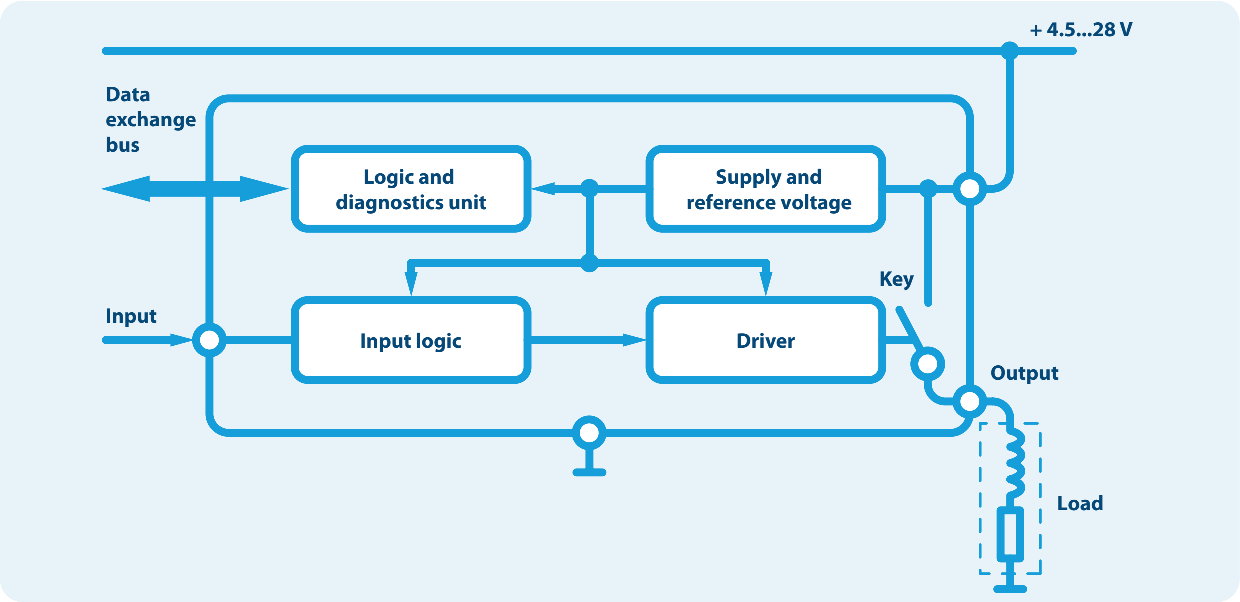
**Relay. Memo diagram**

Semiconductor power switches make it possible to eliminate the aforesaid problems. Let us consider the requirements to power keys operating in the car. Increased humidity and vibration, large spread of ambient air temperatures, possibility of wiring short circuits - all these factors condition the need for the power switch properties illustrated by the diagram.

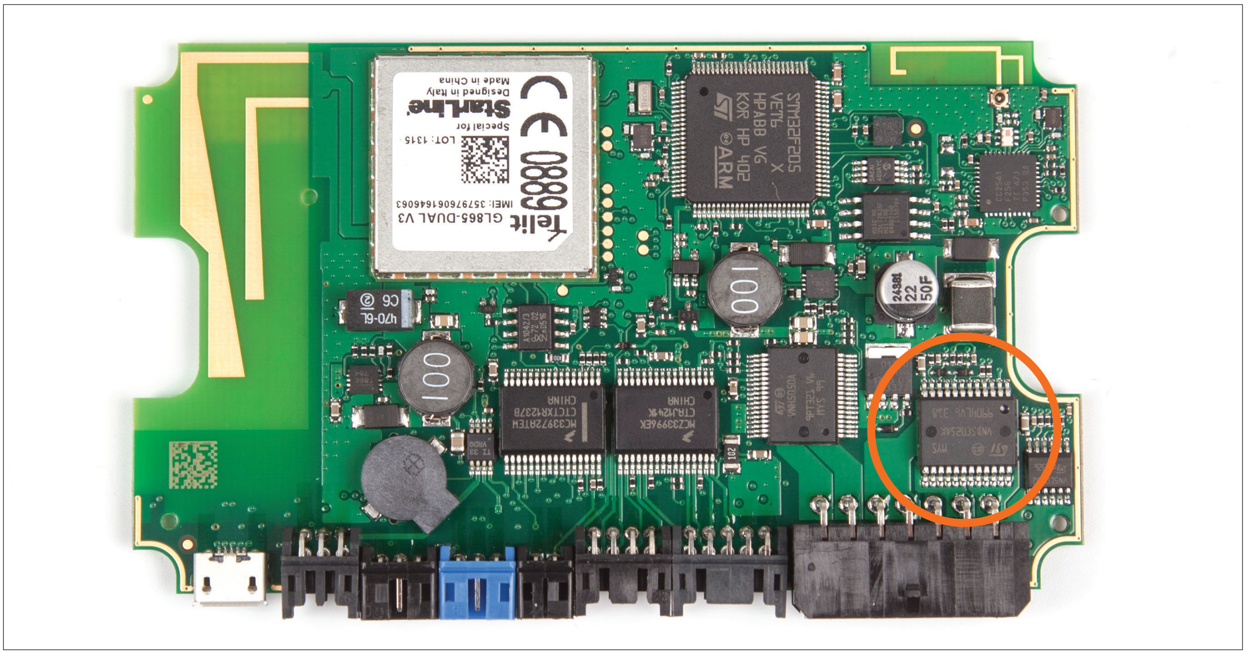
All the stated requirements are to the greatest extent met by the products of the worldwide leader in production of car electronics components — ST MicroElectronics Company. Thus, the microcircuits used in StarLine equipment have power switch with switching current up to 60 A and operating temperature of - 40...+ 150 °C.


Short circuit and overcurrent protection
Thermal protection
Protection against excessive voltage drop and rise
Power key
Electrostatic discharge protection
Fast suppression of self-induced EMF

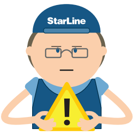
**Power switch structural diagram**



**Standard structural diagram of the smart switch**



**Power switch**



What do we obtain by using such smart electronics? Firstly, reduction of security system unit dimensions. Secondly, short circuit protection. Connection errors are possible during installation, and the car itself is apt to breakdown. It is enough to eliminate the failure and the switch is operable again.

Thirdly, the possibility to find out the cause of protection actuation.

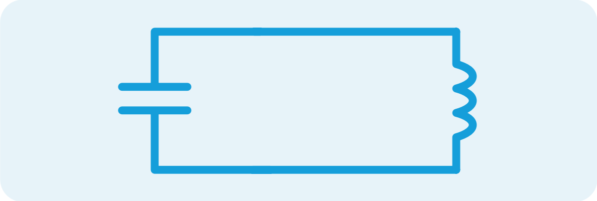
And by no means unimportant factor is the hidden installation of the main unit of the security system. Now it cannot be found according to clicking relays. The thinner unit is easier to hide.

Chapter 2.7

# Oscillating circuit

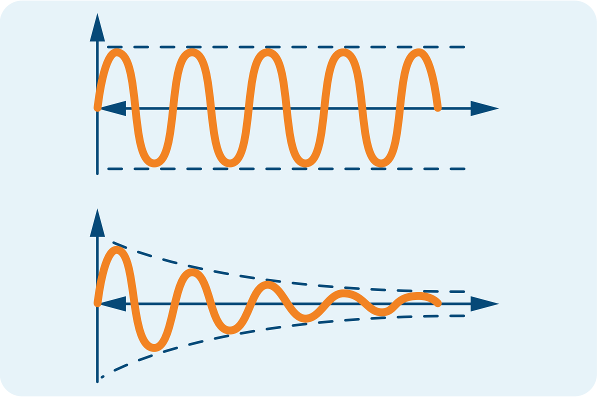
The complex name of "oscillating circuit" means only a combination of two elements — a capacitor and an inductance coil.

Nothing will occur if these elements are simply connected. However, if the capacity is preliminarily charged and the inductance coil is then connected, rather a curious process will start. The discharging capacitor will give the accumulated energy to the coil. When the capacitor has discharged, all the energy will be in the coil which will start giving it, again charging the capacitor. In the "coil — capacitor" system the so-called free oscillations occur; they have certain frequency dependent on capacitor capacitance and coil inductance. This charging-discharging process would continue infinitely long in ideal conditions, however, in reality the energy is consumed for heating of connecting wires, is dissipated in the form of spurious electromagnetic fields. Therefore, oscillations in a real oscillating circuit will be damping and will stop in some time.



**Oscillating circuit**

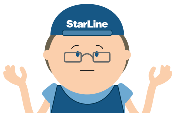
Electrical engineering mainly uses self-sustained oscillations that may last infinitely long. For this, damping in the oscillating circuit is compensated by outward energy.



**Self-sustained and damping oscillations in the circuit**

**What may be such an artful structure be needed in the security system for?**

Most security systems use a transceiver (for two-way communication systems it is available both in the car and in the remote control unit). Information is transmitted between them by means of electromagnetic waves. Well, oscillating circuits are used to create and receive such electromagnetic waves. One of them generates high-frequency oscillations. The second one is well-known to you — it is an antenna.

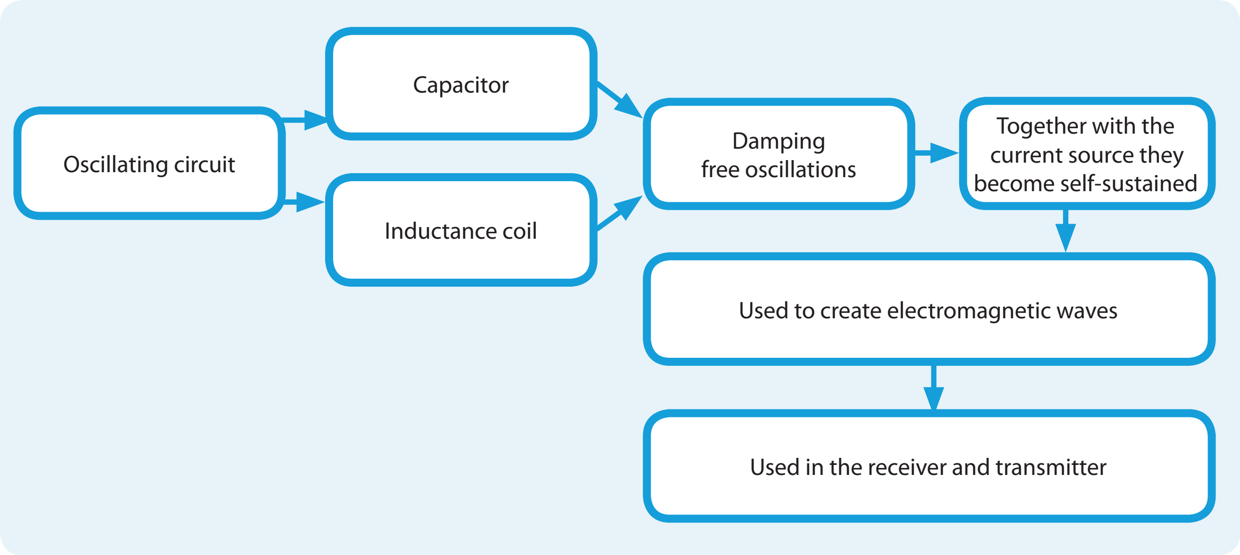


Yes, a piece of wire is also an oscillating circuit.

Its coil contains zero turns, while the surface area of capacitor sheets is equal to the wire cross-sectional area.

Antenna appearance can be different: a telescopic antenna (in the form of a pulling-out metallic rod), and wire section, and a simple track of certain dimensions and shape on a printed circuit board.

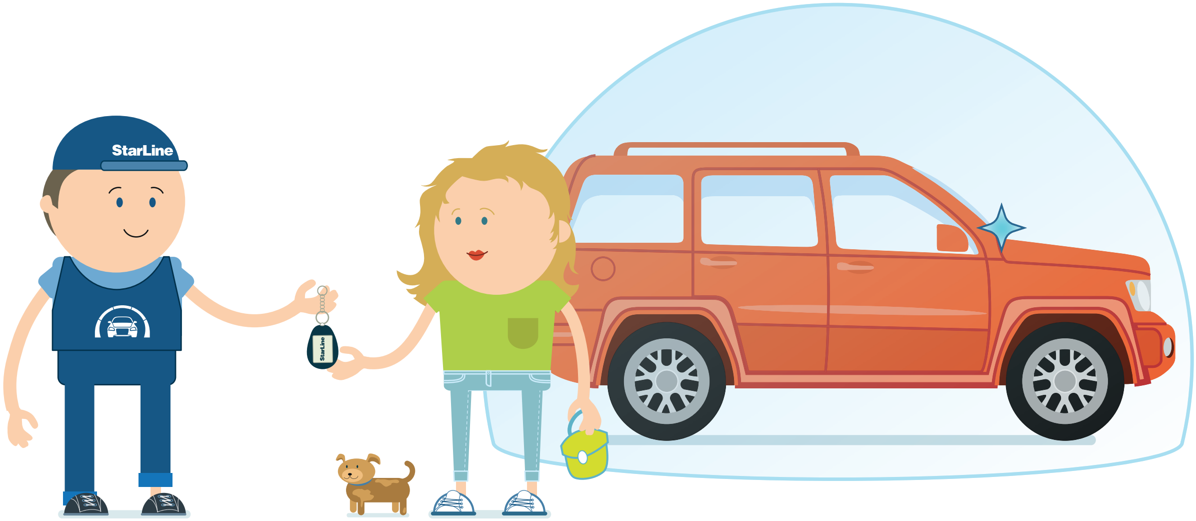
**Example of antenna built into the remote control unit**


Oscillating circuit
Capacitor
Inductance coil
Damping free oscillations
Together with the current source they become self-sustained
Used to create electromagnetic waves
Used in the receiver and transmitter

**Oscillating circuit. Memo diagram**

Part 3

# Structure of car security system



**Sloven's hint:**
**Have you ever installed an alarm system on a foreign car? You think you have already reached the acme of skill? Then skip this chapter, because it is for future professionals.**

***You will learn the following in this part of the book:***

**1)** *how to select components for the car security system and how they operate;*
**2)** *how to protect the car reliably;*
**3)** *what service functions can be provided by the car security system;*
**4)** *how to earn money and earn the reputation of a professional installer;*
**5)** *how to work less and earn more.*

## Chapter 3.1
# Security system functions

### What is the security system needed for?

**These are the three main reasons:**

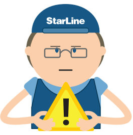
**1)** car theft protection;

**2)** security, i.e. prevention of unauthorized access to the passenger compartment, trunk and under the hood;

**3)** service in the form of additional functions;

**4)** cost-saving for the car owner thanks to discounts for comprehensive and collision car insurance and in case of smart insurance.

**Theft protection** presupposes engine blocking. **Alarm** presupposes a notification (alert) about a criminal attempt on the car by a horn signal, flashing of hazard lights, signal sending to the two-way communication remote control unit and the cellphone (if the GSM network is used).



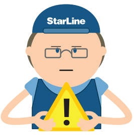
**A correctly installed and set security system "makes noise and flashes" only to the point!**

**Service** is a set of functions providing the car owner with additional comfort. They are the very ones your client might only dream about previously. They are automatic closing of windows and hatch at security arming, trunk opening by means of the security system remote control, and remote engine starting. The list can be continued — all depends on the security system's possibilities, as well as on your fantasy and skill.

So, the question "What is the security system needed for?" is answered as follows: "For the car — for its protection and security, for the owner — for psychological tranquility and comfort. He/she must be assured that his movable property is securely protected".

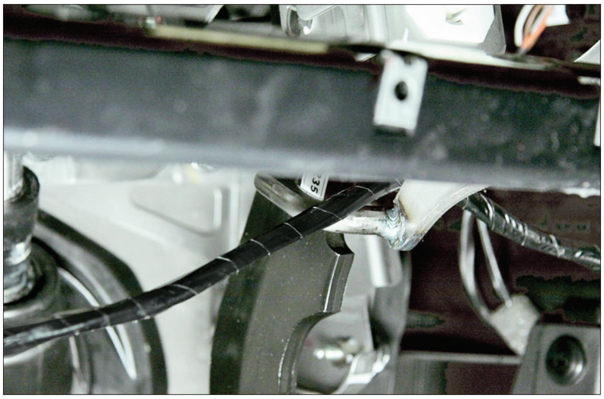
**Sloven's hint:**

**if you don't care much about driver's comfort, do simpler and faster. Nowadays, this will help to make easy money. You are not a psychoanalyst to care about client's "psychological tranquility".**



**Remember that all problems related to improper installation of security system always come back.**

And when the enraged client comes to the managers of your installation center, you'll learn and simple truth: **it is more profitable and safer to work properly at once**.



**Poor quality of security system installation: wires are not fastened**

One must not act so!

How does the security system fulfil its tasks?

### 3.1.1. Theft protection

When at attempt at car theft is made, the installed security system hinders the engine starting. This function was call "Engine blocking". It is also fulfilled by means of breaking the circuit controlling the engine operation. For this a circuit is chosen — from the ignition switch, common circuit of injectors, gasoline pump etc, — it is cur and its ends are connected to the kill-relay contacts. Moreover, various sensors can be blocked, e.g., CSPS (crankshaft position sensor), CmSPS (camshaft position sensor) etc.

### 3.1.2. Security functions

You surely know when the security system is activated and why the alarm signal is issued, but we will nevertheless remind you of the **basic principles** of its **activation** in the arm mode:

**1)** at opening of the doors, hood or trunk;
**2)** in case of an impact on the car body or wheels (in case of a severe impact, the alarm signal lasts for 30 seconds, in case of a weak one — a series of warning short sound and light signals is issued).

Other reasons of alarm signal actuation are possible if additional sensors are used, we will tell about it later. **The advantage of two-way communication systems** is the indication of all actuation reasons on the display of the remote control or your cellphone (if a GSM-interface integrated into the security system is available).

**Security system's reaction at opening of the door**

### 3.1.3. Service functions

**The functions** ensuring additional comfort during car use are called **service** functions, e.g.:
**1)** locking/unlocking of door locks at arming/disarming — simply speaking, remote control of the central lock;
**2)** automatic closing windows and hatch;
**3)** trunk opening be means of the system remote control in the arm mode;
**4)** automatic engine starting be the timer or temperature sensor.

**The number of service functions in StarLine security – telematic systems exceeds fifty.**

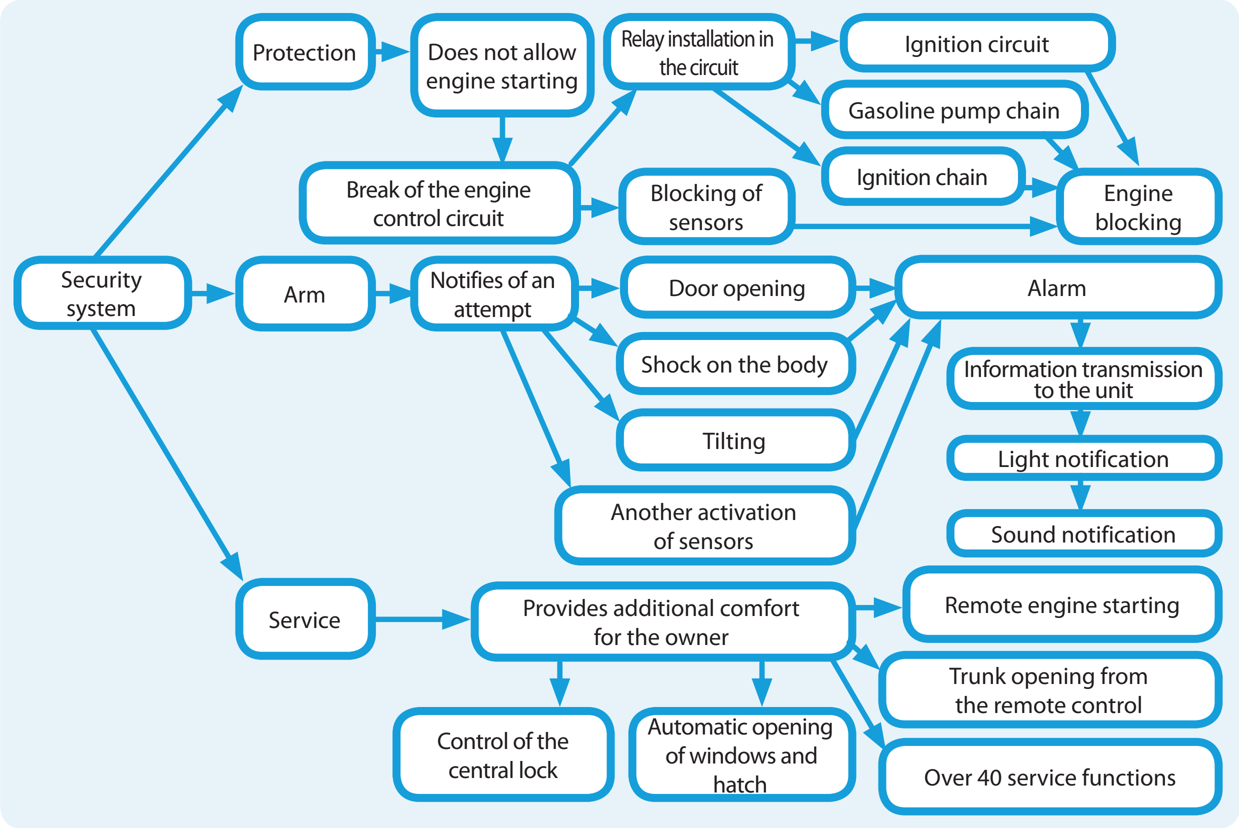
Auxiliary channels of the system are used to implement these functions. "Unconditional logic" of their operation often hinders or makes it impossible to connect to the car's actuation devices. One has to use additional modules or units, complicating the system installation and making it more expensive.

Do you want an example? Here is one for you. KIA Cee'd car of model year 2008. To implement the "comfort" function, the ground should be first supplied to one wire, and then to the second one, with a delay of about 1 second. Duration of these

**Trunk open with remote control**

**Automatic windows closing**

**Automatic engine start by temperature sensor**

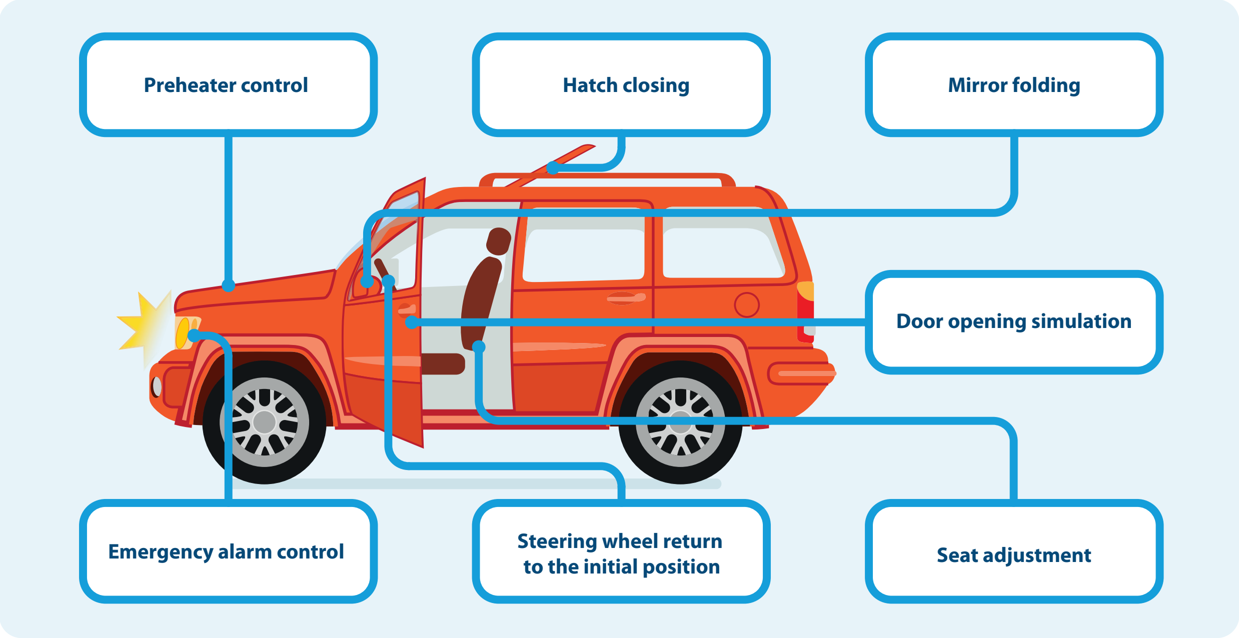

Security system
Protection
Does not allow engine starting
Relay installation in the circuit
Ignition circuit
Gasoline pump chain
Ignition chain
Engine blocking
Break of the engine control circuit
Blocking of sensors
Arm
Notifies of an attempt
Door opening
Alarm
Shock on the body
Information transmission to the unit
Tilting
Light notification
Another activation of sensors
Sound notification
Service
Provides additional comfort for the owner
Remote engine starting
Trunk opening from the remote control
Control of the central lock
Automatic opening of windows and hatch
Over 40 service functions

**Security system functions. Memo diagram**

signals shall be 10 seconds. How were windows closed in most cases? The first wire goes to the body, while the second one receives a signal from the auxiliary channel. And what's the result? Right, a discharged storage battery! The "comfort" unit remains always on — the wire connected by the careless installer to the ground is responsible for its switch-off.

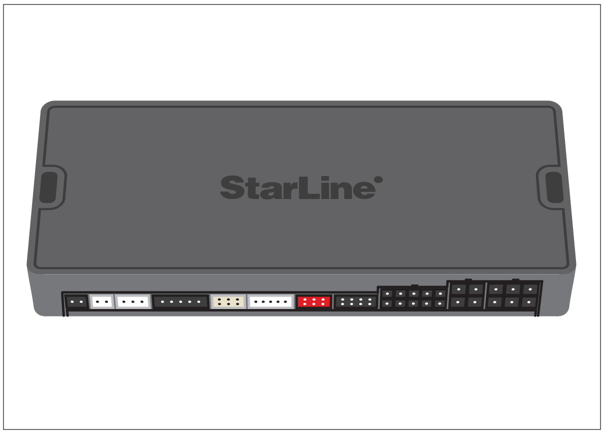
Now the auxiliary **FLEX** channels come to the rescue. How do they operate? Very simply! We assign an event and condition of enable/disable, duration and number of pulses. Let us try and program this together. We will need two auxiliary channels. The enable event for them is "arm activation", the condition is "none". Delay of the first channel in relation to the enable event is 0 seconds, of the second one — 1 second. Operation duration of the first channel is 11 seconds, of the second one — 10. Now let us make connections on the comfort control module. We use the first channel to activate the module itself, and the second one to give a command for window raising. It's ready!

And this is only the simplest case of reasonable use of flexible channels. And so many other examples can be given! Closing of the hatch, control of engine starting preheaters, simulation of driver's door opening upon completion of automatic engine start operation... Implementation of the automatic engine start itself often requires the disabling the wipers, car audio or vice versa, disabling the heating of seats, windows, mirrors. **FLEX** is simply indispensable in case of connection to "smart" ignition locks.



## Chapter 3.2
# Security system composition

The main **advantage of** the recent StarLine developments is the **reliable dialogue code,** protecting against smart hacking (interception of control signals at security deactivation) and the flexible architecture allowing for creation of several models, corresponding to car owner's needs, on one platform.



**Universal main unit of StarLine security system of generation 5**

The security system main unit (system's brain) processes the input signals, including from the remote control, as well as generates output signals. The security system is controlled only by its own remote control, the code whereof is recorded in the central unit memory. When the remote control signal is received, its appurtenance to the given system is checked: whether the remote control code is recorded in the main unit.

The remote control with the liquid-crystal display is the main one and is used for security system control, reception and indication of car state signals. The remote control indicator displays the reasons of security system activation, accompanied with sound and vibration signals. The remote control uses the cursor method for selection of some control commands, enhancing the convenience of security system use. The LED indication remote control is used a standby one — only for system control. The transceiver module ensures remote controls' communication with the

**Remote control with liquid-crystal display**

**LED indication remote control**

**Transceiver module of generation 6 StarLine with a built-in Valet button**

security system main unit. The same as the two-way communication remote control, the module has a receiver and a transmitter. The Valet button allows for calling the two-way remote control from the passenger compartment. Besides, the module board has a three-axis accelerometer, ensuring security system's sensitivity to shocks on the car body and to its tilting. Sensitivity of these sensors is adjusted remotely, using the two-way remote control.

## Additional accessories

**The LED indicator** indicates the security system operation modes. It is connected with the security system central unit by a twin wire.

**The Valet button** is used for programming of operation modes and signal parameters. It is also used for emergency disarming the security system. It is connected with the security system main unit by a twin wire.

