CLAIMS

What is claimed is:

1. An integrity protection failure handling method, applied to first user equipment, wherein the first user equipment performs sidelink communication based on a destination address, and the integrity protection failure handling method comprises:

performing a security control operation in at least a case that an integrity check failure indication for a sidelink signaling bearer is received.

2. The integrity protection failure handling method according to claim 1, wherein the integrity check failure indication is sent by a packet data convergence protocol PDCP entity.

3. The integrity protection failure handling method according to claim 1, further comprising:

performing a security control operation in a case that a sidelink radio link failure is detected.

4. The integrity protection failure handling method according to claim 1, wherein the sidelink signaling bearer is at least one of sidelink signaling bearer 1, sidelink signaling bearer 2, and sidelink signaling bearer 3.

5. The handling method according to claim 1, wherein the security control operation specifically comprises at least one of the following operations:

releasing a data bearer corresponding to sidelink communication performed by the first user equipment based on the destination address;

releasing a signaling bearer corresponding to sidelink communication performed by the first user equipment based on the destination address;

releasing a sidelink interface radio resource control PC5 RRC connection corresponding to sidelink communication performed by the first user equipment based on the destination address;

discarding configuration information corresponding to sidelink communication performed by the first user equipment based on the destination address;

discarding a security key corresponding to sidelink communication performed by the first user equipment based on the destination address; and

stopping a timer corresponding to sidelink communication performed by the first user equipment based on the destination address, or stopping all timers for sidelink communication performed by the first user equipment.

6. The handling method according to any one of claims 1 to 5, in the case that the integrity check failure indication for the sidelink signaling bearer is received, after the performing a security control operation, further comprising:

sending an RRC message to a network-side device, wherein the RRC message is used to report that sidelink communication with the destination address by the first user equipment fails.

~~7. The handling method according to claim 6, wherein the RRC message is further used to indicate that a cause of the sidelink communication failure is integrity check failure.~~

~~8~~7. The handling method according to any one of claims 1 to 5, in the case that the integrity check failure indication for the sidelink signaling bearer is received, after the performing a security control operation, further comprising:

sending indication information to an upper-layer entity of the first user equipment, wherein the indication information is used to notify that a PC5 RRC connection has been released.

~~9. The handling method according to claim 8, wherein the indication information is further used to notify that a cause of the PC5 RRC connection being released is integrity check failure or failure of the PC5 RRC connection.~~

~~10~~8. The handling method according to any one of claims 1 to 5, further comprising:

sending a PC5 RRC message to second user equipment corresponding to the destination address, wherein the PC5 RRC message is used to indicate the second user equipment to stop sidelink communication performed based on the destination address.

~~11. The handling method according to claim 10, wherein the PC5 RRC message carries a sidelink configuration reset indication.~~

~~12~~9. An integrity protection failure handling apparatus, applied to first user equipment, wherein the first user equipment performs sidelink communication based on a destination address, and the apparatus comprises:

a first execution module, configured to perform a security control operation in at least a case that an integrity check failure indication for a sidelink signaling bearer is received.

~~13~~10. The integrity protection failure handling apparatus according to claim ~~12~~9, wherein the integrity check failure indication is sent by a packet data convergence protocol PDCP entity.

~~14~~11. The integrity protection failure handling apparatus according to claim ~~12~~9, further comprising:

a second execution module, configured to perform a security control operation in a case that a sidelink radio link failure is detected.

~~15~~12. The integrity protection failure handling apparatus according to claim ~~12~~9, wherein the sidelink signaling bearer is at least one of sidelink signaling bearer 1, sidelink signaling bearer 2, and sidelink signaling bearer 3.

~~16~~13. The handling apparatus according to claim ~~12~~9, wherein the security control operation specifically comprises at least one of the following operations:

releasing a data bearer corresponding to sidelink communication performed by the first user equipment based on the destination address;

releasing a signaling bearer corresponding to sidelink communication performed by the first user equipment based on the destination address;

releasing a sidelink interface radio resource control PC5 RRC connection corresponding to sidelink communication performed by the first user equipment based on the destination address;

discarding configuration information corresponding to sidelink communication performed by the first user equipment based on the destination address;

discarding a security key corresponding to sidelink communication performed by the first user equipment based on the destination address; and

stopping a timer corresponding to sidelink communication performed by the first user equipment based on the destination address, or stopping all timers for sidelink communication performed by the first user equipment.

~~17~~14. The handling apparatus according to any one of claims ~~12~~ 9 to ~~16~~13, further comprising:

a first sending module, configured to send an RRC message to a network-side device, wherein the RRC message is used to report that sidelink communication with the destination address by the first user equipment fails.

~~18. The handling apparatus according to claim 17, wherein the RRC message is further used to indicate that a cause of the sidelink communication failure is integrity check failure.~~

~~19~~15. The handling apparatus according to any one of claims ~~12~~ 9 to ~~16~~13, further comprising:

a second sending module, configured to send indication information to an upper-layer entity of the first user equipment, wherein the indication information is used to notify that a PC5 RRC connection has been released.

~~20. The handling apparatus according to claim 19, wherein the indication information is further used to notify that a cause of the PC5 RRC connection being released is integrity check failure or failure of the PC5 RRC connection.~~

~~21~~16. The handling apparatus according to any one of claims ~~12~~ 9 to ~~16~~13, further comprising:

a third sending module, configured to send a PC5 RRC message to second user equipment corresponding to the destination address, wherein the PC5 RRC message is used to indicate the second user equipment to stop sidelink communication performed based on the destination address.

~~22. The handling apparatus according to claim 21, wherein the PC5 RRC message carries a sidelink configuration reset indication.~~

~~23~~17. User equipment, comprising a processor, a memory, and a program or an instruction stored in the memory and capable of running on the processor, wherein when the program or the instruction is executed by the processor, the steps of the integrity

protection failure handling method according to any one of claims 1 to ~~11~~ 8 are implemented.

~~24~~18. A readable storage medium, wherein a program or an instruction is stored in the readable storage medium, and when the program or instruction is executed by a processor, the steps of the integrity protection failure handling method according to any one of claims 1 to ~~11~~ 8 are implemented.

~~25~~19. A chip, wherein the chip comprises a processor and a communications interface, the communications interface is coupled to the processor, and the processor is configured to execute a program or an instruction to implement the steps of the integrity protection failure handling method according to any one of claims 1 to ~~11~~8.

~~26~~20. A computer program product, wherein when the computer program product is executed by at least one processor, the steps of the integrity protection failure handling method according to any one of claims 1 to ~~11~~8 are implemented.

~~27. User equipment, configured to perform the steps of the integrity protection failure handling method according to any one of claims 1 to 11.~~