**The limit switch** provides control on hood or trunk opening. It is most frequently installed on the car hood, if it does not have a standard limit switch. When the hood is opened, it closes the contact to the car ground.

**The temperature sensor** is used for automatic engine starting according to the specified temperature. Not all security systems have this function. This sensor is a thermoresistor whose resistance depends on engine temperature value

**LED indicator**

**Valet button**

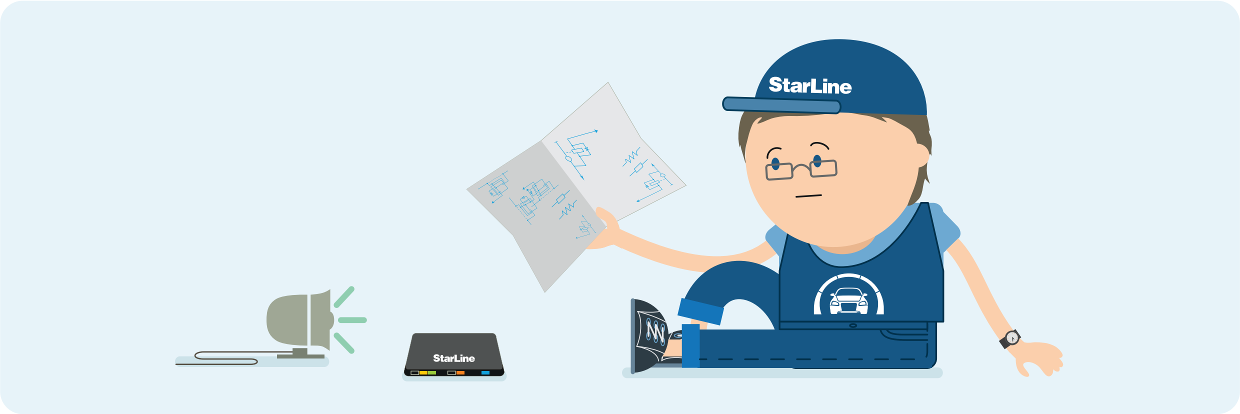
in the sensor installation point. The thermoresistor board is installed in the metallic terminal fastened on the engine housing.

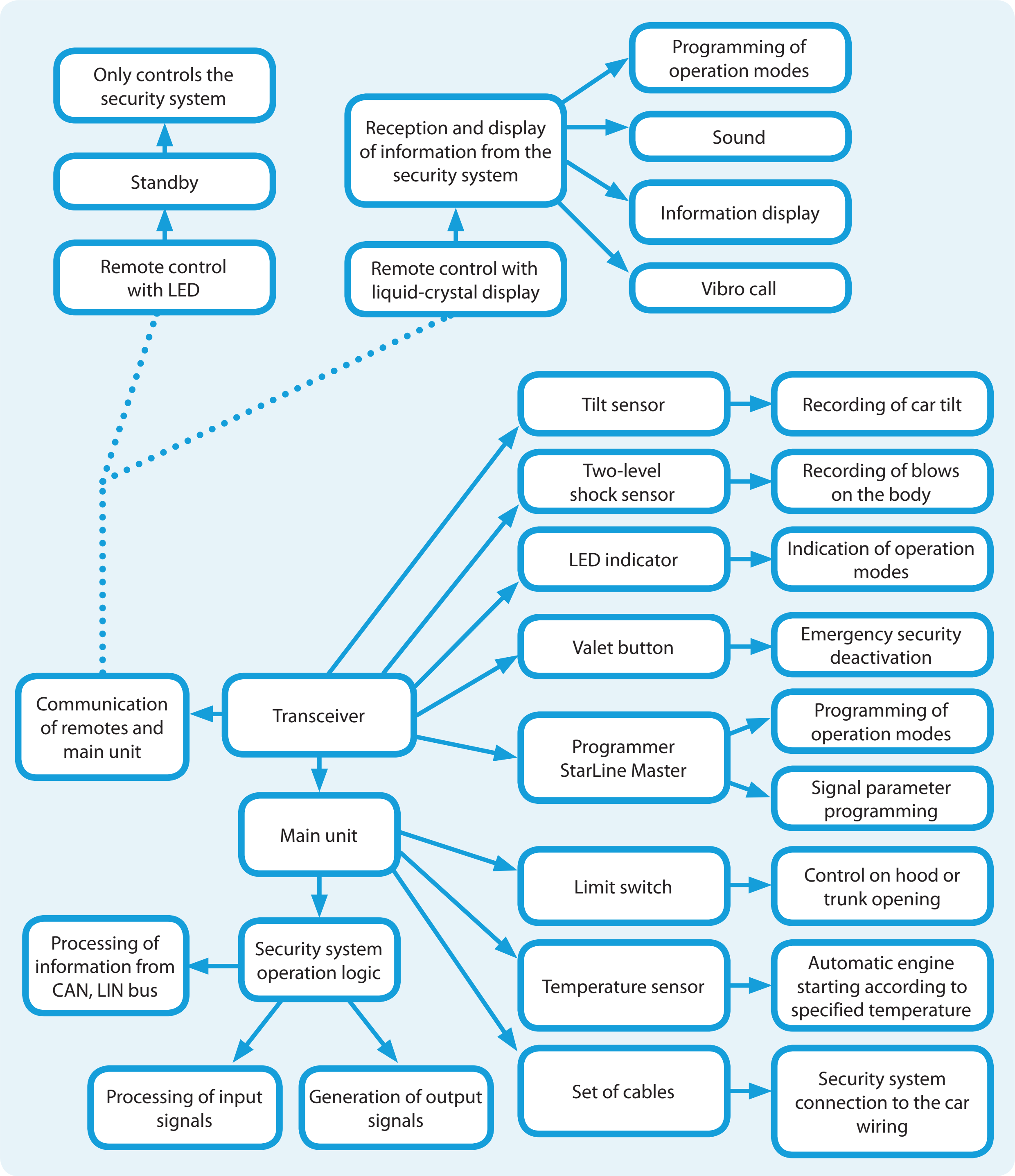
**The set of cables** is necessary for security system connection to the car wiring.

Temperature sensor

Limit switch

Main cable

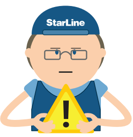



Only controls the security system
Standby
Remote control with LED
Reception and display of information from the security system
Remote control with liquid-crystal display
Programming of operation modes
Sound
Information display
Vibro call
Tilt sensor
Recording of car tilt
Two-level shock sensor
Recording of blows on the body
LED indicator
Indication of operation modes
Valet button
Emergency security deactivation
Communication of remotes and main unit
Transceiver
Programmer StarLine Master
Programming of operation modes
Signal parameter programming
Main unit
Limit switch
Control on hood or trunk opening
Processing of information from CAN, LIN bus
Security system operation logic
Temperature sensor
Automatic engine starting according to specified temperature
Processing of input signals
Generation of output signals
Set of cables
Security system connection to the car wiring

**Security system structure. Memo diagram**

Chapter 3.3

# Radio control of security systems



**A radio channel is used in modern security systems for command transmission from the remote control and reception of alarm messages.**

**The radio channel** has great **advantages** as compared to other communication methods:

**1)** communication is possible not only with direct visibility, but also in case of an obstacle, as well as at long distances;

**2)** data is transmitted via the radio channel noiselessly and unnoticed for surrounding people.

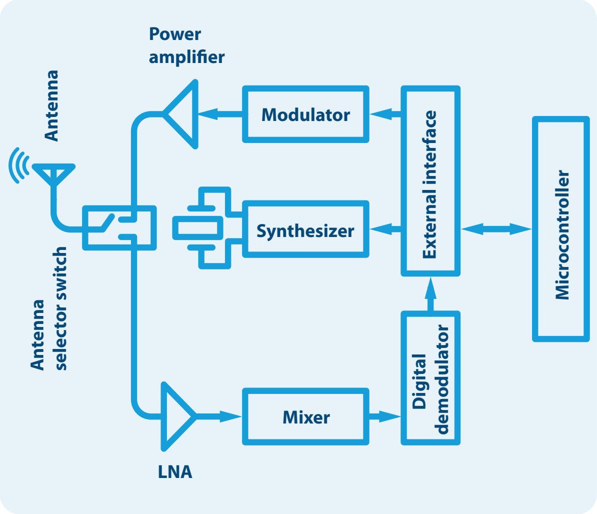
Along with that, using a receiver set for the required frequency, one may intercept the transmitted data. That's why it is usually encoded.

**Sloven's hint: install a car alarm with a static code for the client. It is much cheaper and opens locks in the same way! and the car thief will be grateful to you...**

Modern security systems use only the two-way radio channel, i.e. both the remote control and transceiver in the car may both transmit and receive data. Special microcircuits are used for this purpose — **transceivers**.

The structural diagram of digital transceiver in StarLine systems with a dialogue code is shown in the figure.

The transceiver's main element — the synthesizer — is a high-precision digitally controlled generator, responsible for exchange frequency and for the channel. The synthesizer is used for



**Structural diagram of digital transceiver**

reception and transmission, the frequency within the security system operation range is obtained at the synthesizer output. StarLine systems of generation 5 operate at frequency from 433.05 to 434.79 MHz, StarLine systems of generation 6 — at the frequency of 868 MHz.

Let us briefly **describe the transmitter and receiver operation algorithm:**

**1)** the transmitter receives the high-frequency signal from the synthesizer and modulates it by means of the digital modulator. Then the signal comes to the power amplifier, then to the antenna and is broadcast on the air;

**2)** the receiver amplifies the signal received via the antenna from the air by means of the low-noise amplifier (LNA), and sends it to the mixer. The mixer obtains an intermediate frequency by means of the synthesizer signal, and then the digital demodulator separates the useful information from the signal.

The transceiver microcircuit has an external interface allowing for its connection to the control microcontroller. It is this interface that provides the reception of data which will be then sent on the air or received from the air.

Most operations in the transceiver are performed digitally, which allows for increasing receiver sensitivity and, consequently, increasing communication range and reliability. This can be well illustrated by StarLine security systems with dialogue code.

Generally speaking, **communication range and stability** is affected by many parameters. The main of them are:

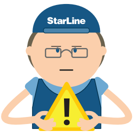
- transmitter power;
- receiver sensitivity;
- modulation type;
- communication channel width;
- number of communication channels;
- landscape.

### 3.3.1. Transmitter power

Remote control transmitter power is limited by battery capacity, while power of the transmitter in the transceiver, installed in the car, can be increased — the car storage battery has much larger capacity and can be recharged. Therefor the control channel has usually shorter range as compared to the annunciation channel.

### 3.3.2. Receiver sensitivity

Receiver sensitivity shows which power the signal must have in order to obtain a useful component at the demodulator output (in order to obtain a clear command from the transmitter from the air). The higher the sensitivity, the farther the transmitter can be placed, ensuring for the receiver a normal level of input signal. Receiver sensitivity is the transceiver's rating at certain conditions such as reception frequency, modulation kind and parameters, channel width etc. But sensitivity is heavily affected by the transceiver's own properties, therefore different microcircuits have different sensitivity with equal channel parameters.

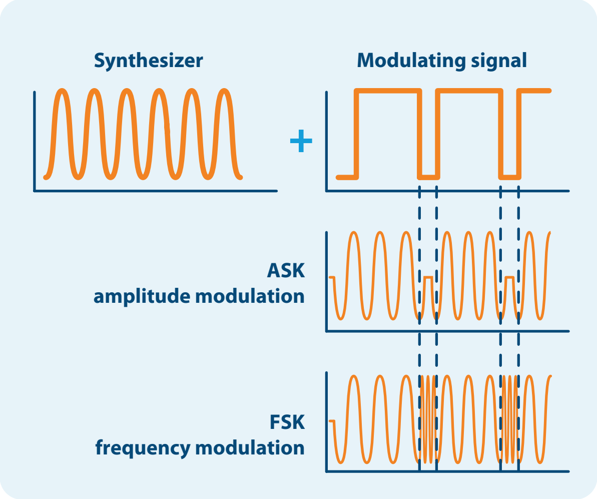


**Receiver sensitivity in the StarLine transceiver is one of the best in the industry.**

### 3.3.3. Modulation type

Modulation is a method to change the clear sine-wave synthesizer signal in order to transmit some useful information. The synthesizer signal changes synchronously with the data coming to the transmitter input. The reverse operation in the receiver (separation of useful data) is called demodulation. Modern security systems use two modulation kinds: amplitude (AM) or frequency modulation (FM).

In case of amplitude modulation, the synthesizer signal changes in amplitude (value). Since the digital data signal is a stream of binary symbols (0 and 1), the most convenient method of amplitude modulation is switch-on and switch-off of the high-frequency signal synchronously with the data signal.



**Amplitude and frequency modulation**

The advantages of amplitude modulation are the low energy consumption (when the signal is off, 0 is transmitter — current is not consumed), but there is also a shortcoming — the low efficiency of data transmission. That is, other conditions being equal, an amplitude-modulated transmitter shall have higher power to ensure the required range.

In case of frequency modulation, the synthesizer signal changes in frequency — when 0 is transmitted, signal frequency decreases, when 1 is transmitted — it increases. Frequency-modulated signals are less sensitive to impulse interference in the radio channel, that's why frequency-modulated systems are more reliable that amplitude-modulation systems.

AM is the first modulation kind mastered in practice, it is still used for long-wave radio communication. Receivers and transmitters using amplitude modulation are much simpler in manufacture and adjustment than, for instance, frequency-modulated receivers and transmitters. However, the market appearance of frequency-modulated single-chip transceivers has turned the tide.

### 3.3.4. Communication channel width

Communication channel width is the frequency range within which the radio signal is transmitted without significant distortion of its shape. Communication channel width affects the receiver sensitivity and, consequently, communication range and stability. The less the channel width, the higher the receiver sensitivity. It occurs because a narrow channel contains less over-the-air noise, which means that the "signal / noise" ratio will be higher.

It would seem enough to minimize the channel width! But it's not all that simple. Width of the channel determines the maximum data transmission rate. It means the narrower the channel, the lower the rate and the less data will find room in it (the same as noise). And the dialogue-based security system needs rather a high exchange rate, because much data is transmitted. Moreover, channel narrowing will require the use of more expensive components and, consequently, increasing the security system price. Modern systems have found an optimal solution with the least narrow communication channel at a

**Radioelectronic noise**

relatively high data exchange rate.

It should be noted that, other conditions being equal, frequency-modulated signals have a lesser channel width that amplitude-modulated systems. This is one more noticeable advantage of frequency modulation, which ensures better communication range and stability.

### 3.3.5. Communication channel protection

New models of StarLine security-telematic equipment uses a noise-like signal. What is this technology and what is it needed for?

Transmitted control commands of the security system are service information and shall be protected against interception/ listening in or suppression by way of jamming and be successfully delivered to the addressee under natural radio interference.

One of the methods to improve data transmission protection is the spectrum broadening method. Initially it was created for intelligence and military purposes. The main idea of the method is to distribute the information signal over the wide radio range band, which will eventually considerably complicate the signal suppression or interception. A variety of the broadening method is the "Direct Sequence Spread Spectrum (DSSS)" method.

This is a method for generation of a broadband radio signal, at which the initial binary signal is converted into a pseudorandom sequence used for carrier modulation.

Each transmitted information bit (logical 0 or 1) is transformed into a sequence of the so-called chips. The number of chips in the spreading sequence determines the factor of initial code extension. The higher the extension factor, the wider the spectrum of the resultant signal and the higher the interference suppression degree. But the spectrum range occupied by the channel extends at that. Extension factor value is usually from 4 to 100.

The first evident result of the use of this method is protection of transmitted information against listening in (the "alien" DSSS-receiver uses a different algorithm and will not be able to decode information not from its own transmitter).

Another most important property of DSSS-device is in the fact that, given the very low power level of their signal, they virtually cause no interference for conventional radio devices (narrow-band high-power ones), since the latter consider the broadband signal to be noise within the acceptable range. And vice versa — conventional devices do not interfere with broadband ones, since their high-power signal "make noise" only in their own narrow channel and cannot fully suppress the whole broadband signal.

StarLine security-telematic systems of generation 5 use DSSS modulation with the initial code extension factor of 8. DSSS is used only in some parcels of the dialogue code. Accordingly, the main purpose of DSSS modulation in systems of generation 5 is the hiding of data from interception.

### 3.3.6. Number of communication channels

Until recently, most security systems used only one fixed frequency from the range of 433.05 - 434.75 MHz, on which all security systems of one model operated. Such single-channel systems caused many troubles for their owners.

Imagine a situation when the alarm is activated on one of the hundreds of cars on a parking lot in front of a supermarket. It will start transmitting the alarm signal, occupying this frequency almost constantly. And owners of other cars will have to press the button several times in order to deactivate security of their cars.

New transceivers allow for arranging multichannel communication, since they have a digital synthesizer frequency whereof can be very easily tuned as distinct from amplitude-modulated systems.

A separate initial channel of data transmission is assigned to each system. The permitted range of 433.05 - 434.75 MHz may accommodated up to 1024 independent channels, therefore the frequencies are “smudged” over the air. The situation with simultaneous operation of several security systems in one channel is unlikely.

Besides, the channel number changes dynamically in the course of dialogue exchange, which allows for still more increased interference immunity of the system.

### 3.3.7. Landscape

External environment, terrain landscape, and city buildings very heavily affect the communication range. That’s exactly why open-space communication range is usually specified in the characteristics — in this case all security systems have similar test conditions and range is determined only by transceiver parameters.

**Do not promise to the client the maximum range of control and annunciation of the security system in a city where the characteristics depend on car’s and remote control’s location.**

Why does this characteristic decrease in city conditions? There are two reasons — obstacles in the way of radio waves way and multipath propagation. So, a radio wave cannot path through reinforced concrete constructions. It is partially absorbed and partially reflected. For instance, a high-rise building between the car and remote control may completely overlap the signal.

**Multipath propagation** is the effect of imposition of several waves on each other. They are reflected from houses, ground surface and reach the antenna with different delay. It may turn out that the sum wave is much smaller than in the absence of reflections, and then the receiver sensitivity will not be enough for stable communication. This effect is called “fading”. The multipath-propagation effect is very well noticeable if the car is on the parking lot in front of a large supermarket. As a rule, shopping mall hangars are built of materials which reflect radio waves well. Having penetrated through the “transparent” parts of the building, the wave is reflected many times inside, and the remote control receives a huge number of copies, the summation whereof may give a very weak signal. That’s why there is the problem of reliable reception of an alarm message inside a supermarket.

Multipath propagation is much more dangerous for amplitude-modulated signals. That’s why modern frequency-modulated transceivers in supermarkets and generally in the city operate more reliably and stably.

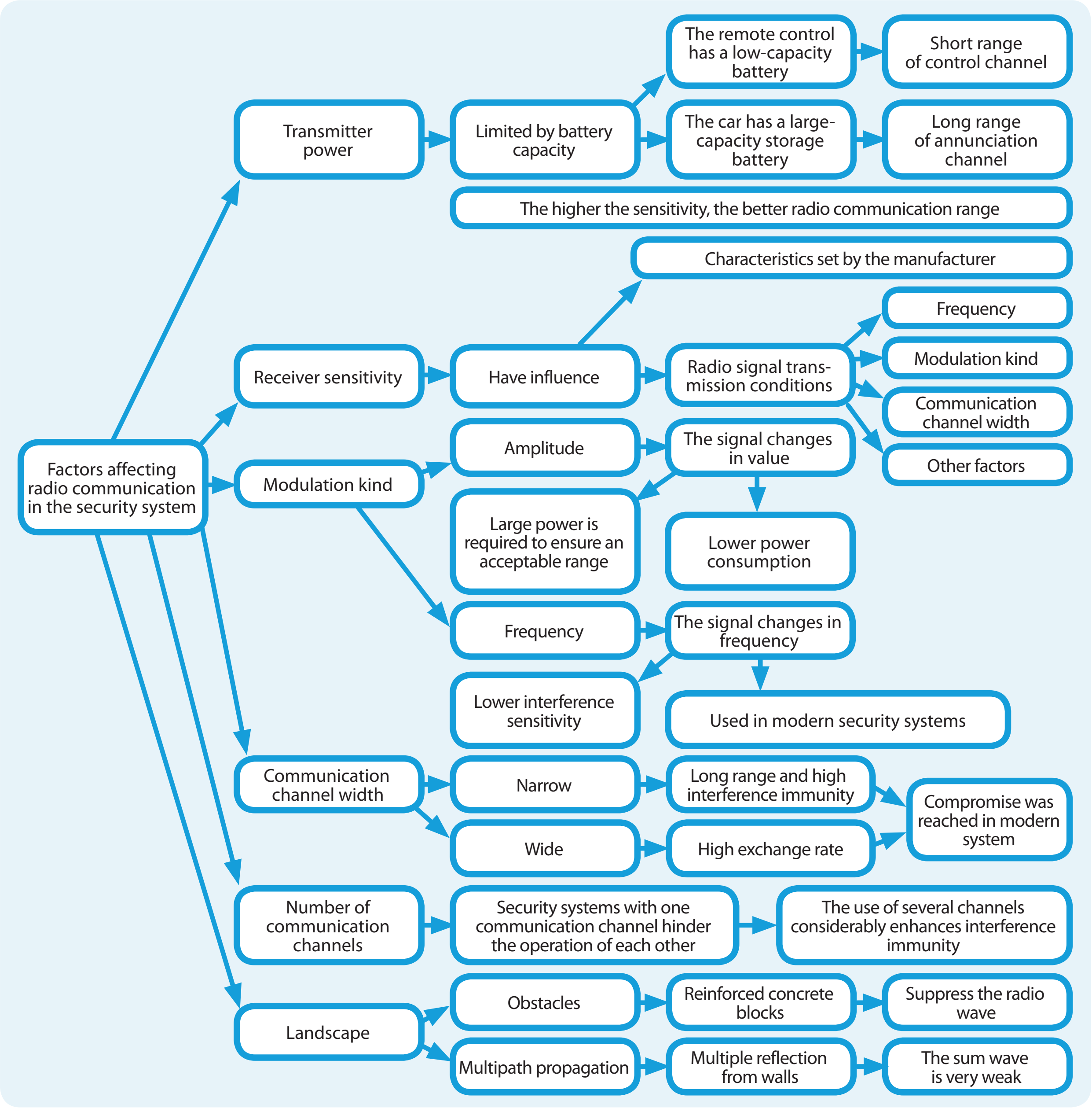
**In the end, let us formulate three items:**

**1)** the use of frequency modulation allowed for creation of a radio channel with greater range and reliability;

**2)** the large number of channels reduces the radio noise, which has a positive impact on communication range and stability;

**3)** the frequency-modulated radio channel better suits for use in the urban area.

Range of the control radio channel for StarLine equipment is 800 m, and that of the annunciation channel — 2,000 m.


Factors affecting radio communication in the security system
Transmitter power
Limited by battery capacity
The remote control has a low-capacity battery
Short range of control channel
The car has a large-capacity storage battery
Long range of annunciation channel
The higher the sensitivity, the better radio communication range
Receiver sensitivity
Have influence
Characteristics set by the manufacturer
Radio signal trans-mission conditions
Frequency
Modulation kind
Communication channel width
Other factors
Modulation kind
Amplitude
The signal changes in value
Large power is required to ensure an acceptable range
Lower power consumption
Frequency
The signal changes in frequency
Lower interference sensitivity
Used in modern security systems
Communication channel width
Narrow
Long range and high interference immunity
Wide
High exchange rate
Compromise was reached in modern system
Number of communication channels
Security systems with one communication channel hinder the operation of each other
The use of several channels considerably enhances interference immunity
Landscape
Obstacles
Reinforced concrete blocks
Suppress the radio wave
Multipath propagation
Multiple reflection from walls
The sum wave is very weak

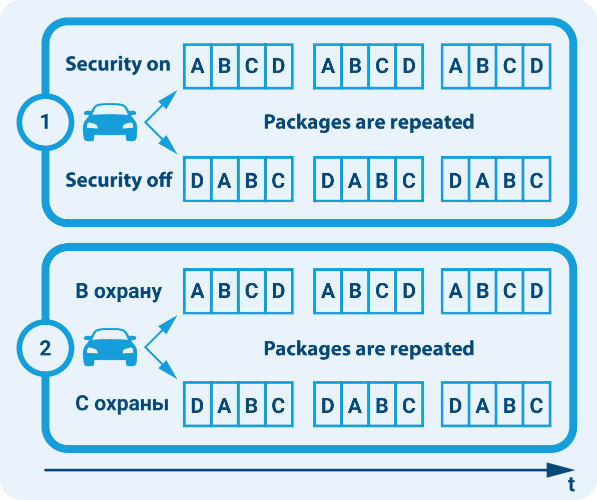
**Radio control of the security system. Memo diagram**

Chapter 3.4

# Encryption algorithms

The radio channel via which data is transmitted between the security system and remote control has one significant disadvantage — radio waves propagate not directionally, and data exchange can be listened to while staying not far from the car owner. Such communication channels are called unprotected and data transmitted on them is **encrypted**.

Data is transmitted via the radio channel in the form of small sequences — packages. Each package can be represented as a command (e.g. "Open the lock"), response to command ("Locks are open") or message ("Attention! Ignition is on! ")



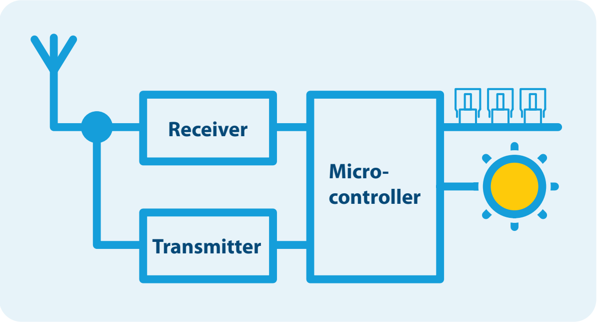
**Static code**

The first alarms with a radio channel had a static code — each command corresponded to its own command package. The package format was selected by the user (or installer), by switching over the sliders inside the remote control or soldering the jumpers.

Since there were few code variants, one's remote control could open another person's car with the same alarm — the package formats were the same. Of course, such coding did not provide any protection — it was enough to listen once to the package, corresponding to the "Disarm" command, in order to access the car later by simply repeating it.

Probably it was then that the first **code grabbers** appeared — technical devices intended for code interception, decoding and repetition. The final aim of the intruder who uses a code grabber is disarming of the "appealing" car and then theft from the passenger interior or car theft.

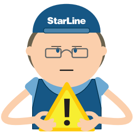
The code grabber structure is similar to the security system remote control layout. The code grabber has a receiver, transmitter, control microcontroller, buttons and indication means (LEDs or liquid-crystal display). Code grabbers are usually assembled as a kitchen-table effort, while the circuit is inserted in the alarm remote control



**Code grabber structure**

housing — it already has buttons and a transceiver with antenna.

The static code did not present a special problem even for the very first code grabbers, that's why soon all manufacturers switched over to dynamic coding.

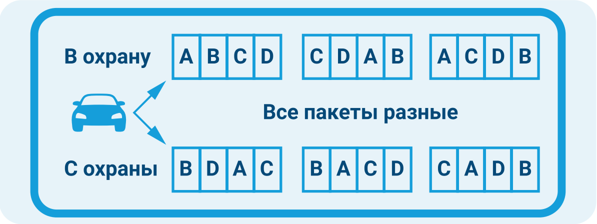


**Dynamic code differs from the static one in change of the package format at each pressing of the button.**

The regularity of these changes is set by the security system manufacturer and is unique for each "security system— remote control" pair. It means that the recorded package cannot be simply repeated — old packages are rejected by the security system.

In the beginning it seemed that the code grabber problem has been solved, but it was not to be!

Dynamic coding was unable to resist new inventions of car hackers. There are some myths about dynamic codes. Thus, the most famous dynamic coding algorithm is "Keeloq" developed in America by "Microchip" Company. There have been rumors of the hacking of "Keeloq" for a long time in the Internet, but it is not so in reality. Analytically, this algorithm is still intact and safe — its unsuccessful instances have been hacked. For instance, many car manufacturers go wrong in using the same key for all systems which allows for creating the so-called "manufactured" code grabbers.



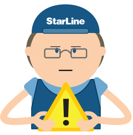
**Dynamic code**

**Dynamic coding can be hacked by several methods.**

The first method: **analytical.** It is based on "gaps" inadvertently or intentionally left in the algorithm by system developers. An example is given below — the same keys in standard security systems of some cars.

The second method: **code replacement**, a method that caused a stir in its time and made security equipment manufacturers separate the commands of security activation and deactivation to different remote control buttons. When this method is used, the code grabber records several parcels of the user's remote control, and then uses one of them for car security deactivation.

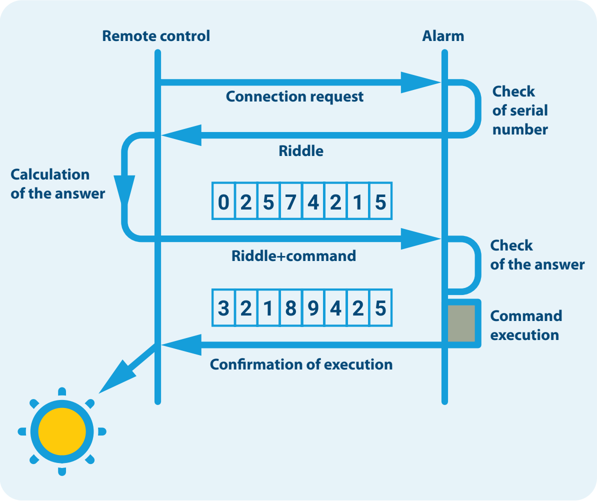
Many manufacturers of car security systems developed their own dynamic codes while making various improvements. Some of them have not been still hacked and apparently can be used in security systems. However, one should realized that **no dynamic code guarantees protection against hacking.**



The most cryptosecure and reliable is dialogue coding which requires a two-way communication channel, i.e. a receiver and transmitter both in the main module and in the remote control.

**The dialogue coding operation algorithm** can be conveniently explained by the example of personages from cryptography and coding manuals — Alice and Bob.

Imagine that Bob has locked himself up in the



**Dialogue code structure**

house and wants to let in nobody except Alice. The door has no peep-hole and the house has no windows. After Bob has heard the knocking on the door, he must check whether Alice is really behind the door. The best method is to ask a question to which only she knows the correct answer. If the person behind the door answers correctly, the door can be confidently opened. The **security system** with dialogue code **operates** in the same way:

1) when the button is pressed, the remote control sends a package with an authorization request ("knocks at the door");
2) the main module, having received it, contrives a "riddle" package, to which there is only one answer. The "riddle" is transmitted to the remote control via the radio channel;
3) the remote control, having "solved the riddle", responds with the confirmation package;
4) the main module checks the answer and, if it is correct, executes the remote control button (opens the door).

Now let us add another personage to our story — Eve, wanting very much to enter Bob's house. Under certain conditions she may eavesdrop the conversation between Bob and Alice and find out the answer to the Bob's riddle. That's why riddles must be different each time. In dialogue code the role of the riddle is played by a random number generated according to a special algorithm. "Random nature" of this number shall be very high.

Let us imagine that Bob's questions are dates of historical events. What will Eve do if she finds it out? Of course, she will buy a history textbook and will be able to penetrate the house after preparation.

Consequently, the process of "riddle solving" in dialogue coding shall **be unique for each "security system — remote control"** pair. **How can this be done? Very simply** — using an encryption key created during remote control assignment to the system. That is, Alice and Bob have to agree in advance the topic on which questions will be asked, and not disclose this to anyone.

Thus, the following shall be ensured to **implement the dialogue code**:

1) qualitative algorithm of random number ("riddle") generation;
2) a unique key for each security system;
3) key replacement in case of repeated remote control assignment to the security system;
4) sufficient length of unique key (protection against searching) — 128 bit.

Запрос
StarLine
Загадка-шифр
Ответ+команда

**Generalized view of dialogue code**

**If any one of these items is not observed — the code is not cryptosecure and can be hacked** by the intruder who has the firmware of the man module or remote control. One more important condition for dialogue coding implementation is a high-quality, **reliable and fast radio channel**, since even one pressing on the remote control button causes active package exchange. If even one of the packages is lost, the whole procedure will have to be repeated.

The Diffie-Hellman algorithm is used for safe assignment of devices (tag registration in the security system).

One of the fundamental cryptography problems is safe communication on a listened channel. Messages must be encrypted and decrypted, but both parties need a common key for that. If this key is transmitted via the same channel, the listening party will also receive it, and encryption will become pointless.

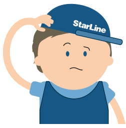
The Diffie-Hellman algorithm makes it possible for both parties to receive a common secret key using a channel unprotected against listening in. The received key can be used for message exchange using a dialogue code.

The dialogue coding operation algorithm can be conveniently explained by the example of already known personages — Alice and Bob.

Imagine that 2 persons who haven't ever met may perform an amazing trick.

Alice and Bob can exchange messages with one another. However, Eve also receives all the messages exchanged by Alice and Bob

The trick is that Alice and Bob can receive a unique common secret message (an encryption key for dialogue), which Eve cannot receive.



**How is this possible?**

Let us consider this by the example of colors. How can Alice and Bob choose a secret color so that Eve could not determine it? The trick is based on two facts:

1. It is very easy to mix 2 colors to obtain a new one.
2. Having a mixed color, it is very difficult to determine the 2 mixed colors.

This is the basis of the Diffie-Hellman algorithm — an operation simple in one direction and difficult — in the other. The solution is as follows:

1. First the public starting colors are chosen. For instance, yellow and white. They are known to everybody — Alice, Bob and Eve.
2. Alice and Bob each choose their own secret colors.
3. Alice and Bob mix their color with the public colors and send it to one another.
4. As a result, Alice has her own secret color and Bob's secret color mixed with the public keys. Similarly, Bob has his own secret color and Alice's secret color mixed with the public keys. Eve has both mixed colors from Alice and Bob.
5. Alice adds her secret color to the mixed color received from Bob. Bob adds his secret color to the mixed color received from Alice. As a result, Alice and Bob obtain the same color consisting of a mixture of public keys and their secret colors
6. Eve cannot obtain this secret color from the public colors and the two mixtures sent by Bob and Alice to each other.

And this is the trick's essence.

In order to do the same with figures, we need a function which is simple to calculate in one direction and difficult in the other. This problem is solved by the so-called discrete logarithm problem in the final field.

Safe data transmission between authorized devices (i.e. registered tag and security system) is ensured using the time-tested block encryption protocol with message authenticity code (MAC) and Counter Mode with Cipher Block Chaining — CCMP. It is used in the WPA2 protocol (for protection of WiFi-networks).

Why do we use an algorithm different from the "dialogue" used for transmission of control commands from the remote control? Bluetooth

Smart means that the connection is constantly maintained. That is, constant monitoring of communication availability is ensured. Data exchange is performed continuously, the tag confirms its nearby presence with a short period, while the central device checks its validity. With this approach, the intruder cannot pretend to be the tag and transmit false data.

The dialogue is suitable for control commands and requires 4 packages (for more detail about the Dialogue Code see page 67), but for constant monitoring the Dialogue is too cumbersome and causes large current consumption.

CCMP is adapted just for constant maintaining of communication with the specified period. A complex procedure of session key generation is performed for connection establishment, but thanks to this the maintaining of connection does not require transmission of large data volumes.

Low energy consumption is ensured by the following factors:

• The high data transmission rate of 1 Mbps (data is transmitted quickly and the receiver and transmitter are off most of the time).

• Scheduled communication establishment (the receiver and transmitter are off between scheduled sessions of communication establishment).

• CCMP-encryption allows for quick data transmission — as compared to the classic dialogue, 3 times less time is required to maintain the "online" status. Special GFSK-modulation with modulation index from 0.45 to 0.55 is used, reducing the peak consumption and allowing for operation from a small battery.

For instance, tags of StarLine security systems establish communication with security systems once a second and transmit the necessary data within tens of a millisecond.

Interference immunity is provided by the following methods:

The spread spectrum technology PROFR (pseudorandom operational frequency readjustment) is used — i.e. the frequency at which data is transmitted is constantly changing.

Frequency channels for connection establishing and maintaining are separated. Thus, devices searching a device to connect to do not hinder the operation of devices which have already established a connection. 3 frequency channel for connection establishment were allotted (annunciation channels), which do not coincide with the most loaded frequency ranges — with WiFi channels.

37 frequency channels are allocated for connection maintaining (data channels).

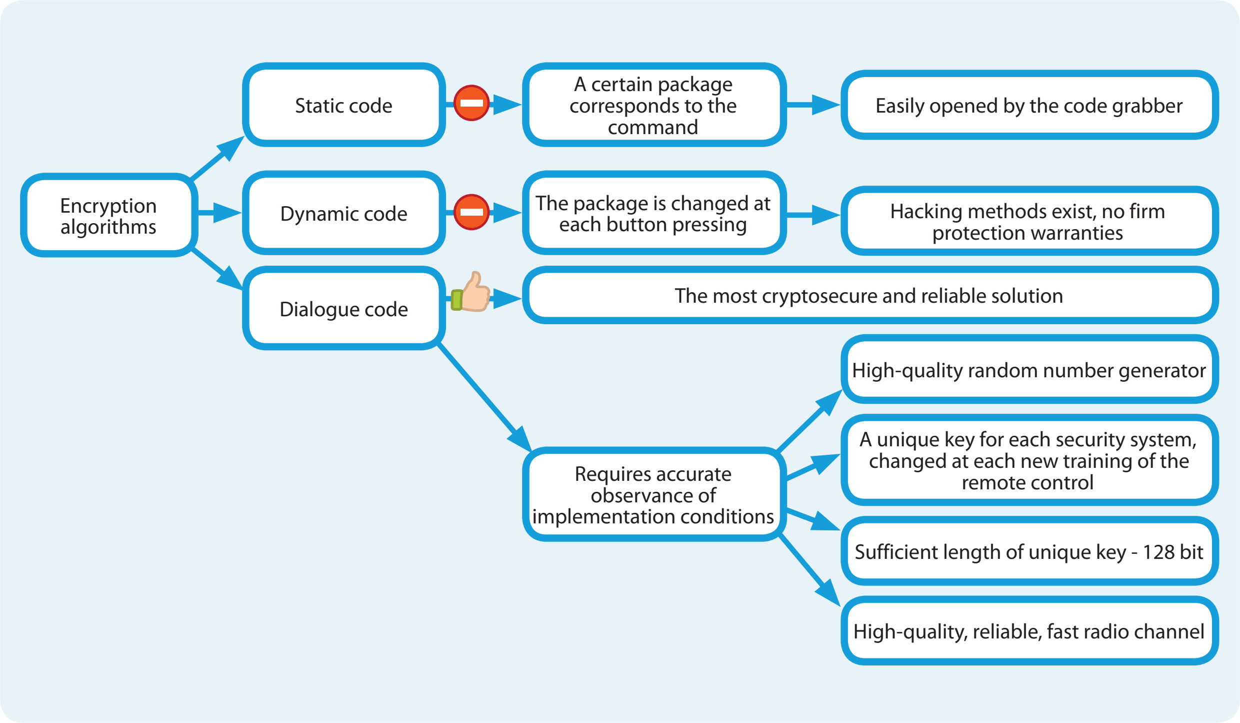
Also 37 PROFR channels ensure good protection against signal scanning. Each pair of Bluetooth Smart devices selects one of 1043 time-frequency matrices of signal coding (i.e. sequences of data transmission on different channels), without knowing which the intruder cannot separate the necessary signal from the air. The same reasons considerably complicate the task of radio signal relaying.

StarLine security systems with dialogue code use a modern radio channel built on a single-chip transceiver. It allows for quick and precise dialogue exchange, while encryption keys, individual for each system, reliably protect against hacking.

We should sum up: **real protection against code grabbers can be only a dialogue code with individual encryption keys**. Old alarm systems with dynamic code are not resistant to hacking.

**Do you know the arrangement of recognition systems in military aviation?**

The friend-or-foe system is used there. If the airborne responder responds incorrectly to a ground request, the aircraft is immediately shot down! Suggest the client to install a recognition system as on aircraft!


Encryption algorithms
Static code
A certain package corresponds to the command
Easily opened by the code grabber
Dynamic code
The package is changed at each button pressing
Hacking methods exist, no firm protection warranties
Dialogue code
The most cryptosecure and reliable solution
Requires accurate observance of implementation conditions
High-quality random number generator
A unique key for each security system, changed at each new training of the remote control
Sufficient length of unique key - 128 bit
High-quality, reliable, fast radio channel

**Encryption algorithms. Memo diagram**

Chapter 3.5

# Security system operation modes

**The security system can be in one of the operation modes:**

**1)** arm;
**2)** disarm;
**3)** alarm;
**4)** panic;
**5)** valet;
**6)** programming mode;
**7)** SLAVE mode;
**8)** engine protection mode;
**9)** car search;
**10)** anti-hijack;
**11)** immobilizer mode;
**12)** no-remote control mode;
**13)** noiseless security.

## 3.5.1. "Arm" mode

When the security activation button is pressed on the remote control, **the security system performs the following actions:**

**1)** the radio signal sent by the remote control is received by the security system and recognized according to the "friend or foe" principle;
**2)** if the remote control is a "friend", the security system checks the inputs: closing of doors, ignition switch-off;
**3)** if there are no signals at the security system inputs, car security is armed: the door locks are locked, command execution is confirmed by light and sound signals (StarLine systems output single signals);
**4)** if some input is activated at the moment of security activation (e.g. the door is not closed), the security system will still enable the arm mode but will warn about the zone, excluded from security, by additional sound signals;
**5)** "arm" mode activation is accompanied with uniform flashing of the system LED located in the car.

## 3.5.2. "Alarm" mode

Warning and alarm signals can be issued upon sensor activation.

The warning signal consists of several short horn signals and light flashes. For instance, StarLine security systems have three sound signals and four flashes.

The alarm signal is generated in the form of a long horn signal and light flashes. Most systems have an alarm signal about 30 seconds long, repeated in cycles 5-7 times.

### 3.5.3. “Disarm” mode

Disarming security by pressing the disarm button on the remote control. **The security system performs the following actions:**

**1)** the main unit, having received the remote control signal, checks its appurtenance to this security system;

**2)** if the remote control is a “friend”, the security system executes the disarm mode, opens the door locks and issues sound and light signals confirming the command execution.

### 3.5.4. “Panic” mode

It is similar to the “alarm” mode, but is is activated not from sensor actuation but forcibly from the remote control. This mode is used to frighten intruders away from the car and attract other persons’ attention to it.

### 3.5.5. Valet mode

It is used when the car is handed over in service. All security functions are disabled in this mode.

### 3.5.6. Programming mode

It is intended for security system programming and setting of its parameters.

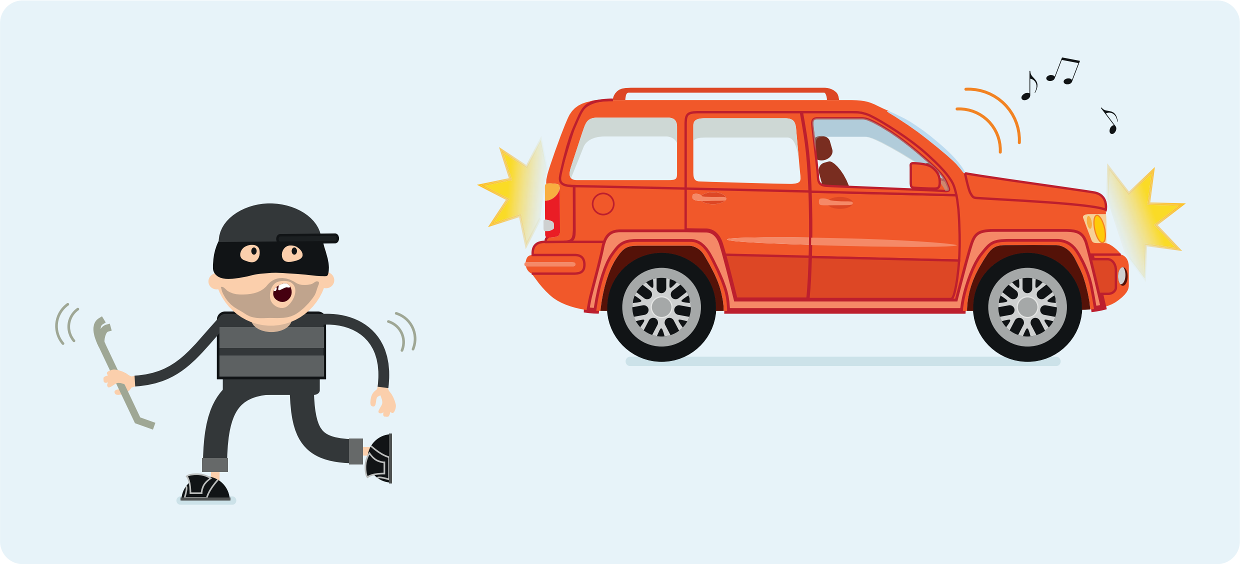
The following can be set in this mode:

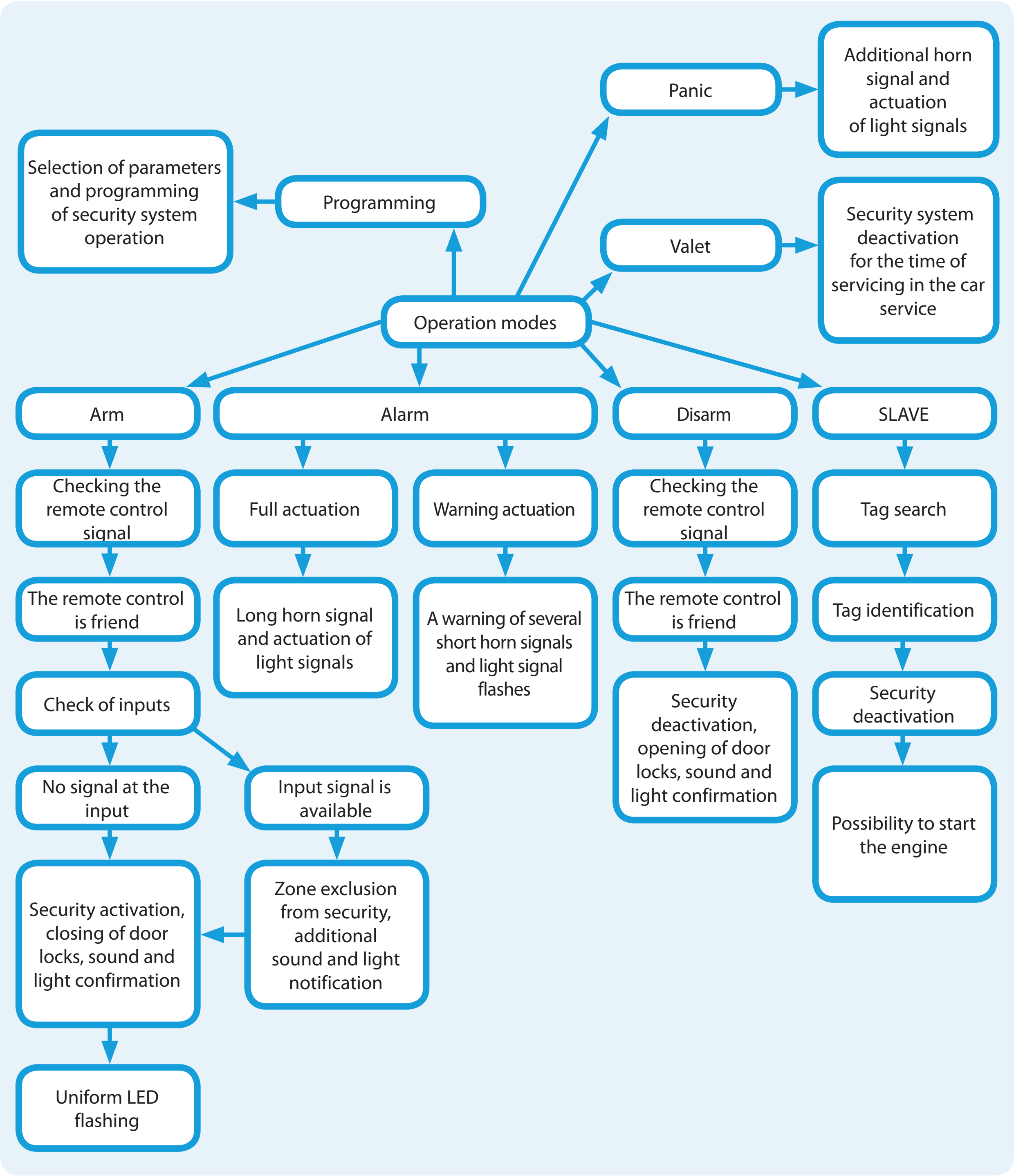
**1)** user functions, e.g. control of the central lock at ignition on, as well as two-stage opening of locks and the immobilizer mode;

**2)** parameters of security system inputs and outputs, necessary during setting (duration of central lock control pulses, interlock output algorithm, duration of additional channel);

**3)** parameters of remote and automatic engine starting

*See the memo diagram as per the materials of this chapter on page 73.*




Operation modes
Programming
Selection of parameters and programming of security system operation
Panic
Additional horn signal and actuation of light signals
Valet
Security system deactivation for the time of servicing in the car service
Arm
Checking the remote control signal
The remote control is friend
Check of inputs
No signal at the input
Input signal is available
Security activation, closing of door locks, sound and light confirmation
Zone exclusion from security, additional sound and light notification
Uniform LED flashing
Alarm
Full actuation
Long horn signal and actuation of light signals
Warning actuation
A warning of several short horn signals and light signal flashes
Disarm
Checking the remote control signal
The remote control is friend
Security deactivation, opening of door locks, sound and light confirmation
SLAVE
Tag search
Tag identification
Security deactivation
Possibility to start the engine

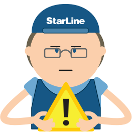
**Security system operation modes. Memo diagram**

### 3.5.7. SLAVE mode

If 5-6 years ago a factory security system was the privilege of premium-class cars only, now its absence is hard to explain. Here the car owner has a question: “It is inconvenient to carry two remote controls, one for the original, the second - for the additional alarm”. And now imagine that the car has the “smart key” function (keyless access). One more question will be added to the previous one: “I’ve paid money for convenience, and you want to make me use a remote control?”

Security system operation in the SLAVE mode is intended for just such cases. The meaning of this word shows that one thing is subordinated to another. Let us consider this mode.

You leave the car and activate its security using the factory remote control or “smart key” unction. The StarLine security-telematic system, using the information from the integrated CAN-module, also arms security. Everything is simple and clear here. And then you disarm car security using the same original remote control. StarLine will also disarm security, but if the owner is not authorized within 20 seconds, the engine will remain blocked and the alarm signal will be issued. Accordingly, if the security system has a GSM module, the car owner will receive the information to his telephone.



**Authorization is a mandatory condition of safety. If it is absent in the SLAVE mode, security is out of the question**

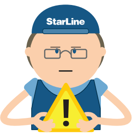
If the original remote control is stolen, the additional security system without the owner authorization function will disarm security and leave the car unprotected. Standard alarm systems in the car are much less protected against electronic hacking.

Authorization in StarLine systems can be performed by several methods:

**The first method** is authorization by means of the remote tag. The tag is the main or additional remote control of the security system. But now it is not needed to take it out of the bag or the pocket and to press buttons. Upon reception of a signal on factory system security deactivation from the CAN-module, the main unit starts searching for the tag remote control. If the system has recognized the tag, engine blocking will be removed. And if the

StarLine
StarLine

intruder has no tag, the car will be immobile and the horn will be sounding. In case of this authorization method, radius of tag recognition is 5-20 meters and can be adjusted during installation.



**The slave system in this case is StarLine, while the master — the factory one. Communication between them is via the CAN-module.**

The car owner has the option to use the StarLine remote control for the conventional purpose as well — arm /disarm security, perform automatic engine start, check the car's state... At that, remote control operational range does not decrease.

**The second method** is authorization via Bluetooth Smart. The smart and safe technology of control and data reception from the car via the protected Bluetooth Smart protocol allows for identification of the car owner's smartphone as the tag.

Let us describe the Bluetooth Smart technology in detail. Bluetooth Smart, also known as Bluetooth Low Energy is wireless communication technology provided in December 2009. The first devices supporting Bluetooth Smart were the top smartphones in 2012. Then the technology became popular and nowadays almost all new smartphones support Bluetooth Smart.

What is the difference of Bluetooth Smart from the previous Bluetooth generations? As a matter of fact, it is simpler to point out their common features. The common features are only the word Bluetooth in the name and the operating frequency range (2.4 GHz). Bluetooth Smart was created a technology for safe data transmission to short distances with the minimum power consumption.

It is these 3 requirements that underlie the security systems with owner identification by tag:

- safe data transmission, i.e. the tag signal cannot be forged;
- operational radius of 10 meters;
- · tag service life from the battery of the minimum dimensions (CR2032) is about 1 year.

And if we add the high interference immunity of the radio signal and the possibility of smartphone use as a tag, t becomes clear that Bluetooth Smart is an ideal variant for security-telematic systems. Let us consider in greater detail the advantages of Bluetooth Smart in the section of car security systems.

**Bluetooth Smart** is a standardized open protocol. Thanks to this all the devices supporting Bluetooth Smart may connect with each other. This allows for connecting smartphones and tablets with the security system by means of Bluetooth Smart.

Also, all the security system units containing Bluetooth Smart can be connected with each other.

The Bluetooth Smart device may play the following roles:

• a peripheral device (a device going online under a schedule and looking for a device to connect to (it searches for the central device where it is registered), thanks to which it consumes very little energy);

• the central device (the device constantly scanning the channels in search of peripheral devices in order to establish connection with those that are registered in it).

Connection is possible only between the peripheral and central devices.

Upon reception of radio packages, the Bluetooth Smart device measures the power level of the signal with which these packages were received. This data is used by the mainl unit of the security system to estimate the distance from the tag to or smartphone.

This is a very useful function allowing for implementing the "hands free" function.

However, there is a fly in the ointment. Bluetooth Smart transmits data at the frequency of 2.4 GHz. Radio signals at the frequency of 2.4 GHz are re-reflected well from other objects, are easily absorbed by water molecules and cannot pass around obstacles. What does it mean?

If the tag is in the front pocket of a person staying with his face towards the car, the measured signal level corresponds directly to the distance between the person and machine. And if the tag is in the rear pocket, signal level will correspond to another distance — either with consideration of re-reflection from a neighboring car or with consideration of absorption of some energy by the human body (composed by 70% of water). And this may correspond to a distance larger in 2-4 times.

That's why ranging accuracy is not very high and is used not for accurate range finding (accuracy up to one meter), but only for an approximate estimation far-near (inside the car or within the range of 30 meters).

### How is Bluetooth Smart used in StarLine security systems?

In StarLine security systems of generation 5 and 6, the smart and safe technology of control and data reception from the car via the protected Bluetooth Smart protocol allows for implementing the following opportunities:

**1)** "Hands free" mode. Authorization in this case is performed automatically. When the owner approaches the car, the security is disarmed and door locks are opened, and if he/she withdraws — the locks are locked and the security mode is activated. Various algorithms of security arming and diarming can be set in the "Hands free" mode from the minimum of several meters up to the maximum possible one — up to 50 meters (for StarLine systems of generation 5).

**2)** Use of a smartphone as a tag for owner authorization (for StarLine systems of generation 6). After disarming of the factory security, the car owner is authorized using the smartphone. The smartphone is used as a tag and allows for engine starting and driving.

**3)** The StarLine mobile application on the owner's smartphone will operate even if the GSM-operator's network is unavailable. For instance, if the car owner is in an underground garage or on a parking lot where the GSM signal is unavailable, he/she will still be able to control the StarLine system by means of a smartphone. Switchover to the Bluetooth Smart mode will occur automatically upon approach to the car to a distance of less than 10-20 meters. The Bluetooth Smart smart technology will ensure a high speed of execution of StarLine security system control commands.

The main unit in StarLine M96/X96 security-telematic systems of generation 6 and the M66 smart tracker operates as the main device, while the tags, smartphone and radio relay — as peripherals.

At present, only Apple smartphones support the role of a peripheral device in the full scope, that's why only iPhone smartphones can be used as a tag.

2 roles of Bluetooth Smart are simultaneously implemented in the main unit in the latest StarLine A96, E96 (and subsequent ones):

**central** — for connection with tags and radio relays;

**peripheral** — for connection with smartphones.

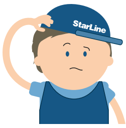
Thanks to this, the smartphone is connected in the central device mode which is standard for it, which allows using both Apple and Android, WindowsPhone smartphones.

**The third method** for owner authorization is the entry of a secret PIN-code after deactivation of standard security. It can be done either using the standard car buttons or by installing an additional secret button. The secret code is set in the process of the special algorithm for secret PIN-code setting.

Chapter 3.6

# Security system operation principle

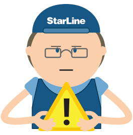
As already noted, the main unit of the security system is responsible for the operation logic of the whole system.



**How does it occur?**

At a certain time moment, an incoming signal comes to the main unit of the security system from the sensor or from remote control via the transceiver.

Depending on the current operation mode and the received signal, the main unit selects a certain action program set by the manufacturer.



**All actions "from the viewpoint" of the main unit consist in generation of signals of certain waveform at the output at the given time moments.**

Chapter 3.7

# New generation security - telematic systems

In contemporary world users appreciate the possibility of quick improvement of their equipment — mobile telephones, computers, cars. Device software is updated over the air. Devices obtain new functions and capabilities.

Security-telematic equipment also pertains to devices that must be updated quickly and simply — in compliance with car owner's wishes and requests.

## 3.7.1. Modular architecture

Most StarLine security systems were developed by development engineers based on the progressive concept of cosmic modular satellites of the future. This concept allows implementing the boldest ideas by antitheft experts. If necessary, the expert may complement the security system with CAN, GSM-interfaces, GPS+GLONASS antenna or exclude the unnecessary items, thus additionally reducing the power consumption of the whole system.

When a new module is added, the security system programs does not need to be updated, the installed module starts operating at once. Individual modules are sold within special sets StarLine Master: CAN, GSM or GPS.

Ancient philosophers affirmed:"Form determines content". Agreeing with this statement, StarLine pays special attention to aesthetics and ergonomics as an important element in the integrated safety concept.

The modular architecture of StarLine security systems makes it possible for installers to install security systems conveniently and quickly, for car owners — to easily improve the security of their car, for the manufacturer — to develop and upgrade individual modules.

## 3.7.2. Software architecture

Installers appreciated the convenient and fast installation of security systems with modular architecture, while car owners — the possibility of upgrade of such system and its reliability.

However, even more readily available methods for security equipment improvement appear as technologies are developing. Let us talk about the new concept of flexible architecture — software architecture.

**What is software architecture?**

All the key technologies are arranged on one printed circuit board. Thereat, it has no jacks, which enhances equipment reliability. Additional functions can be activated by purchasing software, not a module. Thus, only software needs to be updated for system improvement. And this can be done very quickly and simply. The security system main unit and the additional remote control have micro USB jacks, used for equipment setting and update via a computer. Moreover, the whole software, including CAN library, voice files etc can be updated via GPRS (StarLine monitoring server).

## 3.7.3. Security system creation

1) Select the core — StarLine security-telematic system of generation 5 or 6. The model, set, settings depend on car owner's wishes and make/model of his car.

2) Complement the system with security-search

module StarLine M15 eco, StarLine M17.

3) Complement the system with antitheft immobilizer StarLine i95, StarLine i96 CAN.

4) Install electromechanical hood lock StarLine L10, StarLine L11 for reliable protection of the underhood space.

### 3.7.4. StarLine Pobedit

A question may arise:

**how much will such a system cost and how are all its elements coordinated with each other?**

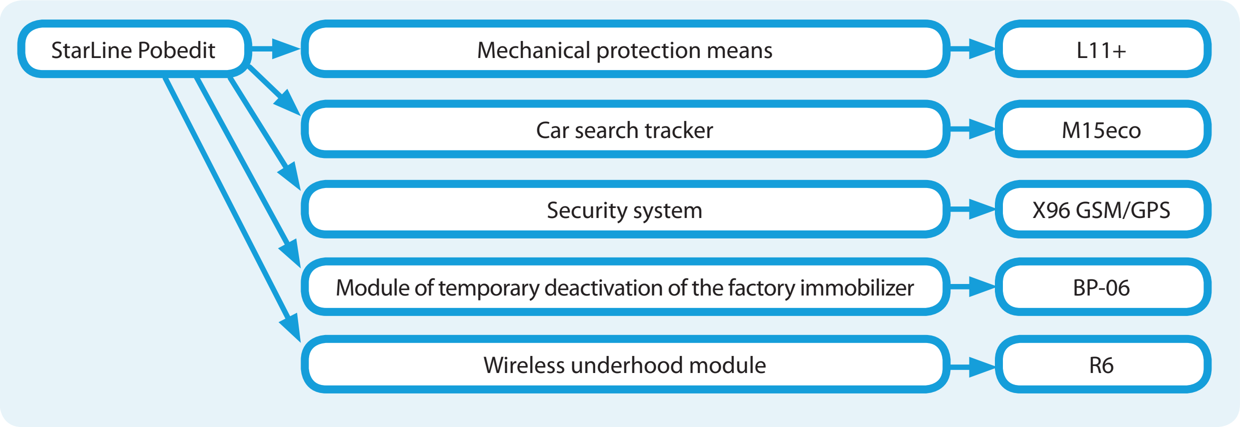
There is a good answer to such questions — the **StarLine Pobedit** system.

StarLine Pobedit implements the integrated safety concept. The intruder will have to overcome all protection levels in order to get the car. And this is very long and expensive, it is simpler to find a car with ordinary alarm. The concept can be demonstrated by an illustration.

Depending on car owner's wishes, a set containing everything necessary should be chosen — the security-telematic system, search beacon, GSM-interface, GPS+GLONASS antenna.

The price of such a set is 10 - 15% lower than the total price of the devices included in it.

**StarLine Pobedit system**

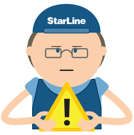

StarLine Pobedit
Mechanical protection means
L11+
Car search tracker
M15eco
Security system
X96 GSM/GPS
Module of temporary deactivation of the factory immobilizer
BP-06
Wireless underhood module
R6

Chapter 3.8

# Use of security system devices

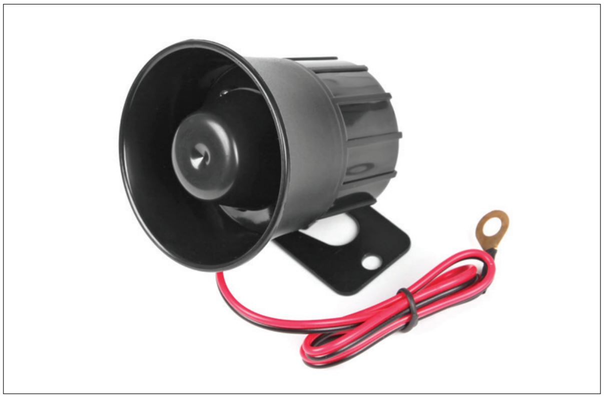
## 3.8.1. Horn

The horn can be stand-alone (with a built-in storage battery) or standard (without a storage battery).



**The horn with standalone power supply will be active not only in case of security system activation, but also in case of car de-energization.**

Such a device will have time to "give voice" if the intruder quickly opens the hood and switches off the storage battery.



**Standard horn of the security system**

The set comprises two keys for disable of the stand-alone horn.

The horn consists of a signal generator, power amplifier and loudspeaker. The generator generates alternating voltage which comes via the amplifier to the loudspeaker coil. Under the impact of alternating voltage, the coil makes an oscillating motion, transmitted to the diffuser. As a result, the diffuser emits a powerful sound wave.

**Sloven's hint:**

**you liked a women client and want to meet her more often? For this, install the horn in a hot place or in a place where it will be exposed to water from puddles, turn the loudspeaker upwards, and take the minus from under a self-tapping screw. Now your chosen one will visit you many a time.**

The stand-alone horn has four connection wires, two of which are for power supply, and the others are inputs for positive or negative starting. The non-stand-alone horn is connected to the security system by two wires.

## 3.8.2. Shock sensor

The shock sensor is usually included in the standard set of most security systems. The sensor converts mechanical oscillations from a shock into an electric signal. Most often it uses a piezoelectric-crystal plate with an additional weight. In case of a blow on the car, the weight starts oscillating together with the plate, causing an electric signal on the plate contacts.

Modern security systems use a three-axis accelerometer. It is an electronic instrument measuring accelerations in three directions and orientation in space. Besides responding to a blow, it also traces the car body position. The advantage of the accelerometer is the possibility of remote setting of sensor sensitivity.

Sloven's hint:

**if you have perfectly installed the whole security system, do not spend precious minutes in setting the shock sensor. Let its actuation from a puff of wind be a fly in the ointment.**

## 3.8.3. Microwave sensor

The microwave sensor responds to object's movement inside the car and at the distance of 0.5-1 m from it. Detection is performed in the high-frequency field created by the sensor. If the instrument "feels" movement near the car, it issues a short warning alarm signal. Detection of an object inside the car causes the full alarm signal at once.

## 3.8.4. Tilt sensor

**Microwave sensor**

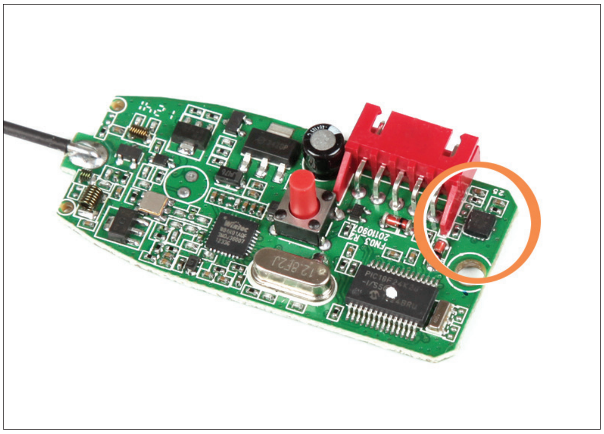
The tilt sensor determines car tilt usually caused by its towing, loading on a tow truck, as well as jacking in order to steal wheels. The operating principle is based on the use of an electronic accelerometer measuring orientation in space and acceleration. StarLine security systems use a three-axis accelerometer integrated in the antenna module.

## 3.8.5. Blocking relay

The kill-relay has three make-before-break contact, which allows using any pair for blocking: the normally open or the normally closed one.

**The following is used for engine blocking:**

**1)** the powerful relay built into the main unit of



**Tilt and movement sensor on the three-axis accelerometer microcircuit**

the security system (the maximum current is 30 A);

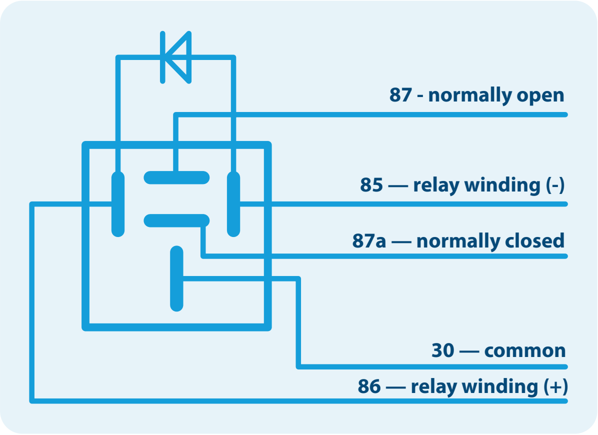
**2)** a standard external car relay (the maximum current is 40 A);

**3)** a digital (wireless) relay (the maximum current is 10 A).

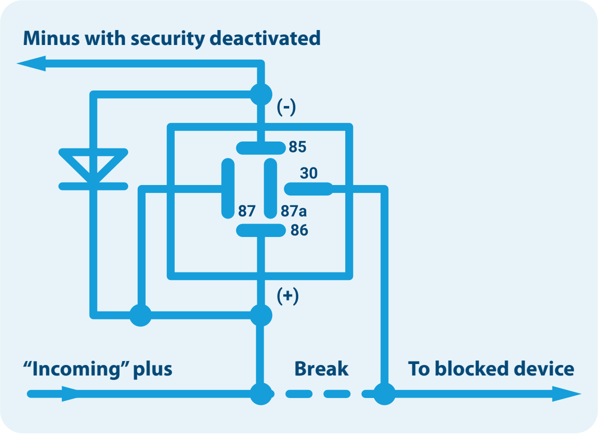
### 3.8.6. External blocking relay

Two variants for connection of an external kill-relay are used. The first one uses a normally open pair of contacts (the minus with security off, the second one — a normally closed pair of contacts (minus security on). The more preferable option is the one with normally open contacts (minus security off), which will prevent the disabling of engine interlock by simple de-energization of the security system or pulling it out of the connector. The relay is controlled by a signal from the central unit of the security system.

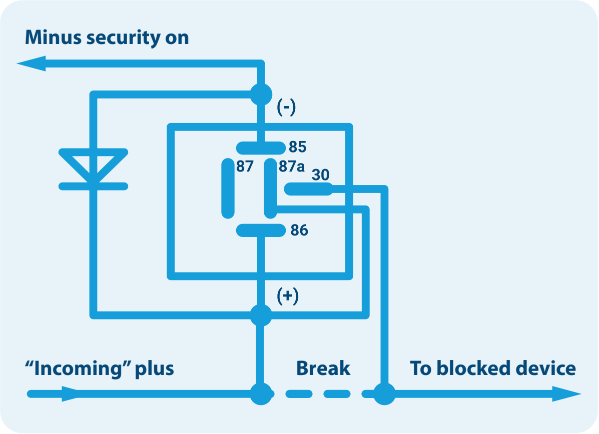
The external relay, in addition to engine blocking, is used to control various power devices (hood lock, electrical drives of door locks). The relay package is sealed. The relay can be installed in any place, avoiding liquid ingress on its leads. In the initial state when voltage is not supplied to the relay winding (the contacts are usually designated with numbers 85 and 86), contacts 30 and 87a are closed, while contacts 30 and 87 are open. When voltage is supplied to the winding (contact 86 to the minus, contact 85 to +12 V) the relay actuates, at which contact 30 is connected with contact 87, while contact 87a opens with contact 30. This relay state persists until relay winding de-energization.



**Blocking relay**



**Blocking "minus with security deactivated"**



**Blocking "minus security on"**

### 3.8.7. Wireless or digital blocking relay

Let us remember what takes up most of the time during system installation? Right, laying of wires under the hood for the horn, limit switch, temperature sensor... Now this is simple! The special wireless underhood module StarLine R6 allows for

**Digital relay**

reducing the number of connections, which means simpler and quicker installation. The module is connected to the horn, lock and limit switch of the hood, engine temperature sensor. In addition, R6 has a dry contact relay for engine blocking.

The StarLine R6 radio relay is controlled via the radio channel and is used with StarLine systems of generation 6. The R6 module must be programmed before use in the car. It will operate only with the security system in whose memory it was recorded.

StarLine R6 need not be used, all underhood connections can be made conventionally: by wires to the main unit.

### 3.8.8. Window raiser control module

Many modern cars are equipped with the standard “Comfort” system (“Total Closure”), closing all doors, windows and hatch when the driver door lock is locked. In cars equipped with a window electrical drive but not equipped with the “Comfort” system, the window raiser control module is used for their automatic closing at security activation. The module can be also used if the car is equipped with a window electrical drive. The module is started by the central unit at security activation and supplies voltage to the window drive electric motors. When the window reaches the stop, the module de-energizes the electric motors.

**Window raiser control module**

### 3.8.9. Factory immobilizer bypass module

The factory immobilizer bypass module is necessary for automatic engine starting. To have the factory immobilizer permit the engine starting, the car’s transponder key is placed in the module and its code is read by the factory immobilizer at ignition switch-on. The module is installed in a hidden, hard-to-reach place (farther from the intruder).

Sometimes situations occur when one of the keys cannot be used for automatic starting. For instance, only 2 keys can be “written” in KIA cars.

One remains with the owner, the other one is hidden in the car. In this case there can be trouble with the insurance company. And the loss of the remaining key will be a headache for the car owner. Of course, a clone can be made, but for some cars it is too expensive or actually impossible. How to act in such cases?

Microprocessor technology did not stay away from this device class as well. The so-called “keyless bypass modules” were developed. Though it is more correct to call them a “microprocessor engine starting device”. These modules can not only simulate the signals, required by the engine

**Module of factory immobilizer bypass**

control unit for starting permission, but in some cases can start the car via the CAN-bus as well. Immobilizer bypass modules are controlled either by analogue signals or by sending a digital signal via a special coded bus. The most widespread products are manufactured by such companies as Sigma 15 (StarLine), iDatalink (ADS Inc. Canada), Fortin (Fortin Electronic Systems).

In modern solutions the bypass module is integrated in the common circuit of the security system. The bypass solutions were implemented in this way in generation 3, 5 and 6 models of StarLine.

### 3.8.10. Antitheft immobilizer

The antitheft immobilizer is used to protect the car against theft and armed seizure. The car equipped with the StarLine immobilizer can be used only if you have the special remote control recorded in the device memory. If the remote control is absent, engine starting is hindered by an additional hidden digital blocking. Car thieves often use the owner's leaving the started car (to open gates, to wipe the glass). Theft can be prevented in this and many other situations by the antitheft immobilizer mode. Moreover, immobilizer blocking will prevent car engine starting even if the security system is disarmed (in case of theft of keys with the security system remote control).

The smart StarLine i96 CAN immobilizer recognizes the owner using the wireless Bluetooth Smart technology and protect the car against theft, blocking the engine when an attempt at unauthorized driving is made.

StarLine i95 and StarLine i95 Lux immobilizers are also used in cars with an automatic and remote engine starting system. These immobilizers let the engine operate unhindered when the car is not moving and block its operation if the car starts moving. Power switches are used to control the hood lock.

### 3.8.11. Security-telematic modules

The remote control and monitoring system allows the owner to use a mobile telephone for state monitoring of the security system and reception of alert signals from it. This system can be simply represented as a mobile telephone with a SIM-car, receiving messages on alarm reasons from the central unit and transmitting them to the car owner's cellphone.

**The multifunction StarLine M22 module** allows for control of remote engine starting, StarLine security equipment, Webasto and Eberspacher starting preheaters from the mobile telephone.

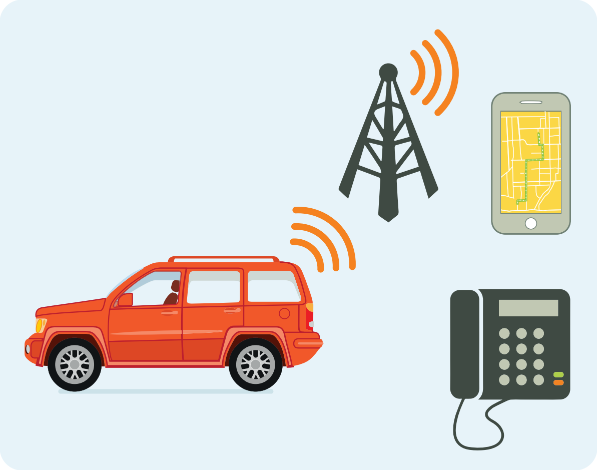
**Immobilizer relay**

**Immobilizer tag**

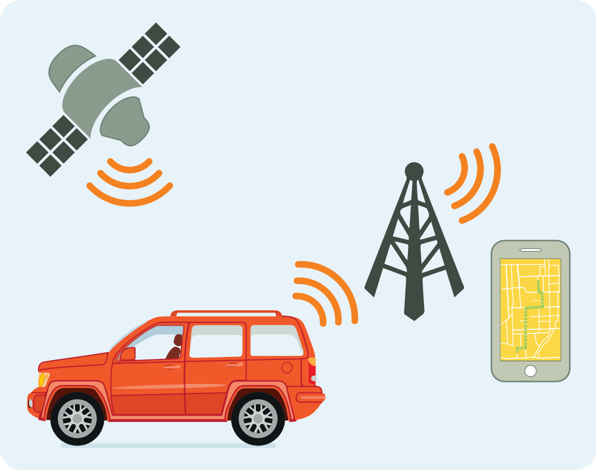
**The smart multifunction GSM, GPS+GLONASS security and monitoring system StarLine M32** guarantees reliable car protection. It allows for gratuitous monitoring of the transport vehicle, control of remote engine starting, as well as Webasto and Eberspacher starting preheaters from the mobile telephone.

**The information-search systems** are represented by StarLine M15 eco, StarLine M17 devices.

StarLine M15 determines car location and helps find it, for example, on an impound yard, in order city or country. Thanks to the waterproof housing and a nano-membrane, the tracker can be hidden in the most unexpected place (for the thief) both inside and outside a car, a motor boat, a truck.



**Notifications by means of security-telematic module**



**Operation of Starline M32 security-telematic module**

StarLine M17 has the GSM+GPRS interface and GPS+GLONASS antenna, thanks to which it will be able to find the car using satellites or cellular retranslators. A link to the map with car coordinates will be sent to the owner's cellphone. The tracker is miniature and can find room on the palm. It has its own power source — lithium batteries intended for two years of standalone operation in the power-saving mode. Compactness and standalone power supply allow for hiding the device in car passenger compartment without its referencing to the vehicle power system. The car owner sets the devices by means of SMS-commands from the cellphone. Along with that, one can receive data about car speed, temperature in the passenger compartment, degree of battery discharge.

StarLine M17 is used for protection, monitoring and search of cars, motorcycles and cargo vehicles.

**Advantages of StarLine trackers:**

- the system has no unmasking wires (only in StarLine M15 eco);
- the device cannot be found by air scanners and GSM-signal detectors because the system operates in the pulse mode;
- ·the system will not suffer from suppression of the GSM/GPS/GLONASS signal, because it can

work for a long time in the standalone mode, thereat the jammer will be switched off sooner or later, communication will be restored and the device will send the car coordinates to the owner;

- thanks to the miniature sizes, the device can be hidden in most unexpected and hard-to-reach places where it will be very difficult to find it (under plastic bumpers, spoilers, spotlights, under the passenger compartment upholstery, in headrests and seats, in ventilation ducts etc);
- no subscriber fee — expenses only on the cost of outgoing SMS-messages;
- independent installation is possible, which ensures additional cost-saving and secrecy;
- the device can be easily moved from one observation object to another;
- ·flexible (and simple) settings allow for independent setting of the optimal mode.

### 3.8.12. 2CAN+2LIN-modules

CAN modules should be studied in greater detail, because the majority of car manufacturers equip their cars with a CAN-bus. Having no idea about the CAN-bus, you risk to lose clients who drive new foreign cars.

**Security-search tracker StarLine M15 eco**

**Sloven's hint: ignorance is blessing. You are not a theorist. Neither are you a historian. What for all this nonsense about what began when, what it ended with and how it works. There is a module and its diagram — what more do we need?**

It is no secret that the client is anxious about the installer's level of expertise, and if you answer the questions "What for?" and "Why?" by: "It must be so!", the customer may lose confidence and goodwill towards you. By explaining some interesting facts and peculiarities to the client, you will improve the client's opinion of you and communication will become easier.

As the car design became more complicated in the end of the past century, car manufacturers faced two issues: saving of wires and convenient error diagnostics. Both problems were solved by using serial data buses. The most successful for car industry at that time was the CAN bus (Controller Area Network), developed by Robert Bosh GmbH (Germany) for numerically controlled machines (NCM).

**One of the indisputable advantages of CAN over other buses was its interference immunity.**

The differentiated twisted pair allowed for undistorted data transmission in a car filled with interference. Moreover, the bus (more correctly, the data transmission protocol) was initially well-protected against errors.

Over the past years several varieties of this bus have appeared, besides, manufacturers have elaborated a concept for the construction of data transmission networks in car, which is not limited to the CAN bus only.

**Currently three versions of the CAN bus are used in cars:**

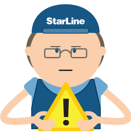
**1)** FT (Fault Tolerant) — fault tolerant bus. The most reliable modification of the CAN bus. The main difference is the possibility of operation in case of failure (rupture, ground fault or power supply) of a conductor;

**2)** SW (Single Wire) — single-wire bus better known in car industry as GM-CAN, because it is used by General Motors Corporation. The main peculiarity is the initially single-wire operation mode, but very low data transmission rate.

**3)** HS (High Speed) — high-speed bus. The main difference from FT-CAN is the high data transmission rate necessary in modern cars, but impossibility of single-wire mode operation.

CAN bus adapter, CAN-module, multiplexor — there are many names, technical and ideological solutions. The transition to digital data transmission buses, namely CAN, caused the fact that installers in some cars encountered problems when receiving signals on door opening or central lock control, hazard lights. In most cases this problem can be solved by significant disassembly of the car and connection to certain points in control units. But this is a challenging way fraught with difficulties in warranty maintenance. And then CAN modules came to the rescue.

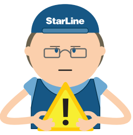
Reading and transmitting modules allow not only for receiving of information of events significant for the security system (door opening, ignition switch-on etc), bus also for control of some car systems (central lock closing/opening, enable/disable of hazard lights, arming/disarming of factory alarm, window closing).



**The considerable differences between models of various manufacturers are the set of implemented functions and number of supported car models.**

The simplest to implement and at the same time an ineffectual method is the use of different modules for different car brands. The second, more convenient one, is the user's upgrade of the necessary car brand in the module. The third one is support of all car brands in one module.

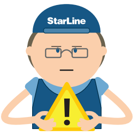
It is this method, most suitable for the installer, that is implemented in the StarLine 2CAN+2LIN modules developed and manufactured by SPA StarLine. The library of cars built into the module is regularly updated and replenished with new models. Nowadays security equipment manufacturer increasingly frequently use integrated CAN-modules. Such an approach allows reducing the installation time because it is unnecessary to connect the module and security system. At the same time, external CAN modules are in demand for connection of security systems and additional equipment via the CAN-bus. SPA StarLine makes both security systems with an integrated 2CAN+2LIN-interface and external CAN-modules (e.g. StarLine Sigma 15 or StarLine Sigma 10).



**Depending on car model, it may comprise several CAN buses.**

For instance, the motor, passenger compartment, multimedia, diagnostic buses. Connection is usually made to the passenger compartment bus, which is responsible for transmission of door state information, for control of the central lock, "comfort" system, and hazard lights.

One of the main advantages of StarLine 2CAN+2LIN modules is the simultaneous support of two interior CAN buses. Another important difference is the fact method of module adaptation for a specific car: the matching and setting of StarLine 2CAN+2LIN is performed on a computer using the convenient website can.starline.ru and Programmer StarLine CAN-Telematics.



**The use of CAN-modules allows not only for reading of car state information but also for implementing innovative car protection technologies.**

**The iCAN technology** allows for implementing digital blocking via the car's standard circuits without damaging them. Engine blocking is performed by deactivating the standard execution units responsible for engine operation.

The innovation in engine blocking via the CAN bus is not the physical interruption or shunting of a signal, but transmission of certain commands via a digital bus to the electronic control unit, after which the software disables the actuating elements responsible for engine operation. The car stops. This ensures the maximum secrecy and reliability of such blocking, because connection to the car digital bus is possible anywhere.

**The iCAN technology** is a joint development by StarLine and Andrei Kondrashov Laboratory. Advantages of the iCAN technology as compared to analogue connection:

- minimum interference in the car's standard circuits. Blocking is performed without rupture of wires or shunting of the sensor signal for engine stop;
- the blocking cannot be deactivated by standard methods;
- the device cannot be detected by standard diagnostic means because it does not "click" as the regular relay and does not create breaks of the car's standard circuits;
- implementation of iCAN blocking does not require connection of additional mechanical devices;
- simple activation procedure, reducing the time for blocking implementation during security system installation.

**The iKEY technology** is a technology for keyless bypass of the factory immobilizer, allowing for automatic and remote engine starting without the standard car key.

**Operation description:**

The device reads the data transmitted from the factory key to the immobilizer at the moment of ignition on. Then it generates an individual code and sends it to the electronic car control unit at the moment of remote starting. The software copy of the key is generated directly by the device or using the CopyKey service.

**Advantages:**

- cost-saving. Installation of the security system does not require the purchase of an additional key and a bypass module for implementation of remote starting.
- insurance benefit. Observance of the insurance company's requirement - all factory keys are kept by the car owner.

**Keyless blocking** is an innovative technology for blocking of the Keyless-system via the digital CAN bus.

The most popular method for theft of cars equipped with a keyless access system is by way of relaying of the signal of the factory car key ("long arm" or "fishing rod").

Many modern cars of the premium and business class are normally equipped with a keyless system for interior access. They have different names: Keyless, Smart Key etc. This system operates as follows: the owner with the key comes to the car and the Keyless system recognizes owner and unlocks the central lock when owner touches the door. All the owner has to do is press the engine starting button.

Contemporary car thieves have found a vulnerability in these systems. Repeaters can transmit the signal, received from the factory key, to a distance of up to 1 km. Two persons are required in order to use a repeater. One of the intruders is near the car, the other is near the owner. They deceive the Keyless-system using two transceivers: the transmitting module sends the signal from the factory key to the receiving module. The car "thinks" the owner is near and disarms the factroy alarm, allowing engine starting by button pressing. This method became very popular among car thieves.

For protection from the repeater, theft protection specialists have decided to block the Keyless-system operation while the security system is in the armed mode. Keyless blocking disables the keyless access system operation in the "Arm on" mode via the car's digital bus. Upon return to the "Disarm" mode — operation of the keyless access system is restored. The keyless access system operation is disabled by sending a special command via the digital bus.

StarLine security systems use an innovative technology of Keyless blocking via the digital CAN bus. This makes it possible for theft protection specialists to protect the car efficiently, avoiding interference in car's electric circuits.

**The standard functions of a reading and transmitting CAN-module by the example of the StarLine Sigma 15 module:**

- state of limit switches of the doors, hood and trunk, pedal of the brake and hand brake;
- status of ignition, ACC and factory security system;
- gearbox position and engine operation monitoring;
- control of the central lock, factory security system, hazard lights and "Comfort" function.

The Sigma 10, 15 modules are intended for installation on cars together with electronic equipment of any manufacturers. The module allows for implementing such functions in the car as hidden engine blocking using the iCAN technology, keyless bypass of the factory immobilizer using the iKEY technology (only Sigma 15), control of the central lock, standard security system and "comfort" function, reading of statuses of the limit switches, ignition, ACC etc.

Advantages:

- support of all kinds of digital buses: CAN, LIN, UART, K-Line;
- support of iCAN, iKEY technologies, Keyless blocking;
- support of a great number of cars;
- open digital protocol SigmaBUS, reducing the number of connections in the car.

It should be borne in mind that CAN-module's capabilities depend not only on its manufacturer but also on the car itself.

The list of supported functions is different for different cars. For instance, availability of the hood limit switch signal often depends on availability of the factory security system. The set of functions that can be implemented by the security system using the CAN bus is determined by the car manufacturer and car model. Before installing the security system on a specific car you should get ready, study the installation peculiarities, elaborate a plan thus saving your own time and client's time.

How can information about the CAN-bus of the chosen car be obtained? You can ask a more experienced friend who has already installed a security system with CAN-module on the given car model, or study internet forums dedicated to installations.

However, the best decision will be to obtain information from the manufacturer of security systems or the CAN-module. As a rule, all manufacturers of CAN-modules provide such information. It can be a document with a list of cars and functions supported via CAN or a description of all functions and their peculiarities for one chosen car.

SPA StarLine engineers have gathered all the necessary information in one place. A separate resource was created as a result — **can.starline.ru**, completely dedicated to description of CAN in all cars. Here you will find information about all supported functions in each car, description of operation peculiarities for each function, photographs of connection points, firmware of all versions for CAN modules with a revision history, software "StarLine Master Programmer", which can be used to set the module or, if necessary, to update the CAN module software.

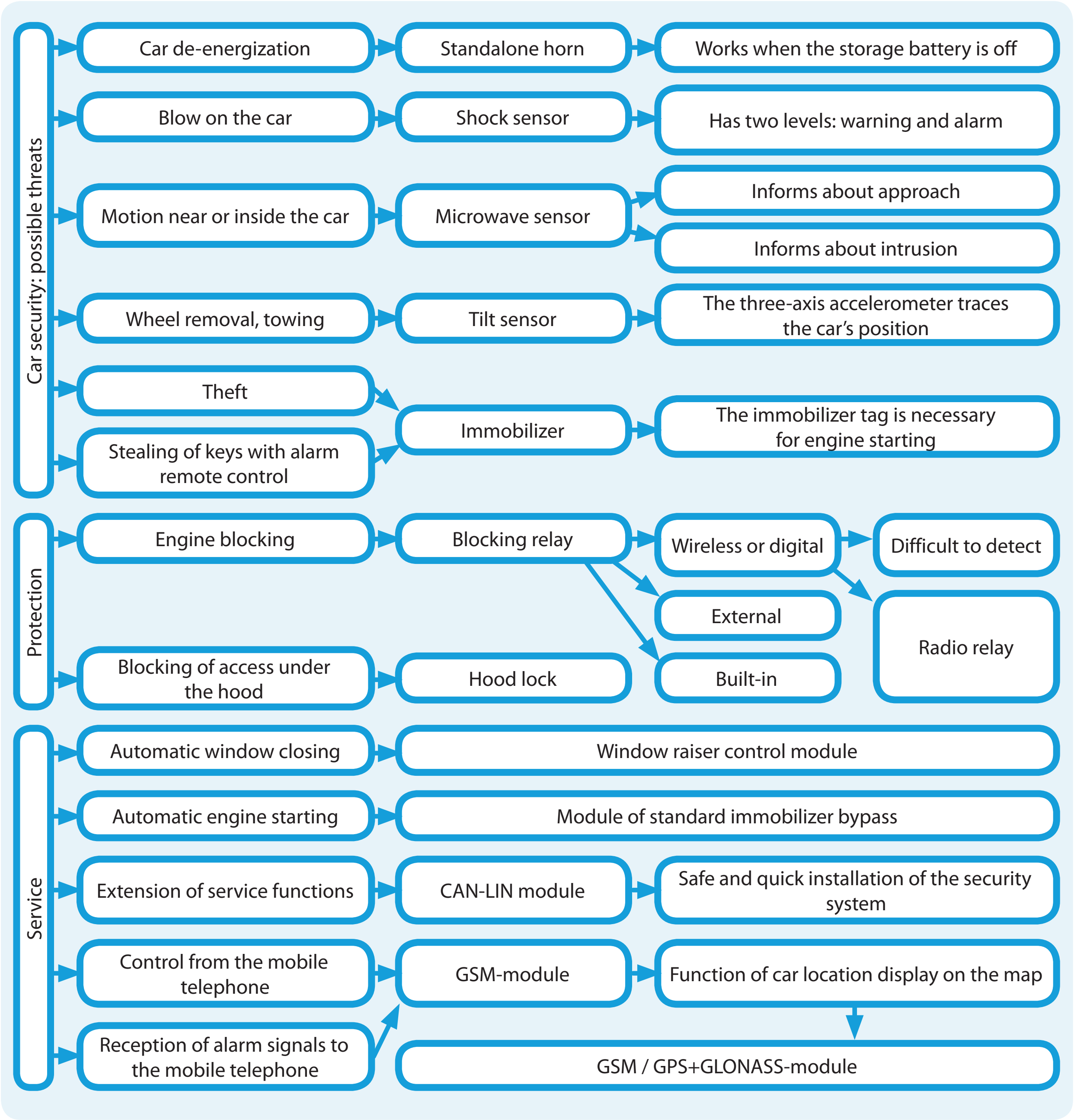
The **can.starline.ru** website has convenient functions for model search, viewing of the car list and information about each of them. There you can also leave feedback, suggestions or contact the technical support service and ask questions.

Another data transmission bus is LIN (Eng. Local Interconnect Network) is a standard of an industrial network developed by a consortium of European car manufacturers and other well-known companies, such as Audi AG, BMW AG, Daimler Chrysler AG, Motorola Inc., Volcano Communications Technologies AB, Volkswagen AG and VolvoCar Corporation.

The LIN bus has a peculiarity: it is single-wire and "slow" — about 20 kbps. The main tasks fulfilled by LIN are joining of car assemblies (such as door locks, windshield wipers, window raisers, car audio control and climate control, electric hatch etc) in a single electronic system. LIN and CAN complement each other and allow for joining all electronic modules of the car into a unified circuit. As distinct from the CAN protocol, LIN presupposes availability of one Master-assembly and many Slave-modules.

The LIN bus became rather widely used in modern car electronics. It is used for window raiser and central lock control in many cars (e.g. Mazda, Nissan, Mitsubishi). In modern VAZ cars all the capabilities of the security system and the car can be implemented only by connecting to the LIN-bus.

The universal StarLine 2CAN+2LIN modules provides fast and easy connection to the car's digital buses, ensuring careful installation of security-telematic equipment and the minimum interference in the car electronics.


Car security: possible threats
Car de-energization
Standalone horn
Works when the storage battery is off
Blow on the car
Shock sensor
Has two levels: warning and alarm
Motion near or inside the car
Microwave sensor
Informs about approach
Informs about intrusion
Wheel removal, towing
Tilt sensor
The three-axis accelerometer traces the car's position
Theft
Stealing of keys with alarm remote control
Immobilizer
The immobilizer tag is necessary for engine starting
Protection
Engine blocking
Blocking relay
Wireless or digital
Difficult to detect
External
Radio relay
Built-in
Blocking of access under the hood
Hood lock
Service
Automatic window closing
Window raiser control module
Automatic engine starting
Module of standard immobilizer bypass
Extension of service functions
CAN-LIN module
Safe and quick installation of the security system
Control from the mobile telephone
GSM-module
Function of car location display on the map
Reception of alarm signals to the mobile telephone
GSM / GPS+GLONASS-module

**Security system components. Memo diagram**

Chapter 3.9

## Telematics, monitoring — advantages

**Telematics** is a combination of telecommunication and information technologies. Telecommunication technologies are used for data reception and transmission via various communication channels. And the task of information ones — is to convert this data into the form understandable by the ordinary person. Car telematics — is the exchange of messages and commands between the car and external sources via internet.

**The following components are necessary for implementation of telematic services:**

- **Equipment able to go on-line**. In StarLine equipment it is performed by means of GSM/GPRS-interfaces. But any equipment without the corresponding software is just a heap of metal. It means the following component is necessary:
- **Firmware with software of the central unit and GSM/GPS devices.** So, security-telematic equipment transmits data. And in what form will the owner see them and how will owner be able to control his car? The third item is intended for that:
- **WEB and mobile applications of owners' cars.** What does it mean? All is simple! There are mobile applications for owners of telephones with the iOS, Android, Windows Phone or Windows Mobile operating system; they allow for car control, obtaining information about its state, identify the position and many other things. But owners of devices with other operating systems were also not forgotten. Any user of Telematics may visit the website **starline.online**.

  This is both a monitoring portal and an online service for control of StarLine security-telematic services.

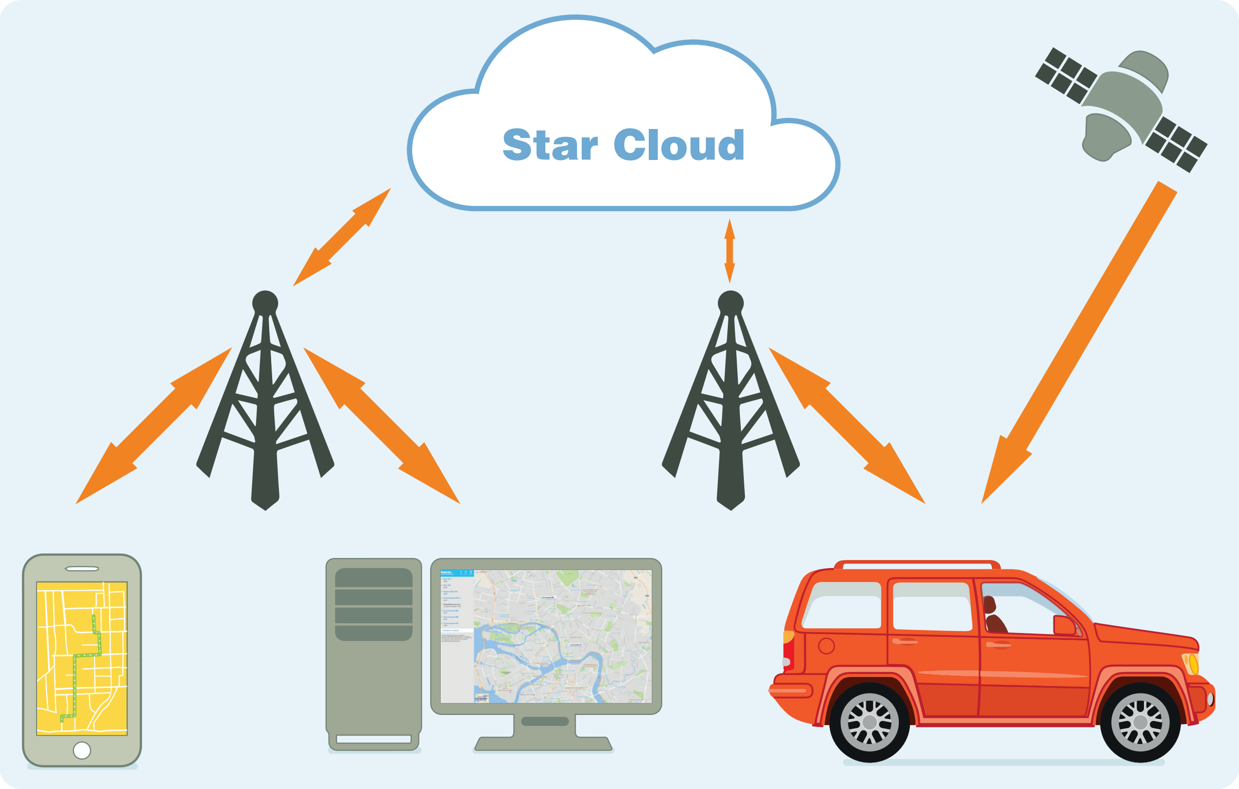
And now let us consider the following situation — you control your car by means of the mobile application and your neighbor — from a desktop

computer. Evidently these devices have different computing powers. But the command execution speed is the same. Why? Thanks to the fourth element of Telematics:

- **Server infrastructure.** It is evident from the figure below that the car owner uses not the computing resources of his devices, but the resources of the StarLine DATA-center for information processing. StarLine servers save the history of events and motions of all telematic StarLine devices connected to the system. Data transmission and processing by means of powerful server infrastructure is often called "Cloud technologies". And we all use these technologies every day. Yandex, Google, Amazon are examples of resources where they are used.

The prospects of telematic technology use are enormous. **Here are short capabilities of telematic technologies:**

- Telematics allows for detection of transport vehicle failures, which increases its reliability and reduces the maintenance cost.
- Telematics records the data about the accident and communicates it to government agencies, medical organizations, thus reducing the time of emergency team response and accelerating the medical aid to car accident victims
- Telematics serves as a platform for road information delivery in the on-line mode, thus saving the driver's time and unloading complex traffic areas.
- Telematics allow for synchronization of data exchange between the car and the user staying at home or in the office, while such information in its turn allows for reducing the insurance losses from thefts, fraud and accidents.
- Telematics allows for identifying the position of an object, driving routes, events within the accuracy of a meter.



**Results of Telematics use are as follows:**

- High comfort.
- High safety.
- Faster decision-making speed.

**Three main areas of Telematics can be distinguished:**

1. Smart insurance
2. Smart diagnostics
3. Smart monitoring

Let us consider these notions in detail.

### Smart insurance

Most cars are now purchased on credit. Consequently, comprehensive and collision car insurance is also mandatory. And what do we have? The insurance company may estimate its risks only based on driver's experience and age. As a result, the insurance cost for an inexperienced or young car owner increases many times and exceeds one hundred thousand rubles. And this with the car price below one million rubles. Clearly, many people are scared away from such sums and the car remains in the car showroom. The result is — the client refuses to buy the car, the dealer and insurance company lose a client. Actually only 15% of this number of potential insured parties (car buyers) drive really bad, 85% have statistically average skills, while 5% are excellent drivers. And the task of Telematics is to help the insurance company identify the clients to whom a discount can be granted. How does Telematics meet such a difficult challenge? All becomes simple and clear when StarLine security-telematic devices and the corresponding capabilities of StarLine server infrastructure are used. The device sends different information to the server (route points, speed, mileage, abrupt accelerations...). The information is analyzed by mathematical algorithms and is used to make a decision on driver's qualification and risks. And, accordingly, on the insurance amount. Accelerometers, built in the modern StarLine equipment, provide easy diagnostics of road traffic accidents and simplify the obtaining of insurance payments.

### Smart diagnostics

Everyone has desired to forget various trifles related to the car — extending the insurance, driving to the technical inspection, changing oil.

Telematics helps the car owner get rid of this burden. Reading the information from the CAN bus, smart StarLine equipment transmits all the necessary data to the server — mileage, errors, engine operation modes... And it sends you a message when it's time to drive to the scheduled technical inspection. If this information is transmitted directly to the dealer (naturally, with car owner's consent) to the **dealer.starline.ru** software, one can register on-line for a visit to the service.

Or imagine the following situation — the CHECK ENGINE lamp lights up unexpectedly. What an error is this, can driving be continued? There is a huge number of questions and most can be answered only at the dealership. And it's such a long way off... Here Telematics will help. Having decoded the error code, it will notify whether you can slowly drive to the service or it is better to call a tow truck. And it will even tell the tow truck's telephone!

For training of safe driving, StarLine equipment uses sensitive accelerometers that may record abrupt turns, braking or hazardous overtaking. The information is transmitted and analyzed on the StarLine server. Hazardous deviations from the norm and summed up and reduce the assessment of driving quality. The car owner may see the assessment of his driving style on the WEB and mobile application screen and get tips on improving safety and cost-effectiveness of his drives.

### Smart monitoring

Even having only a personal car, we try to optimize the expenses on its upkeep. The same applies even more to companies with a large fleet. Monitoring of mileage, speed infringements, parking lots and parking places, fuel consumption and tire pressure allows for reduction of operating costs. It is always useful to know that your car is following the specified route but is not parked near a construction shop awaiting a random client.

Another useful property of smart monitoring is geofences. When the car enters the marked geofence or leaves it, the corresponding notice is sent to the owner's telephone at once. A geofence can also be used to separate a specific route, and when the car leaves it the monitoring server will report this at once.

The commercial monitoring application StarLine Autopark will provide the following for the car owner:

- monitoring of transport vehicle location in real time mode (monitoring of the fact and direction of driving, driving speed, deviation from the route and driving schedule, entering/leaving the controlled zone);
- optimization of expenses on transport vehicle fleet operation (saving of fuel consumption, absence of unauthorized trips and downtime, monitoring of operation time);
- automatic notification of deviations from the standard situations;
- reduction of cost of mobile telephone talks;
- ation of detailed reports on mileage, operating hours, fuel and other key indicators (adjusted individually).

Monitoring of the GSM communication channel is very important in the use of security-telematic equipment.

It is a known fact that car thieves use mobile communication jammers. When such a device is switched on and GSM communication between the base station and telematic device is interrupted, the car owner will receive an alarm message from the StarLine server.

Telematics has much more possibilities than we have described. Car electronics becomes all the more complex day by day. As a matter of fact, it becomes a wheeled computer. On the other hand, having learned to read and process the necessary information, we are approaching the time when cars will have a full-fledged artificial intelligence and will completely take over the driving control.

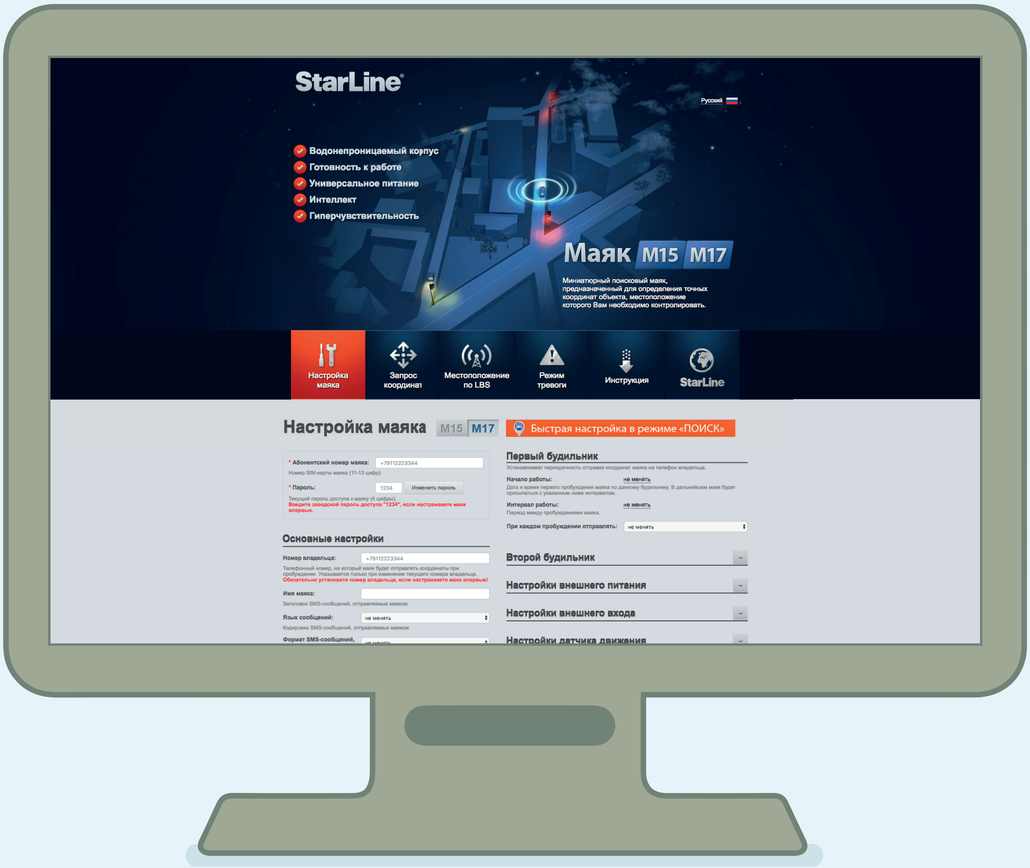
Let us consider another component of StarLine telematic services — **setting of StarLine M15 and M17 Trackers.**

What does competent installation of a tracker mean?

Right, it means its correct setting and hiding well. The method of hiding depends only on installer's skill and fantasy, while setting is a standard and necessary procedure. Trackers of all manufacturers are set by means of SMS. You will agree that this is long, expensive and inconvenient.

StarLine trackers can be set using the modern technologies for data transmission and processing. Using the **mayak.mobi** website, the installer or owner will set the StarLine M15 or M17 tracker within only a couple of minutes.

StarLine M15 and M17 search trackers can also be quickly set by means of the convenient screen on the main monitoring website **starline.online**



- Водонепроницаемый корпус
- Готовность к работе
- Универсальное питание
- Интеллект
- Гиперчувствительность

## Маяк M15 M17

Миниатюрный поисковый маяк, предназначенный для определения точных координат объекта, местоположение которого Вам необходимо контролировать.

## Настройка маяка

* Абонентский номер маяка: +79112223344

Номер SIM-карты маяка (11-13 цифр).

* Пароль: 1234

Текущий пароль доступа к маяку (4 цифры).
Введите заводской пароль доступа "1234", если настраиваете маяк впервые.

### Основные настройки

Номер владельца: +79112223344

Телефонный номер, на который маяк будет отправлять координаты при пробуждении. Указывается только при изменении текущего номера владельца.
Обязательно установите номер владельца, если настраиваете маяк впервые!

Имя маяка:

Заголовок SMS-сообщений, отправляемых маяком.

Язык сообщений: не менять

Кодировка SMS-сообщений, отправляемых маяком.

Формат SMS-сообщений, не менять

### Первый будильник

Устанавливает периодичность отправки координат маяка на телефон владельца.

Начало работы: не менять

Дата и время первого пробуждения маяка по данному будильнику. В дальнейшем маяк будет просыпаться с указанным ниже интервалом.

Интервал работы: не менять

Период между пробуждениями маяка.

При каждом пробуждении отправлять: не менять

### Второй будильник

### Настройки внешнего питания

### Настройки внешнего входа

### Настройки датчика движения

Chapter 3.10.

# Smart car

The smart car is a global trend in car industry development in the past few years and for several decades to come. Smart cars include environmentally-friendly electric cars or cars with alternative energy sources, cars connected to the Internet and providing various services — remote control and telemetry of car parameters, determination of driver's state and driving style, provision of services for automatic payment of parking, driving on toll roads and many other things.

Even now there are cars with well-developed driver assistance systems, most global car manufacturers and IT-companies are working on creation of standalone transport vehicles. The main argument for creation of standalone cars is the increase of safety level — the robot will not lose its nerves in a traffic jam, its will not fall asleep behind the steering wheel and no one will teach it the road traffic rules. The next argument is saving of transport vehicle users' time which they can spend for other more important things on the road. The owner of a standalone car may comfortably check electronic mail, respond to urgent letters or calls, without the risk of an accident due to his inattention behind the steering wheel.

Standalone cars may also reduce the traffic intensity on roads and parking loads — if we take a personal car, the average time of its use does not exceed 5% according to various estimates. A standalone car will be able to drive children to a school or kindergarten, pick up grown-up family members and drive them to work, return home to the parking lot, and drive all family members back at the necessary time. It is again saving — time, money, because a car is one of the most expensive purchases in a family, and if two cars are needed?

Wide prospects are provided for commercial transport as well — automated pits with harmful labor conditions, automatic public transport and many others.

## 3.10.1. International developments

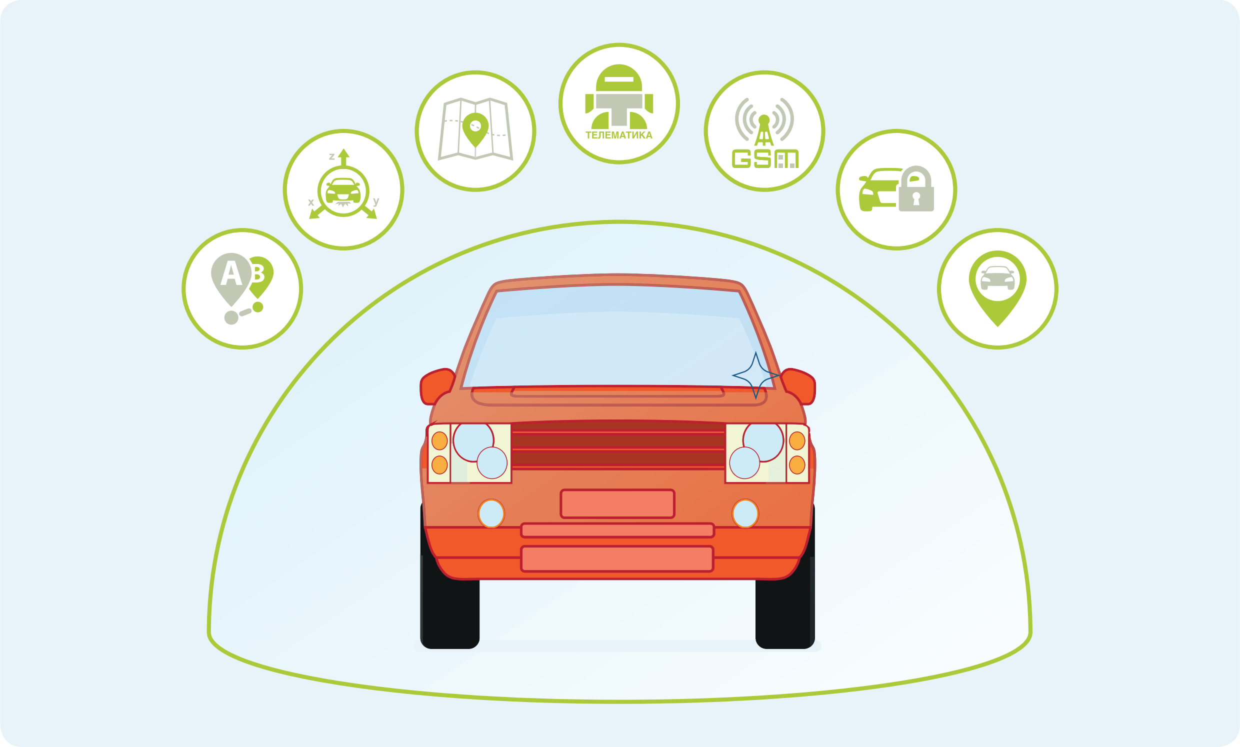
All global manufacturers even today are equipping their cars with driver assistance systems (ADAS — Advanced driver assistance systems). The availability of some of them has become not only a routine but a mandatory conditions for obtaining of vehicle type approval, such as the anti-lock braking system or the system of emergency accident response. Given below is only a partial, incomplete list of existing driver assistance systems.

### 3.10.2. Driver assistance systems

**The anti-lock braking system** (ABS) prevents car wheel blocking during braking. At present it is a mandatory element in vehicle type approval, in other words, it is compulsory for all new cars. Many delusions are related to the operation of this system, such as the braking path decrease at operation of ABS (it is not so, braking path may become slightly longer) or the fact that ABS itself actuates the brakes (ABS can only unblock the wheel, i.e. reduce the braking force). The ABS is aimed at maintaining car controllability during braking, while avoiding wheel blocking. The experienced driver independently uses cadence braking in case of the risk of wheel blocking, an inexperienced driver, especially in an emergency, is usually unable to release the brake pedal for a short time thus maintaining the car controllability.

**The electronic stabilization system** (ESP) — (ESP) is another basic driver assistance system, aimed at preventing car skipping. Car wheel speed sensors are used for system operation, the same as for ABS. Moreover, the ESP uses a sensor of steering wheel turning angle (due to this the system knows the direction in which the driver wants to drive) and gyro sensor determining the actual car turn in relation to its vertical axis. The ESP uses this data to decide on which wheels should be braked for car stabilization.

As a rule, the ABS and ESP functions in modern cars are combined in one unit. An important fundamental difference of the ABS and ESP systems is that ABS can only reduce the braking force on one or several wheels, while ESP, vice versa, — increase



it due to the special modulating pump.

**ACC (adaptive cruise control,** radar cruise control) is a system automatically maintaining the specified car driving speed and a safe distance to onward vehicles. Nowadays the system is usually made using a radar tracing the distance to the obstacle and the speed of approach to it.

**Head lighting control system** (Intelligent Light System, Adaptive highbeam etc) is a system for highbeam control preventing the dazzling of drives of oncoming vehicles. Depending on implementation, the system may switch the light over to low beam, recognizing the oncoming vehicles by means of a video camera, or actively control the light beam to maintain excellent visibility for the driver, while preventing the dazzling of oncoming and preceding vehicles, control the light beam, tracing the road bends (the technology of lamp turning depending on steering wheel turning was first implemented by the Czech Tatra Company in the 30-ies of the XX century).

**The parking assist system** The parking assist system is used to increase comfort and safety during parking maneuvers. Most systems ensure parallel and perpendicular car parking in the automatic or semi-automatic modes. Some systems also ensure parking at an angle to the traffic way. The system uses ultrasonic sensors to find a free place and to position the car during parking and determine obstacles.

The semi-automatic parking system assumes the functions of searching for a suitable place and steering wheel control, while the driver controls brake and accelerator pedals. The automatic system parks the car in the fully automatic mode, while in the most advanced systems the driver may stay even outside the car.

**The lane change assist system** (Blind spot monitor, Side Assist, Lane Change Warning etc.) warns the driver about the risk of collision at lane change. The environmental conditions are perceived using sensors (radars and cameras), permanently tracing the presence of an obstacle in the car's "blind" zone and warning the driver by a visual, sound or tactile signal (steering wheel vibration). If the driver did not switch on the turn indicator, the system signals about a present in the "blind" zone by a light indicator (usually located in the side mirror area), if the turn indicator is on, the driver is warned about the danger also by an acoustic signal or by steering wheel vibration.

Another important driver assist function implemented by means of the same sensors (radars in the rear bumper) is a system for assistance at departure from the perpendicular parking lot by reverse motion — the driver's field of view in this situation is restricted by the cars parked nearby and the driver does not see the cars driving on the road. The system of parking lot departure assistance warns the driver about the hazardous situation.

**The emergency braking system** (Collision avoidance system, Collision mitigating system, Autonomous emergency braking) is intended to prevent or mitigate the consequences of car collision or driving on a pedestrian. The system uses a frontal radar and a frontal camera. The radar measures the distance to the obstacle and speed of approach to it. Machine vision algorithms analyze the information from the frontal video camera and recognize cars, pedestrians and bicycles. When the risk of collision is detected, the system sends a signal to the driver in advance, and if the driver does not respond, it activates the braking system to reduce speed or stop the car. This system is considered very efficient for mitigation of accident consequences and will soon be compulsory for all new cars.

**The Lane Keeping Assist System** (LKAS) The Lane Keeping Assist System (LKAS) is intended to prevent unintended departure of the car from the traffic lane. It is a development of the Lane departure warning system (LDWS). Both systems use a frontal video camera and computer vision algorithms to find road marking. In case of unintentional departure from the lane (the turn indicator is off) the system warns the driver thereof (LDWS), and if the driver does not respond, it actively acts on the steering to hold the car.

The joint operation of some systems even today means a certain degree of car independence. Car independence levels are specified in the SAE J3016

| Level SAE | Name | Description | Control of driving direction, acceleration and deceleration | Perception of the environment | Redundancy | System capabilities |
|---|---|---|---|---|---|---|
| The driver estimates the environmental conditions | | | | | | |
| 0 | No automation | The driver controls the car independently, incl. by means of assistance systems (e.g. ABS and ESP) | Driver | Driver | Driver | - |
| 1 | Driver assistance | The assistance system in certain modes controls the steering wheel control or acceleration / deceleration using information about the environmental conditions. The driver fulfills all other functions for dynamic control of the transport vehicle | Driver and system | Driver | Driver | Work in some driving modes |
| 2 | Partial automation | The assistance system in certain modes controls the steering wheel control and acceleration / deceleration using information about the environmental conditions. The driver fulfills all other functions for dynamic control of the transport vehicle | System | Driver | Driver | Work in some driving modes |
| The automated control system estimates the environmental conditions. | | | | | | |
| 3 | Conventional automation | The control system fulfills all car control functions while expecting the driver to respond properly to the interference request | System | System | Driver | Work in some driving modes |
| 4 | High automation level | The control system fulfills all car control functions even if the driver does not respond properly to the interference request | System | System | System | Work in some driving modes |
| 5 | Full automation | The automated driving system fulfills all functions of dynamic transport vehicle control in any traffic situation and at any environmental conditions in which the driver (person) is able to control the vehicle | System | System | System | All driving modes |

**Car independence levels**  
**SAE J3016. Copyright © 2014 SAE International.**

standard. SAE — Society of Automotive Engineers.

### 3.10.3. Smart car in Russia

Russian and all global car manufacturers are actively developing driver assistance systems and standalone driving system. There are existing and actively developed projects for development of standalone transport vehicles both in the car segment and in the commercial and public transport segment. There are world-class IT-companies in Russia, actively developing these technologies — both in the form of their own projects and by developing customized systems for European car manufacturers.

Computer vision and artificial intelligence system are nowadays a science-intensive, highly competitive field, that's why Russian companies present great interest for global giants of the field.

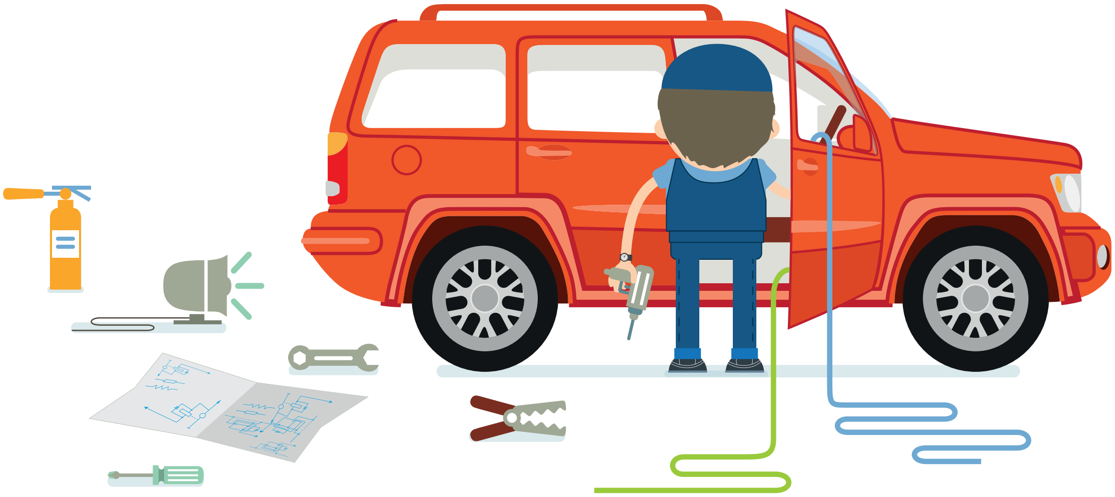
### 3.10.4. Technologies for smart car implementation even today based on StarLine security-telematic systems

The goal of StarLine Smart Car project can be worded as follows: development of a technology for automated car control corresponding to the third level as per the SAE J3016 classification. To achieve this goal, ScPA StarLine is actively cooperating with companies which are acknowledged experts in some area or other, with companies which have innovative ideas and knowledge and want to solve a similar task together.

ScPA StarLine is actively cooperating with leading higher education institutions — students, postgraduate students, researchers and is looking to cooperate with anyone able and wishing to participate in such an ambitious project.

Part 4

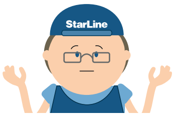
# Installation rules



An ugly aircraft will not fly well.
A. N. Tupolev

*The epigraph is fully true for security equipment installation. Install the security system badly — it will answer in kind! You will repair it under the warranty and no one will pay to you for such work. If you follow our recommendations, you will have lesser free-of-charge repairs, possibly it will drop to zero.*

*The main rule is: low-quality work — much work and low pay, high-quality work — less work and high pay.*



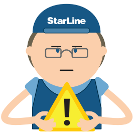
**The client who came several times for repeated repair will not drive his next car to you.**

And if you have done your work with all responsibility, whom will he ask to install a new security system? He will come to you! Moreover, he will recommend you to friends and colleagues. And this means your money!

**If you want to calmly answer clients' telephone calls and not be ashamed before them, devote some time to studying the installation rules.**

We have generalized our experience and want to share it with you. This part contains only practical advice.

## Chapter 4.1
# Wiring installation

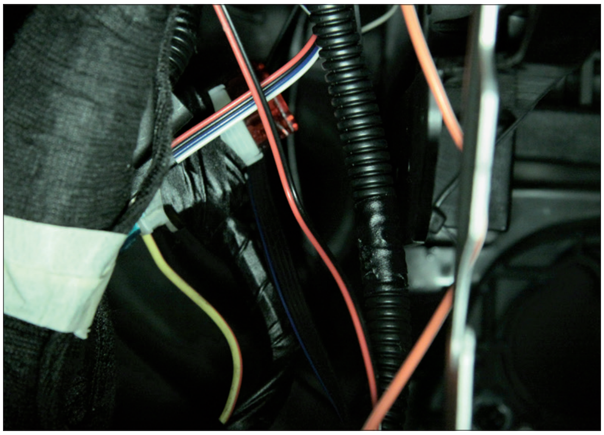


**All wires and harnesses must be wrapped in insulating tape or placed in a corrugated pipe.**

Fulfillment of this rule will protect the wires from damage and you will not have to buy a new car for the client. Besides, a neat harness can be easier disguised as a factory one. If you are too lazy to fasten the wires — a fallen-out harness may come under the pedals or into the radiator fan. Do not skimp on clamps and insulating tape. Better spend 100 rubles (including them in the client's bill) than to splice broken wires later.

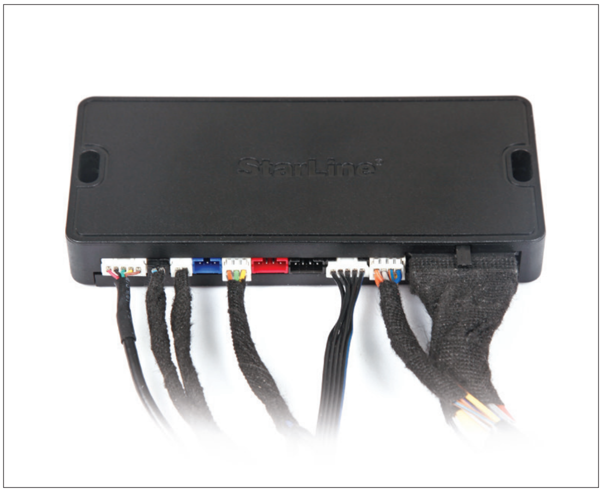
**Corrugated pipe**

**Sloven's hint: the client's life is dull and monotonous! You can make it more cheerful - prepare a surprise for him: fallen-out wires under the pedals. That's why do not bundle the wires, let them hang.**



**Wires without harness**

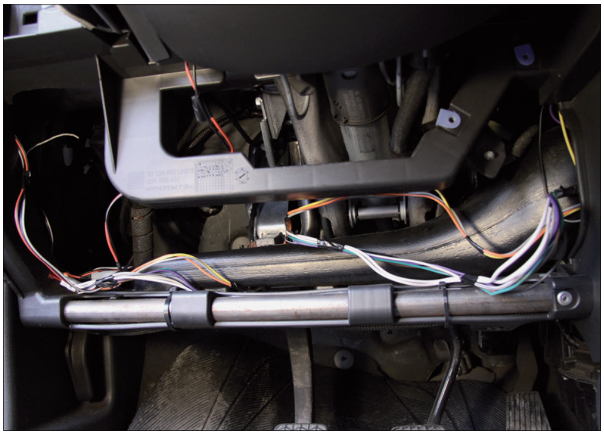
The wires are not bundled.
It is ugly and dangerous!



**Wires in insulating tape**

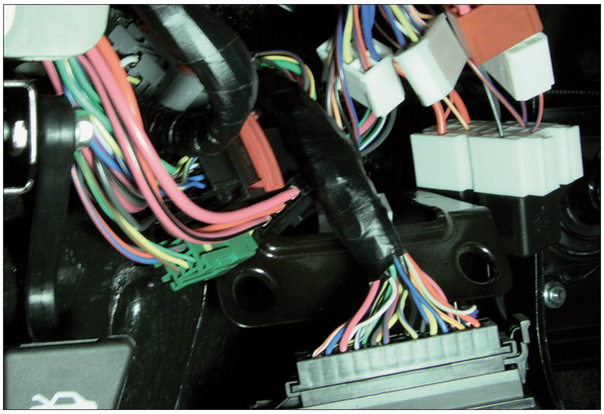
Good quality: all wires are protected.

Wiring should be installed **avoiding** the use of the brake system elements (tubes and hoses), engine cooling and steering system.



**Loose wires**

Poor quality: the wires hang loose and may come under one's feet or be wound onto the steering shaft.



**Wires disguised as the factory wiring**

Good quality: try to find the non-standard wires!

**Sloven's hint:**

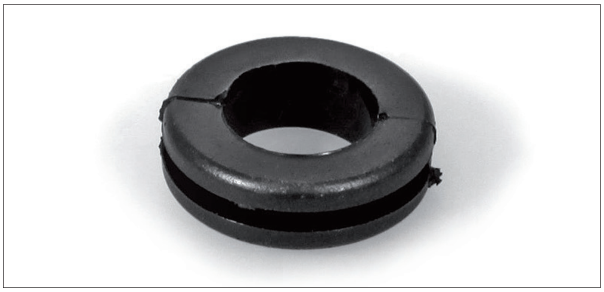
**how to study the design of car wiring? Make more holes for wire installation without sealing them! To have some expensive unit broken (for instance, BSI unit for "Opel Corsa D" at the price of 25 thous. rubles). The study material will come to you on its own, and not once! You'll train in assembly-disassembly of the passenger compartment in search of a failure and save up money for gratuitous replacement of this unit.**

You must have seen non-connected factory connectors in some cars. This is wiring provided by the manufacturer for various sets. Sometimes it can and must be used. Why install wires if somebody has already done it for you?

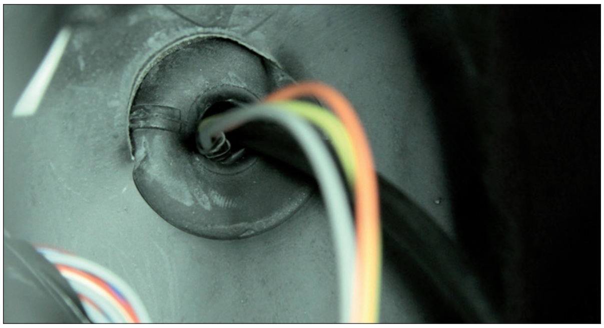
**Protection, protection and protection again.** again. This rule is also applied for wire installation under the hood. Usually the factory holes are used, but if they are unavailable or hard to reach, you can drill a hole on your own. Make sure a lead-through is installed and the passage area is sealed.

**Sloven's hint:** the client has no rain sensor in the car? Then make a gift to him — do not seal the drilled holes. Water in the passenger compartment will always prompt the driver that it is raining.

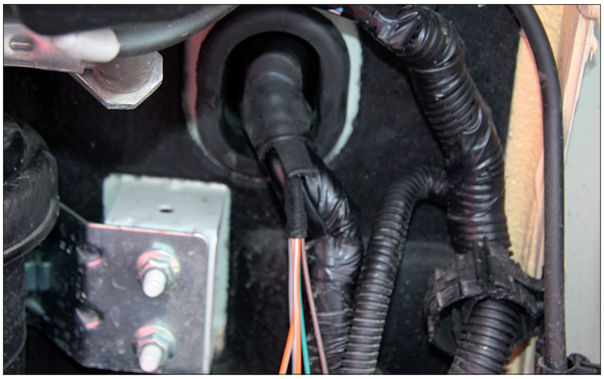
**The holes for the hood lock cable, windshield washer tube, steering shaft, pedals should not be used for wire installation from the passenger compartment to the engine compartment.**


Lead-through

**Poor quality: wires are laid under the hood together with the washer hose.**

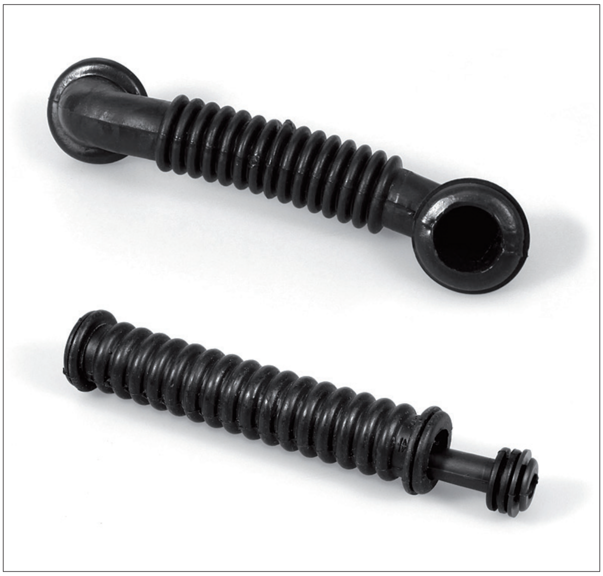

Wiring and washer hose

**Good quality: the best place for harness installation under the hood.**

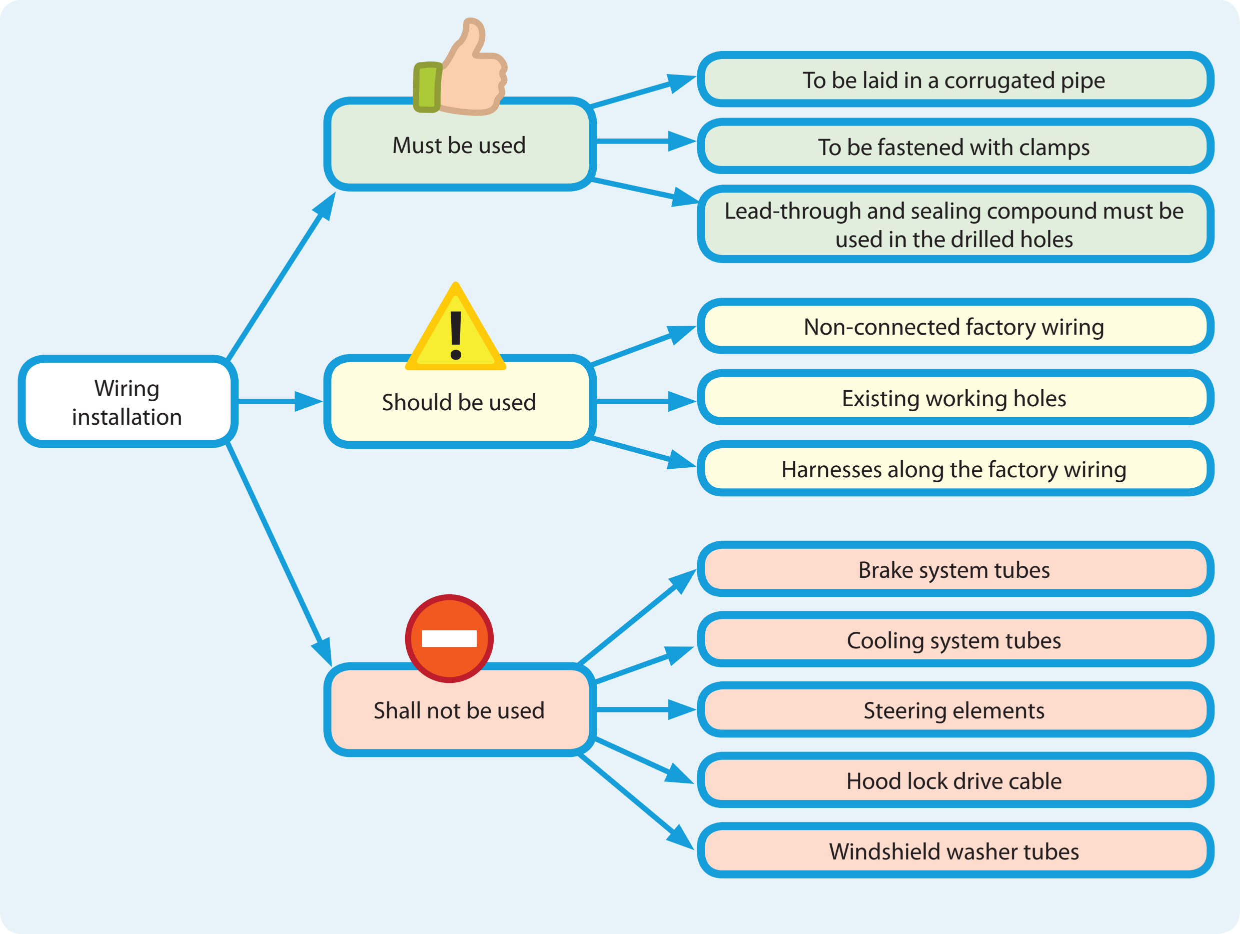

Harness laid through the factory hole

Sometimes it is necessary to pass wires in the car doors. In this case, pull wires through the standard rubbers from the post to the door. If such rubbers are not available — place your own ones.

**The wires from the pillar to the door shall not be tensioned. Let them be in torsion but not in bending.**


Sleeves for wire laying in the door

And now imagine that you are not an installer but a car mechanic. A car arrived where the heater radiator needs changing. You start removing the dashboard and are hindered by some wires not related to the factory wiring. Many car mechanics will simply cut them off. And the car will be driven for restoration to the installer, i.e. to you. It will be good if you prove that these wires did not come off themselves but were cut intentionally. The client in such cases will swear that nothing was done to the car, it has broken down of itself. To avoid such situations and to save time and nerves, lay the harnesses on the factory wiring. Car manufacturers install the wiring so that it does not hinder repair, and you can use this peculiarity.


Wiring installation
Must be used
To be laid in a corrugated pipe
To be fastened with clamps
Lead-through and sealing compound must be used in the drilled holes
Should be used
Non-connected factory wiring
Existing working holes
Harnesses along the factory wiring
Shall not be used
Brake system tubes
Cooling system tubes
Steering elements
Hood lock drive cable
Windshield washer tubes

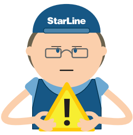
**Wiring installation. Memo diagram**

Chapter 4.2

# Installation of security system elements

## 4.2.1. Installation of security system unit

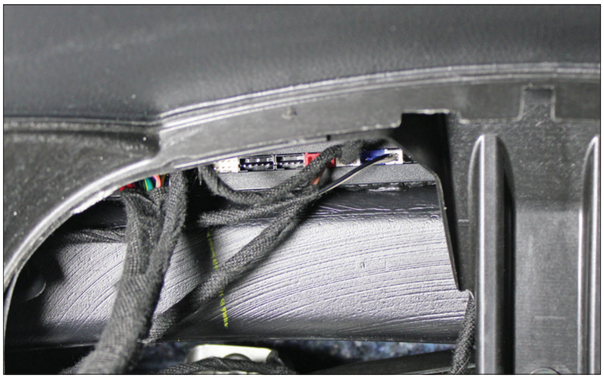
A security system unit falling on the driver's feet during driving is not very pleasant. It is good if the client gets off with nothing more than a fright. And if the fallen-out unit hinders emergency braking? Be sure, you will have problems in both cases! That's why it better to fasten the security system elements beforehand.



**The rule is simple — fasten everything that may hang loose.**

Using double-sided Scotch tape for this purpose is not the best option. It dries up with time and everything falls down. Nothing better has been devised than the clamp and self-tapping screw.

**Sloven's hint: if you dislike the client, do not fasten the unit and alarm sensors. He will do everything on his own, and at the same time will study the wiring layout of his car.**



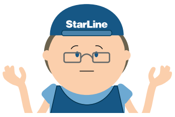
**Fastening the security system unit**

**Good quality: the security system unit is fastened by 2 self-tapping screws.**

Installation of a security system with CAN-module is a feast for the installer! One connects few wires and gets much money! Install the main unit in the least expected place: in the trunk, behind the rear seat back, under the carpet. The car must have a lot of dry secret places!

**Such installation will encumber the car thief's actions and may become a source of additional income for you.** If you correctly explain the advantages of such installation to the client, you may count upon gratitude in return. And it should not be always measured in money. The customer may simply recommend you to his friends. And they, possibly, will bring new clients.

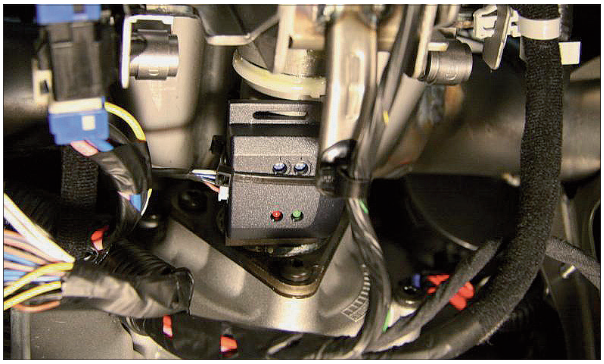
### 4.2.2. Installation of sensors



**What would you do to another person's car making unreasonable noise at night below your windows?**

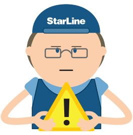
The same the owner wants to do to the installer who was too lazy to install and set the sensors correctly. Most sensors shall be placed in the center of the zone protected by them. The best place for shock sensor installation is the steering column base because this part of the car transmits vibrations well and installation can be conveniently performed there.

For microwave (radar) sensors, installation in the center of the protected zone is even more important than for shock sensors. This is due to the fact that the microwave sensor creates a round-shaped protective field which must be uniform on all sides. A good place for radar sensor installation is the space between the car roof and the ceiling (if there is enough place). But the ceiling in some cars (e.g. "Toyota") is manufactured using copper chips hindering the sensor operation. A good place for this sensor is the console behind the front seats.



**Shock sensor installation on the steering column base**

**The microwave sensor shall be arranged so that its microwave emission passes unhindered through the car glass.** The metal does not pass such waves. If the sensor is placed on the central console, it is necessary to choose a place where the car owner will not leave coins, paper clips and other metallic objects. This may cause a change in sensor sensitivity and false actuation.



**Be sure to fasten everything securely! A loose sensor will not make client's sensations more pleasant and you will not get more money.**

**Sloven's hint: do not adjust the security system sensors! Let the client hear when someone goes or drives near his car. Those might be car thieves!**

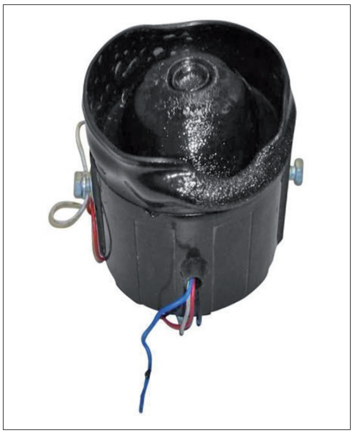
### 4.2.3. Installation of horn

**The rules for horn installation are simple:** with the loudspeaker downwards, in a dry place remote from hot exhaust pipes, ground in one of the places provided by the manufacturer.

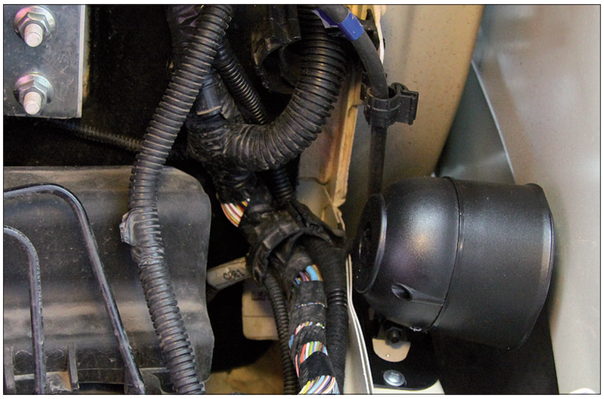
**For better protection of the horn from water, a 2-3 mm hole can be drilled in the emitter's upper point.** You'll forever forget how to remove and dry the horn!

Many people have seen molten horn housings in cars. As a result, the installer suffers direct losses. It will not be accepted from you under the warranty, which means that you'll install a new one for the client at your own expense. If you can spare your money, continue installing horns in the hottest places under the hood (near the exhaust manifold, radiator).

The result of improper installation in a hot place.



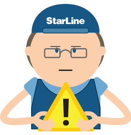
**Molten horn**



**Horn protected from moisture and temperatures**

Proper installation.

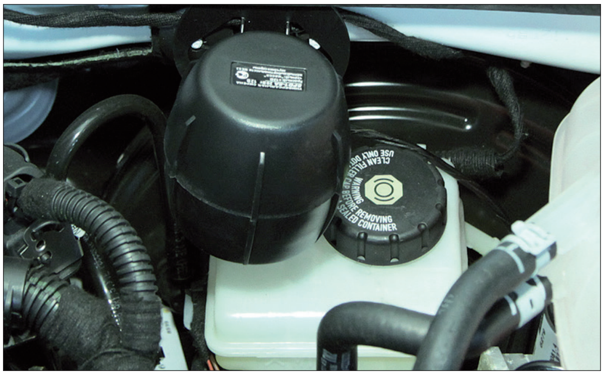
And now let's again imagine that you are not an installer but a car mechanic. You want to refill brake fluid (antifreeze, hydraulic steering fluid — anything). You open the hood and see a horn above the tank cover. We will not give the words addressed to the installer.



The advice is simple — the horn must not hinder the car servicing.

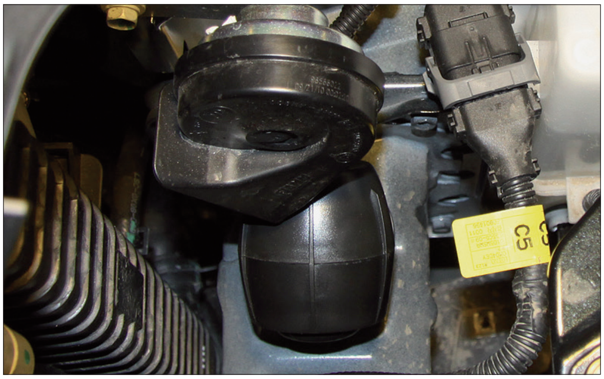
It must not hinder the refilling of fluids, oil level check, replacement of fuses and lamps. Hide it farther away from inquisitive glances and mischievous hands.

**Sloven's hint:** if you want to go home from the work as soon as possible — install the horn in a way convenient for you. Don't let car mechanics relax during car servicing. This is their work, not yours!



**Horn overlapping the tank cover**

Poor quality: it will be difficult to change or refill brake fluid in case of such arrangement!

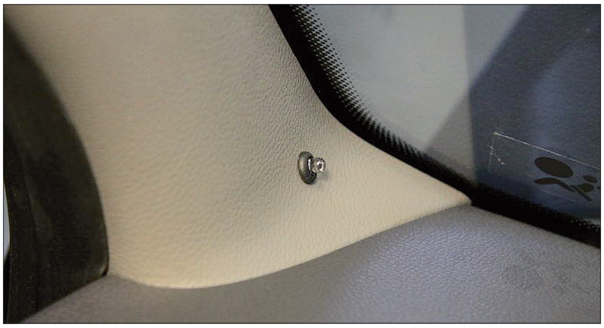


**Horn under the headlamp unit**

Good quality: the horn under the headlamp unit is safe.

### 4.2.4. Installation of light-emitting diode

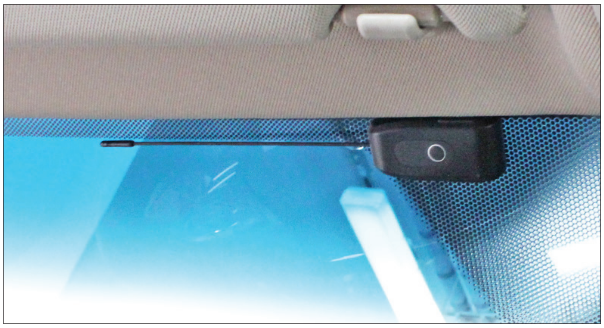
The main rule for LED installation: it must be seen from the driver's seat and from outside the car.



LED in Renault Logan

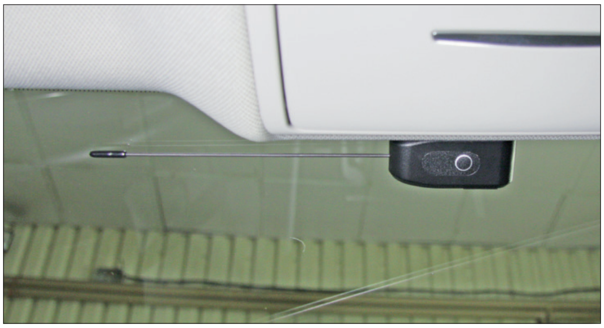
### 4.2.5. Installation of security system antennas with two-way communication

We often have to listen to clients' grumble: "Your security system does not respond well to the remote control, the range is short..." If we look into this problem, what do we have? The no-good installer, without reading the manual, installed the transceiver module on the windshield silk-screen printing. His intentions might be benevolent (the antenna is almost unnoticeable from outside the car), but he overlooked one point. The paint used to apply the image contains much iron. It is as good as sticking the module on a steel sheet! When the antenna module was moved to a clean area of the windshield, all problems disappeared at once!



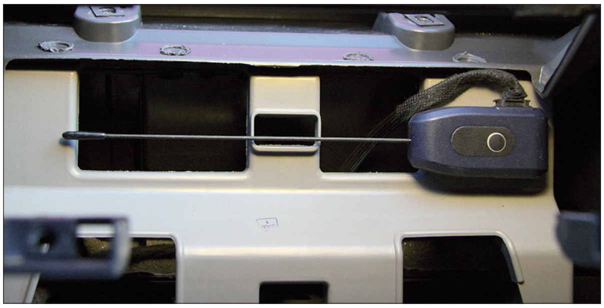
Transceiver module on silk-screen printing

Incorrect installation on silk-screen printing — reduced range of the security system.



Transceiver module on clean windshield

Correct installation — nothing hinders signal reception and transmission.

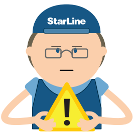


Transceiver module under the dashboard cover plate

Correct installation — nothing hinders signal reception and transmission.

### 4.2.6. Installation of GSM/GPS-antennas

Before final fastening of the GSM/GPS-antenna, assemble the whole structure “in the air” and check quality of reception/transmission. The most convenient antenna locations: under the windshield or rear window, in bumpers, spoilers. Some cars have windshields with protection against the radio emission of road radars. In this case, antennas installed under them may fail to operate.

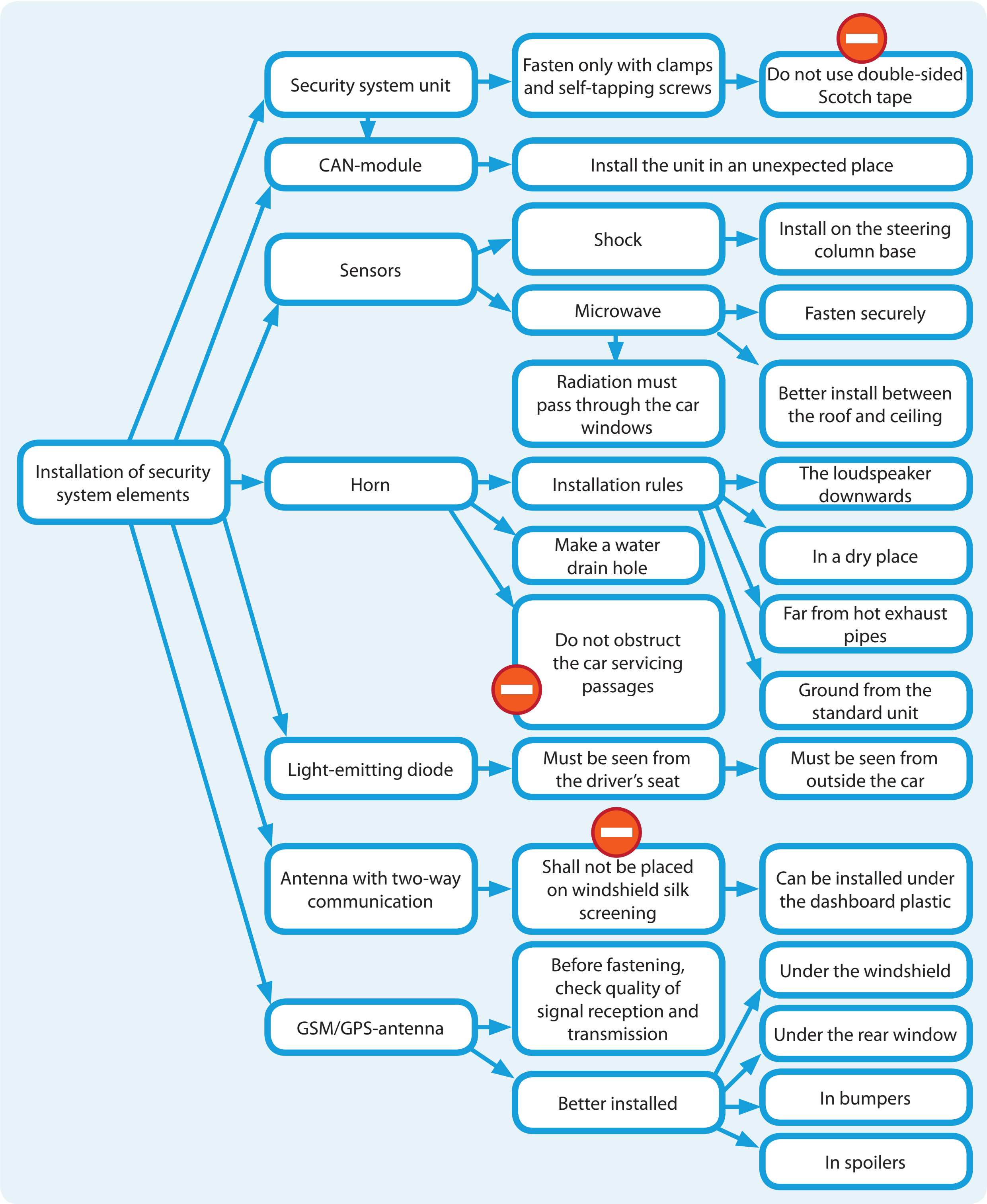


**Another useful advice: be sure to read the security system manual.**

They are compiled by developers and installers like you. The documentation contains answers to many questions arising during installation.

*See the checklist diagram “Installation of security system elements” on page 115.*

**Documentation for StarLine security systems**

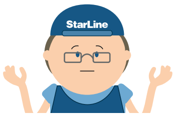

Installation of security system elements
Security system unit
Fasten only with clamps and self-tapping screws
Do not use double-sided Scotch tape
CAN-module
Install the unit in an unexpected place
Sensors
Shock
Install on the steering column base
Microwave
Fasten securely
Radiation must pass through the car windows
Better install between the roof and ceiling
Horn
Installation rules
The loudspeaker downwards
Make a water drain hole
In a dry place
Far from hot exhaust pipes
Do not obstruct the car servicing passages
Ground from the standard unit
Light-emitting diode
Must be seen from the driver's seat
Must be seen from outside the car
Antenna with two-way communication
Shall not be placed on windshield silk screening
Can be installed under the dashboard plastic
GSM/GPS-antenna
Before fastening, check quality of signal reception and transmission
Under the windshield
Under the rear window
Better installed
In bumpers
In spoilers

**Installation of security system elements. Memo diagram**

Chapter 4.3

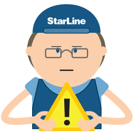
# Installation methods

Electricians justly say that there are two causes of a failure: a contact where it must not be and no contact where it must be. In our case this statement is 100 % true.



**Most problems in security system operation are related to sloven (one cannot say otherwise) connection of wires.**

Your inventory includes two main methods of wire connection: **twisting and soldering**. Which of them you choose depends on your personal preferences because they are identical in most cases.

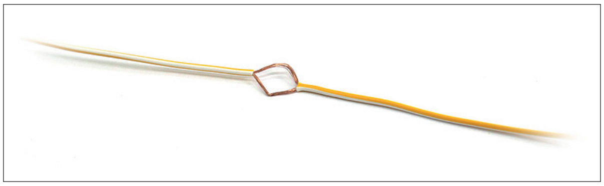


**Soldering is mandatory in power circuits of security system with autostart!**

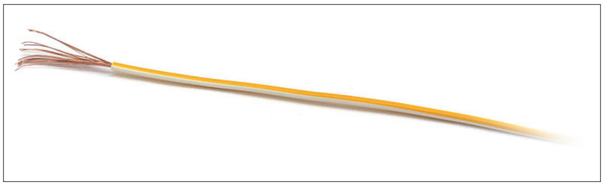
## 4.3.1. Twisting

Which method do you use for wire splicing? Most probably, it is twisting. It really is the fastest connection method. It will also be rather reliable if done in the way shown below. The photographs show: there is no trickery here.

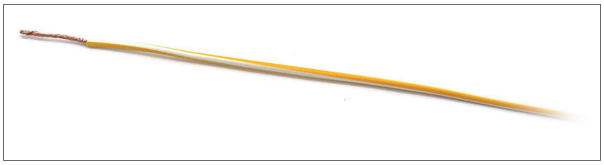
### How to make high-quality twisting



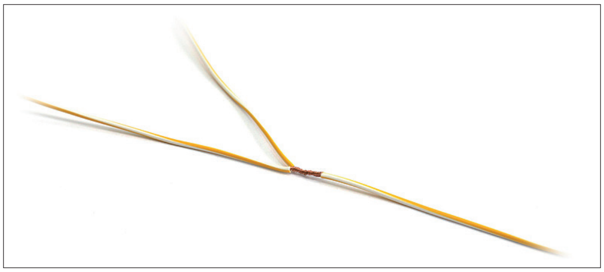
**1.** Cut off the insulation of the first wire to 1.5-2 cm and move the strands apart.



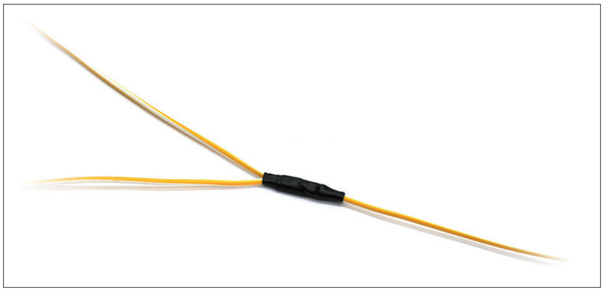
**2.** Cut off the insulation of the second wire to 1.5-2 cm.



**3.** Twist all strands of the second wire between each other.

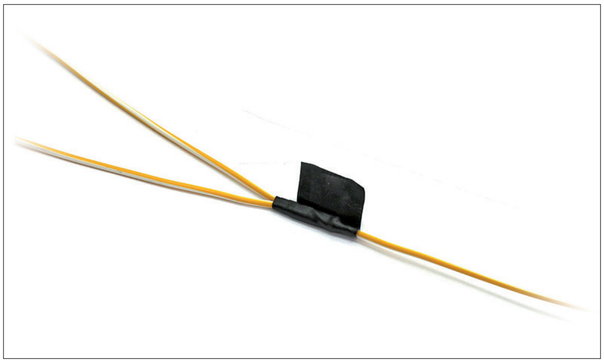


**4.** Pass a single wire between the strands and wrap the first wire with it



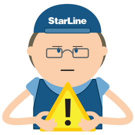
**5.** Insulate the connection.

Twisting is half the work. It must be properly insulated. You certainly know how to use insulating tape but pay attention to the following: do not leave free tape ends (flags). This may cause wire exposure and short circuit.



**Improper insulation of the connection - free ends of the insulating tape are left**

**Free tape ends (flags) shall not be left.**



**Another advice: use high-quality insulating tape, but not the household one sold in any hardware store.**

**High-quality insulating tape, e.g. IZT 1925 fleece**

**Sloven's hint: do not spend time and money on high-quality insulation of the wiring. And if the client's car flames up due to molten wire — it must have been struck by a lightning. Or even a meteorite.**

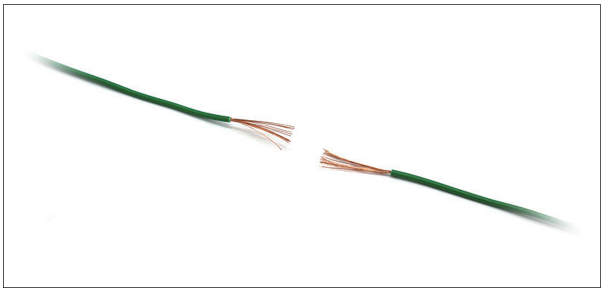
### 4.3.2. Soldering

What is the customers' most frequent problem! The car does not start! Let us leave aside the clients' fecklessness (discharged storage battery, discharged remote control battery) and let us reveal the root cause of car failure. In 80% cases it is bad contact of the blocking.

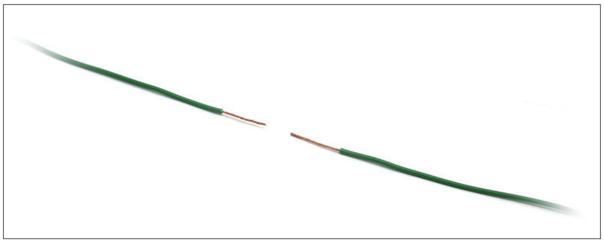
There are some simple recommendations for making a reliable connection using a soldering iron. Then you'll have more time for rest.

**Sloven's hint: do you lack thrill? Do you like to visit enraged clients at night on the other end of the city? Then continue making blocking on twisted wires. And I will solder and do more pleasant things.**

## How to make high-quality soldering

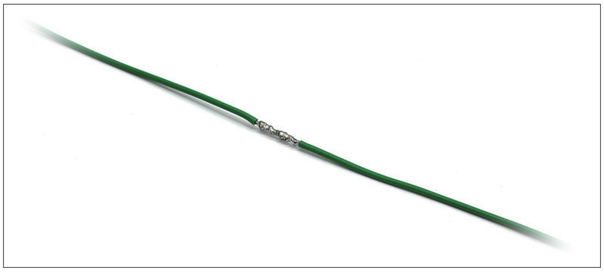


1. Remove insulation from wires at a distance of 1.5-2 cm from the edge.



2. Twist all strands in each wire between each other.

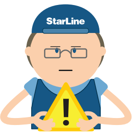
3. Twist the wires "towards" each other.
4. Solder using lead-tin solder POS-61 with liquid flux LTI-120 or another neutral flux. Solders with colophony can be used. The simplest liquid flux is made of colophony with pure alcohol (colophony 15-30%, ethyl alcohol 70-85%). The surfaces being soldered shall be immobile until complete hardening of the solder. **Even negligible motion of parts in relation to each other and the moment of solder crystallization reduces the connection strength to a great extent.** If necessary, remove the flux residues.



5. After cooldown, thoroughly insulate the connection.

**Active fluxes shall not be used (containing acids and other corrosive substances), e.g. zinc chloride.**

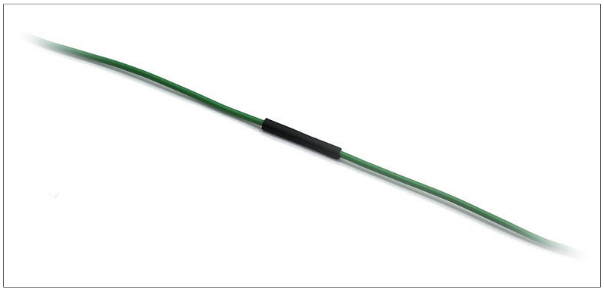
If blocking is done under the hood (it should be done exactly there), unsealed insulation of the soldering area will cause much trouble for you.



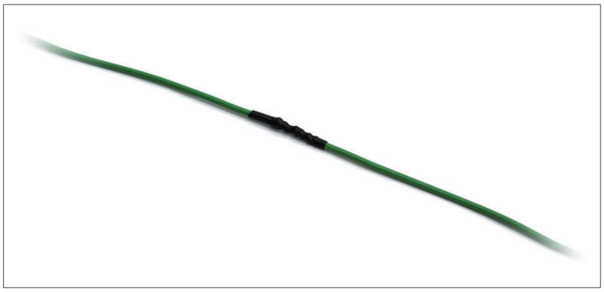
**The standard insulating tape that we use will not ensure leak tightness. Heat-shrink insulation was invented for your convenience.**

## How to seal the soldered joint properly

1. Before twisting, put a heat-shrink tube, preferably with a glue layer inside, onto one of the wires.
2. Twist and solder the wires.
3. If a heat-shrink tube without glue is used, coat the soldering area with "88 Luxe" or "Moment" glue.



**4.** Move the heat-shrink tube to the soldering area.



**5.** Heat up the heat-shrink tube, the connection is ready!

**What should be used to heat up the heat-shrink tube?**

**Twin mounting wire**

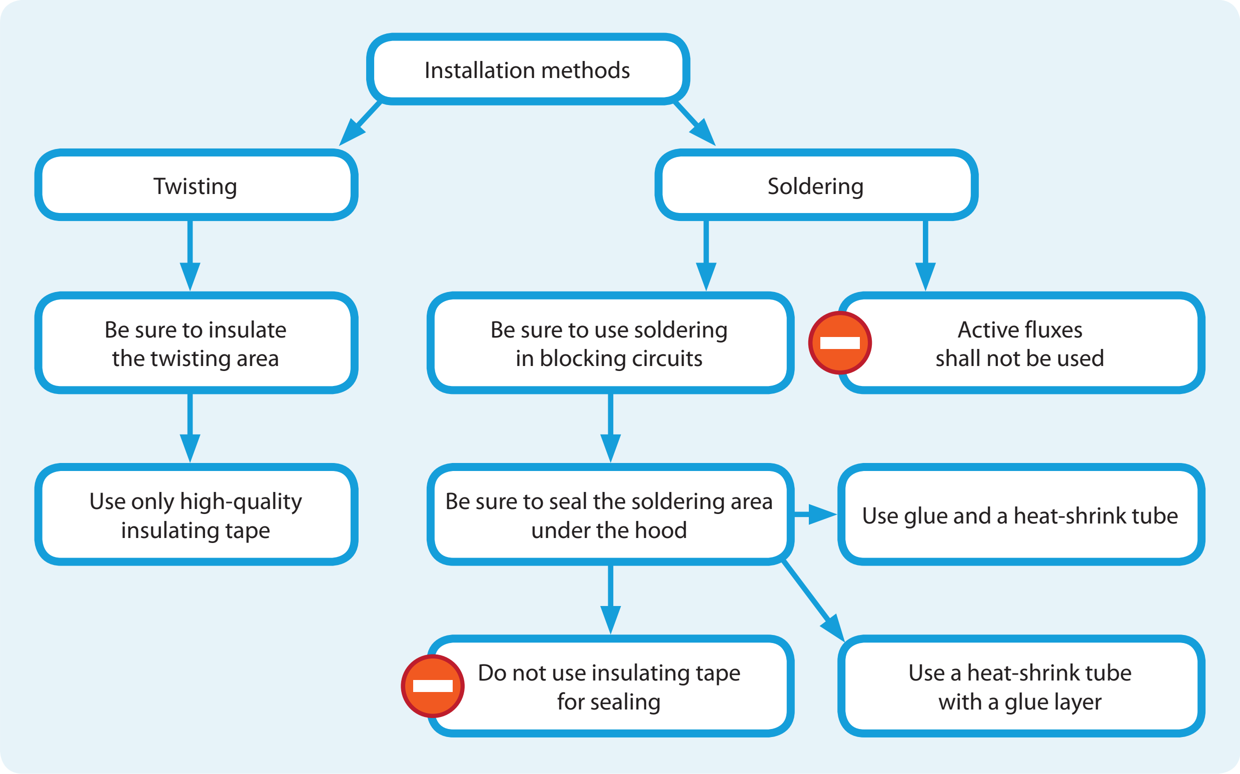
**Heat gun**

**It can be done properly only using a heat gun, but not a cigarette lighter. Lighter flame is difficult to adjust and may melt the insulation.**

### 4.3.3. Wire selection

A question often arises: how to select wire thickness? The simplest answer is — the wire must have the same thickness as the extended one. In complex cases you should use the Ohm’s law described in the first part of this book.

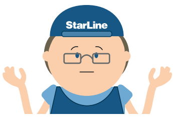
A single mounting wire will suit in many situations. If you install an additional drive, a twin wire will be more convenient.


Installation methods
Twisting
Soldering
Be sure to insulate the twisting area
Be sure to use soldering in blocking circuits
Active fluxes shall not be used
Use only high-quality insulating tape
Be sure to seal the soldering area under the hood
Use glue and a heat-shrink tube
Do not use insulating tape for sealing
Use a heat-shrink tube with a glue layer

**Installation methods. Memo diagram**

Chapter 4.4

# Installation tools



**Of course, you can strip wires with your teeth, but proper tools will save you costs of dentist's services.**

Expenses on the tools will pay back after two or three orders, while after that they will work only for your benefit.

**The installer's minimum set** shall comprise the following items:

1. Side-cutting pliers with insulated handles (several tools should be available — for thin and thick wires);

2. Stripper for wire stripping;

3. Knife;

4. Mounting set for passenger compartment disassembly;

5. Crimper for terminal crimping;

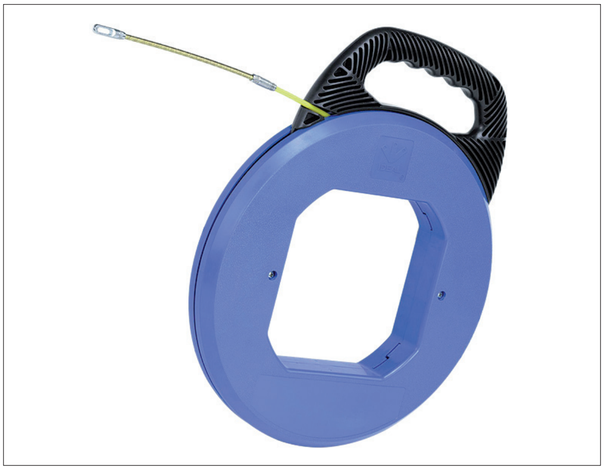
6. Set of screwdrivers;

7. Set for work with special fasteners (TORX);

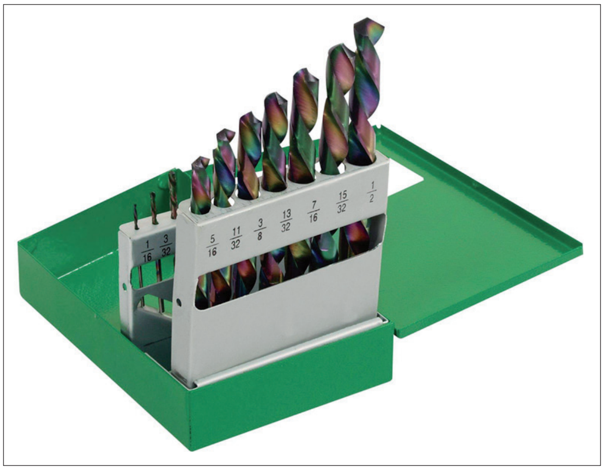
8. Soldering iron (two should be available — one with the power of 60 — 100 W for soldering large-section wires, the other with the power of 40 W for more precise works);

9. Set of 7-17 mm wrenches;

**10.** Set of 7-17 mm sockets;



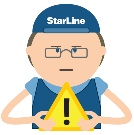
**11.** Nylon pulling tool;



**12.** Set of 1-10 mm metal drills;

**13.** Recharged battery screw driver;

**14.** Tools storage and carriage box.

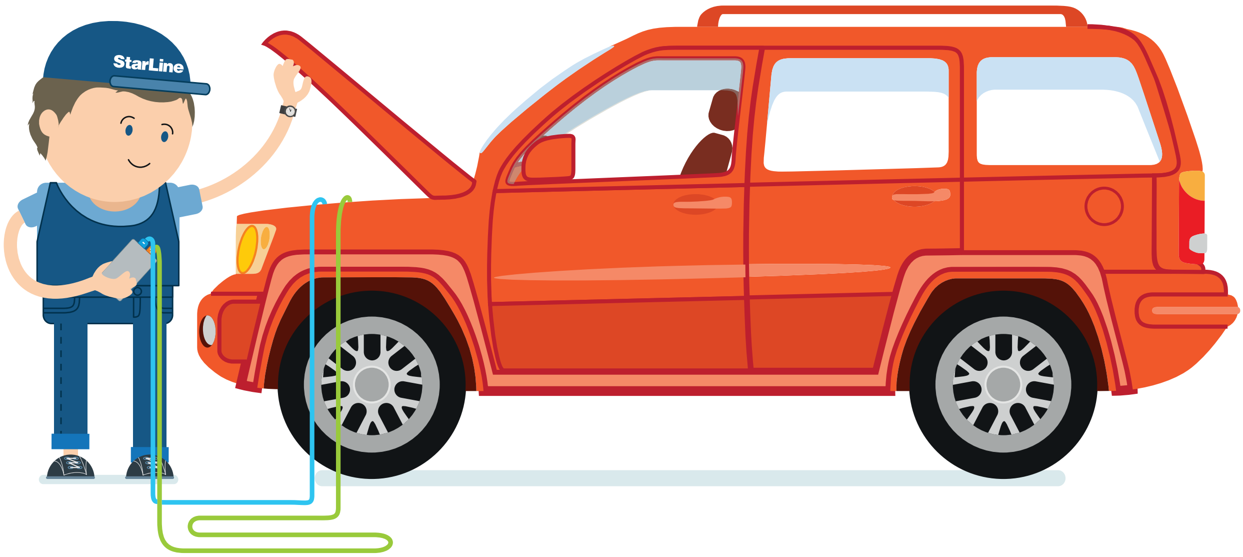


**Do not economize on tools! Choose professional equipment. For instance, Gedore, Wurth, King Tony tools.**

This also applies to any other equipment. Otherwise, at the most inappropriate moment the side-cutting pliers will break down, the soldering iron will burn out, while the drill will turn out to be untempered. You will need other instruments as well with the course of time, but these tools will suffice at first.

Part 5

# Check-out equipment



*Use check-out equipment — probes and measuring instruments, — but not the trial and error method. This will save you the expenses on replacement of damaged electronic internals of the car, which are much more expensive than measuring instruments. Special attention should be paid to their selection.*

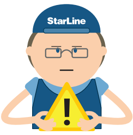
Chapter 5.1

# Probe

**Usually it is used for the following purposes:**

- monitoring of voltage presence in the checked circuit;
- search of circuits necessary for security system connection;
- approximate estimation of circuit section resistance.

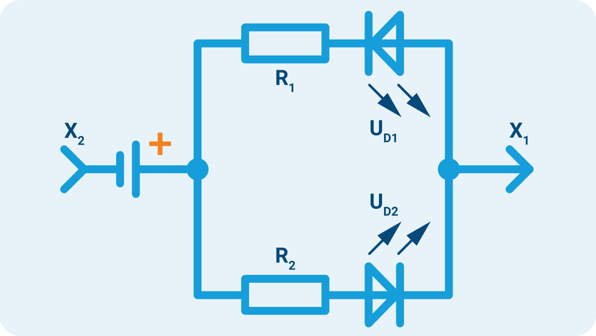
### 5.1.1. Logic probe



**This is the installer's main tool.**

You can assemble the simplest probe on your own.

**Tips on selection of circuit elements:**



**Probe electric layout**

- any LEDs can be used. Red — VD1, green — VD2;
- resistor resistance shall be: R1 = 1 kOhm, R2 = 200 Ohm;
- power supply is provided by two AA batteries (to reduce probe size, they can be replaced by lithium batteries of the remote control);
- use the following as contacts: X1 — a sewing needle (convenient for piercing the wire insulation); X2 — alligator clamp (wire length should be 70-80 cm);
- use any box of suitable size as the housing.

**How to operate the probe:**

- connect connector X2 to the ground;
- touch the contact (wire) under checking with needle X1;
- observe the LEDs, if:

  • the red one is illuminated, it is a positive wire;

  • the green one is illuminated — it's negative;

  • both LEDs are illuminated, the contact has alternating voltage;

  • neither LED is illuminated, there is no voltage (circuit discontinuity).

**Caution: the probe and "test lamp" shall not be inserted in the socket!**

### 5.1.2. So-called "test lamp"

As such, the "test lamp" is a conventional low-power car lamp placed in a housing with a probe. It allows for determination of voltage presence, simulate the signals of some electronic systems of the car (central lock, limit switches, switch on of marker lights and swivel lights in some cars). The power of the lamp used in the "test lamp" shall not exceed 2 W (current not more than 0.2 A).

**The "test lamp" is less convenient than the logic probe, because it does not determine circuit discontinuity.**

**"Test lamp"**

**How is the «test lamp» used?**

Connect the alligator clamp to the ground. Connect the probe to the contact of the circuit under checking. The lamp will be illuminated if the circuit under checking has a positive.

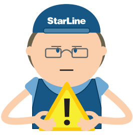
**The "test lamp" should not be used in modern cars — the electronics can be damaged by connecting it to low-power circuits.**

For instance, when supplying a signal to a sensor you might, as a minimum, introduce an error in the car engine or AGB "brain".

**Sloven's hint: the installer with the "test lamp", the same as the mine picker, errs only once. Because then he saves up money for a long time and pays for the damaged equipment. And lastly, he buys a tester.**

Chapter 5.2

# Tester (multimeter)



**The most important installer's tool is the tester (multimeter).**

It should be used when searching the necessary circuits in modern cars (especially unfamiliar ones). At present, digital multimeters are most widely spread.

The multimeter is an electronic measuring instrument combining several functions.

These are the voltmeter, ammeter and ohmmeter in the minimum set. Portable models of digital multimeters are better suited for our purposes.

**Multimeter**

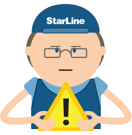
**Advanced multimeter models have the following functions:**

- measuring direct/alternating voltage up to 1000 V with resolution from 0.1 mV;
- measuring direct/alternating current up to 10 A with resolution from 0.1 μA;
- measuring resistance up to 40 MOhm with resolution from 0.1 Ohm;
- continuity test — measuring electric resistance with signaling of low circuit resistance;
- diode test — continuity check of semiconductor diodes and determination of voltage drop on them;
- measuring harmonic signal frequency;
- measuring capacitance, inductance, temperature (may be needed when setting automatic start on cars with a keyless access system).

### How to select a multimeter for professional installation?

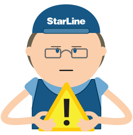
When selecting a specific model, **attention must be paid to the following factors:**

- convenience of use;
- housing strength;
- probe quality;
- display lighting;
- possibility to measure temperature, capacitance, inductance.



**The multimeter may also help in failure diagnostics.**

Sometimes clients complain that the security system discharges the storage battery. The multimeter will help you prove quickly with reason and that you have done the work properly. Measure the car consumption current. If it exceeds 100 mA in the rest mode (all the doors are closed, ignition and all devices are off) — switch off the security system. If the current decreases — the problem lies in it. But in this case the security system is not always faulty!



**Power supply of the security system in many cars (Audi, BMW) must be provided from certain places! Otherwise, the car does not "fall asleep".**

*For more detail see: http://en.wikipedia.org/wiki/ Multimeter*

Chapter 5.3

# Oscilloscope

When the security system is connected it is often **needed to estimate the signal waveform and amplitude.** The oscilloscope is intended for these purposes.

**A digital one- or two-channel oscilloscope is best suited for our needs.**

It can be used to easily find the signal circuits of different car sensors (position of the crankshaft and camshaft, throttle and accelerator pedal), to find a tachometer signal for autostart systems.

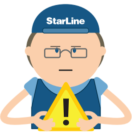
**Digital oscilloscope**

*For more detail see: http://en.wikipedia.org/wiki/ Oscilloscope*
*Standard oscillograms for different kinds and types of sensors — http://opel-corsa.5go.ru/html/6_2_4.htm*

Chapter 5.4

# Spectrum analyzer

Most of you must have encountered the following situation: you have installed and checked the security system — everything is working. After you drove the car to another place — the remote control operation range decreased and communication between it and the main remote control was lost completely. The reason is a source of strong radio emission or interference in the radio frequency range close to the security system operation frequency.



**The spectrum analyzer allows for estimating the level and frequency of such interference.**

Only large companies can afford this expensive instrument (about 100-150 thous. rubles), but it will be good to have some idea of it.

**Spectrum analyzer**

*For more detail see:*
*Frequency meter — http://ru.wikipedia.org/wiki spectrum analyzer — http://ru.wikipedia.org/wiki*
*Procedure for radio frequency interference control using a spectrum analyzer — http://www.ccc.ru/magazine/depot/06_12/read.html?0103.htm*

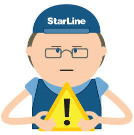
Part 6

# Safety rules for installation

*Many problems in security system installation arise due to non-observance of the elementary safety rules. Burnt-out wiring, dirty passenger compartment — that's what may deprive you of earnings. Please read this chapter: we will not disclose anything fundamentally new to you, but will warn you about possible errors.*

Chapter 6.1

# Car interior and body damage protection

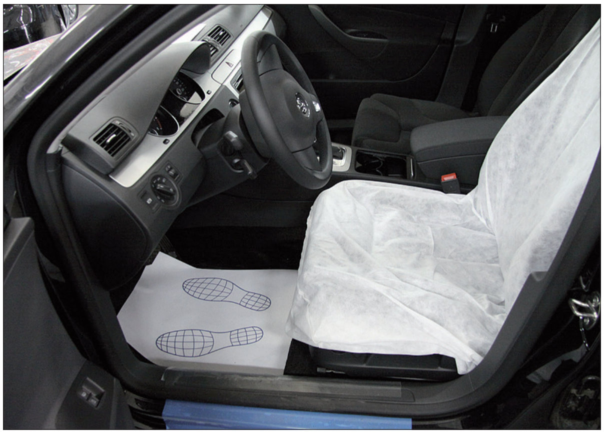


**As theatre begins at the cloakroom, installation also begins with protective covers to be put onto the seats and steering wheel before entering the car.**

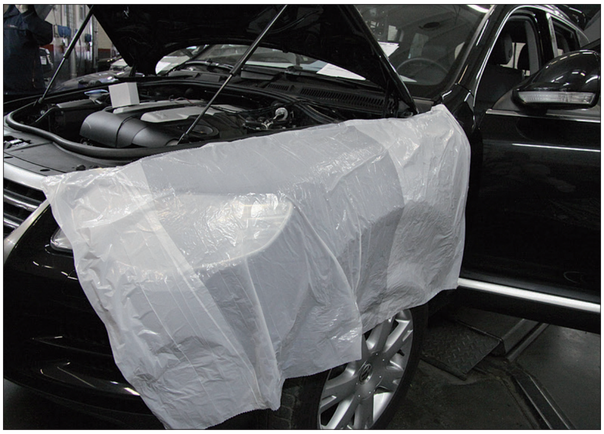
The client will be satisfied with your precaution, because in this way you protect the interior against dirt (or, vice versa, do not get dirty yourself). A single-use mat should be also placed on the floor. Another element to be protected are the car splash boards.

**Sloven's hint:**

**the more buttons and zippers has the installer's suit, the more elegant it is! However, not all scratches, left by such beauty, can be eliminated by polishing. For reference: the painting of one part at an official dealer costs from 10,000 (ten thousand!) rubles. Ignore the protection of car splash boards as long as possible and gather the information on painting cost at other dealers.**



**Protective covers**

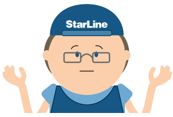


**Protection of car splash boards**

Chapter 6.2

# Wire installation

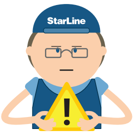
**Sloven's hint: while ordinary people have their toast landing buttered side down, installers' drill during wire installation always exits into a hose, standard wiring or vacuum booster. So, in order not to differ from all other losers, do not look where the drill goes out, before drilling a hole from the interior under the hood in the engine tunnel.**



**The easiest thing to get away with when hitting the wire harness is the restoration of wiring.**

But the Murphy's Law holds true even in this case: it is difficult to get to it, and sometimes removal of various assemblies is needed. But you can also hit a vacuum booster and a hose. In such a situation the replacement of the damaged unit is inevitable.

As a matter of fact, a standard hole can be almost always found in the modern car for wire installation from the interior to the underhood space.



**Try to drill as few holes as possible in the body and interior elements.**

Many car manufacturers prohibit this. Otherwise — say farewell to the warranty. All the aforesaid applies to installation of the horn and limit switch: too long self-tapping screws can bring about many troubles.

**As regards soldering:** there is a couple of simple rules to save time and money for interior restoration.

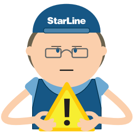
**Never leave the soldering iron in a car interior! Especially if it is hot.**

When you finished soldering, put the soldering iron on a support near the car. It is better to bend down once again than to drop it on the dashboard or the floor.

**Cover the areas where the solder may drip!** Believe us: traces of hot tin sometimes cannot be removed. The recommended protection includes single-use paper mats, heavy paper (tear apart the security system packaging box).

3. Another instrument sometimes causing much trouble is the **portable lamp**.

**LED hand lamp**



**Use only a luminescent hand lamp, or better a LED hand lamp.**

**Luminescent hand lamp**

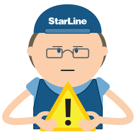
The conventional filament lamp may (it will certainly happen so!) burn through the carpet or melt the plastic in the car interior. You never know – you might suffer a burn.

Chapter 6.3

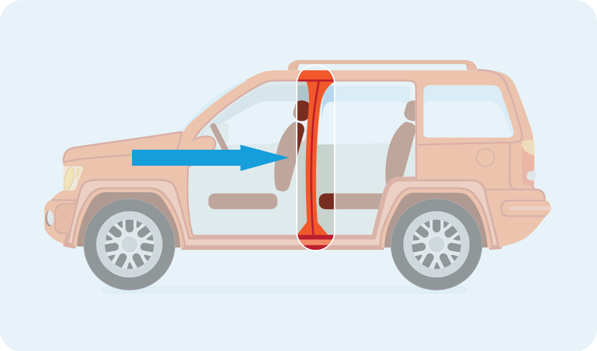
# Shock sensor setting

**How do you set the shock sensor?**

We foresee the popular answer: “Hitting the body pillar with your fist”. Have you never had to eliminate dents from such adjustment? Continue setting in this way. And you can also hit on the windshield. Only beware of being hit on the forehead yourself.

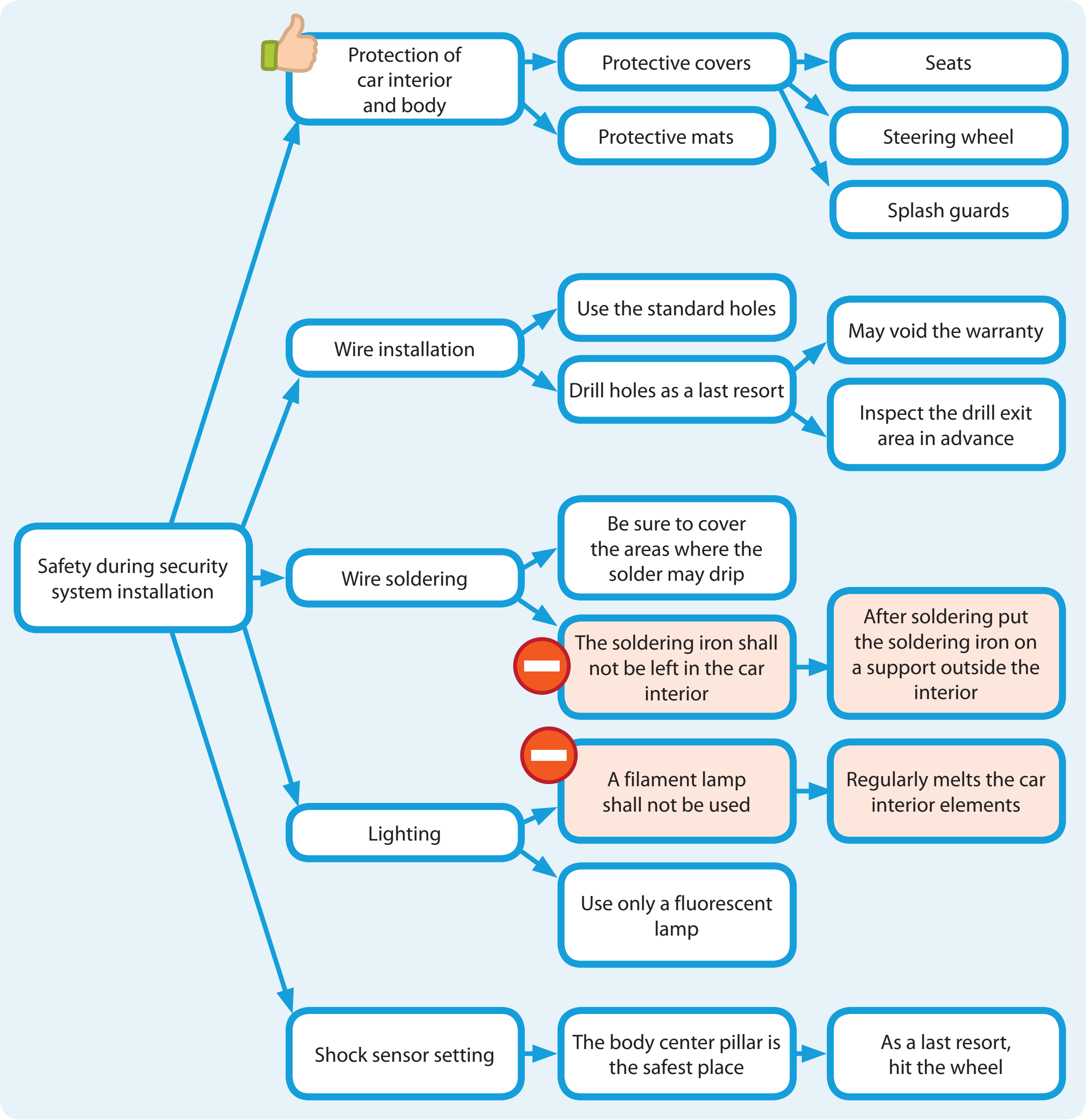


**The safest place for test blows is the car center pillar.**



**Zone for check of shock sensor setting**

If there is no pillar (coupe or cabriolet), setting is possible by hitting on the wheel.


Safety during security system installation

Protection of car interior and body

Protective covers

Seats

Steering wheel

Splash guards

Protective mats

Wire installation

Use the standard holes

Drill holes as a last resort

May void the warranty

Inspect the drill exit area in advance

Wire soldering

Be sure to cover the areas where the solder may drip

The soldering iron shall not be left in the car interior

After soldering put the soldering iron on a support outside the interior

Lighting

A filament lamp shall not be used

Regularly melts the car interior elements

Use only a fluorescent lamp

Shock sensor setting

The body center pillar is the safest place

As a last resort, hit the wheel

**Safety during security system installation. Memo diagram**

Chapter 6.4

## Safety during connection of security system wires

**It can be said at once that the storage battery need not be disconnected. Moreover, in some cars it shall not be removed!**

But if you decided to do so, first disconnect the minus terminal. If you start with the plus — short circuit will occur between the wrench and the body. Some car audios are protected from stealing by a code. You will have to enter it after reconnecting the storage battery. Be sure to ask the car audio code from the client (if any)!

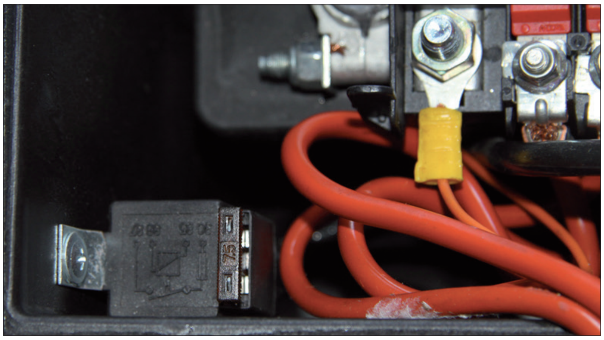
**Wire connection sequence** shall be as follows:

1. **Ground.** The most correct way is to crimp the ring lug on the wire and fasten it with a bolt or a nut to a body area with stripped paint.
2. **CAN-bus** (if available). Having connected it the last, you may cause a lot of errors. If you have a friend diagnostician or spare money, connect it when you want.
3. **Security system outputs** (hazard lights, central lock, horn, auxiliary channels).
4. **Security system inputs** (limit switches, tachometer, temperature sensor).
5. **Connectors for the security system unit**
6. **Power supply plus**

**The positive contact is always connected the last.**

It should be noted that the standard harness of the security system always has several fuse holders. Some are intended for power supply of powerful devices (door locks actuators, hazard lights), others — for power supply of the security system main unit. Install a fuse if you want to protect the car against possible inflammation.

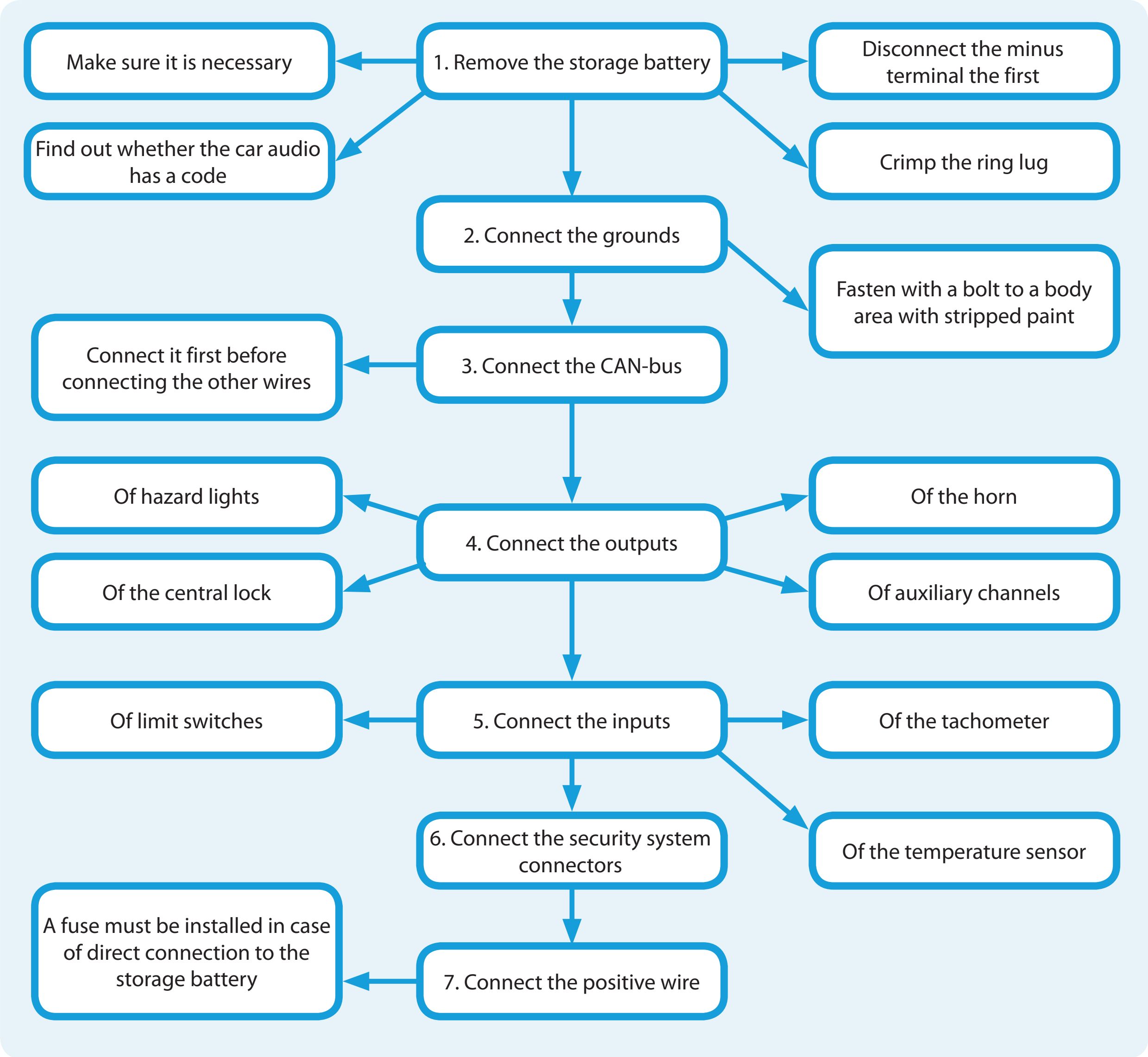
When connecting directly to the storage



**Connecting a load to the storage battery via a relay and fuses**

battery plus, the fuse must be installed right near the terminal.

**This part of the book has told you about the basic installation rules. But it is the simple principles outlined here that make up correct, and most importantly — safe installation.**

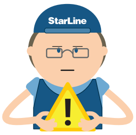

Make sure it is necessary
1. Remove the storage battery
Disconnect the minus terminal the first
Find out whether the car audio has a code
Crimp the ring lug
2. Connect the grounds
Fasten with a bolt to a body area with stripped paint
Connect it first before connecting the other wires
3. Connect the CAN-bus
Of hazard lights
Of the horn
4. Connect the outputs
Of the central lock
Of auxiliary channels
Of limit switches
5. Connect the inputs
Of the tachometer
6. Connect the security system connectors
Of the temperature sensor
A fuse must be installed in case of direct connection to the storage battery
7. Connect the positive wire

**Procedure for connection of security system elements. Memo diagram**

# Concluding remarks

Progress does not stand still: cars are changing, technologies used in car security-telematic equipment are improved, — and clients become all the more demanding. The capabilities of security equipment that inspired wonder yesterday, today are becoming a compulsory component in the functional set of a standard security system.

And this means the requirements to professional skills and training of specialist installers are consistently becoming stricter. We hope the "Skilful master handbook" will extend your knowledge, while **Sloven's hints** will warn you against excessive time, emotional and financial expenses.



**"There's no limit to perfection" is a manifest truth. And it is known to be always out there...**

# Index of figures

# Short index of terms

**Anode** — the positive pole of a current source or an electrode connected to it (19, 33, 44).

**GLONASS** (Global Navigation Satellite System) — a Soviet and Russian satellite navigation system (78, 79, 85).

**Dialogue code** — a cryptosecure method for car alarm protection against electronic hacking, using unique encryption keys for each system (55, 67, 70).

**Immobilizer** — an electronic device hindering the car motion by disabling the main electric circuits in the engine (15, 71, 72, 79, 83, 84, 90).

**Cathode** — the negative pole of a current source or an electrode connected to it (19, 33, 34, 44).

**Transponder key** — a car ignition key containing a miniature microcircuit with a unique code and a transceiver for sending this code to the immobilizer (15, 83).

**Code: dialogue, dynamic, static** — types of algorithms of command transmission from the remote control to the main alarm unit via a radio channel (55, 62-70).

**Code grabber** — a device intended for interception of the car alarm code (65, 66, 70).

**Modulation: amplitude, frequency** — modulation kinds in which changeable parameters of the carrier signal are amplitude or frequency respectively (60, 62, 69).

**Multimeter** — a measuring instrument combining several functions (128, 129).

**Oscilloscope** — an instrument for studying amplitude and time parameters of an electric signal (14, 130).

**Power switches** — a semiconductor device allowing for switching of high-current loads and having a multistage overload and short-circuit protection (45, 46, 84).

**Spectrum analyzer** — an instrument for monitoring and measurement of the energy distribution of electric (electromagnetic oscillations) in the frequency band (131).

**Zener diode** — a semiconductor diode intended for voltage stabilization in power sources (33, 34).

**Telematics** — a combination of telecommunication and information technologies. Car telematics is the wireless exchange of messages and commands between the car and external sources (87, 93-95).

**Transceiver** — a transceiver transmitting and receiving encrypted data at a certain frequency (59-63).

**ADAS** (Advanced Driver Assistance Systems) — driver assistance system (98).

**CAN** (Controller Area Network) — a serial interface for creation of a distributed network of microprocessor devices (74, 75, 78, 79, 84, 86-91, 110, 139).

**GPS** (Global Positioning System) — a satellite navigation system developed by the US Department of Defence (78, 79, 85, 86, 93, 114).

**FLEX** — flexible service channels allowing the installer to program additional service functions of car alarm (54).

**iCAN** — digital blocking via the car's standard circuits (88, 90).

**iKey** — a technology for keyless bypass of the standard immobilizer (88, 90).

**Keeloq** — a floating code technology of Microchip Company (66).

**Keyless** — a keyless system for car cabin access (74, 88, 89).

**LIN** (Local Interconnect Network) — an industrial network standard developed by a consortium of European car manufacturers and other well-known companies (90, 91)

**SLAVE** — a car alarm function allowing for car security control from the standard remote control (71, 74, 90).

**SMD** (Surface Mounted Device) — surface-mounted devices (20, 38).

**Zener Diode** — see Zener diode (33, 34).

## For Notes

# For Notes

# For Notes

# For Notes

LLC “SPA StarLine”

Information and reference publication for car safety specialists

Alexander Alexandrovitch Borisov,
Mikhail Yuryevitch Kurchin etc.

SKILLFUL MASTER HANDBOOK

Compiler
Semyon Alexeyevitch Potryasayev,
Diana Viktorovna Yunak

Idea author and editor-in-chief
Temur Asrorovitch Amindzhanov

Project coordinator
Diana Viktorovna Yunak

Literary editor and proofreader D. V. Yunak, T. S. Parvan
Art director, art and technical editor F. B. Akhmetov
Graphic designer M. V. Borscheva
Photographers D. V. Vedernikov, A. V. Saukkonen

Passed for printing on 27.06.2017. Offset paper. Size 84 × 108 1/16.
Offset printing.
Circulation 4000 copies. Order No. 15845.

LLC “SPA StarLine”
194044, Saint Petersburg, Komissara Smirnova Str. 9, letter A, office 204
www.starline.ru
reklama@starline.ru

Printed at the printing office LLC LD-PRINT
196644, Saint Petersburg, Kolpinsky District, Saperny Settkenent,
territory of Baltica Company, building w/o number, letter F.
Tel. (812) 462-83-83, office@ldprint.ru